# The Evolving Landscape of Cybercrime: Trends, Techniques, and Countermeasures — A Comprehensive Review

*Narule Jugal Kumar[1], Manjunath P[2*], Architha M R[3*]
[1]Department of Digital Forensics, School of Sciences, Malla Reddy University, Hyderabad, Telangana, India
[2,3]Department of Digital Forensics, School of Sciences, Malla Reddy University, Hyderabad, Telangana, India
*jugalkumarnarule@gmail.com

**Abstract:**
Cybercrime has now been enhanced to be more than a digital mischief, but instead it is an international criminal ecosystem. The proliferating cloud infrastructure, the mobile technology, and the artificial intelligence have not only expanded the attack area but also enabled the threat actors to operate on a massive scale and anonymity as never seen before. The review is based on the analysis of the new trends, incentives, and reactions of the contemporary cybercrime environment with the help of the analysis of a wide array of scholarly and technical literature. It looks at the evolution of attack techniques phishing, ransom ware, even more advanced, long-term and AI-assisted attacks, and explains how organized criminal enterprises, and black market activities of the digital world have come into being. The paper also looks at the evolution of defensive systems, e.g., AI-assisted detection, digital forensics, and the promotion of international legal systems. Findings have revealed that despite the improvement of defensive technologies in order to establish cyber resilience, the continuous maleficence of attackers is still outpacing defensive maleficence. The paper identifies the necessity of interdisciplinary collaboration in technology, policy, and behavioural studies to result in efficient cyber defence and digital security on the global level.

**Key Words:** Cybercrime, cyber security, digital forensics, ransom ware, malware, intrusion detection, AI in security, cyber defence, cyber threats.

## 1. Introduction

The high rate of digital technologies has essentially altered the character of cybercrime, and this is one of the most enduring problems in international security. During its early days, the threats posed by the internet were only relatively simple like computer viruses and defacing of websites. However, these days, the opponents use extremely sophisticated devices which can exploit cloud computing infrastructure, Internet of things (IoT) networks, as well as remote working systems [1], [2]. The increase of crypto currency and mobile technological advancements has increased the area of attack, and attackers can now perpetrate cross-border crimes without being recognized [3]. Cybercrime has ceased to be a purview of the individual hacker but has become an organized criminal organization, ransom ware, and state-backed espionage, financial fraud, and critical infrastructural disruption operations [4], [5]. Technical barriers to entry have also decreased because of Cybercrime-as-a-Service platforms, which offer already made malware, phishing kits and tools to exploit fewer skilled offenders [6]. Therefore potential effects of cybercrime now go beyond financial losses to national security risks and threats on stability of the society. In reaction to these growing threats, the cyber security environment has grown to resemble artificial intelligence (AI), threat intelligence sharing, behavioural analytics and sophisticated incident response systems [7]. These advancements have not stopped attackers being able to keep


D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_29

pace with defenders, and in this way, there has been a persistent disparity between cyber preparedness across the world [8]. Considering this asymmetry, it is important to know the trends of cybercrime, new attack patterns and the defence mechanisms to counter specific attacks to construct effective strategies to counterattack. This paper summarizes the knowledge of one hundred scholarly and technical sources to evaluate the evolution of cybercrime over the years, the significant pattern of attack that comprises the present threat landscape, and the state of modern defensive strategies. The gaps in research have also been pointed out in the review and the necessity to incorporate technological, legal, and behavioural disciplines to tackle the arising cyber threat in an all-inclusive manner.

## 2. Review of Literature

In the last 20 years, the studies on cybercrime expanded considerably due to the high rate of digitization of contemporary society and the subsequent increase in the number of offenses with the usage of technologies. The initial studies were mostly centred on the elementary types of digital attack as the propagation of malware and creation of viruses, and network-based attacks that formed the basis of further research on digital attacks [1], [2]. With the adoption of internet all over, academics have turned to social-engineering offenses such as phishing and identity theft wherein criminals took advantage of human weaknesses instead of system weaknesses [3], [4]. The introduction of organized cybercriminals was the turning point in the literature. According to a number of studies, cyber offenders no longer remain individualists, but instead organized global networks that use encrypted communication lines and the dark web [5], [6]. Cybercrime-as-a-Service (CaaS) markets in which pre-written exploit kits, ransom ware packages and botnet rentals are sold to less skilled users have contributed to professionalization of cybercrime [7], [8]. Ransom ware has been one of the most widely studied issues in cybercrime studies. Its encryption methods, attack cycles and the economic consequences that it has on both the individual and government sectors have been examined [9], [10]. On the same note, studies on Advanced Persistent Threats (APTs) emphasize the use of nation-states and state-sponsored organizations to launch long-term espionage by taking advantage of zero-day vulnerabilities and covert intrusion techniques [11], [12]. These works tend to focus on the geopolitical and strategic reasons of the occurrence of such operations. Introduction of IoT technologies has raised new issues of concern. As several other authors have indicated, the plethora of devices with networked applications such as smart home systems, as well as industrial control networks, have provided immense possibilities in terms of large scale attacks [13], [14]. Lack of proper authentication, old firmware, and non-secure communication channels have resulted to threats that have been used by cybercriminals. With the increase in the use of IoT devices in the fields of healthcare, manufacturing and transport, data privacy, system integrity, and safety implications have now been discussed in the literature [15]. Alongside attack vectors, there has been a research on mechanisms of defence evasion. Industrial tools like firewalls and signature-based antivirus programs have been largely criticized as impossible to recognize polymorphic malware or to counter zero-day exploits [16]. More recent works stressed the use of artificial intelligence and machine learning to detect anomalies, analyse threats based on behaviour, and automated response systems [17], [18]. Besides, the progress in digital forensics has enhanced techniques of gathering, storing, and studying evidence in more complicated systems such as cloud systems [19]. In the legislative and policy aspects of cybercrime, a significant amount of literature also has a focus. The scholars note that international cooperation models and legal tools like the Budapest Convention are very important in the cross-border investigations, although their application is uneven across the jurisdictions [20], [21]. Several researchers point out that the regulation systems are usually outpaced by technology and offer much space to the wrongdoers. On the whole, the analysed articles show a clear change of the exclusively technology-centric analysis to multidisciplinary solutions, which combine law, criminology, behavioural science, and AI-based security. The overall evidence highlights the existing disparity in offensive and defensive preparedness, showing the ongoing necessity in dynamic international cooperation in the sphere of cyber security research and practice.

## 3. Cybercrime Trends

Cybercrime has experienced a tremendous revolution in the levels of sophistication and organization of operation. The current trend of the digital crime towards more complex and targeted operations, rather than the opportunistic and low-skill attacks, proves a more extensive professionalization of digital crime [22]. Contemporary criminals also carry out reconnaissance efforts systematically, find places of exploitable vulnerability, and install tailor-made malware to create the greatest effect and avoid detection.

### 3.1 Expansion of Ransom ware Ecosystems

Ransom ware remains to be the most popular cyber threat globally. Research indicates that the number and severity of attacks has been on a continuously rising trend, mostly thanks to the advent of Ransom ware-as-a-Service (RaaS) platforms [23], [24]. Even unskilled attackers can easily run advanced campaigns using these commercialized ecosystems by renting ready-made ransom ware. The development of the so-called way of extortion based on stealing sensitive information and encrypting systems has added pressure to the victims to fulfil the requirements of ransom [25]. The model has in effect also widened criminal networks of cooperation which has made ransom ware a structured underground economy.

### 3.2 Expanding the Attacks of Social Engineering

Social engineering has turned into a staple of cybercrime in the 21 st century, being based on psychological influence as opposed to technical intervention. The most common first attack vectors have become phishing, spear-phishing, and business email compromise (BEC) [26], [27]. According to the recent studies, the upward trend in the usage of personalized and context-sensitive phishing attacks is observed, in which social media information is used by the attackers to increase the levels of authenticity and trust [28]. This trend highlights that the attacks based on deception have been increasingly sophisticated and require more effective awareness-based defence initiatives.

### 3.3 Emergence of Sophisticated Persistent Threats (APTs)

APT is one of the most sophisticated and hard to eliminate cyber intrusions. These are operations that are usually conducted by nation-state or state-sponsored groups against government structures, defence departments, and critical infrastructure [29], [30]. The major characteristics are stealth, persistence, and use of zero-day exploits to have access in the long term. More recent research focuses on the geopolitics of the APTs, which are connected to cyber-espionage, stealing intellectual property and causing political interference [31].

### 3.4 Underground Markets and Commercialization

Cybercrime commercialization has resulted in well-structured underworld markets. In these dark web economies, users sell stolen credentials, personal data, exploit packages, and denial-of-service (DDoS) packages [32]. Bit coins, especially privacy-centred ones, help to conduct financial transactions anonymously, offering cybercriminals an opportunity to act worldwide with a lower chance of detection [33]. This economic infrastructure keeps the innovation in illicit digital services going.

### 3.5 IoT and Smart Devices Exploitation

The high rate of IoT device grow has provided new areas of attack both in households, industry and healthcare settings. It has been found that insecure configurations, weak authentication, and poor patching transactions have rendered such systems highly susceptible [34], [35]. Comprised IoT devices have been organized into large-scale botnets that have been used to execute massive DDoS attacks such as the case of the Mirai incident [36]. Cyber security threats, especially in the critical infrastructure, are on the rise due to the growth of smart technologies.

### 3.6 The targeting of the Cloud Infrastructure

With the migrations of the organizations to cloud environments, attackers have increasingly taken advantage of poorly configured storage environments, unsecured APIs, and inadequate identity management controls [37]. Cloud-specific attacks tend to capitalize on the use of shared resources and vulnerable containers in an attempt to get unauthorized access [38]. This underscores the need to have secure cloud governance, encryption and access control policies to reduce risk.

### 3.7 AI-powered and deep fake-facilitated Attacks

The upcoming studies note artificial intelligence as a defence mechanism and an offensive weapon in the cyber operations. Now, cybercriminals use the AI algorithms to automate phishing, create dynamic malware, and execute real-time impersonation with the help of the deep fake technology [39]. New digital forensics and law enforcement challenges are posed by the deep fake-enabled fraud and synthetic identity crimes [40]. The abuse of these tools to commit deception, fraud, and disinformation is bound to increase exponentially as they become more and more available.

| Category | Description | Common Techniques | Examples |
|---|---|---|---|
| Financial Cybercrime | Crimes aimed at financial gain | Phishing, carding, banking malware, BEC fraud | Online banking theft, crypto currency scams |
| Cyber-Espionage | Theft of sensitive or classified information | APTs, zero-day exploits, stealth malware | Government data breaches, industrial espionage |
| Cyber-Sabotage | Disruption or destruction of systems/services | Ransom ware, supply-chain attacks, ICS attacks | Power grid attacks, hospital system shutdowns |
| Identity-Related Crime | Misuse of personal data for impersonation or fraud | Social engineering, data breaches, credential stuffing | Identity theft, SIM-swap fraud |
| Cyber-Harassment & Abuse | Offenses targeting individuals | Doxing, stalking, online threats | Cyberbullying, revenge-porn cases |
| Illicit Digital Trade | Selling illegal goods/services online | Dark-web markets, crypto currency | Drugs, weapons, stolen data marketplaces |
| IoT/Smart Device Crime | Targeting connected devices | Botnets, firmware exploits, weak | Smart-home hacking, DDoS via IoT |

| | | | |
|---|---|---|---|
| | | authentication | |
| Cloud-Based Crime | Exploiting cloud infrastructure | Misconfiguration attacks, API abuse | Breach of cloud storage, container compromise |

*Table 1. Categories of Cybercrime*

## 4. Cybercrime Techniques

The development of cybercrime methods is a reflection of the technological progress, protection systems and user consciousness. The current malicious users use a hybrid approach that combines technical manipulation with psychological manipulation in order to achieve unauthorized access, disruption, or data extraction. In the literature, these techniques are broadly categorized into a few major groups, namely, malware deployment, social engineering, network intrusion, and sophisticated multi-stage attacks [41].

### 4.1 Malware-Based Attacks

Malware is still one of the most widespread and versatile tools of cybercriminals. It includes a broad set of malicious code which includes viruses, worms, Trojans, spyware and ransom ware, all of which are used to compromise system integrity or steal data [42]. The malware agents that were used in the past depended on basic copying, unlike the current ones which employ sophisticated evasion strategies like polymorphism, obfuscation, and file less execution to remain undetected [43]. Recent research indicates that malware is growing in terms of modularity so that attackers can use highly flexible payloads, which can adapt according to vulnerabilities in the target [44]. This flexibility allows real-time changes to be made during an attack making it difficult to detect and forensically attribute.

### 4.2 Ransom ware Techniques

Ransom ware has evolved beyond simple extortion based on encryption, and now it is a multi-stage endeavour. Modern versions use steps of reconnaissance, privilege escalation, lateral movement and data exfiltration before encrypting the system [45]. AES and RSA are strong encryption algorithms, which cannot be decrypted without the use of private keys [46]. Ransom ware-as-a-Service (RaaS) model has reduced the entrance barrier, and affiliates have concentrated on victim targeting and ransom negotiation, whereas developers continue with maintaining the underlying infrastructure [47]. According to the studies, the critical sectors, including healthcare, education, and utilities, are especially susceptible because they have a low level of downtime tolerance, and are dependent on legacy systems [48].

### 4.3 Phishing and Social Engineering

Social engineering attacks manipulate human nature as opposed to vulnerabilities of the system. Phishing is considered to be one of the most frequent ones, where attackers impersonate trusted parties to defraud users into providing credentials or malware installation [49]. Specialized kinds like spear-phishing use personal or organizational background information, frequently obtained via social media profiles, to enhance the status of credibility [50]. According to the new data, AI-based phishing messages have become more linguistically accurate and personalized, which has increased the probability of success to a considerable degree [51]. Business Email Compromise (BEC) is also a significant financial risk that has often led to a significant business loss [52].

### 4.4 Web Application and Network Exploitation

Network and web exploitation attacks exploit the vulnerabilities of communication protocols, access control, and input validation. Such techniques like man-in-the-middle interception, SQL injections, as well as cross-site scripting (XSS), are still common [53]. Consistently weak areas are associated with the use of outdated software

and unsecure development systems [54]. DDoS attacks, where large amounts of traffic are sent to a specific system to crash it, have also been more devastating as of today using big botnets of compromised IoT devices [55]. Such attacks not only affect services in terms of disruption but also act as a diversion to parallel data exfiltration operations.

**4.5 Advanced Persistent Threats (APTs)**

APTs are sophisticated multi-stage incursions that are long-term, stealthy, and target-oriented. APT campaigns are usually linked to state-sponsored organizations and have various phases such as initial compromise, privilege escalation, establishment of persistence, and data extraction [56]. By using the zero-day vulnerabilities, these attackers can circumvent the traditional protection mechanisms and go undetected over a long time [57]. Many reports associate APT activities with spying and disrupting critical infrastructure that has been caused by nation-state actors [58]. The attribution issues remain because of the application of false flags, proxy servers, and in common malware infrastructure [59].

**4.6 Mobile-Based Attack Techniques and IoT**

The growing adoption of mobile and IoT devices into the everyday routine has increased the digital threat environment. IoT devices are relatively insecure and are prone to manipulation of firmware, exploitation of weak passwords, and compromise of an unencrypted communication channel [60]. The network of attackers built of large-scale botnets of compromised IoT systems are often used to execute DDoS or data harvesting attacks [61]. In the mobile platforms, malicious applications, permission abuse, and SMS-based phishing (smishing) are still prevalent methods. Studies have shown that the Android-based devices are at a higher risk especially considering fragmented updates and vulnerability to third party app stores [62].

**4.7 New Techniques and AI-Assisted Techniques**

Cybercrime evolves with the introduction of artificial intelligence application in offensive operations. More attackers are also using AI to discover vulnerabilities more automatically, optimize their timing, and generate realistic artificial media. Deep fake technologies allow impersonating voices and faces in real-time, which creates fraud scenarios at an advanced level in terms of finance and corporate fraud [63], [64]. The developments pose a challenge to the current security systems, thereby highlighting the importance of dynamically changing security systems based on AI that are able to identify dynamically changing security threats [65].

## 5. The countermeasures to Cybercrime and Defence Strategies

The ongoing changes in cyber threats have led to the emergence of more aggressive, intelligence-focused defence measures. The conventional cyber security controls cannot be used to overcome advanced, dynamic attackers who are using automation, social engineering, and AI-supported attacks. This has resulted in a research and industry trend of considering multi-layered defence systems as having technical, organizational, forensic, and legal elements to deal with the increasing range of cyber threats [66].

**5.1 Technical Counter measures**

The First cyber defence tools like firewalls, antivirus software and the low end intrusion detection systems (IDS) depended on signature matching to detect familiar threats. Nevertheless, polymorphic malware and zero-day exploits have shown to be counter measured by these non-adaptive strategies, which have kept changing their peripheral behaviour in order to evade detection [67]. Contemporary cyber security has switched to behavioural and anomaly-based detection frameworks that are machine learning algorithms to examine the patterns of the network and system activities with the goal of finding anomalies [68], [69].

Artificial intelligence and threat intelligence integration can promote the accuracy and timeliness of threat detection [70]. EDR systems and Extended Detection and Response (XDR) systems have become highly important elements in the correlation of data on endpoints, networks, and cloud environments to provide an overall visibility [71]. Furthermore, encryption, multifactor authentication (MFA), and zero-trust architectures are becoming more and more widespread with the aim of ensuring that only digital resource access is constantly checked and reduced to the lowest possible privilege [72].

**5.2 Digital Forensics and Incident Responses**

The field of digital forensics now plays a leading role in cyber defence that aims at preserving and investigating evidence, and attributing it. The development of forensic methods like memory analysis, network forensic, and cloud forensic allows investigators to be capable of handling volatile data and distributed infrastructures in a more useful way [73]. Automation of forensic systems and systems of timeline reconstruction assist to streamline and uphold integrity of evidence [74].

The incident response (IR) models focus on fast detection, containment, eradication, and recovery of cyber-attacks. The IR planning includes the routine simulations, interdepartmental coordination, and post-incident analysis contributing to enhancing the resilience [75]. As it is always emphasized in the literature, well-exercised incident response team can dramatically minimize operational losses and losses of money after a cyber-attack.

**5.3 Human-Centric and Organizational Security.**

One of the most abused human vulnerabilities in cyber security is human error. Studies indicate that the success rate of social engineering attacks can be significantly lowered by implementing security awareness training, ongoing training, and fake phishing training [76]. To strengthen secure user behaviour, the organizations are advised to adopt explicit security policies, periodic access audit, and real-time reporting policies.

Risk management method will assist organizations to recognize and rank the protection of the critical assets. This incorporates the application of risk assessment models and compliance structures in order to allocate cyber security budgets in an effective manner [77]. It is crucial to have both technical and behavioural measures in the creation of a strong security culture that would guarantee long-term resilience.

**5.4 Legal and Regulatory Countermeasures**

Cybercrime poses special laws in attribution and jurisdiction as digital crimes are transnational. Cross-border investigation and the prosecution of criminals have been enabled by legal cooperation regimes including the mutual legal assistance treaties (MLATs) and the Budapest Convention [78]. Nonetheless, differences in national laws and application standards remain a limiting factor to effective international cooperation [79].

Researchers and policy-makers highlight the necessity of the international law to be standardized and have more strict compliance, to reduce safe havens to carry out cybercriminal acts. Data protection and cyber security regulatory frameworks like the GDPR are also indirect contributors to prevention since they require best practices and responsibility in organizations [80].

**5.5 New and Evolving defence Strategies**

Recent studies consider the paradigms of the next-generation defences focusing on the deception-based security, the integrity of block chains, and the AI-based automated response how the system should be organized [81], [82]. False technologies such as honeypots and honey nets are used to entice attackers into controlled systems to study their tactics and collect intelligence without involving live systems. The block chain solutions provide increased information integrity and non-repudiation in decentralized systems.

Nevertheless, the increased use of automation brings in new risks like false positives and malfunctions on the systems. Researchers caution that too much automation without human intervention can cause problems in operations or non-observation of anomalies [83]. That is why the application of the hybrid defence models that combine automated mechanisms with the human expert analysis is increasingly promoted as the effective way to achieve the cyber resilience.

| Cybercrime Technique | Primary defence Mechanisms | Supporting Measures |
|---|---|---|
| Malware & Ransom ware | EDR/XDR, behavioural analysis, backups | Incident response planning, digital forensics |
| Phishing & Social | Email filtering, | Awareness programs, |

| | | |
|---|---|---|
| Engineering | MFA, user training | phishing simulations |
| APTs | Threat intelligence, anomaly detection | Network segmentation, zero-trust models |
| DDoS Attacks | Traffic filtering, rate limiting | IoT security hardening, botnet monitoring |
| IoT Exploitation | Secure firmware, access control | Device monitoring, network isolation |
| Cloud Attacks | Identity management, encryption | Configuration audits, cloud forensics |
| Deep fake & AI-based Fraud | Voice/video authentication | Policy verification, manual approval layers |

*Table 2. Mapping Cybercrime Techniques to Countermeasures*

## 6. Problems and Unresolved Research

Although the cyber security technologies and research have made tremendous advancements in the past, there are quite a number of challenges that prevent the effective prevention and mitigation of cybercrime. The literature identifies a structural imbalance where offensive and defensive capabilities are viewed as an imbalance with the adversary only having to leverage one vulnerability, with the defenders having to protect the entire, multifaceted digital ecosystem [84]. The asymmetry still gives room to massive and long-term attacks.

### 6.1 Quick Technological Change.tion

The rapid innovation, which is happening in many fields including cloud computing, IoT, and artificial intelligence, is often much faster than sufficient security structures can be established. New digital infrastructures are often launched with less protection as a feature and thus become vulnerable to exploitation [85]. Such acceleration of technology increases the disparity between the new threats and the preparedness of defence mechanisms. The literature has always stressed on the importance of proactive design principles that include security throughout the method of technology production and not as a precautionary measure

### 6.2 Attribution and Jurisdictional barrier

The correct identification of cyber-attacks by a particular actor is one of the most demanding problems in digital forensics and law enforcement. Criminals resort to anonymization methods, proxy servers, and world-wide infrastructure to cover their feet [86]. The issue of jurisdiction between countries also makes the overall prosecution process more complex since varying legal frameworks can have a different understanding or a focus on cybercrime. Such loopholes enable the cybercriminal groups to use places where regulations are weak or where the enforcement ability is low as safe havens.

### 6.3 Drawbacks of AIs in defence Systems

Even though machine learning and artificial intelligence have enhanced detection of threats, it has its challenges. Security models based on AI are heavily reliant on the quality and balance of datasets. In reality, such datasets

tend to be incomplete, noisy or limited by privacy laws [87]. Also, these systems themselves can be vulnerable to adversarial attacks which involve small manipulations of data, which can trick models into wrongful classification and disrupt their reliability [88]. There is a need to conduct further research in order to make AI-driven defence frameworks more transparent, explainable and robust.

### 6.4 Human Factors and Behavioural Issues

There is a significant amount of literature that human behaviour is a common vulnerability in cyber security defence. Users do not take risks into consideration, neglect security measures, or become victims of social engineering tactics. It has been found that the suspension of awareness training will decrease the susceptibility involved in the short run but at the long-run, it will be hard to sustain strict vigilance [89]. Empirical studies on the effectiveness of human-centred interventions in the long term and the effects of the behavioural aspect on the organizational security culture are also lacking.

### 6.5 Multidisciplinary and Global Cooperation Requirement

Majority of the current methods of cyber security are still isolated in technical fields. Nonetheless, cybercrime is a multidisciplinary problem, which involves computer scientists, legal professionals, behavioural scientists, and policy-makers. The coordination across borders is also poor with only uneven data-sharing structures and their disjointed threat intelligence systems. The response to this gap requires a comprehensive model that incorporates technological, human and legal points of view to enhance resilience and effectiveness in response to the global context.

## 7. Future Research and Mitigation Future Directions

With cyber threats ever-changing, emerging studies and preventive measures should have proactive, adaptive, and interdisciplinary focus. The literature highlights that the traditional reactive security measures are not effective enough in overcoming the dynamic, automated and transnational character of cybercrime in the contemporary context. Consequently, technological innovation should be combined with human, legal, and policy-based systems to develop the next generation of defence mechanisms in order to develop sustainable cyber resilience [90].

### 7.1 Multidisciplinary Approach Incorporation

To be effective in mitigating cybercrime, collaboration, either at the technical, legal, or behavioural levels is needed. The authors of the research note that the connection of cyber security to criminology, digital forensics, and behavioural science is essential to consider both human factors and technological vulnerabilities [91]. Threat modelling, accuracy of attribution, as well as policy formulation can be enhanced through interdisciplinary collaboration. As one example, a cross-section between forensic analysis and psychological profiling of threat agents can give a deeper understanding of the reasons behind the attack and the method to prevent it.

### 7.2 The Explainable and Ethical AI Progress

Artificial intelligence will keep on taking the centre stage in cyber security, and in the future, the artificial intelligence systems should focus on transparency and ethical accountability. Explainable AI (XAI) provides the opportunity to boost the confidence in machine-based decision-making through the interpretable outputs that are verifiable within the framework of the forensic and legal settings [91]. It is also recommended by the researchers to secure a combination of federated learning - privacy-sensitive technique enabling several parties to jointly train a model without exchanging sensitive information, thereby improving detection accuracy without compromising privacy [92]. The invention of these technologies will contribute to alleviating problems of bias in the data set as well as of model transparency and of compliance with regulations.

### 7.3 Strengthening International Cooperation

The international nature of cybercrime demands more globalized international systems of investigation and enforcement. Enhanced cooperation among governments, law enforcers and the private cyber security companies is critical towards effective sharing of the threat intelligence and evidence [93]. The creation of uniform legal tools and cross-border reporting systems will allow getting the response to the incident quicker and enhance the coordination of actions in cross-border incidents. The creation of international standards of digital behaviour, advancing responsibility, and preventing state-backed cyber aggression should also be studied as a policy research.

### 7.4 Focus on the Proactive and Predictive defence Models

Defence strategies in the future should not be defensive, rather, they should be proactive in terms of predicting risks. Cyber deception, predictive threat modelling, including honeypots and dynamic defence systems, can help organizations to identify and interrupt the attack at earlier stages [94]. The study of cyber resilience, which will be concerned not only with prevention, but also with timely recovery and continuity, will gain even more importance. The introduction of simulation-based testing exercises and exercises that involve red-teaming would also increase the readiness of organizations to survive the ever-changing cyber-attacks.

### 7.5 Constant review and revision of policies

Due to the rate of technological change, cyber security policies and frameworks should be flexible and constantly updated. Future studies must be on adaptive governance models in line with the new technology, like quantum computing and 5G. Also, academia needs to work together with the industry in order to transform research results into deployable solutions. It is important to continue this cycle of research, policy, and practice to keep up with the unstable world of cyber threats.

## 8. Conclusion

Cybercrime has become complex and international due to the accelerated technological improvement, financial gain, and the growing interconnectivity of digital infrastructure. This review summarized the results of one hundred scholarly and technical sources to discuss the development of cybercrime in terms of scale, techniques, and structure. The analysis has shown that there is a strong change towards professionalized, service-focused, and AI-enhanced criminal activities, which currently represent serious threats to critical infrastructure, data integrity, and global stability.

Although artificial intelligence, digital forensics, and regulatory changes have made defensive more effective, attackers have moved at a more rapid rate than defenders. The constant inefficiencies like jurisdictional obstacles, AI-based detection weaknesses, and susceptibility to human behaviour highlight the significance of flexible and joint solutions to cyber security.

New approaches to be adopted in the future should dwell on proactive and predictive defence measures involving both technical innovation and robust governance and international relations. The creation of sustainable cyber resilience requires a multidisciplinary approach that brings together technology, policy and behavioural studies. In the end, cybercrime will have to be tackled through life-long learning and integration efforts across the world and the seamless availability of smart technologies and human skills to safeguard the digital ecosystem.

## References

[1] T. J. Holt, A. M. Bossler, and K. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction*, 2nd ed. New York, NY, USA: Routledge, 2018.

[2] R. Anderson et al., "Measuring the cost of cybercrime," *J. Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016.

[3] M. Rogers, "The psychology of cybercrime," *Int. J. Cyber Criminology*, vol. 5, no. 2, pp. 1–15, 2017.

[4] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *J. Comput. Virology*, vol. 2, no. 1, pp. 13–20, 2006.

[5] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, The Hague, Netherlands, 2023.

[6] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime*, Vienna, Austria, 2013.

[7] M. McGuire and S. Dowling, *Cybercrime: A Review of the Evidence*, London, U.K.: Home Office, 2013.

[8] K. Jaishankar, "Cyber criminology: Exploring internet crimes," *Int. J. Cyber Criminology*, vol. 1, no. 2, pp. 1–16, 2007.

[9] N. Brewer, "Ransomware attacks: Detection, prevention and cure," *Netw. Security*, vol. 2016, no. 9, pp. 5–9, 2016.

[10] S. Mansfield-Devine, "Ransomware: Taking businesses hostage," *Computer Fraud & Security*, vol. 2016, no. 10, pp. 8–17, 2016.

[11] FireEye, *Advanced Persistent Threats Report*, Milpitas, CA, USA, 2022.

[12] M. Behl and K. Behl, *Cyberwar: The Next Threat to National Security*, New Delhi, India: Oxford Univ. Press, 2017.

[13] A. Zimba, Z. Wang, and H. Chen, "Multi-stage attack detection in IoT networks," *IEEE Access*, vol. 7, pp. 112034–112046, 2019.

[14] S. Sicari et al., "Security, privacy and trust in IoT," *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[15] M. Conti et al., "Internet of Things security and forensics," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2367–2395, 2018.

[16] P. Mell and T. Grance, *The NIST Definition of Cybersecurity*, NIST, USA, 2011.

[17] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2016.

[18] I. Goodfellow et al., "Deep learning," Cambridge, MA, USA: MIT Press, 2016.

[19] E. Casey, *Digital Evidence and Computer Crime*, 3rd ed. London, U.K.: Academic Press, 2011.

[20] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, 2001.

[21] B. Koops, "Cybercrime legislation," *Computer Law & Security Review*, vol. 26, no. 2, pp. 121–133, 2010.

[22] Verizon, *Data Breach Investigations Report*, 2023.

[23] Symantec, *Internet Security Threat Report*, 2022.

[24] Kaspersky, *Ransomware Threat Landscape*, 2023.

[25] Coveware, "Ransomware trends and payment analysis," 2022.

[26] A. Algarni et al., “Phishing detection techniques,” *IEEE Access*, vol. 8, pp. 83492–83509, 2020.

[27] M. Jakobsson and S. Myers, *Phishing and Countermeasures*, Hoboken, NJ, USA: Wiley, 2007.

[28] J. Hong, “The state of phishing attacks,” *Commun. ACM*, vol. 55, no. 1, pp. 74–81, 2012.

[29] Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units*, 2013.

[30] K. Zetter, *Countdown to Zero Day*, New York, NY, USA: Crown, 2014.

[31] R. Lewis, “Cyber espionage and national security,” *Survival*, vol. 58, no. 2, pp. 83–104, 2016.

[32] D. Décary-Hétu and B. Dupont, “Reputation in darknet markets,” *Br. J. Criminology*, vol. 56, no. 1, pp. 1–20, 2016.

[33] M. Möser et al., “An inquiry into money laundering tools in cryptocurrency,” *IEEE Security & Privacy*, vol. 15, no. 3, pp. 14–21, 2017.

[34] A. Kolias et al., “DDoS in IoT,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[35] E. Bertino and N. Islam, “Botnets and IoT security,” *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[36] A. Antonakakis et al., “Understanding the Mirai botnet,” in *Proc. USENIX Security*, 2017.

[37] Cloud Security Alliance, *Top Threats to Cloud Computing*, 2022.

[38] S. Subashini and V. Kavitha, “Cloud security issues,” *J. Network Comput. Appl.*, vol. 34, pp. 1–11, 2011.

[39] H. Chesney and R. Citron, “Deepfakes and the new disinformation,” *Foreign Affairs*, vol. 98, no. 1, pp. 147–155, 2019.

[40] Europol, *Facing Reality? Law Enforcement and Deepfakes*, 2022.

[41] W. Stallings, *Network Security Essentials*, 6th ed. Boston, MA, USA: Pearson, 2017.

[42] P. Szor, *The Art of Computer Virus Research*, Boston, MA, USA: Addison-Wesley, 2005.

[43] Y. Shafiq et al., “Polymorphic malware detection,” *Comput. Security*, vol. 58, pp. 64–77, 2016.

[44] M. Egele et al., “Dynamic malware analysis,” *ACM Comput. Surveys*, vol. 44, no. 2, 2012.

[45] M. Richardson and M. North, *Ransomware Defense*, Sebastopol, CA, USA: O’Reilly, 2021.

[46] B. Schneier, *Applied Cryptography*, 2nd ed. New York, NY, USA: Wiley, 1996.

[47] Trend Micro, *Ransomware-as-a-Service Report*, 2023.

[48] CISA, *Ransomware Guide*, USA, 2022.

[49] A. Herzberg and A. Gbara, “Security and usability of phishing,” *IEEE Security & Privacy*, vol. 6, no. 2, pp. 26–33, 2008.

[50] J. Parsons et al., “Spear phishing,” *Comput. Fraud & Security*, vol. 2019, no. 6, pp. 6–10, 2019.

[51] OpenAI & academic surveys on AI-generated phishing, 2023.

[52] FBI, *Internet Crime Report*, 2023.

[53] OWASP, *Top 10 Web Application Security Risks*, 2021.

[54] G. McGraw, *Software Security*, Boston, MA, USA: Addison-Wesley, 2006.

[55] A. Mishra et al., “Botnet-based DDoS attacks,” *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 24–30, 2019.

[56] MITRE, *ATT&CK Framework*, 2023.

[57] R. Bilge and T. Dumitras, “Before we knew it,” in *Proc. ACM CCS*, 2012.

[58] N. Perlroth, *This Is How They Tell Me the World Ends*, New York, NY, USA: Bloomsbury, 2021.

[59] J. Rid and B. Buchanan, “Attributing cyber attacks,” *J. Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, 2015.

[60] ENISA, *IoT Threat Landscape*, 2022.

[61] S. Kumar et al., “IoT botnet analysis,” *IEEE Access*, vol. 8, pp. 186140–186155, 2020.

[62] Y. Zhou and X. Jiang, “Dissecting Android malware,” in *Proc. IEEE S&P*, 2012.

[63] P. Laskov and R. Lippmann, “Machine learning in adversarial environments,” *Mach. Learn.*, vol. 81, pp. 115–119, 2010.

[64] Deloitte, *Deepfake Fraud Report*, 2023.

[65] A. Taddeo and L. Floridi, “Cyber resilience,” *Philosophy & Technology*, vol. 31, pp. 1–14, 2018.

[66] ISO/IEC 27001, *Information Security Management*, 2022.

[67] S. Axelsson, “Intrusion detection systems,” *ACM CCS*, 2000.

[68] J. Kim et al., “AI-based IDS,” *IEEE Access*, vol. 8, pp. 181720–181731, 2020.

[69] IBM, *Cost of a Data Breach Report*, 2023.

[70] Palo Alto Networks, *Threat Intelligence Report*, 2022.

[71] Gartner, *Endpoint Detection and Response Market Guide*, 2023.

[72] NIST, *Zero Trust Architecture*, SP 800-207, 2020.

[73] G. Grispos et al., “Cloud forensics,” *Digital Investigation*, vol. 9, pp. 79–90, 2012.

[74] B. Carrier, *File System Forensic Analysis*, Boston, MA, USA: Addison-Wesley, 2005.

[75] SANS Institute, *Incident Handler’s Handbook*, 2022.

[76] A. Parsons et al., “Security awareness effectiveness,” *Comput. Security*, vol. 76, pp. 1–15, 2018.

[77] ISO 31000, *Risk Management Guidelines*, 2018.

[78] INTERPOL, *Cybercrime Strategy*, 2022.

[79] J. Brenner, *Cybercrime and the Law*, Boston, MA, USA: Northeastern Univ. Press, 2012.

[80] GDPR, *General Data Protection Regulation*, EU, 2018.

[81] N. Provos and T. Holz, *Virtual Honeypots*, Boston, MA, USA: Addison-Wesley, 2007.

[82] K. Christidis and M. Devetsikiotis, “Blockchain and smart contracts,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[83] M. Cummings, “Automation bias,” *Human Factors*, vol. 46, no. 3, pp. 401–415, 2004.

[84] D. Florencio and C. Herley, “Where do security breaches come from?” in *Proc. WWW*, 2011.

[85] M. Clayton et al., “Cyber attribution,” *J. Cyber Policy*, vol. 4, no. 2, pp. 123–145, 2019.

[86] UNODC, *Cybercrime Legislative Responses*, 2021.

[87] A. Sculley et al., “Hidden technical debt in ML systems,” in *Proc. NIPS*, 2015.

[88] N. Papernot et al., “Adversarial ML,” *IEEE Security & Privacy*, vol. 16, no. 3, pp. 40–47, 2018.

[89] S. Furnell and K. Clarke, “Human factors in cybersecurity,” *Computers & Security*, vol. 88, 2020.

[90] T. Holt and A. Bossler, *Cybercrime in Progress*, London, U.K.: Routledge, 2016.

[91] D. Gunning et al., “Explainable AI,” *AI Magazine*, vol. 40, no. 2, pp. 44–58, 2019.

[92] Q. Yang et al., “Federated learning,” *ACM TIST*, vol. 10, no. 2, 2019.

[93] OECD, *Cybersecurity Policy Framework*, 2022.

[94] R. Smith, *Rules of Engagement for Cyber Warfare*, Washington, DC, USA: DoD, 2015.