INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909

Volume 4, Issue 1, 2026

# CYBERCRIME PREVENTION AND DIGITAL EVIDENCE: A LEGAL FRAMEWORK FOR COMBATING EMERGING CYBER THREATS

**Tahir Mahmood[1], Nadia Saleem[*2], Akhtar Ali Ansari[3], Ghulam Arbi[4], Dr. Muhammad Iqbal[5]**

[*1,3]*LLM, University of Lahore (UOL), Pakistan*
[2]*LLM Corporate Law Nottingham Trent University, UK*
[4]*Ph.d Scholar, Lincoln University College Malaysia (LUC)*
[5]*PhD Law District and Sessions Judge*

[*1]tahirnawaz222@gmail.com, [2]adv.nadia.saleem@gmail.com, [3]akhtaraliansariadv@gmail.com, [4]arbighulam90@gmail.com, [5]c.muhammadiqbal@gmail.com

**Corresponding Author: ***
**Nadia Saleem**
**DOI:** https://doi.org/10.5281/zenodo.23393971

| Received | Accepted | Published |
|---|---|---|
| 01 January 2026 | 15 January 2026 | 31 January 2026 |

## ABSTRACT

*Digital technologies are rapidly changing criminal activity, creating new and greater challenges for criminal justice systems, lawyers, and the police. This study investigates cybercrime prevention and digital evidence from a legal and criminal justice perspective, covering new cybercrime threats, legal tools, investigative powers, digital evidence, and institutional coordination. Financial cybercrime, ransomware, ID theft, cyber-enabled violence, online exploitation, and critical infrastructure attacks are significant threats identified in the analysis. It also explores the increasing role of digital evidence in the identification of offenders and the determination of criminal liability, such as electronic communications, data of mobile devices, cloud files, transactions, metadata, and network information. Specific attention will be paid to issues encountered with evidence preservation, evidence encryption, storage in the cloud, cross-border access to evidence, authentication, and chain of custody. The study also presents shortcomings of existing national cybercrime legislation, jurisdictional restrictions, lack of specialized staff, lack of forensic support, and fragmentation of the coordination of cybercrime response between law enforcement, prosecutors, courts, technology providers, and international partners. The results have revealed that it is not enough to criminalize infringement on the internet; a more comprehensive approach is needed to be employed when fighting cybercrime effectively. It will involve the use of integrated legal procedures, special investigative skills, consistent digital-forensic practices, timely international cooperation, public-private information-sharing, and ongoing judicial and prosecutorial training. The study also highlights the need to maintain privacy, due process, proportionality, and fundamental rights in the context of the expansion of investigative powers. By bolstering these interdependent elements, the detection, investigation, prosecution, and prevention of cybercrime can be enhanced, and criminal justice institutions can be better equipped to deal with the ever-changing nature of digital threats.*

***Keywords:***
*Cybercrime Prevention; Digital Evidence; Digital Forensics; Cybercrime Law; Criminal Justice*

## INTRODUCTION

The widespread use of digital technologies, the Internet connection, cloud computing, social media, and financial services on the web has revolutionized modern society, as well as providing opportunities for criminal activities to thrive (Munir, 2024; Abraha, 2021). The problem of cybercrime is becoming a major issue for legal and criminal justice systems because criminals can use the Internet to carry out criminal activities in multiple countries, remain anonymous, alter information, and victimize multiple users in a relatively brief period of time. Unauthorized access to computer systems, identity theft, online financial fraud, ransomware attacks, cyberstalking, data breaches, digital extortion, and distribution of illegal content have become more complex (Bankole et al., 2022). Cybercrime differs from traditional crimes in that it can be carried out from a distance, and may be perpetrated by individuals from one jurisdiction, victimized by individuals in other jurisdictions, involve digital infrastructure from another jurisdiction, and may entail financial transactions from other jurisdictions. The transnational nature does present significant challenges to police, prosecutors, courts, and policymakers in combating cybercrime and holding those responsible for it to account(Casino et al., 2022).

Criminal investigations have also been impacted by cybercrime's evolution. Cybercrime has also impacted the nature of criminal investigations. Information created, stored and/or communicated using digital devices and information systems is replacing or supplementing traditional physical evidence. Electronic evidence, such as emails, electronic communications, transaction records, computer files, mobile information, social networking information, internet logs, cloud-based information, metadata, and other electronically stored information, may contain critical evidence regarding the commission of an offence and the activities or identity of an alleged offender(Curtis & Oxburgh, 2023). Digital evidence can link suspects to victims, provide a timeline of events, patterns of communication, and aid in or refute allegations that are made in court. But its evidentiary value is very dependent on the proper identification, acquisition, preservation, examination, documentation, and presentation. Evidence management is particularly complex for criminal justice institutions because the information can be easily altered, deleted, encrypted, and transferred and can be accessed remotely(Dreier et al., 2024). Digital evidence is, therefore, increasingly playing an important role in the modern-day policy framework of cybercrime. Criminal justice systems need to have clearly defined legal rules on the collection and preservation of electronic evidence, and ensure investigative powers are in line with privacy, due process and other fundamental rights. Authorized searches, electronic surveillance, access to personal data, interception of communications and seizure of digital devices, as well as cross-border data acquisition, are issues that must be addressed with a clearly defined legal framework (Munir, 2025). Meanwhile, gaps in national cybercrime laws, as well as variations in jurisdiction requirements, can make it difficult to investigate offenders or digital infrastructure outside the country where a cybercrime offense is reported. The successful investigation and prosecution of cybercrime, therefore, increasingly requires effective cooperation, mutual legal assistance and provision of information, as well as compatibility of evidence standards, at the international level(Dreier et al., 2024).

Institutional and technological constraints also hinder law enforcement in responding to the threats in the cyber arena. Forensic investigators need to have experience in digital forensics, cybersecurity, collection and preservation of electronic evidence, as well as being aware of new technologies. Prosecutors and judges also must muster a level of knowledge and understanding to assess the reliability, authenticity, relevance, and admissibility of digital evidence(Dudani et al., 2023). Poor forensic capability, training and technical resources, lack of institutional coordination and legal support can impact the success of cybercrime enforcement. These challenges highlight the need to go beyond technology in preventing cybercrime. To implement it, there needs to be an integrated framework that links legislation, law enforcement,

digital forensics, prosecution, judicial processes, privacy protections, and international cooperation(Dunsin et al., 2024).

In this context, it is particularly important to study cybercrime prevention and cyber evidence from a legal and criminal justice perspective, to allow for effective responses to the new cyber threats. A full solution must not only deal with the criminalization and prevention of cybercrime, but also the processes used to acquire, preserve, analyze, and present digital evidence in criminal proceedings (Dupont & Whelan, 2021). In this paper, the authors explore the evolving nature of cybercrime, legal tools for its prevention and prosecution, the significance and challenges of digital evidence, institutional capacity in criminal justice systems, and the need for a balance between investigative needs and privacy and human rights. It also reviews the steps to enhance law enforcement cooperation, forensic institutes, prosecutors, courts, technology providers, and international partners. This holistic approach can help improve cybercrime investigations, robust evidence collection and management, and a more agile criminal justice system to meet the evolving challenges of cybercrime.

**Emerging Cybercrime Threats and Their Criminal Justice Implications**

Today's cybercrime world has outgrown hacking and unauthorized access to become financially driven, identity theft crimes, ransomware, online crimes of fraud, cyberstalking, exploitation crimes, and critical infrastructure attacks. These crimes have immense implications in the field of criminal justice, as the crimes can be automated, remotely coordinated, and committed from different jurisdictions. The FBI's Internet Crime Complaint Center (IC3) received more than 859,532 complaints of Internet crime across the United States in 2024, with reported losses of over $16.6 billion, compared to the approximately $12.5 billion reported in 2023. These figures not only show the increasing economic cost of cybercrime, but also highlight that only reported and detected incidents are included in the figures and that cybercrime may be significantly bigger than current figures suggest(Fukami et al., 2021).

**Financial Cybercrime, Identity Theft, and Ransomware**

Financially motivated cybercrime is one of the fastest-growing types of cybercrime. Offenders can gain access to money without ever meeting their victims through phishing, business email compromise, investment fraud, online shopping fraud, cryptocurrency scams or identity theft. Investment fraud accounted for the greatest amount of reported losses to IC3, totaling around $6.57 billion in 2024, the FBI reported. The investment schemes involving cryptocurrencies were of particular concern as they allowed digital assets to be easily transferred between jurisdictions, and they also made it difficult to recover these assets. Business email compromise is another significant criminal justice issue, as it can allow criminals to use an executive, employee, or business partner to trick a victim into wiring money(Göbel et al., 2025).

There's another related threat, similar to ransomware, which is ransomware. Criminal groups gain access to networks, encrypt or steal information, and demand ransom for decryption or not publishing sensitive information. The financial damages are not the only criminal justice implications for ransomware, as it can impact hospitals, government services, education and critical services. Investigators need to determine the starting point of access, find the makeup of the malware, track cryptocurrency transactions, secure compromised systems, and link digital activity to known perpetrators. The organization of the ransomware groups across the globe makes the task of prosecution difficult since the victim, servers, cryptocurrency pockets, and suspects could be in various countries(Gruber et al., 2023).

**Cyber-Enabled Violence, Exploitation, and Attacks on Critical Infrastructure**

Cybercrime is not only a threat to the safety and security of individuals and societies, but also to financial systems. Cyberstalking, online harassment, doxxing, intimate-image abuse, child sexual exploitation, impersonation, and technology-facilitated threats can result in severe psychological and social distress. These crimes pose greater difficulties in providing evidentiary

proof since offenders can communicate using temporary websites, virtual private networks, encrypted communications, or false accounts. To maintain the rapid changes of information on the platform and to link digital accounts to people in the real world, criminal justice agencies need to be able to maintain the data and adhere to procedural protections and privacy rights. In addition to the wider impacts, there are these consequences from attacks on critical infrastructure(Gruber et al., 2022). Interdependent digital infrastructure is critical for energy systems, telecommunications networks, transportation systems, financial institutions, healthcare facilities, and government databases. If a cyber attack is successful against such systems, they can disrupt critical services and even pose a public-safety challenge. The criminal justice response should therefore be more than just the traditional investigation process, moving into the realm of prevention and intelligence sharing, incident response, and protection of nationally significant systems. This is especially challenging to do since an attacker may be able to hide the real source of the attack via a compromised computer, a proxy infrastructure, a botnet and/or a server in a third country(Hameed et al., 2021).

**Criminal Justice Challenges Created by Emerging Cyber Threats**

The main criminal justice challenge is the speed of change in technology and the ability of legal and investigative bodies to keep up. Conventional investigative and judicial procedures may take a lot longer, while a vulnerability can be exploited by the cybercriminal in minutes. Digital evidence may also be lost quickly, as there are variations in how long cloud storage, messaging systems, internet service providers, and social media platforms will keep records of a particular type. Investigators, therefore, need to have timely legal access to subscriber, traffic data, stored content, records, etc. The next big hurdle is jurisdiction. A single cybercrime could involve a victim in one country, an offender in another, servers in a third country, cryptocurrency transactions in a variety of other countries. Digital crime is not a localized affair, and domestic police powers are usually local only. International cooperation is then essential, as is mutual legal assistance, extradition, coordinated investigations, and common standards for using electronic evidence, to ensure effective prosecution(Ho & Ko, 2024).

With the rise of artificial intelligence comes new risks such as automated phishing attacks, deepfake fraud, synthetic identities, and high-level social engineering. It is therefore important that criminal justice institutions establish specialized cybercrime units, digital forensic skills, trained prosecutors, and judicial skills. Not only is technological capacity to be increased, but also the capacity of investigators to be exercised under well-defined legal and human rights protections. The modern criminal justice framework should ensure prevention, fast and effective investigation, trustworthy digital evidence, collaboration between countries and proportional prosecution to address the increasingly complex characteristics of cybercrime(Horsman, 2022).

**Legal Framework for Cybercrime Prevention and Prosecution**

Clear substantive criminal laws, investigative powers, evidentiary rules, institutional responsibilities and mechanisms for international cooperation are all crucial to the effectiveness of cybercrime control. Cybercrime is often a multi-jurisdictional crime, involves rapidly evolving technology, and is an offense that leaves behind evidence that is held by a private individual or on infrastructure outside of the investigating State. In this context, the question of criminalizing illegal online activity cannot be separated from the process of investigation and prosecution. So, modern cybercrime laws must cover not only the criminalization of illegal online activities but also the procedural aspects of the investigation and prosecution of cybercrime. Significant strides have been achieved in recent years, not just internationally, but also some blind spots in the law remain. By December, 2025, according to a 2026 assessment by the Council of Europe, 134 states (69% of the UN Member States) had substantial criminal law provisions largely established on computer offenses. But just 54% had specific procedural powers that were, to a large

extent, already in place to secure electronic evidence, indicating that criminalization has progressed faster than criminal investigative and evidentiary reform(Horsman, 2023).

**National Cybercrime Legislation and Procedural Powers**

The general definition of cyber offenses, the penalties for committing them, who can investigate, and what electronic evidence can be obtained and used in criminal proceedings is provided by national legislation. The modern cybercrime laws encompass offenses like illegal access to computer systems, unlawful interception, data and system interference, computer-related fraud, misuse of digital devices, identity-related crimes, and others that are committed through technology. Illegitimate access to data or systems, illegal interception, data interference, financial crimes committed with computer technology, privacy crimes, and technology-facilitated exploitation are among the key areas covered by national cybercrime laws identified by the United Nations Office on Drugs and Crime (UNODC). Pakistan is a good example and has a domestic law related to electronic crimes known as the Prevention of Electronic Crimes Act (PECA) 2016, which outlines the legal framework for combating electronic crimes and the investigative process. The bill has since been amended multiple times (Horsman & Sunde, 2022). The 2025 amendment added provisions to create a regulatory authority and protection body for social media, which will regulate any unlawful or offensive content, set standards for social media platforms, promote online safety, and regulate non-compliant platforms. The introduction of these laws is just one example of cybercrime laws moving away from computer crimes and into platform governance, online safety, and regulating communication in the online world(Ismail & Zainol Ariffin, 2025).

Also, a comprehensive legal framework is necessary to provide specific procedural authority to search and seize digital devices, ascertain computer data, obtain subscriber information, access stored electronic information, and intercept communications when legitimate. These powers require judicial authorization, proportionality conditions, documentation, and protection from arbitrary interference with privacy. This is especially true as digital investigations can yield a vast amount of personal information. The lack of specific restrictions in a legal framework that allows investigative powers free rein can give rise to issues of due process and privacy. On the other hand, overly stringent procedures may render it impossible for investigators to get the evidence before it gets deleted, encrypted, or transferred. Cyber law harmonization is important as it has been seen in the international development of cybercrime law. Convention on Cybercrime, opened for signatures in Budapest in 2001, contains substantive criminal-law provisions, procedural mechanisms for the production of electronic evidence, and mechanisms for international cooperation. As of December 2025, 81 states had joined, with other states having signed or been invited to join. The Convention of the Council of Europe also says that the Convention has had an impact on the domestic cybercrime legislation in about 85% of the world's states. This is proof of its continued relevance as a model for the development of legislation on the national level(Klasén et al., 2024).

**International Cooperation, Jurisdiction, and Prosecution**

Cybercrime is an international phenomenon, making it one of the greatest challenges in prosecution. An offender can work from one country, the victim in another, servers in a third, and money in a few different countries via financial institutions or cryptocurrency services. It typically does not cross borders, but digital evidence can cross borders with almost the blink of an eye. Therefore, there is a need for mechanisms such as extradition, mutual legal assistance, preservation of electronic evidence, information sharing, and cooperation between competent authorities for effective prosecution. The Budapest Convention is dedicated to tackling these issues. It offers mechanisms for emergency handling of data and mutual legal assistance, and states are obliged to cooperate as far as possible within its international cooperation framework.

They must also establish competent authorities and establish 24/7 points of contact for quick assistance in criminal investigations. The Second Additional Protocol further expands this framework with the aim of further promoting international cooperation and exchanging electronic evidence. By April 2026, 52 states had signed up to the Second Additional Protocol and four states had ratified it, reflecting a trend towards increased awareness of the need for quicker methods to secure cross-border electronic evidence(Kwon et al., 2024).

One of the most recent advancements is the United Nations Convention against Cybercrime, which was agreed upon by the UN General Assembly on 24th December 2024. It is the first-ever globally comprehensive treaty with a specific focus on cybercrime, and aims to ensure greater cooperation between countries and the sharing of electronic evidence for serious crimes. It is important because it is establishing a more comprehensive worldwide instrument that can be used in conjunction with the regional instruments, and can stimulate the development of compatible instruments in states with various legal traditions. Even so, there is a need for further harmonization of the law. Variations in how cybercrime is defined, evidence collection, privacy rights, evidence retention, and judicial authorization requirements can slow investigations and foster jurisdictional disputes. Effective prosecution therefore cannot be achieved unless better legislation is also in place at the domestic level, as well as compatible procedures at the international level. The future cybercrime legal framework should include well-defined crimes, reasonable investigative powers, effective rules on the preservation and collection of cyber evidence, judicial oversight, human rights protection and effective international collaboration. Such integration can lessen jurisdictional barriers, and may not erode the fundamental principles of legality, privacy, due process and the rule of law in the context of the expanding role of cybercrime law enforcement(Kwon et al., 2024).

**Law Enforcement Capacity and Digital Forensic Challenges**

The success of cybercrime laws will rely on the ability of law enforcement agencies to identify crimes, prosecute offenders, and produce technically sound investigations and cases for prosecutors and courts. The nature of cybercrime investigations is different from normal policing in many ways, as investigators should be knowledgeable about computer networks, mobile devices, cloud networks, cryptocurrencies, malware, encrypted communications, and online platforms. This issue is already taking a toll on criminal justice systems. According to the 2025/2026 Asia and South Pacific Cyberthreat Assessment (January 2024-March 2025), over half of the countries surveyed reported cybercrime accounting for at least 30% of all recorded crime in their country. It also revealed that 33 percent of the countries surveyed experienced over 10,000 instances of phishing in 2024, with over 6.5 billion cyber threats detected and mitigated across the region in 2024. Limited availability of specialized forensic tools, cybercrime training and technical capacity were specifically cited as ongoing challenges for law enforcement in the fight against cybercrime by INTERPOL(Lewulis, 2021).

**Institutional Capacity, Specialized Training, and Inter-Agency Coordination**

This is not the role of a traditional police investigator—criminals have modified the way they operate and work to suit contemporary needs, and those needs are matched by the requirements of contemporary criminal law enforcement. The cybercrime units require network analysts, malware analysts, open-source intelligence analysts, cryptocurrency analysts, online fraud analysts, mobile-device analysts, and electronic evidence analysts. Technical knowledge is also required by prosecutors and judges, as the investigation can go wrong at this stage if the investigators are unable to show how the evidence was collected, preserved, authenticated, and connected to a specific suspect. It is reflected in international capacity-building programs, which call for such expertise. In 2023, the United Nations Office on Drugs and Crime (UNODC)

was trained and technologically supported by 6,618 criminal justice practitioners such as first responders, investigators, prosecutors, judges, and digital-forensics specialists. The program included topics on digital forensics, electronic evidence, cryptocurrencies, malware and ransomware, darknet investigations, and online child exploitation. UNODC also reported an expansion of its program to 65 countries(Neale et al., 2022). INTERPOL has also increased the amount of specialized training. In 2024, it joined 6 other organizations to expand its Global Academy Network to 17 members and delivered training to its members to reach over 3,300 individual participants across the globe. For the 2024 edition of the Digital Security Challenge, organized by INTERPOL and the Council of Europe, 47 law-enforcement participants from 21 countries took part in training to test their digital-forensic and investigative skills in simulated cybercrime scenarios. Such statistics show that capacity building is not a luxury in the fight against cybercrime; it's an institutional necessity. Rapidly growing caseloads have real-world implications, as Pakistan shows. According to official National Assembly information, in 2023 the number of cybercrime complaints received via the national investigative system is 134,710, in 2024 – 161,828 and in 2025 – 157,465. During the same period, registered cases increased from 1,375 in 2023 to 1,667 in 2024 and 2,256 in 2025, while accused arrests increased from 2,007 to 2,157 and 2,916, respectively. Yet convictions declined from 92 in 2023 to 60 in 2024 and 39 in 2025. The volume of complaints and relatively few convictions emphasize the significance of the quality of the investigations, the quality of forensic evidence, and the capacity of the prosecution and institutional coordination(Ngejane et al., 2021).

To successfully counter cybercrime, police, specialized cybercrime agencies, financial-intelligence units, prosecutors, forensic laboratories, telecommunication firms, internet service providers, banks, cryptocurrency platforms and international institutions should collaborate closely with each other. INTERPOL's GLACY-e programme focuses on improving cooperation between law-enforcement agencies, financial-investigation units and prosecutors in the fight against the generation of criminal proceeds online. All of these can otherwise lead to duplicated investigations, delayed evidence requests, poor financial tracing, and loss of timely electronic evidence(Nicolás-Sánchez & Castro-Toledo, 2024).

**Digital Forensic Infrastructure, Evidence Recovery, and Technical Challenges**

Digital forensics provides the technology that is used to convert electronic information into criminal evidence. The investigators may have to look at the deleted files, examine the browser history, investigate the metadata, look at how devices communicate with each other, how the devices communicate with accounts and IP addresses, look at suspicious software, trace financial transactions, recover information from mobile devices, and find the link between devices and people. The process needs to be carried out in a forensic manner, as any changes to a device or digital file may raise questions of authenticity and reliability(Nisioti et al., 2023). The acquisition, documentation, forensic imaging and hashing, chain-of-custody, storage, and repeatable examination processes are therefore the necessary controls that must be observed. Technical surroundings are becoming increasingly challenging. In addition, encryption can make it hard for investigators to gain access to communications or the content of devices; cloud computing can make it possible for evidence to be stored in multiple countries; ephemeral messaging can result in information being lost; and cryptocurrency transactions can make traditional financial investigations more challenging. The existing cyber-capacity programs of INTERPOL therefore feature expert training on cryptocurrency investigations and malware analysis, in addition to training on acquiring electronic evidence from service providers from various jurisdictions(Nordvik et al., 2021; Veksler et al., 2025).

The sheer amount of digital information also poses a problem in the forensic workload. One investigation can include multiple devices, computer systems, cloud systems, social media

accounts, email accounts, financial records and network logs. The manual examination process is therefore inefficient and requires special acquisition and analytical software in the forensic laboratories. But access to tools is not even. The 2025/2026 regional evaluation by INTERPOL clearly highlighted the need for more specialized forensic equipment and technical capacity of the participating countries. Concurrently, 66.7% of the countries surveyed noted using AI tools or systems in predictive analysis, digital forensics, and threat detection as part of their institution's approach to cybercrime, suggesting AI-investigation is beginning to become part of institutional responses(Rachut & Maurer, 2024). Digital forensic issues are important, especially because success in investigations does not necessarily lead to prosecutions. Evidence is required to be legally obtained, technically authenticated, properly preserved, and communicated to the prosecutor and courts. Investigators are thus in need of standardized forensic procedures and ongoing training, not just one-off technical training. Investments should be made in forensic laboratories, in analytical tools and tools that have been licensed, in secure evidence storage facilities, in mobile and cloud forensics facilities, in cryptocurrency-tracing facilities, and in specialist personnel. The best way to do this is an integrated model that brings together the technical skills, forensic capabilities, legal knowledge, and international collaboration of the law-enforcement community. Even extensive Cybercrime legislation might result in feeble criminal justice results if institutions are not able to transform reported cyber incidents into admissible proof and prosecutions(Rakha, 2024).

**Privacy, Human Rights and Procedural Safeguards in Cybercrime Investigation**

As cybercrime investigations have grown more common, there has been a significant shift in the law, with criminal justice authorities increasingly seeking more invasive access to digital information and individuals having rights to privacy, data protection, freedom of expression and due process. A tension is especially important given that communication, location data, financial records, cloud-stored files, browsing history, photos, and metadata are all examples of electronic evidence. In fact, the European Union has estimated that about 85% of criminal investigations include digital evidence, which shows how much electronic information has penetrated into today's criminal investigations(Tok et al., 2025). Meanwhile, international laws and regulations are not uniformly applicable. As of December 2025, 97% of UN Member States had either implemented cybercrime and electronic-evidence reforms or had been making progress on reforms, while 54% had specific procedural powers largely established in order to secure electronic evidence. The lack of protective safeguards can lead to over-surveillance, access to data without authorization, or excessive interference in the privacy of others and is very important(Ratul et al., 2024).

The Budapest Convention establishes a valuable guideline that procedural powers shall include human rights considerations, proportionality, independent/frequently judicial oversight, explicit grounds for the application, and restrictions on the scope and duration of investigative powers. These protections are especially vital in situations where investigators are conducting searches of personal devices, intercepting communications, accessing traffic or subscriber information, or requesting information from a service provider(Roberts et al., 2024). Digital investigations may yield a tremendous amount of information in addition to the evidence they were investigating for, which can include the collection of third-party information that may be irrelevant and/or highly sensitive. It is thus imperative that the principle of necessity and proportionality be included in the definition of a legitimate investigative purpose in the procedural law in order to prevent investigators from accessing and retaining personal data without a proper basis. Recent European e-evidence reforms illustrate: reforms of 2023 introduce measures for personal-data protection, for legal (as opposed to technical) remedies for individuals affected by the production, and for an intervention by the authorities in certain instances, when production is requested but should not take place. Another

concern with cross-border information collection is that the information could be sent across jurisdictions with different privacy and procedural rules(Romaniuk & Ablamskyi, 2024).

The UN Convention against Cybercrime, adopted on 24 December 2024, thus puts emphasis on international cooperation, along with references to human rights and personal data protection; at present, 95 signatories and 3 parties to the Convention have done so, and to date, the Convention has not yet come into force, as 40 ratifications are needed. These principles—the purpose limitation, data minimization, necessity, proportionality, independent review and effective remedies—are reflected in the treaty framework. These safeguards are crucial to help prevent that the means of investigation are used for arbitrary surveillance or limitations on legitimate expression. A shift in thinking is needed to treat privacy and human rights as part of a successful cybercrime investigation, not an obstacle, and for this, the legal powers to search, judicial oversight, evidence-integrity requirements, limitations on data retention, effective remedies and clear accountability mechanisms are essential to successfully conduct a digital investigation in alignment with the rule of law(Sandoval et al., 2024).

**Strengthening the Criminal Justice Framework for Cybercrime Prevention**

Attacks on the cybercrime front are growing in size and sophistication, and criminal justice systems need to shift from responding to crime to a system of criminal justice that also incorporates preventative measures, specialized enforcement, digital forensics, international cooperation, and rights-based legal protections. There are special reasons to be concerned about strengthening institutions, especially in developing regions, where technology has been developed before law enforcement has been able to keep up. According to INTERPOL's 2025/2026 Evaluation of the Asia and South Pacific region, more than half of the surveyed countries reported that more than 30% of the crime reported locally occurred in the field of cybercrime. Additionally, over 135,000 ransomware attacks were also recorded in 2024, a 92% increase in DDoS attacks, and over 6.5 billion cyber threats were detected and mitigated throughout the region in 2024. These developments show the need for coordinated institutional, technological, legal and international measures to develop cybercrime prevention in a more robust way(Steinmetz et al., 2024).

**Strengthening Specialized Law Enforcement and Digital Forensics**

The most important thing is to establish specialized cybercrime units with sufficient manpower, forensic laboratories and investigative technology, and regular training of professionals to build a professional team. Mobile forensics, network analysis, malware investigations, cryptocurrency tracing, cloud evidence acquisition, open-source intelligence and online financial investigations are all necessary skills for cybercrime investigations. These are technically complex cases, and general policing structures are not likely to be effective. In 2023, UNODC assisted 65 countries with the Global Program on Cybercrime, and trained 6,618 criminal justice practitioners comprising investigators, prosecutors, judges, first responders, and digital-forensics specialists. These statistics do show the magnitude of the capacity to build a justice system for cybercrime(Stoykova, 2023).

Digital forensic infrastructure also needs to be improved by implementing standardized protocols for evidence collection, forensic imaging, hashing, evidence preservation, chain of custody documentation, and expert reporting. Agencies need to ensure digital evidence repositories are secure and acquire expertise in encrypted devices, cloud, cryptocurrency evidence, and deleted or fragmented data. INTERPOL discovered that specialized tools and technical expertise for law enforcement in the Asia and South Pacific region are still lacking. Meanwhile, 66.7% of the countries surveyed indicated the use of AI tools to assist with investigations, such as predictive analysis, digital forensics, or threat detection, highlighting the growing role of technology in investigations(Stoykova, 2024).

**Improving Legal Procedures, Evidence Management, and Judicial Capacity**

Electronic evidence procedures need to be established, and there needs to be a strengthening of institutions. Legally defined preservation, search, seizure, disclosure, and cross-border acquisition of digital information mechanisms must be developed for investigators. These powers should be subject to judicial authorization and proportionality requirements to avoid unwarranted surveillance and privacy intrusions during effective investigation. The global position of the legislation is much better and still has some flaws. As of December 2025, 134 countries (69% of UN Member States) had substantive provisions on cybercrime in place, and more than 97% of UN Member States were working towards or had completed broader legislative reforms. However, a process law on electronic evidence is not fully developed yet, thus demonstrating the need for more than criminalization(Stoykova, Andersen, et al., 2022).

The capacity of the Judiciary is also essential. Specialized training for prosecutors and judges on authenticity, reliability, and metadata, forensic imaging, digital chain-of-custody procedures, cloud evidence, cryptocurrency evidence, and expert testimony. The courts need to be able to tell the difference between evidence or information that is technically sound and evidence or information that has been illegally acquired or poorly preserved. This needs to be complemented by a better framework which would create a set of reporting obligations and accreditation procedures for the digital-forensics laboratories. This would minimize the amount of conflicts of evidence, and it would make crimes against the computer more consistent(Stoykova & Franke, 2023).

**Expanding International and Public–Private Cooperation**

Often, cybercrime is transborder, and local laws and policies are ineffective without regional cooperation. Criminal justice agencies should set up an expedient information exchange mechanism with foreign agencies, various international bodies, financial institutions, telecom companies, Internet companies, and cybersecurity companies. It's practical – like, for example, the Asia and South Pacific Joint Operations Against Cybercrime established by INTERPOL. 26 countries were involved in Operation SECURE (from November 2024 to April 2025), which led to the removal of over 20,000 malicious IP addresses and domains, the arrest of 30 individuals, and the collection of over 100 GB of data. The findings highlight the usefulness of joint multinational investigations. Electronic evidence should also be rapidly and streamlinedly made available for international use(Stoykova, Nordvik, et al., 2022).

On 24 December 2024, the United Nations Convention against Cybercrime was adopted by the United Nations General Assembly, which establishes a worldwide system for international cooperation and sharing of electronic evidence concerning serious crime. The Convention had 82 signatories and 3 parties, but had not yet entered into force, as the 40 ratifications needed to come into effect have not been secured as of September 2026. States should therefore give high priority to the ratification, implementation and development of their domestic procedures that are in line with the Convention. Cooperation of the private sector is also a must, as often technology firms possess evidence for investigators. There should be formal channels set up for lawful preservation and disclosure requests, emergency reporting, fraud detection and threat intelligence sharing. Having clear legal guidelines can assist companies in working with investigators while maintaining the privacy of legitimate users(Sunde, 2022).

**Prevention, Public Awareness, and Rights-Based Cybercrime Governance**

An effective criminal justice system also needs to decrease victimization before crimes are committed. Governments should launch national awareness programs related to phishing, financial fraud on the internet, identity theft, ransomware, social engineering, and safe use of the Internet. This is especially relevant as cybercriminals utilize human nature more and more, and not just technical weaknesses. In Asia-Pacific, 33 percent of

countries reported over 10,000 online-scam cases, with 5.5 individuals clicking phishing links each month, about twice the global average, according to INTERPOL(Surakanti et al., 2025).

Public awareness should thus be included in national cybercrime plans and not be considered an afterthought. However, prevention should, at all times, be consistent with fundamental rights. Investigative powers should be legally, necessarily, proportionately, and with judicial monitoring, data protection, and due process regulated. Over-surveillance or the availability of private communications may erode public trust and afford room for institutional mistreatment. The goal should be to build a system of criminal justice that is speedy and effective in identifying and responding to true cybercrime threats, while maintaining privacy and procedural fairness(Thornton & Bagheri Zadeh, 2022).

**7. Conclusion**

This escalation in the scale and complexity of criminal activities has created cybercrime a significant challenge for criminal justice. This study concluded that financial fraud, ransomware, identity theft, cyber enabled violence, online exploitation and attacks on critical infrastructure can no longer be addressed with traditional policing methods. The analysis revealed that digital evidence has become a critical piece in cybercrime investigations, yet it must be properly collected by legal authorities, preserved in a trustworthy manner, subjected to forensic analysis, authenticated, and presented in a courtroom. The study also revealed that national legislation, jurisdictional issues, lack of procedures, lack of specialized investigators, lack of forensic infrastructure and challenges in collecting evidence across international borders are all significant impediments to effective cybercrime prosecutions. They are challenges that illustrate the need to align substantive cybercrime laws with the implementation of effective procedural powers and internationally agreeable evidence-management mechanisms. The effective use of specialized cybercrime units, trained prosecutors and judges, accredited digital-forensic laboratories and uniform procedures for evidence-handling are critical to improving investigative and judicial results. International cooperation must also be a key element, as cybercrime often crosses multiple jurisdictions, is served by foreign service providers and has an international digital infrastructure. Multagency collaboration between law enforcement, financial institutions, technology firms and international organizations can help preserve evidence, identify offenders, trace finances and prosecute offenders more quickly. While strengthening investigative capacity, an adequate balance should be struck between privacy, proportionality, legality, and due-process protection. Cybercrime prevention, in general, needs a comprehensive criminal justice approach that includes legislation, specialized enforcement, digital forensics, institutional coordination, international cooperation, public awareness and human rights protection. This can help build a resilient system for criminal justice institutions to deal with new cyber threats, and not leave behind basic legal protections because of technological developments.

**REFERENCES**

Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, *29*(2), 118-153. https://doi.org/10.1093/ijlit/eaab001

Bankole, F. O., Taiwo, A. A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation*, *40*, 301348. https://doi.org/10.1016/j.fsidi.2022.301348

Casino, F., Pina, C., & López-Aguilar, P. (2022). SoK: cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, *8*(1), tyac014. https://doi.org/10.1093/cybsec/tyac014

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, *96*(4), 573-592. https://doi.org/10.1177/0032258X221107584

Dreier, L. M., Vanini, C., Hargreaves, C. J., Breitinger, F., & Freiling, F. (2024). Beyond timestamps: Integrating implicit timing information into digital forensic timelines. *Forensic Science International: Digital Investigation*, *49*, 301755. https://doi.org/10.1016/j.fsidi.2024.301755

Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, *47*, 301576. https://doi.org/10.1016/j.fsidi.2023.301576

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Australian & New Zealand Journal of Criminology*, *54*(1). https://doi.org/10.1177/0004865821103925

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*, 301169. https://doi.org/10.1016/j.fsidi.2021.301169

Göbel, T., Breitinger, F., & Baier, H. (2025). Optimising data set creation in the cybersecurity landscape with a special focus on digital forensics: Principles, characteristics, and use cases. *Forensic Science International: Digital Investigation*, *52*, 301882. https://doi.org/10.1016/j.fsidi.2025.301882

Gruber, J., Hargreaves, C. J., & Freiling, F. (2023). Contamination of digital evidence: Understanding an underexposed risk. *Forensic Science International: Digital Investigation*, *44*, 301501. https://doi.org/10.1016/j.fsidi.2023.301501

Gruber, J., Voigt, L., Benenson, Z., & Freiling, F. (2022). Foundations of cybercriminalistics: From general process models to case-specific concretizations in cybercrime investigations. *Forensic Science International: Digital Investigation*, *43*, 301438. https://doi.org/10.1016/j.fsidi.2022.301438

Hameed, U., Qaiser, Z., & Qaiser, K. (2021). Admissibility of Digital Evidence: A perspective of Pakistani Justice System. *Pakistan Social Sciences Review*, *5*(4), 518-530. https://doi.org/10.35484/pssr.2021(5-IV)40

Ho, H., & Ko, R. (2024). Using Situational Crime Prevention (SCP)-C3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes. *Journal of Cybersecurity*, *10*(1), tyae020. https://doi.org/10.1093/cybsec/tyae020

Horsman, G. (2022). Conducting a 'manual examination' of a device as part of a digital investigation. *Forensic Science International: Digital Investigation*, *40*, 301331. https://doi.org/10.1016/j.fsidi.2021.301331

Horsman, G. (2023). Digital evidence strategies for digital forensic science examinations. *Science & Justice*, *63*(1), 116-126. https://doi.org/10.1016/j.scijus.2022.11.004

Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science & Justice*, *62*(2), 171-180. https://doi.org/10.1016/j.scijus.2022.01.002

Ismail, I., & Zainol Ariffin, K. A. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE*, *20*(9), e0331683. https://doi.org/10.1371/journal.pone.0331683

Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*, *362*, 112133. https://doi.org/10.1016/j.forsciint.2024.112133

Kwon, D., Borrion, H., & Wortley, R. (2024). Measuring Cybercrime in Calls for Police Service. *Asian Journal of Criminology*, *19*(3), 329-351. https://doi.org/10.1007/s11417-024-09432-2

Lewulis, P. (2021). Digital forensic standards and digital evidence in Polish criminal proceedings. An updated definition of digital evidence in forensic science. *International Journal of Electronic Security and Digital Forensics*, *13*(4), 403-417. https://doi.org/10.1504/IJESDF.2021.116024

Munir, B. (2024). Artificial intelligence and legal decision-making in the USA and Pakistan: A critical appreciation of regulatory frameworks. *Global Foreign Policies Review*, 48–58.

Munir, B. (2025). *Artificial intelligence for lawyers: Navigating novel methods and practices for the future of law*. Punjab Law Book House.

Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, B. (2022). The case for Zero Trust Digital Forensics. *Forensic Science International: Digital Investigation*, *40*, 301352. https://doi.org/10.1016/j.fsidi.2022.301352

Ngejane, C. H., Eloff, J. H. P., Sefara, T. J., & Marivate, V. N. (2021). Digital forensics supported by machine learning for the detection of online sexual predatory chats. *Forensic Science International: Digital Investigation*, *36*, 301109. https://doi.org/10.1016/j.fsidi.2021.301109

Nicolás-Sánchez, A., & Castro-Toledo, F. J. (2024). Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective. *Crime Science*, *13*, 11. https://doi.org/10.1186/s40163-024-00209-7

Nisioti, A., Loukas, G., Mylonas, A., & Panaousis, E. (2023). Forensics for multi-stage cyber incidents: Survey and future directions. *Forensic Science International: Digital Investigation*, *44*, 301480. https://doi.org/10.1016/j.fsidi.2022.301480

Nordvik, R., Stoykova, R., Franke, K., Axelsson, S., & Toolan, F. (2021). Reliability validation for file system interpretation. *Forensic Science International: Digital Investigation*, *37*, 301174. https://doi.org/10.1016/j.fsidi.2021.301174

Rachut, S., & Maurer, J. W. (2024). The European regulation on E-Evidence and the balance between data protection and cross-border security. *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, *1*(15), 33-45.

Rakha, N. A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, *16*(2), 23-54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Ratul, M. H. A., Mollajafari, S., & Wynn, M. (2024). Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability*, *16*(24), 10885. https://doi.org/10.3390/su162410885

Roberts, S. C., Zahabi, M., McCarthy, L., Lanclos, C., & Romero, J. (2024). Law Enforcement Perspectives on Police Vehicle Cybersecurity. *Transportation Research Record*, *2678*(1). https://doi.org/10.1177/21695067231192578

Romaniuk, V. V., & Ablamskyi, S. Y. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*, *2*. https://doi.org/10.32631/pb.2024.2.13

Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: a systematic review. *Crime Science*, *13*, 41. https://doi.org/10.1186/s40163-024-00239-1

Steinmetz, K. F., Schaefer, B. P., McCarthy, A. L., Brewer, C. G., & Kurtz, D. L. (2024). Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units. *Criminal Justice Policy Review*, *35*(4). https://doi.org/10.1177/08874034241265106

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Stoykova, R. (2024). A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. *Computer Law & Security Review*, *55*, 106040. https://doi.org/10.1016/j.clsr.2024.106040

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, *40*, 301351. https://doi.org/10.1016/j.fsidi.2022.301351

Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, *45*, 301554. https://doi.org/10.1016/j.fsidi.2023.301554

Stoykova, R., Nordvik, R., Ahmed, M., Franke, K., Axelsson, S., & Toolan, F. (2022). Legal and technical questions of file system reverse engineering. *Computer Law & Security Review*, *46*, 105725. https://doi.org/10.1016/j.clsr.2022.105725

Sunde, I. M. (2022). AI-based Law Enforcement Online: The Impact of the European Artificial Intelligence Act (AIA). *Bergen Journal of Criminal Law & Criminal Justice*, *10*(2), 29-50. https://doi.org/10.15845/bjclcj.v10i2.3844

Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations – a systematic literature review. *International Journal of Information Security*, *24*, 210. https://doi.org/10.1007/s10207-025-01131-y

Thornton, G., & Bagheri Zadeh, P. (2022). An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis. *Forensic Science International: Digital Investigation*, *41*, 301379. https://doi.org/10.1016/j.fsidi.2022.301379

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International: Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Veksler, M., Akkaya, K., & Uluagac, S. (2025). Practitioner-driven framework for AI adoption in digital forensics. *Forensic Science International: Digital Investigation*, *55*, 302030. https://doi.org/10.1016/j.fsidi.2025.302030

IEER
Institute for Excellence in Education & Research