Cybercrime Investigation: Modern Trends, Challenges, and the Role of Digital Evidence

Manisha Ambawta[1*], Dr Aditi choudhary[2]

*[*1]PhD Scholar, School of Law, Manav Rachna University, Faridabad, E-mail: advocatemanisha66@gmail.com*
[2]Assistant Professor , School of Law, Manav Rachna University, Faridabad, E-mail: aditi@mru.edu.in

Abstract
The rapid digital transformation of business environments has created new opportunities for innovation, entrepreneurship, and global economic integration. However, the increasing reliance on digital infrastructures has also intensified exposure to cyber threats that affect organisations, particularly small and medium-sized enterprises (SMEs). Cybercrime activities such as phishing, ransomware attacks, financial fraud, and data breaches have become major challenges for digital economies and entrepreneurial ecosystems. This review paper examines modern trends in cybercrime affecting digital businesses and explores the role of cybercrime investigation in addressing these emerging threats. The study synthesises existing literature on digital transformation, cybercrime patterns, investigative technologies, and digital evidence management. It highlights the importance of digital forensics, artificial intelligence, blockchain analysis, and open-source intelligence as critical tools in modern cybercrime investigations. The paper also discusses major challenges faced by investigators, including cross-border jurisdictional issues, technological anonymity, regulatory limitations, and resource constraints in developing economies. Furthermore, the review emphasises the implications of cybercrime for sustainable entrepreneurship and digital economic development. Strengthening cybersecurity governance, improving digital literacy, and promoting collaboration between public and private sectors are identified as key strategies for enhancing cyber resilience. The study concludes that integrating advanced investigative technologies with effective governance frameworks is essential for combating cybercrime and protecting digital ecosystems in the evolving digital economy.

Keywords: Cybercrime Investigation, Digital Evidence, Cybersecurity, Digital Transformation, Sustainable Entrepreneurship

1. INTRODUCTION

The digital economy has expanded at a very impressive rate, and it has therefore affected the business environment in a fantastic manner, particularly in newly established entrepreneurial ecosystems across the globe. More and more frequently, SMEs use digital platforms, cloud services and online communication tools to increase the efficiency and growth of operations and competitiveness. Digitalisation has assisted companies to adopt newer models and participate in international value chains in an improved way. Nevertheless, a greater dependence on digital infrastructure has also brought with it new technological vulnerabilities that organisations need to deal with in a meticulous manner that can guarantee their sustainability and stability in terms of operation. The small and medium enterprises are still poorly equipped to manage cybersecurity threats because of financial constraints, technical skills, and organisational awareness, which exposes them to cyber threats (Junior et al., 2023).

Digital transformation has emerged as one of the key sources of the current business growth, enabling organisations to introduce technologies like artificial intelligence, data analytics, and cloud computing into their business process. The technologies help companies to make better decisions, increase customer interactions, and create new services and products that aid in competitive strengths. However, digital technologies are introduced at the same time, which exposes organisations to cybersecurity risks capable of affecting business processes and exposing sensitive data. Organisations that have adopted digital systems without proper cybersecurity systems are likely to suffer severe consequences, including data breaches, disruption in account operations, and loss of money. As a result, any business that is going through a digital transformation should consider the possibility of cyber-attacks and take strategic measures to alleviate the risk impact (Benjamin et al., 2024).

With the increased integration of digital technologies in the processes of organisations, cybercrime has become one of the biggest challenges that impact contemporary businesses. Phishing attacks, ransomware attacks, and online fraud are the types of cybercrimes that target businesses that are very dependent on the online system and banking. The vulnerability of SMEs is especially high since they do not always have dedicated teams working on cybersecurity, as well

as the sophisticated security infrastructure that would protect against a highly advanced cyber-attack. Due to the quick development of digital crime methods, companies seeking to ensure safe online spaces and, at the same time, develop and expand in competitive markets have faced significant operational pressures (Awan et al., 2025). The effects of cyber threats are particularly severe in developing and emerging economies, in which SMEs are key in the development of the economy and creation of employment. SMEs in most Asian economies play a major role in the productivity of the nation, innovativeness, and entrepreneurship. Although most of these organisations have economic significance, a significant number of them lack fully developed cybersecurity policies or risk-management policies. The growing digital connectivity and the online nature of businesses have broadened the attack prospects against cybercriminals, exposing business organisations to a wide range of cyberattacks that can disrupt the financial stability of a business and business continuity. According to empirical studies conducted among Malaysian SMEs, the adoption of digital technology has exacerbated cybersecurity threats and posed new difficulties in organisations that have tried to protect digital resources and systems (Arifin et al., 2025).

The complexity of cybersecurity issues affecting organisations has also increased in light of the growing introduction of digital technologies into business activities. Sophisticated digital systems such as cloud computing infrastructures, Internet-connected devices, and digital payment systems provide numerous opportunities where hackers can use system vulnerabilities. In order to address these weaknesses, organisations ought to adopt holistic solutions to cybersecurity, not just the technological components of addressing them but also the organisational risk-management policies. It is also an essential organisational resiliency competency in the digital era because it is the potential of organisations to identify cybersecurity risks and proactively make mitigation efforts by ensuring that main data and functional systems are secured (Saeed et al., 2023).

The other dilemma pertains to the goodwill of SMEs to implement cybersecurity solutions that incorporate both the software and human components of information security. The failure to implement powerful cybersecurity challenge is an issue that most organisations experience because of the strength of the new digital environments and cyber threat dynamics. The literature on cybersecurity preparedness models emphasises the role of using a socio-technical thinking model that combines technological protection with employee education, governance framework, and organisational strategies that would effectively guard against digital resources (Perozzo et al., 2022). Recent technological advances have transformed the situation in the field of cybersecurity once again, introducing artificial intelligence and automated threat-detection systems. The technologies provide organisations with novel prospects to enhance cybersecurity potentials by allowing for identifying anomalies faster, conducting a better threat assessment, and addressing risks proactively. Nonetheless, the incorporation of AI into cybersecurity systems also provokes new issues related to data confidentiality, transparency of the algorithm, and the trustworthiness of the system. Research about AI-supported cybersecurity systems highlights the relevance of systematic strategies that can help SMEs to embrace the advanced security systems and handle the risks linked to the new systems (Ullah et al., 2025).

In addition to technological transformations, organisations should also embrace a well-organised cybersecurity governance infrastructure to adequately deal with digital threats. Effective risk-management systems may assist organisations in finding out the vulnerabilities, assessing possible risks, and establishing security controls, which safeguard digital property and guarantee business continuity. A proper cybersecurity governance involves the need to incorporate all the information security policies, technological protective measures, and organisational review systems into a wider scope of strategic management (AL-Dosari and Fetais, 2023).

Although there has been a growing awareness of cybersecurity risks, several organisations still encounter challenges in conducting proper security practices. The lack of cybersecurity skills, the lack of financial resources in the field of security technologies, and the lack of the organisational awareness of cyber threats usually prevents the implementation of the complex approaches to cybersecurity. Research on the analysis of situational awareness and decision-making in the context of SME leaders suggests that the gaps in situational awareness often do not allow organisations to perceive vulnerabilities in their digital ecosystems that can postpone required protective measures (Chang et al., 2025).

Moreover, increased usage of digital technologies has posed new governance issues to organisations that seek to have secure digital environments. As companies keep increasing their adoption of digital environments and data-driven technologies, they also need to enhance cybersecurity readiness to protect the digital environment and ensure the trust of their stakeholders. Studies that investigate the trends of digital adoption by companies prove that all cybersecurity strategies should keep up with the

development of new technologies to guarantee the stability and security of the contemporary digital ecosystem (Jasiak et al., 2025).

Considering the growing reliance of organisations on digital technologies, cybercrime investigation has been an invaluable aspect of ensuring secure online environments. An effective cybercrime investigative system also allows organisations and policy makers to identify cyber threats, monitor criminal activities and protect confidential data in the internet. Digital proofs, forensic analyses and advanced investigative technologies are crucial in warning of crime operations and bringing to book those in charge in the current digital platforms.

The provided review paper examines the most recent trends in the area of cybercrime investigation, determines the main issues, which are associated with the approach to digital evidence, and explores the nature of investigative technologies in addressing cyber threats, which are related to digital business and SMEs. By synthesising the recent studies about the tendencies in the field of cybercrime, cybersecurity systems and approaches to investigation, the study will contribute to the improvement of the current knowledge regarding the ways in which cybercrime investigation can be utilised to facilitate digital resilience and sustainable economic development.

2. DIGITAL TRANSFORMATION AND ENTREPRENEURIAL ECOSYSTEMS IN ASIa

2.1 *Digital Entrepreneurship and Innovation Ecosystems*

Nowadays, the digital transformation is among the most important factors of the contemporary entrepreneurial ecosystems in the global arena. With the emergence of digital technologies into the business processes, business people have managed to develop new forms of business models that are largely reliant on digital infrastructure, data analytics and online platforms. These technological changes have greatly altered the way organisations generate value, relate to their customers and how they compete in international markets. Digitisation of innovation systems has also guaranteed the appearance of new entrepreneurial opportunities through the reduction of barriers to entry and an opportunity to scale up operations of companies quickly in the digital environment (Nambisan et al., 2019). Digital technologies enable innovation systems to enable startups and emerging businesses to engage stakeholders, including technology providers, research institutions, and investors. Such interlocked networks are important in enhancing knowledge exchange and the commercialisation of innovative ideas. Digital ecosystems consequently offer the entrepreneur access to resources and the technological capabilities that would otherwise have been unreachable to smaller organisations. These processes have reinforced the significance of digital technologies as one of the determinants in entrepreneurship and economic development in modern economies (Kraus et al., 2022).

2.2 Expansion of SMEs and Startup Economies in Asia

The medium and small-sized firms form an important part of the economic growth in most of the Asian economies. The growing use of digital technology has enabled SMEs to become more competitive in that they are able to increase their efficiency in operations, increase their coverage to a wider market, and expand into international trade. Digitalisation allows the smaller organisations to compete better with the larger companies by having access to digital platforms and technological advances to access wider customer bases. Internationalisation of online markets has also promoted entrepreneurship in the developing economies. There are digital tools that allow business organisations to discover the world beyond geographical boundaries and be a part of global markets via online communications and digital services. Consequently, the notion of entrepreneurial performance has become more attached to organisational capacity to incorporate digital technologies and implement them in their strategic business. The literature review of the connection between digitalisation and entrepreneurial performance suggests that implementing digital technologies plays an important role in business growth, productivity, and competitiveness in the global economy (Ţurcan et al., 2022).

2.3 Digital Platforms, Fintech, and E-Commerce Growth

Digital platforms have become the new infrastructure of modern entrepreneurship that allows businesses to relate to customers, partners, and suppliers via digital systems that have been integrated. Figure 1 presents the association between digital transformation, digital platforms, and new cybercrime threats.

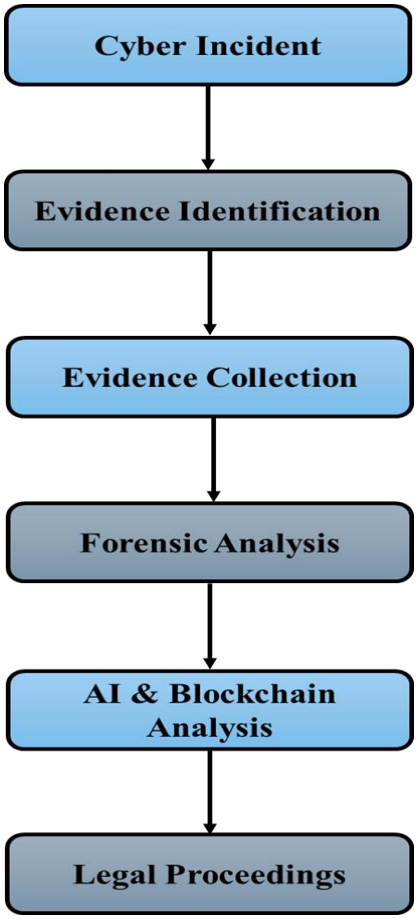

Figure 1. Conceptual framework linking digital transformation, digital exposure, and emerging cybercrime threats with cybercrime investigation mechanisms

Fintech technologies and e-commerce platforms have changed the process of conducting transactions and managing the financial operations of businesses to a large extent. Such technologies have made payments easier, access to financial services better and the development of online marketplaces that promote innovation by entrepreneurs. The massive growth of the e-commerce industry has opened new grounds for startups and SMEs to conduct their businesses in the highly competitive digital markets. Business model Entrepreneurs can now create a platform-based business model that is based on digital infrastructure to provide products and services across geographical borders. Digital platforms also support the aspect of innovation by facilitating firms to test new service models, data-driven strategies, and approaches to digital customer engagement. With the further development of digital sources, they are becoming more significant to the evolution of the entrepreneurial ecosystem and contribute to the sustainable development of business.

2.4 Cybersecurity as a Foundation for Sustainable Business Environments

Although digital transformation has massive opportunities in the context of entrepreneurial development, it also presents advanced cybersecurity issues that organisations must resolve. Companies based online are becoming increasingly vulnerable to cyber-attacks that can compromise business, sensitive data, and destroy customer confidence. Cybersecurity is thus critical in determining the continuity and state of digital entrepreneurial environments. To mitigate the risk of further cyber threats against organisations, there is a need to develop effective cybersecurity awareness and education programs. The fact that many SMEs do not have enough resources and knowledge to enforce strong cybersecurity practices predisposes them to cyberattacks, especially. Cybersecurity awareness of both employees and decision-makers can also go a long way in enhancing the capacity of an organisation in detecting and applying the necessary security measures against a possible risk. Training and education programs are thus regarded as important elements of organisational cybersecurity practices (Bada & Nurse, 2019). Besides the awareness programs, digital forensics and biometric systems have also advanced, which has improved the functionality of

cybercrime investigations. The current investigative technologies allow authorities and organisations to investigate digital evidence, identify cyber threats, and react better to cyber incidents. Biometric systems and multimedia forensic technologies have extended the boundaries of cybercrime investigations because they allow the investigator to track digital activities and determine possible offenders in digital settings (Thakur et al., 2024). In general, digital transformation is still transforming the entrepreneurial ecosystems, introducing new possibilities of innovations and business growth and entering the global markets. Simultaneously, the growing importance of using digital technologies also causes the consideration of cybersecurity frameworks that could help to safeguard digital infrastructures and guarantee the long-term sustainability of the entrepreneurial activities of contemporary digital economies.

3. Modern Trends in Cybercrime Affecting Digital Economies

3.1 Phishing and Financial Fraud Targeting Digital Businesses

The proliferation of online enterprises and business models through the blistering development of digital entrepreneurship has ensured that organisations become more vulnerable to cybercrime activities. Online banking services, digital platforms and e-commerce services have become core elements in the economic activities of the modern world, enabling businesses be able to conduct their operations in digital ecosystems around the world. Digital entrepreneurial ecosystems have promoted the process of innovation and market growth; however, they have also introduced new points of vulnerability that are exploited by cybercriminals. Since organisations are becoming more dependent on digital infrastructure to execute financial transactions and handle sensitive information, cybercriminals have devised advanced means of controlling digital systems and deceiving users to gain monetary advantages (Sussan & Acs, 2017). Phishing is regarded as one of the most common ways of cybercrime used to target online companies and online customers. Such attacks are typically performed through fraudulent email messages, websites, or messages that are supposed to fool people into giving information such as login information, financial information, or personal identification information. The digital businesses are vulnerable especially in that they usually interact with the customers through electrical communication media. Such interactions are used by the cybercriminals to pose as legitimate organisations or service providers and therefore gain illegal access to digital systems and financial resources. The development of the digital entrepreneurial landscapes has added to the scale and complexity of the phishing attempts. An automated tool and social engineering tricks are employed in the modern networks of cybercriminals to execute large-scale phishing attacks, which may involve thousands of users. Such campaigns are usually structured to resemble genuine corporate messages, which is hard to see by an individual and business. The dangers of phishing and financial fraud are now a significant issue for organisations striving to ensure a safe digital environment, as digital platforms keep growing in the world.

3.2 Ransomware Threats to SMEs and Startups

Another significant cybercrime threat to digital businesses, especially the small and medium-sized ones, is ransomware attacks. Ransomware normally entails the use of malicious software that encrypts organisational data and requires them to pay a sum to allow them to regain access to the encrypted information. These attacks have the potential to lead to major operational and financial losses to organisations that use digital infrastructure in undertaking their day-to-day activities. The digital transformation has provided conditions where a massive amount of business information is stored in digital systems, all interconnected, such that organisations are becoming more lucrative prey of the ransomware attacks. SMEs and startups tend to be more susceptible, since they do not possess or employ developed cybersecurity systems and information security teams. These organisations are therefore often targeted by cybercriminals because they have a greater chance of paying the ransom requests to resume business. Increasing dependence on cloud computing, remote work solutions, and internet-based communication tools has only increased the possible harm, resulting in the occurrence of a ransomware attack. After cybercriminals have infiltrated organisational networks without the authorisation of the organisations, it takes a short time before ransomware spreads to various systems and affects important business operations. Consequently, ransomware has emerged as one of the most harmful types of cybercrime to contemporary digital economies.

3.3 Cryptocurrency and Blockchain-Related Cybercrime

The advent of cryptocurrencies and blockchain technologies has brought new aspects to cybercrime activities. Cryptocurrencies allow users to engage in financial transactions via decentralised online networks without necessarily using conventional banking systems. Although these technologies have many advantages in terms of financial innovation and digital entrepreneurship, they provide an

opportunity for cybercriminals to use illegal financial activities anonymously. Cybercriminals often transfer illegal money in cryptocurrencies; launder money acquired in the process of cybercrime and get payments in ransomware attacks. Cryptocurrency systems are decentralised and pseudonymous, which complicates the process of tracking financial transactions and identifying people who act as criminals in the cybersphere. Due to the increased adoption of digital currencies in the global financial system, the rate of cybercrime that involves cryptocurrency transactions has increased tremendously. Criminology studies have noted that the activities of cybercrime are becoming more complex in the digital financial world. The contemporary cybercriminal networks tend to cross national borders and use sophisticated technological equipment to engage in illegal activities in the digital markets. To address the dynamic nature of cybercrime, one will need to apply interdisciplinary methods based on the study of technological, economic, and criminological facets of cybercriminal conduct (Onwuadiamu, 2025).

3.4 Cloud and Mobile Platform Vulnerabilities in Digital Enterprises

Mobile technologies and cloud computing have become part and parcel of online business. Cloud platforms are also becoming increasingly used by organisations to store their data, manage their applications, and facilitate the remote working environment. Mobile gadgets and online applications also allow businesses to communicate with customers and partners via online platforms and online communications.

Cloud and mobile technologies have a lot of advantages, but they also create a high level of cybersecurity vulnerability that can be used by cybercriminals. Poorly set-up cloud systems, ineffective authentication facilities, and poor application programming interfaces may provide points of entry to cyber attackers who may want to gain unauthorised access to the organisational network. When the attackers access the cloud-based systems, they can steal classified information, interfere with services, or insert malicious software in the organisational systems.

Digital environment cybercrime activities are mostly influenced by the technological developments that create better avenues through which the criminals utilise the system vulnerability. The fast growth of digital technologies has consequently posed complicated dilemmas to organisations trying to defend digital assets and secure operation environment. To overcome these obstacles, the digital systems should be monitored constantly, and more sophisticated cybersecurity plans should be created to identify and eliminate cyber-attacks (Kshetri, 2016).

3.5 Artificial Intelligence and Emerging Cybercrime Technologies

Artificial intelligence and machine learning are among the technological innovations that have changed the way cybersecurity is applied and the ways of how cybercrime is planned. By using artificial intelligence, organisations can examine a substantial amount of data, identify abnormalities and determine possible cyber threats much more effectively. Such technologies have the potential to enhance the capacity of cybersecurity experts to conduct surveillance on digital networks and react in response to cyber-attacks.

However, artificial intelligence technologies are also beginning to be applied by cybercriminals in order to make cyberattacks more advanced. Artificial intelligence-designed malware, artificial intelligence-based phishing campaigns, and smart social engineering tricks allow criminals to be more successful at their actions and overcome traditional cybersecurity defence. Digital technologies are changing and becoming more sophisticated in cybercrime practises that are becoming difficult to detect. The contemporary digital economies are dynamic and changing and therefore face hacking in organisational settings. Businesses are supposed to keep on adapting their strategies on cybersecurity to meet new technological challenges and learn to keep the digital systems safe in the hands of rogue individuals. The interaction of technology and cybercrime behaviour supports the necessity of developing a comprehensive regulation approach of both investigations and prevention to address cybercrime within the novel digital environments (Broadhurst et al., 2013).

4. CYBERCRIME INVESTIGATION AND DIGITAL EVIDENCE IN THE DIGITAL ECONOMY

4.1 Role of Digital Forensics in Cybercrime Investigation

Digital forensics is an inseparable component of cybercrime inquiry and organisations and law enforcement agencies are steadily coming to rely on computer technologies to communicate, execute business, and store data. Digital forensics practises involve locating, conserving, interpreting and reporting on electronic data that could be used in court in a criminal case. Table 1 presents some of the key digital forensic methods applied in investigations of cybercrime.

Table 1. Digital forensic techniques used in cybercrime investigation

Technique	Purpose	Application

Computer Forensics	Recovery and analysis of digital files	Investigating hacked systems
Network Forensics	Monitoring network traffic	Identifying cyberattack sources
Mobile Forensics	Analysis of smartphone data	Tracking cybercriminal communication
Blockchain Analysis	Tracking cryptocurrency transactions	Ransomware investigations
OSINT Analysis	Collecting public digital intelligence	Identifying cybercriminal identities

Due to the constantly changing dynamics of cybercrime activities, investigators are forced to embrace more sophisticated forensic methods to gather and analyse digital evidence from various sources, including computers, mobile devices and cloud systems. Computer forensics has become a very important branch of the law in the contemporary world due to the increased use of electronic documents and computer records as evidence in courts of law. Cybercrime evidence can consist of emails, transactional records, network logs, and metadata that will assist the investigators in reassembling the offences of cybercrime and pinpointing the perpetrators of unlawful acts.

Figure 2 demonstrates the cybercrime investigation and digital evidence processing life cycle.

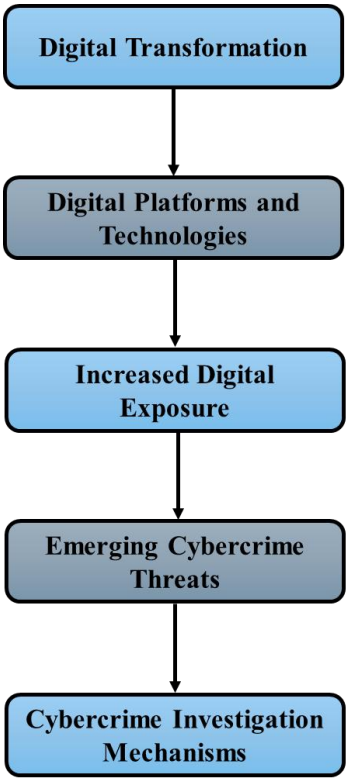

Figure 2. Cybercrime investigation lifecycle from cyber incident detection to legal proceedings

Digital evidence should be handled with a lot of care so that it is admissible in a court of law and not corrupted during the investigation process. Studies indicate that computer forensic practices are important in proving the reliability of electronic documents as credible tools of evidence in criminal justice systems (Hardinanto et al., 2023).

4.2 Artificial Intelligence and Data Analytics in Cybercrime Detection

The significance of digital data is rapidly expanding, and the conventional means of investigation are no longer effective in identifying advanced cyber threats. Computerised tools to investigate cybercrime have thus become part of artificial intelligence and better data analytics. These technologies can facilitate the processing of high quantities of digital information by the investigators in a relatively short period of time and reveal the patterns which could reveal the existence of malicious actions in the digital networks. It is possible to use artificial intelligence systems to analyse network traffic and detect abnormal behaviours of the system and suspicious communication patterns that can indicate cyberattacks. The machine learning algorithms also enable the investigators to come up with predictive models that can enable the detection of potential threats before they can cause immense damage to the digital infrastructures. Use of artificial

intelligence in cybersecurity has therefore resulted in improved efficiency in threat detection, and also improved the ability of organisations to respond to cyber attacks. Together with artificial intelligence, open-source intelligence (OSINT) has become one of the important tools of investigation by cybersecurity experts nowadays. OSINT is the fusion and analysis of publicly accessible data, which includes websites, social media and online databases. OSINT methods assist investigators in tracking criminal activities in cyberspace, determining digital identities, and collecting intelligence that aids in investigating cybercrimes. The increasing relevance of OSINT within the sphere of cybersecurity studies reveals the opportunity to enhance situational awareness and other investigation abilities in the online setting (Yadav et al., 2023).

4.3 Blockchain Analysis in Financial Cybercrime Investigations

The growing popularity of e-financial technology has posed new threats to cybercrime investigators. The digital platforms, electronic payment systems, and cryptocurrency transactions are now highly involved in financial systems and require specific investigative methods. The digital currencies rely on blockchain technology, which suggests that the centralised records of transactions are stored in distributed networks. Though blockchain systems provide a level of transparency because transaction ledgers are publicly visible, the anonymity of digital wallet addresses may complicate the process of identifying the individuals involved in financial cybercrime activities. Often, cybercriminals use cryptocurrency systems to make illegal purchases, clean up money gotten because of the commission of other types of crimes and pay ransomware. Consequently, researchers are forced to invent analytical approaches that will allow tracking blockchain operations and detecting suspicious financial operations in online networks. The spread of digital financial systems has contributed to shaping the wider financial inclusion and economic development as well. Digital financial platforms help individuals and organisations to engage more in financial markets; however, it also leaves new vulnerabilities that can be abused by cybercriminals. Research studies on financial systems note that the development of digital financial infrastructure needs to be enhanced through stricter regulatory frameworks and technological security to ensure that financial transactions and mishaps that occur in digital economies are safeguarded by stronger mechanisms (Magalhães-Timotio et al., 2022).

4.4 Real-Time Monitoring Systems and Cyber Threat Intelligence

The real-time monitoring systems and cyber threat intelligence platforms are important in enhancing cybersecurity defences and assisting in investigations of cybercrime. The systems continue monitoring the network activities and they identify any suspicious activities and send alerts that assist organisations to respond to any potential cyber-attack in real-time. Real-time monitoring systems are likely to integrate different data sources that include network logs, security sensors and digital communication systems to provide a comprehensive perspective of organisational digital infrastructures. Cyber threat intelligence is the process of information gathering and evaluation of information about cyber-attacks, vulnerability and symptoms of attack. Through the analysis of threat intelligence data, investigators and cybersecurity experts will be able to detect the new trends in cybercrime and devise strategies to eliminate possible risks. Threat intelligence platforms also enable the sharing of information between organisations so that they can exchange information on cyber threats and build resilience in the collective cybersecurity. Cyber threat intelligence reports are gaining more importance to international organisations and law enforcement agencies interested in cybercrime activities globally and the development of coordinated responses to novel threats. Such reports can be useful in understanding cybercriminal networks, methods of attack and technological weaknesses that can impact organisations that conduct business in the online space. Multinational security agencies have also raised concerns over the increasing complexity of organised cybercriminals and the need to increase investigative power to overcome the emerging challenges (Europol, 2014).

4.5 Digital Innovation and Investigative Ecosystems

The creation of digital technologies also affected the design of investigative ecosystems, assisting in cybercrime investigations. Online platforms enable cybersecurity expert individuals, police, and technology firms to collaborate in managing cyber threats. These cooperation ecosystems help the stakeholders to exchange their knowledge and technical abilities and research to upgrade the approaches of cybercrime prevention. The digital entrepreneurship environments have in addition demonstrated how digital infrastructures can be interwoven to facilitate innovation and exchange of knowledge among organisations. Intelligence sharing and collective efforts in cybersecurity and cybercrime investigations can be implemented in a similar format, and the investigators will be able to take advantage of technological innovations and common intelligence sources. Developments in the

sphere of digital ecosystems, in turn, suggest that strengthening the capabilities of investigative institutions and enhancing the overall resilience of the digital economies to the work of cybercrime will become possible (Song, 2019).

5. CHALLENGES IN CYBERCRIME INVESTIGATION WITHIN EMERGING ECONOMIES

5.1 Jurisdictional Complexities in Cross-Border Cybercrime

The transnational character of cybercriminal behaviour is one of the greatest problems in the investigation of cybercrime. Cybercrime is often committed by criminals, reciprocal and digital infrastructure in other countries, and this poses complicated jurisdictional challenges to law enforcement agencies. Table 2 gives the key issues that plague the investigation of cybercrime in emerging economies.

Table 2. Key challenges in cybercrime investigation

Challenge	Description	Impact on Investigation
Cross-border Jurisdiction	Cybercrime often occurs across multiple countries	Legal and cooperation delays
Encryption Technologies	Secure communications hide criminal activity	Difficulty accessing evidence
Institutional Capacity	Limited forensic expertise in developing countries	Weak investigation capabilities
Delayed Incident Reporting	Businesses hesitate to report cyberattacks	Loss of critical digital evidence
Legal Framework Limitations	Laws lag technological changes	Difficult prosecution

When international borders are involved in the activities of cybercriminals, the investigators must go through different legal frameworks, procedural policies, and data protection legislations that can jeopardise the ability to collect digital evidence in time. Such jurisdictional lines tend to slow the investigation process and make it hard to prosecute criminals. Trends in cybercrime in Asian countries show that transnational cybercrime is on the rise as digital technology facilitates the ability of the perpetrator to work anonymously in geographically faraway places (Broadhurst and Chang, 2012).

5.2 Encryption and Anonymity Technologies

There are also advanced tools that have been presented by technological advancements that can be used by cybercriminals to hide their identities and go unnoticed. Legitimate benefits of encryption technologies, anonymising networks, and secure communication platforms can be used for illegal purposes as well as legitimate ones. In many cases, cybercriminals use encrypted messaging solutions and anonymisation technologies to conceal their online traces and escape the attention of investigators. Consequently, the police have a fair share of difficulties when trying to monitor the tracks of cybercriminals and extract digital evidence within encrypted spaces. The use of artificial intelligence technologies is also becoming a subject of discussion as a potential solution to better cybercrime prevention and the increase in investigation abilities within the digital world (ALkharabsheh et al., 2024).

5.3 Institutional and Resource Constraints in Developing Countries

Emerging economies are also characterised by a high level of institutional and resource constraints, which hamper their capacity to carry out successful cybercrime investigations. Low availability of advanced forensic equipment, lack of cybersecurity infrastructure and the lack of trained cybersecurity experts can undermine the capability of institutions to identify and respond to cyber threats. Most organisations in the emerging economies are unable to implement holistic cybersecurity structures that would facilitate the effective process of cybercrime investigation. Moreover, the fast growth of the digital economy has increased the rates of digital transactions and online services, and they need more powerful cybersecurity management systems to secure the critical digital infrastructures. A study of the digital economy in developing countries shows that poor management capacity to deal with cybersecurity issues is also one of the biggest barriers to dealing with cyber threats in the most effective manner (Odejayi, 2023).

5.4 Delayed Reporting and Digital Awareness Gaps among Businesses

An additional critical issue with respect to cybercrime investigation is the slowness of cyber incidents reporting by organisations and businesses. There are also financial losses and legal consequences, which make many organisations reluctant to report cyberattacks because they fear to damage their reputation. Consequently, the occurrence of cybercrime is usually not detected promptly, and this makes the investigation process

difficult and chances of recovering the digital evidence are low. Moreover, insufficient cybersecurity education among workers and the executives of organisations may ensure that companies are not able to detect the initial hints of cyber threats. Enhancing digital forensic preparedness in organisations is hence key to enhancing efficiency to cybercrime investigations and facilitate prompt response towards cyber incidents (Zainudin et al., 2024).

5.5 Legal Challenges in Digital Evidence Admissibility

The legal structures relating to investigations of cybercrimes should always develop to accommodate intricacies involved in digital evidence. Digital evidence is vastly different as compared to traditional evidence in that it is really easy to modify, duplicate or even ruin material of evidence unless it is properly handled. Courts thus must have stringent protocols of gathering, storing and presenting digital evidence to make it authentic and reliable in the court of law. Nevertheless, a lot of the legal systems continue to struggle with the adaptation of the laws that exist to the dynamically evolving digital world. The jurisprudence of cybercrime is still volatile and in a way the governments and international bodies still seek to enhance regulatory structures that combat emergent cyber threats. Researchers have emphasized that modern legal issues associated with cybercrime investigation need modern legal policies and better coordination among law enforcement organs and courts (Amoo et al., 2024).

6. DIGITAL EVIDENCE AND LEGAL FRAMEWORKS IN ASIAN ECONOMIES

6.1 Nature and Characteristics of Digital Evidence

The emergence of digital evidence in the contemporary cybercrime cases has emerged as a major component of the contemporary cybercrime investigation cases as societies continue to rely on digital technologies to communicate, conduct business, and store information. Compared to traditional physical evidence, digital evidence is in electronic forms like emails, system logs, records that are made in case of transactions and metadata that is created by the digital devices and the Internet. Such types of evidence have the capacity to offer useful information about user behaviour, system operationalities and communication patterns, which assist the investigators to recreate cyber incidents. Nevertheless, the digital evidence is difficult to examine as it is intangible and can be easily changed which poses a great challenge in the course of investigation. Unless digital evidence was preserved and documented correctly, it can be altered, corrupted, or erased, thus losing its credibility in court. The increasing amount of cybercrime in the COVID-19 crisis also proved the relevance of digital evidence in determining cyber offenders and examining trends in online victimisation in the world of the internet (Lee et al., 2025). The online activities leave digital evidence that is usually used to conduct investigations. Data like IP addresses, time stamps, browsing history and communication logs enable investigators to trace the existence of suspicious traffic as well as to reconstruct the flow of events that lead to cyber incidents. Due to the fact that cybercrime is often committed in complex digital infrastructures involving a number of devices and networks, investigators are required to use specialised forensic tools and analysis methods that are useful in gathering, preserving, and analysing digital evidence in the most effective manner.

6.2 Chain of Custody and Evidence Integrity

The integrity of digital evidence is crucial to its reliability when it comes to the investigation process. Chain of custody is a term that is used to describe the paper-trail that evidence is followed over its litigation, storage, transfer and examination. This is to ascertain that the digital evidence has not been tampered with and that the evidence is authentic and has not been changed and manipulated through the investigation. The fact that it is very easy to copy or alter digital files makes investigators put in place stringent measures to ensure that the evidence is in its original form. The digital forensic practitioners are usually involved in creating forensic images of the storage device, roll the cryptographic hash values to ensure data integrity, and keep a detailed account of every interaction with the evidence. Such steps assist in making sure that digital evidence can be proven and used in court. When the chain of custody is not adhered to or properly recorded, then the evidence could not be admitted in court since there is no certainty that it is authentic or reliable.

6.3 Regulatory Frameworks Governing Cybercrime

The rising cases of cybercrime have prompted governments and international bodies to come up with legal frameworks that will help in controlling the activities conducted online as well as prosecuting cybercriminal behaviour. The proper cybercrime law needs to address cybercrime like unauthorised access of systems, online fraud, theft of data and even cyber harassment. Nonetheless, technological changes tend to outpace the legal system and hence it is challenging to develop elaborate regulatory systems capable of successfully dealing with the challenges associated with cyberspace. Cybersecurity development is an even greater challenge to developing countries in the

process of creating policies and regulatory frameworks. Most of the emerging economies are yet to establish the institutional framework necessary to handle digital infrastructures and implement cybercrime laws. The reinforcement of legal and cybersecurity is vital in this regard to make sure that digital transformation will help to benefit the economy without leaving loopholes in digital ecosystems. Attempts to mitigate cybercrime are also tightly connected with the projects aimed at unlocking the digital potential of the developing economies and ensuring an inclusive presence in the global digital market (Świątkowska, 2020).

6.4 Institutional Cooperation and International Cyber Law

Cybercrime cases more often than not require that actors and digital systems be found in a variety of jurisdictions and as such international coordination is very critical in enforcing the law. The agencies of law enforcement, the regulatory bodies and the cybersecurity institutions should have to cooperate and exchange information, coordinate investigations, and harmonise the legal systems that regulate prosecution of cybercrimes. International collaboration allows law enforcement to access online evidence in other countries and monitor international networks containing cybercriminals. There have been other complications to the legislation of cybercrime and the international cooperation due to the emerging technologies like artificial intelligence and sophisticated ransomware systems. Laws have to be developed to respond to the technologically advanced crimes without undermining the level of protection of digital privacy and civil liberty. Experts have highlighted that legislations on cybercrime in the future should integrate the knowledge of technology and adaptable laws to tackle the new digital challenges (Do & Selvadurai, 2025). The issue of institutional co-operation also affects the way digital evidence is handled and introduced in the context of criminal investigation. The regulatory requirements also influence the investigators to collect, preserve and analyse digital data in a manner that would make it admissible in court. Literature shows that legal provisions also influence the investigative procedure to a considerable extent, as they establish norms of dealing with digital evidence and forensics (Kyslenko et al., 2024). The prosecution of cybercrimes is always likely to be successful with the help of legal professionals, cybersecurity specialists and digital forensic investigators. Such multidisciplinary work allows the courts to analyze difficult pieces of digital evidence and define clear connections between the crime of cybercriminals and the suspects. Enhancement of collaboration between technical professionals, law enforcement agencies, and courts thus continues to be a crucial factor in enhancing efficiency in addressing cybercrimes and effective application of digital evidence in the current legal systems (Shami et al., 2025).

7. IMPLICATIONS OF CYBERCRIME FOR SUSTAINABLE ENTREPRENEURSHIP

7.1 Financial and Operational Risks for SMEs

The cybercrime poses both financial and operational risks to the small and medium enterprises (SMEs) that use digital technologies to conduct their daily operations. The more organisations are embracing digital platforms, cloud services and online payment systems, the more vulnerable they are to cyber threats that may cripple business operations. There is a risk of financial losses and disruption of operations and harm to digital infrastructure due to the cyberattacks that could be ransomware, phishing, and data breaches. The SMEs are especially at risk since most of them have minimal cybersecurity investments and lack a risk management infrastructure. The digital forensic investigations are thus becoming critical to detecting cyber threats and ensuring that the effects of cybercrime cases on the business operations are curbed. Adequate analysis of digital evidence assists an investigator to know how cyberattacks happen and it is through this that organisations can enhance their security systems in case of occurrence of such attacks again. Nevertheless, the admissibility and reliability of digital evidence continue to be the most important questions of the investigation of cybercrime since the courts must be provided with high-quality forensic confirmation of the fact that electronic evidence has not been altered in the course of the investigation (Yeboah-Ofori and Brown, 2020).

7.2 Impact on Innovation and Startup Ecosystems

Cybercrime also interferes with the sphere of innovation and development of enterprises that have a strong dependence on digital technologies. Technology-oriented business ventures and digital startups tend to be data-intensive processes and Web-based platforms to create new products and services. Examples of cyber threats to the digital systems include derailing the innovation processes, postponing product development, and discouraging investors in new ventures. According to the growing complexity of digital infrastructures, advanced data analytics have also broadened the scope of cybersecurity investigation. The big data technologies enable the investigators and cybersecurity experts to explore large pools of online data to identify cybercrimes and patterns of malicious activity within the digital networks. The implementation of big data computing in the digital

forensic investigation, thus, contributes to the enhancement of cybersecurity performance and helps to facilitate the safety of innovative digital businesses (Satpathy et al., 2018).

7.3 Business Trust, Reputation, and Consumer Confidence

Credibility and reputation are also the building blocks of successful online entrepreneurship. Companies that are in the online business level should ensure that they have a good relationship with their customers, partners and other stakeholders who use the safe digital platform to communicate and transact their finances. Incidents of cybercrimes can badly destroy the image of an organisation by revealing sensitive customer data or shaking service provision. These events tend to undermine the trust of consumers and diminish the reputation of online enterprises that compete within the market. Businesspeople should hence lay more emphasis on cybersecurity policies that safeguard customer information and provide a safe online business. The literature review about digital entrepreneurship has brought to the fore the importance of digital security practices as an aspect of business strategy in organisations, with the future growth of entrepreneurial ecosystems. Both those entrepreneurs who are proactive in mitigating cyber threats are in a better place to keep businesses growing and ensure confidence in the digital world (Nicolau et al., 2022).

7.4 Cybersecurity as a Component of Sustainable Economic Development

The issue of cybersecurity has a significant role in facilitating sustainable economic growth in digital economies. Table 3 spells out strategic cybersecurity strategies that could be used to increase resilience among SMEs.

Table 3. Cybersecurity strategies for SMEs and digital enterprises

Strategy	Description	Expected Benefit
Cybersecurity Governance	Adoption of structured security policies	Stronger organisational protection
Digital Awareness Training	Employee cybersecurity education	Reduced human error
AI-based Security Systems	Automated threat detection	Faster incident response
Public-Private Collaboration	Cooperation with cybersecurity agencies	Information sharing
Regulatory Compliance	Adoption of legal cybersecurity frameworks	Improved digital trust

With the transition to a more digitised business environment and financial systems, there is a need to secure digital infrastructure to achieve economic stability and facilitate entrepreneurship. The cybersecurity frameworks are useful in ensuring the digital technologies are adopted to enhance economic growth and innovation safely and efficiently. Studies conducted to investigate the linkage between cybersecurity and sustainable development reveal that digital infrastructures that are secure are fundamental in enhancing resilient digital economies. Cybersecurity practices lead to the long-term sustainability as they help to preserve critical digital assets, minimize losses in the economy related to cybercrime, and enhance institutional confidence in digital systems (Sulich et al., 2021). Entrepreneurial organisations also need to create strategic capacities that would empower them navigate well in the highly dynamic and uncertain digital environments. The business world is usually unpredictable, uncertain, complex, and uncertain (VUCA) in nature, which needs agility and flexibility to react to the technological changes and cybersecurity issues. The capability of SMEs in planning cybersecurity into digital transformation initiatives hence emerges as a determinant of sustainable business development and competitive edge (Troise et al., 2022). Moreover, the modern business ecosystems are also becoming more influenced by financial technologies through fintech-based platforms that offer new financial services and digital payment solutions. The technologies can be used to ensure the sustainability of the economy by creating access to finance and also aiding entrepreneurship in different sectors. Nevertheless, the fast development of fintech systems also comes with new cybersecurity challenges that should be resolved to have secure financial transactions and safeguard digital financial infrastructures (Arshi et al., 2024).

8. STRATEGIC RESPONSES FOR STRENGTHENING CYBER RESILIENCE

8.1 Cybersecurity Governance in Entrepreneurial Organisations

Since digital technologies are now deeply integrated into the current business contexts, entrepreneurial organisations need to have well-developed cybersecurity governance frameworks to ensure the security of their digital resources and business systems. Cybersecurity governance is the combination of policies, technological protection as well as risk management strategies which inform how organisations deal with cyber risks. Good governance also makes sure that issues concerning cybersecurity are factored into the process of making strategic decisions and management practices of the organisation. Cybersecurity

frameworks like the National Institute of Standards and Technology (NIST) cybersecurity framework include well-organized information that organisations may follow to evaluate cybersecurity threats, employ protective measures, and continuously observe digital systems. These frameworks assist organisations to create systematic ways of managing cybersecurity and enhancing resilience to cyber threats (Möller, 2023).

8.2 Capacity Building and Digital Literacy Programs

Another essential aspect of enhancing cyber resilience is the aspect of enhancing cybersecurity knowledge and capabilities either in organisations or the society. Numerous cyber-attacks are happening due to the absence of adequate awareness on cyber threats or the lack of adherence to safe practices on the internet. A capacity building program and digital literacy initiatives consequently comes in handy to mitigate cybersecurity vulnerabilities. There has been a growing realisation by governments and institutions of the necessity to invest in cybersecurity education and professional training as an effort to fill the shortage of cybersecurity specialists around the world. Cybersecurity competencies can be developed with the aid of programs that enable organisations to receive the necessary expertise to detect cyber threats, take protective measures, and respond adequately to cyber incidents. Programs to enhance cybersecurity expertise have also been linked to aid in developing and enhancing the workforce to reduce the skills gap in cybersecurity careers (Spanou, 2024).

8.3 Public–Private Partnerships in Cybersecurity

Another strategy that can be relevant in enhancing cybersecurity resilience in digital economies is the involvement of the government and private industries in partnerships. The issue of cybersecurity cannot be resolved by government agencies or individual organisations only since cyber threats usually cut across numerous industries at the same time. Government-industry collaboration with the research institutes and technology providers can facilitate knowledge and resource sharing as well as intelligence about threats that can enhance cybersecurity preparedness.

By engaging in partnerships, organisations can come up with strategies to monitor cyber threats jointly, to counter cyber-attacks and to enhance the security of digital infrastructure. Such collaborations also facilitate the formulation of cybersecurity standards and best practices that inform organisations to adopt effective security practices. With the cyber threats constantly changing, the interconnection between the citizens and the business sector is ever becoming more significant to have strong digital ecosystems that can react to the new cyber security threats.

8.4 Institutional Reforms and Policy Development

Cybersecurity strategies on national and organisational levels need to be reinforced through institutional reforms and policy development. As the digital transformation is fast approaching, the governments must update regulatory systems and institutional structures to address the new cyber threats. Effective cybersecurity policies should provide legal pointers of the manner of securing digital systems, managing cyber threats, and prosecuting cybercriminals.

When the conventional information security is transformed to the more comprehensive cybersecurity approaches, it could be taken as the sign of the increasing nuances of digital infrastructures and the increasing importance of the protection of interdependent digital systems. The most recent methods of cybersecurity should address the technological, organisational, and societal dimensions of cybersecurity instead of concentrating on the technical level. As noted by scholars, the cybersecurity frameworks must incorporate technological protective strategies with governance arrangements as well as policy initiatives that help to coordinate the actions against cyber threats (Von Solms & Van Niekerk, 2013).

8.5 Regional Cooperation for Cybercrime Prevention

International cooperation between governments and international organisations in the region is also essential in dealing with cybercrime. The world of cybercriminals often transcends national boundaries and countries must cooperate in the prevention or investigation of cybercrime. The regional cooperation initiatives may help to share cyber threat intelligence, harmonise cybersecurity laws and support collective investigations of transnational cybercrime networks. Nevertheless, technological solutions are not enough to increase cyber resilience, it must also be supported by enhancing the level of awareness of cybersecurity risks among the people. Education of individuals and organisations on secure online behaviour and prevention of cyber threats is generally done through cybersecurity awareness campaigns. Although they are essential, numerous awareness campaigns cannot bring about long-term behaviour change because of the communication strategy constraints and little contact with the target markets. The effectiveness of these campaigns needs to be enhanced hence to promote a culture of cybersecurity awareness to help enhance the wider

cyber resilience campaigns (Bada et al., 2015). In general, to enhance cyber resilience, coordinated actions are needed which includes governance models, education programs, joint ventures, and policy or legislation. Together with these strategies, organisations and governments will have a chance to develop comprehensive cybersecurity strategies which guarantee the security of digital infrastructures and support development of digital economies in a sustainable way.

9. FUTURE DIRECTIONS FOR CYBERCRIME INVESTIGATION AND DIGITAL SECURITY

9.1 Emerging Investigative Technologies

The facial aspect of cybercrime investigations continues to alter due to the dynamism of the sphere of digital technologies. The new investigative technologies are slowly coming into the picture in the detection, tracking, and stop of a cybercriminal in the digital networks. The modern forensic investigations of cybercrime are anchored on the advanced digital forensic tools with a capacity to examine large volumes of electronic data created by digital devices, communication systems, and cloud computing infrastructures. The tools enable investigators to reconstruct cybercrimes, identify bad actors, and trace digital activities through systems that have relationships. Technological advances such as the use of automated software in forensic analysis, advanced malware detection software, and blockchain analysis software are also boosting the investigative capabilities greatly. Automated forensic tools enable investigators to run through digital evidence in an efficient way as they scan through digital storage devices and network systems of interest quicker in search of suspicious trends or concealed information. In the same vein, blockchain analysis tools can help the investigators to relate cryptocurrency transactions to cybercrime incidents like ransomware payments and financial fraud. With the advancement of less-lethal methods used by cybercriminals, there will always be a need to create more sophisticated investigative technologies to reinforce the system of cybercrime detection and response. Table 4 summarises emerging technologies that can be used to investigate cybercrime and provide digital security.

Table 4. Future technologies supporting cybercrime investigation

Technology	Role in Cybercrime Investigation	Future Potential
Artificial Intelligence	Detect anomalies and cyber threats	Predictive cybersecurity
Blockchain Analytics	Trace cryptocurrency transactions	Financial cybercrime detection
Big Data Analytics	Analyse large digital datasets	Pattern recognition
Cloud Forensics	Investigate cloud-based attacks	Remote investigation capabilities
Threat Intelligence Platforms	Share cyber threat information	Global cybercrime monitoring

9.2 AI-Driven Cybercrime Detection

In the applied field of cybercrime detection and investigation, artificial intelligence (AI) will revolutionize the processes in the future. Cybersecurity systems based on AI have the ability to process large volumes of data created by digital infrastructures, as well as detect patterns on network traffic that can be indicative of cyber threats. Machine learning algorithms can learn continuously on new data and therefore cybersecurity systems will be able to enhance their threat detection against time. Real-time cyber threats detection systems based on AI can contribute significantly to the effectiveness of organisations to detect cyber threats. Such systems are able to always scan digital networks, identify possible behaviour and automatically execute security measures in case of any potential threat. As an illustration, AI technologies can spot abnormal activity regarding the patterns of logins, abnormal data transfers, or suspicious communication actions, which can signal unauthorised system access. Even though they have advantages, AI-based cybersecurity systems also introduce the transparency, algorithmic bias and system reliability as new issues. With more organisations implementing AI-based cybersecurity tools, one of the issues that will emerge is to make sure that such technology is run in a transparent fashion and in accordance with ethics and regulatory requirements. Future studies must thus aim at enhancing the reliability, accountability, and security of cybercrime detection systems that are based on AI.

9.3 Digital Resilience in Entrepreneurial Ecosystems

The increasing digitalisation of entrepreneurial ecosystems has led to the development of new opportunities to innovate and develop economically, whereas the ecosystems have also become more vulnerable to cyber threats. Digital enterprises, SMEs and startups tend to have a heavy dependency on digital platforms and cloud infrastructures to sustain their business operations. Cybercrime cases, therefore, may be disastrous to the entrepreneurial enterprises through interference with business, loss of customer information and loss of organisational reputation. Any future cybersecurity plans must then focus on digital resilience in the entrepreneurial ecosystems. Digital resilience

means that organisations are capable of predicting cyber threats and effectively responding to cyber incidences and fast recovery in the event of disruption due to cyber-attack. To develop digital resilience, it is necessary to integrate technological protection and risk management strategies in an organisation as well as employee awareness programs. To ensure the security and sustainability of business environments, entrepreneurial organisations need to incorporate cybersecurity concerns into their digital transformation strategies. This involves the enactment of strong cybersecurity policies, investing in secured digital infrastructures as well as a culture of cybersecurity awareness within employees. The increasing importance of digital resilience in a certain way will allow the entrepreneurial ecosystems to become innovative and develop further in the digital worlds that become more and more complicated.

9.4 Strengthening Cyber Governance Frameworks

Cyber governance systems are supposed to be adopted to address the dynamic nature of cybercrime and cybersecurity. The concept of cyber governance can be described as the integration of policies and regulatory frameworks, organisational structures and coalitions that shape how the organisations and governments manage cyber risks. The presence of various digital technologies in the process of their continuous evolution necessitates alterations in cyber governance structures to respond to the emerging forms of cybercrime and threats to the technologies. The future strategies of cyber governance should focus on improving the linking of governments, the organisations of the private sector and the international organisations. In many cases, the participants of cybercrime may be situated in two or more jurisdictions and this necessitates cooperation between various nations to effectively cut the cases and prosecute them. Governments are therefore supposed to develop regulatory mechanisms that will assist in sharing of information, collaborating on investigations and responding to cyber threats. In addition, the value of cybersecurity education, human capacity development, and institutional capacity development are expected to be brought out in cyber governance structures. The most important aspect of addressing the rising rate of cyber threats is training a skilled cyber security workforce and to ensure that the organisations have the knowledge necessary to handle the digital security threats. Institutions of academia, industry, and government are also supposed to be urged to cooperate to promote research and innovation in the cybersecurity with the input of policymakers. Overall, the future of cybercrime investigation and digital security will be stipulated by the implementation of hi-tech technologies, strong organisational culture, and appropriate governance systems. By finding a new way to the future that deals with technological progress through robust regulating structures, organisations and governments would be in a position to improve their ability to prevent cybercrime and protect digital ecosystems against emerging threats.

10. CONCLUSION

The fast development of digital technologies has dramatically changed the contemporary business landscape and exposed it to cyber-attacks at the same time. With the rise in organisations depending on digital infrastructures, cybercrime has become a significant issue to digital economies, entrepreneurial ecosystems, and small and medium-sized enterprises. The presented review shows that all types of cybercrime like phishing, ransomware attacks, crimes involving cryptocurrency, and digital fraud are constantly developing along with the development of technologies and thus cybercrime investigation is gaining significant importance as a part of digital security. The paper shows that digital forensic methodologies, artificial intelligence, blockchain analytics, and open-source intelligence are gaining relevance as the tools that can be used to identify and investigate cybercrime activities. These technologies facilitate the capability of investigators to analyse digital evidence, track cybercriminal networks, and react well to developing cyber threats. Nevertheless, the investigation of cybercrimes is facing serious challenges such as cross-border jurisdictional issues, technological unidentification, legal constraints to deal with digital evidence, and a lack of cybersecurity facilities in developing economies. The implications of the broader findings of cybercrime on sustainable entrepreneurship and digital economic development are also highlighted. Such cases of cybercrime have the potential to interfere with the business processes, affect consumer confidence, and suppress innovation in digital entrepreneurial ecosystems. Thus, cybersecurity governance enhancement, enhanced digital literacy, and government, business, and cybersecurity institution collaboration are the key elements to improving cyber resilience. Future plans must be aimed at ensuring that there is an amalgamation of superior investigative technologies and reliable regulatory systems as well as capacity building programs. These co-ordinated efforts will be essential in ensuring security of digital infrastructures and making digital economies sustainable in the long-term in a more interconnected world.

REFERENCES

1. Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. *arXiv preprint arXiv:2309.17186*.
2. Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19*(2), 134-153.
3. Awan, M., Alam, A., & Kamran, M. (2025). Cybersecurity challenges in small and medium enterprises: A scoping review. *Journal of Cyber Security and Risk*, *2025*(3), 89-102.
4. Arifin, M. S. M., Radzi, S. M., Nawi, N. A. M. M., Rosman, M. R. M., & Alimin, N. A. (2025). Cybersecurity Threats among SMEs in Malaysia: Risks and Challenges. *Journal of Information and Knowledge Management*, *15*(SI1).
5. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.
6. Perozzo, H., Zaghloul, F., & Ravarini, A. (2022). CyberSecurity readiness: a model for SMEs based on the socio-technical perspective. *Complex Systems Informatics and Modeling Quarterly*, (33), 53-66.
7. Ullah, M. S., Ahsan, M., & Yaqub, N. (2025). AI-Enabled Cybersecurity for Small and Medium-Sized Enterprises (SMEs): A Systematic Review and Evidence-Informed Assessment Framework. *Journal of Computing & Biomedical Informatics*.
8. AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, *12*(17), 3629.
9. Chang, Y., Heller, O., Shlomo, Y., Bar-Noy, I., Bokobza, E., Grinstein-Weiss, M., & Zhang, N. (2025). Mind the gap: Revealing security barriers through situational awareness of small and medium business key decision-makers. *arXiv preprint arXiv:2506.10025*.
10. Jasiak, J., MacKenzie, P., & Tuvaandorj, P. (2025). Digital Adoption and Cyber Security: An Analysis of Canadian Businesses. *arXiv preprint arXiv:2504.12413*.
11. Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410.
12. Thakur, R., Kumar, S., Singh, S. K., Singla, K., Sharma, S. K., & Arya, V. (2024). Cyber Synergy: Unlocking the Potential Use of Biometric Systems and Multimedia Forensics in Cybercrime Investigations. In *Digital Forensics and Cyber Crime Investigation* (pp. 241-267). CRC Press.
13. Ţurcan, R., Ţurcan, I., & Stratila, A. (2022). The impact of digitalization on the development of entrepreneurial performance in the context of globalization. In *European integration through the strengthening of education, research, innovations in Eastern Partnership Countries* (pp. 165-171).
14. Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. *International journal of information management*, *63*, 102466.
15. Nambisan, S., Wright, M., & Feldman, M. (2019). The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Research policy*, *48*(8), 103773.
16. Sussan, F., & Acs, Z. J. (2017). The digital entrepreneurial ecosystem. *Small business economics*, *49*(1), 55-73.
17. Onwuadiamu, G. (2025). Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136.
18. Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*(3), 313-338.
19. Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, K. H. (2013). Organizations and cybercrime.
20. Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1), tyz003.
21. Europol, E. C. C. (2014). Internet organised crime threat assessment (IOCTA). *The Hague, Lyon*, 45-67.
22. Song, A. K. (2019). The digital entrepreneurial ecosystem—a critique and reconfiguration. *Small Business Economics*, *53*(3), 569-590.
23. Hardinanto, A., Arief, B. N., & Setiyono, J. (2023). The Significance of Computer Forensics in Electronic Documents as Evidence in Criminal Law. *Jurnal Cakrawala Hukum*, *14*(2), 155-166.
24. Magalhães-Timotio, J. G., Barbosa, F. V., & Ferreira, B. P. (2022). Constructing a composite financial inclusion index for Brazil. *Revista Gestão & Tecnologia*, *22*(1), 168-192.

25. Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. *Artificial Intelligence Review*, *56*(11), 12407-12438.
26. Zainudin, N. M., Hasbullah, N. A., Wook, M., Ramli, S., & Razali, N. A. M. (2024). Digital Forensic Readiness in Cybersecurity: A Review of the Literature and Identification of Knowledge Gaps. *Zulfaqar Journal of Defence Science, Engineering & Technology*, *7*(1).
27. ALkharabsheh, M. M., Alshraideh, M., & Salah, I. (2024). Enhancing Cybercrime Deterrence with Artificial Intelligence. *International Journal of Advanced Networking and Applications*, *15*(4), 6015-6027.
28. Odejayi, R. O. (2023). *Cyber Security Management: The Security Implications of the Digital Economy Across Sub-Saharan Africa Countries* (Doctoral dissertation, Mykolo Romerio universitetas.).
29. Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205-217.
30. Broadhurst, R., & Chang, L. Y. (2012). Cybercrime in Asia: trends and challenges. *Handbook of Asian criminology*, 49-63.
31. Lee, J. R., Ayerza, J. M., Lee, W. G., Jadidi, V., & Holt, T. J. (2025). 11. Cybercrime: Offending and Victimization during the COVID-19 Pandemic. *Crime, Corrections, and the COVID-19 Pandemic: Responses and Adaptations in the US Criminal Justice System*, 211.
32. Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series*, *33*, 2020-01.
33. Do, T. H., & Selvadurai, N. (2025). Future Crime: A Theoretical Foundation for Designing Effective Cybercrime Laws in the Age of AI and Ransomware. *NCJL & Tech.*, *27*, 91.
34. Kyslenko, D., Kyslyi, A., & Tymoshenko, Y. (2024). The Effect of Regulatory Requirements on Digital Evidence Handling in Cybercrime Investigations. *Review of Law and Social Sciences*, *2*(1), 9-22.
35. Shami, A. Z. A., Saleem, M., & Ashraf, J. (2025). Cybercrime and Digital Evidence: Investigating the Challenges and Opportunities in Prosecuting Cybercrime and Handling Digital Evidence. *Research Consortium Archive*, *3*(2), 401-411.
36. Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*(1), 1-8.
37. Satpathy, S., Mallick, C., & Pradhan, S. K. (2018). Big data computing application in digital forensics investigation and cyber security. *International Journal of Computer Science and Mobile Applications*, 129-136.
38. Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia computer science*, *192*, 20-28.
39. Nicolau, C., Nichifor, E., Munteanu, D., & Bărbulescu, O. (2022). Decoding business potential for digital sustainable entrepreneurship: what Romanian entrepreneurs think and do for the future. *Sustainability*, *14*(20), 13636.
40. Troise, C., Corvello, V., Ghobadian, A., & O'Regan, N. (2022). How can SMEs successfully navigate VUCA environment: The role of agility in the digital transformation era. *Technological Forecasting and Social Change*, *174*, 121227.
41. Arshi, A. S., Islam, S., Tamanna, A. Y., Sultana, S., & Ikram, S. B. (2024). Fintech for Sustainability in Business and Economics Research: Trends and Future Agendas. *Business Perspective Review*, *6*(1), 34-53.
42. Möller, D. P. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 231-271). Cham: Springer Nature Switzerland.
43. Spanou, D. (2024). The EU Cybersecurity Skills Academy: A silver bullet to address the cyber security skills gap in the European Union?. *Cyber Security: A Peer-Reviewed Journal*, *7*(3), 229-236.
44. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.
45. Bada, A., Sasse, M. A., & Nurse, J. R. (2015). Cybersecurity awareness campaigns: Why do they fail. *Journal of Cyber Policy*, *1*(2), 157-179.