iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84650

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

AI-Driven Cybercrime and Autonomous Malware: Technological Threats, Legal Challenges and the Need for a New Cybersecurity Framework

Ms, Basabi Pandey[1], Ms. Mansi Srivastava[2], Ms. Seema Choudhary[3], Mr. Davesh Rawat[4]
[1]*Assistant Professor, Innovative Institute of Law, Greater Noida*
[2]*Ph.D. Scholar, COER University, Roorkee*
[3]*Advocate, District and Sessions Court, Hapur*
[4]*Assistant Professor, SDGI Global University, Ghaziabad*

Abstract: ***Artificial intelligence (AI) is transforming the cyber threat landscape by enabling malware and cyber operations that are adaptive, autonomous and scalable in ways that traditional tools could not achieve. AI-driven cybercrime and autonomous malware can dynamically modify their behaviour, choose attack paths, and evade detection without continuous human supervision, thereby challenging existing technical defenses and legal frameworks that were designed around static code and human-controlled attacks. This paper argues that the convergence of AI and cybercrime requires a recalibration of international and domestic cybersecurity law, including clearer liability standards for AI-enabled offences, updated treaty frameworks, and the development of a risk-based, technology-neutral cybersecurity architecture capable of addressing autonomous threats.***

I. RESEARCH BACKGROUND

A. *Emergence of AI-Driven Cybercrime*

Security research and industry reports since 2024–2026 document a shift toward an "AI-driven" future of cybercrime, with confirmed cases of AI-orchestrated attacks, deepfake-enabled social engineering, and AI agents outperforming human penetration testers at discovering vulnerabilities. AI-powered malware is defined as malicious software that uses AI models or AI-assisted workflows to improve development, targeting, evasion, automation, or execution; in advanced forms, it relies on model inference during runtime to decide what to do next. Autonomous malware represents a subset of AI-driven threats, characterized by embedded AI models that allow the code to make independent decisions, adapt tactics in real time, and pursue high-level goals without direct human command-and-control.

B. *Conceptualizing Autonomous Malware*

Analyses of autonomous malware emphasize three core capabilities: context-aware decision-making, behavioral adaptation, and decentralized operation. Instead of following a predetermined script, autonomous malware treats the target environment as a dynamic space, testing multiple escalation paths and selecting those with the lowest detection probability, often leveraging reinforcement learning or AI-based code mutators. These systems can learn from failed attempts, modify persistence mechanisms, and alter behavioral patterns to evade signature-based and heuristic detection, posing a qualitatively different challenge compared with traditional malware.[7][8][9][11][^4]

C. *Legal and Policy Context*

International legal frameworks, such as the Budapest Convention on Cybercrime and emerging instruments like the United Nations Convention against Cybercrime (the "Hanoi Convention"), were negotiated before widespread deployment of AI-enabled cyber threats. Scholarship reviewing these instruments concludes that they criminalize core cyber-dependent offences (unauthorized access, data interference, system interference, computer-related fraud) and provide procedural tools for electronic evidence, but lack specific or robust provisions on AI governance or AI-enabled cyberattacks. Recent research on AI-enabled cyberterrorism and AI misuse in transnational crime likewise finds that existing international law is technology-neutral in principle but under-articulated in relation to AI, leading to gaps in attribution, jurisdiction, and specialized obligations for AI-specific threats. [2][12][13][14][15][16][^17]

D. Scope and Limitations of the Study

This paper focuses on AI-driven cybercrime and autonomous malware as distinct, though overlapping, phenomena: AI-driven cybercrime refers broadly to cyber offences enhanced or enabled by AI (including deepfakes, automated phishing, adaptive ransomware), while autonomous malware refers to malicious code with embedded AI capable of independent decision-making. The analysis is limited to criminal and regulatory aspects of cybersecurity law and does not offer detailed technical specifications of AI models or cryptographic protocols, though it draws on computer science literature to explain how AI is embedded into attack logic.

Geographically, the study places particular emphasis on international frameworks (Budapest Convention, UN Convention against Cybercrime) and selected domestic responses from Europe, the United States, China and other jurisdictions where criminal liability for AI-enabled crimes has been examined. Due to space and data constraints, the paper does not provide an exhaustive survey of national cybersecurity legislation, nor does it empirically measure attack prevalence; instead, it conducts doctrinal and policy analysis using representative case law and treaty documents.

Technologically, the paper assumes a moving frontier: as AI models, reinforcement-learning agents and autonomously propagating code evolve, specific examples may be overtaken by newer threats. The discussion therefore aims to identify structural legal and technical issues that remain relevant even as the underlying AI techniques change, such as attribution of responsibility, evidentiary standards, and design of technology-neutral yet AI-aware obligations.

E. Research Methodology

The study adopts a doctrinal, analytical and comparative legal methodology, combined with interdisciplinary engagement with cybersecurity and AI-technical literature. First, treaty texts and official explanatory materials of the Budapest Convention on Cybercrime and the United Nations Convention against Cybercrime are examined to identify how they define offences, evidence rules, and cooperation mechanisms applicable to AI-enabled cybercrime. Second, scholarly commentary and policy papers on AI and cybersecurity are analyzed to map perceived gaps, especially concerning autonomous malware, AI-driven cyberterrorism, and AI-enhanced transnational crime. Third, representative case law involving autonomous worms, botnets and automated cyberattacks—such as United States v. Morris, United States v. Ancheta, and United States v. Brovko—is reviewed to understand how courts attribute liability to human actors when malware or bots operate autonomously. Fourth, technical literature is consulted to characterize AI-driven malware architecture and its implications for detection and defense, including machine-learning-based attack strategies and autonomous behavior. Finally, building on these sources, the paper develops a normative proposal for a new cybersecurity framework that is AI-aware, focusing on risk-based obligations, explainability, secure development, accountability chains and enhanced international cooperation. The methodology is qualitative and normative, not empirical; it does not conduct statistical analysis of incidents but draws on documented cases and expert assessments to support its arguments.

II. TECHNOLOGICAL THREATS: AI-DRIVEN CYBERCRIME AND AUTONOMOUS MALWARE

A. AI Techniques in Cyber Offence

Machine learning and other AI techniques are now integrated across the malware life cycle, from reconnaissance and vulnerability discovery to exploitation, lateral movement and exfiltration. Reports describe AI agents that automate the generation of phishing content, perform real-time language adaptation for social engineering, and discover misconfigurations or zero-day vulnerabilities more efficiently than human operators. In autonomous malware, lightweight embedded models can evaluate local defenses, select stealthy persistence mechanisms, and alter code fragments using AI-generated mutators, thereby evading static and behavioral detection.[9][18][6][7][^8] AI also enables large-scale deepfake-driven fraud, where synthetic audio and video are used to impersonate executives or customers, combined with automated decision-making systems that route fraudulent transactions or change account credentials. AI-driven cyberterrorism, as analyzed in recent scholarship, includes the use of autonomous malware to compromise critical infrastructure, AI-enhanced surveillance and targeting tools, and AI-generated disinformation campaigns that can destabilize democratic processes.[13][16][12]6]

B. Characteristics of Autonomous Malware

Autonomous malware is distinguished from traditional malware by its ability to act as an AI agent pursuing a high-level objective, rather than a script executing pre-coded instructions. It typically possesses an onboard AI model that allows it to sense its environment, evaluate options, and choose actions such as whether to escalate privileges, pivot to new hosts, or lie dormant to avoid sandboxing. Some implementations use reinforcement learning, whereby the malware learns from successes and failures in exploitation, improving its strategies over time and across different networks.[4][7][8]9]

Comparative analyses show that autonomous malware is more adaptive, stealthy and resilient than traditional malware, as it can alter indicators of compromise, modify network behaviours, and coordinate in swarms without centralized command-and-control. This makes it less susceptible to signature-based detection and complicates attribution, because the precise behavior may differ significantly from instance to instance and evolve during an operation.[21][7][9][4]

C. AI-Driven Ransomware and Botnets

Recent cybersecurity reports warn that AI capabilities are maturing into fully autonomous ransomware pipelines that allow individual operators and small crews to target multiple victims simultaneously at unprecedented scale. AI can automate target selection based on profitability or vulnerability profiles, customize ransom notes, and dynamically adjust encryption and exfiltration strategies based on observed defenses. Botnets enhanced with AI may optimize resource usage, detect sinkholing attempts, and autonomously reconfigure to maintain resilience against takedown operations.[19][6][7][21]

Case law involving botnets and automated propagation—such as United States v. Ancheta and United States v. Brovko—illustrates that courts treat these semi-autonomous systems as instruments of human operators, emphasizing their orchestration, control and profit motives. However, as botnets become more autonomous, designing legal standards that capture the degrees of human involvement and foreseeability becomes increasingly complex, necessitating clearer doctrines on negligence, recklessness and strict liability.[5][3][19][21]

III. LEGAL CHALLENGES: ATTRIBUTION, LIABILITY AND JURISDICTION

A. Technology-Neutral Criminal Responsibility and AI

International criminal law and domestic criminal law generally reject the notion of AI systems bearing criminal responsibility and insist that crimes remain imputable to human actors such as programmers, developers, commanders and operators. Analyses of modes of liability for AI-enabled crimes show that existing frameworks—perpetration, instigation, aiding and abetting—can be applied to situations where humans deliberately use AI as tools for criminal conduct. AI systems, including autonomous malware, are treated as instruments; liability is attributed to those who design, deploy or benefit from their operation.[3][5][13][19]

International criminal law is considered technology-neutral: a crime is a crime whether committed using a gun or a computer, and AI applications are viewed as tools rather than legal subjects. Yet, technology-neutrality does not fully address novel evidentiary and attribution issues, particularly when autonomous systems act in ways that may diverge from their initial programming or exploit emergent vulnerabilities.[25][13][^3]

B. Case Law on Autonomous Worms and Botnets

United States v. Morris (1991) involved one of the first major prosecutions under the Computer Fraud and Abuse Act (CFAA), where the defendant released the "Morris worm" that replicated autonomously across thousands of internet-connected computers. The court held that releasing the worm constituted unauthorized access and damage, emphasizing that the actus reus lay in the defendant's deployment of the code, and that mens rea was satisfied by knowingly releasing a program capable of causing harm. This case established that human actors are criminally responsible for autonomous propagation of malware.[19][21]

In United States v. Ancheta (2006), the defendant operated a botnet infecting thousands of computers and rented them out for spamming and attacks, profiting from the use of autonomous "zombie" machines. The court found that Ancheta orchestrated and controlled the botnet, attributing the actions of bots to him as instruments, and imposed imprisonment and asset forfeiture. Similarly, United States v. Brovko (2020) involved participation in a botnet scheme targeting financial institutions, where the court held the defendant responsible for designing malware, directing the botnet and profiting from fraud, despite the bots acting independently.[^19] These cases, alongside other automated cyber-attack prosecutions, reinforce key principles: AI bots and autonomous malware are instruments; mens rea is human-centric; and liability depends on foreseeability, control and benefit in relation to automated systems. However, they also highlight emerging challenges in proving chains of control and intent when AI components introduce unpredictability or self-optimization beyond the original design.[5][21][3][19]

C. Attribution and Evidentiary Complexity

Forensic analysis of automated cyberattacks must establish the chain of custody and integrity of digital evidence, attribute attacks to persons or entities, and demonstrate the reliability of forensic tools, including those that may themselves use AI. Automated attacks generate large volumes of logs, scripts and autonomously propagated artefacts, requiring advanced forensic techniques such as network forensics, malware analysis and AI-based anomaly detection, which raise issues of relevance, privacy and explainability.[18][21]

When AI is "in the loop" of forensic analysis, courts must evaluate evidence generated by opaque or proprietary AI tools, considering whether their methods are transparent and scientifically reliable. Attribution is further complicated by the transnational nature of AI-enabled attacks and by the potential for AI-generated misdirection, such as false flags and synthetic identities. These factors strain traditional doctrines on sufficiency of evidence and standards of proof, especially in cross-border prosecutions where electronic evidence must be collected, preserved and shared across jurisdictions.[23][25][13][22][21][18]

IV. JURISDICTIONAL AND TREATY GAPS

The Budapest Convention on Cybercrime, adopted in 2001 and in force since 2004, remains a foundational instrument for criminalizing cyber threats and enabling international cooperation in electronic evidence. It covers offences such as unauthorized access, data and system interference, computer-related fraud, and distribution of child exploitation material, and sets out procedural powers and cooperation mechanisms for investigating cybercrime. Nonetheless, analyses indicate that the Convention lacks explicit provisions addressing AI-driven threats such as automated phishing, deepfakes, and adaptive malware, and does not include robust AI-governance obligations.[14][15]

The United Nations Convention against Cybercrime (Hanoi Convention), adopted by the General Assembly in December 2024 and opened for signature in Hanoi in October 2025, establishes the first universal framework for investigating and prosecuting cyber-dependent and cyber-enabled offences and sharing electronic evidence. It requires states to criminalize certain forms of cybercrime, including illegal access, data interference and online child exploitation, and creates a 24/7 cooperation network, but uses technology-neutral language focusing on criminal acts rather than specific technologies.[26][27][24][20][17][23]

Research on the intersection of the UN cybercrime treaty and AI-enabled threats point to critical regulatory gaps, noting that the treaty's effectiveness varies across incident types and that many AI-related crimes span multiple jurisdictions, challenging coordination in investigation, attribution and prosecution. Although the treaty can be applied to AI-generated child sexual abuse material and other serious offences, scholars recommend augmenting it with AI-specific annexes or interpretive guidance. Overall, both the Budapest and Hanoi Conventions provide a baseline framework but do not yet fully address AI-driven cybercrime and autonomous malware.[24][22]

V. NEED FOR A NEW CYBERSECURITY FRAMEWORK

A. Limitations of Existing Legal Instruments

Studies on cybersecurity and AI in international law conclude that existing frameworks lack robust provisions to address AI-enabled cyber threats, particularly in terms of explicit obligations on AI design, deployment and oversight. While the Malabo Convention, Budapest Convention and EU GDPR contribute to cybercrime regulation and data protection, none specifically regulate AI-powered malware or autonomous cyber operations, and AI is absent or only generally referenced in their texts.[15][16][^2]

Research on AI-driven cyberterrorism highlights a critical legal gap: the absence of a definition of AI-driven cyberterrorism, unclear attribution standards and inadequate enforcement mechanisms tailored to AI-enhanced attacks. International criminal law instruments do not comprehensively regulate AI misuse in transnational crime, leading to disparities in national regulation and difficulties in harmonizing responses. The rapid evolution of AI technology therefore outpaces the development of legal regulations, creating loopholes that perpetrators can exploit to evade accountability.[16][12][13][22]

B. Principles for an AI-Aware Cybersecurity Framework

An effective AI-aware cybersecurity framework must remain technology-neutral while incorporating AI-specific risk considerations, thereby aligning with existing criminal law doctrine that treats AI as an instrument but recognizing its distinctive capabilities.

Scholars propose that international frameworks be updated or supplemented to include AI-specific annexes, interpretive guidance or protocols, defining AI-enabled cybercrime categories, clarifying attribution standards and establishing obligations on AI risk assessment and governance.[2][25][22][16][^3]

Key principles emerging from legal and policy analysis include: accountability chains that link AI developers, deployers and operators; explainability and transparency requirements for AI systems used in sensitive domains; obligations to implement AI-driven behavioral analysis and anomaly detection in critical infrastructure; and enhanced mechanisms for cross-border evidence sharing and mutual legal assistance tailored to AI-rich environments.[7][21][^2]

C. Integration with Cybersecurity Practice

Technical literature emphasizes that AI-powered behavioral analysis and anomaly detection are among the few viable defenses against malware that can "think" for itself, adapt in real time and operate autonomously. Autonomous malware forces defenders to move beyond signature-based detection to systems that continuously monitor behavior, external calls and process changes, using AI to detect anomalies and potential threats.[1][4][18][7]

A new framework would therefore need to integrate legal obligations with best practices for AI-enhanced cybersecurity, such as mandating risk-based deployment of AI detection systems in critical sectors, requiring secure AI development lifecycles, and establishing standards for testing and certification of AI tools used in defense and forensics. Coupling legal mandates with technical standards can help ensure that states and private actors maintain adequate capacity to detect and respond to AI-driven threats.[21][7]

VI. SUGGESTIONS AND POLICY RECOMMENDATIONS

A. International Treaty Reform and Harmonization

First, states and international bodies should work toward a globally binding legal framework or protocol focusing specifically on AI and cybersecurity, complementing existing instruments like the Budapest and Hanoi Conventions. This could take the form of an AI and Cybersecurity Treaty or annexes that define AI-driven cybercrime categories (including autonomous malware, AI-driven ransomware, AI-based deepfake fraud and AI-enhanced cyberterrorism), set minimum criminalization standards and mandate cooperation in prevention, attribution and response.[12][22][16][2]

Second, existing conventions should be amended or supplemented to include victim compensation mechanisms for AI-enabled cyber threats, particularly where financial fraud and large-scale data breaches are involved. Current frameworks often focus on criminalization and sanctions without ensuring restoration and deterrence through compensation, which can be critical in high-impact AI-driven attacks.[26][2]

Third, international organizations such as the Council of Europe and the United Nations should continue mapping AI-related cybercrime and electronic evidence issues, as already initiated by working groups under the Budapest Convention framework, and translate findings into concrete legal reforms. This process should be inclusive, involving states from different regions, technical experts and civil society to balance security, innovation and human rights concerns.[27][28][29][24]

B. Domestic Law Reform and Capacity Building

At the domestic level, jurisdictions should clarify how existing criminal law applies to AI-enabled crimes, codifying that AI systems are instruments and specifying modes of liability for developers, deployers and operators based on intent, foreseeability and control. Legislatures may introduce aggravating circumstances where AI is used to enhance the scale or sophistication of offences, as some European laws already do, and create new offences related to unlawful dissemination of AI-generated or altered content that harms privacy and reputation.[3][5]

States should also strengthen their capacity to investigate AI-driven cybercrime by embedding cyber and AI expertise within prosecution authorities, appointing cyber liaison experts and developing technical competencies for forensic analysis of automated attacks. Training programs for judges, prosecutors and law enforcement on AI concepts, autonomous malware behavior and evidentiary issues will be essential to ensure effective adjudication.[25][13][^21]

C. Technical and Regulatory Measures for Autonomous Malware

Regulators and industry should collaborate on standards for secure AI development and deployment in both offensive and defensive contexts, including requirements for documentation, safety testing and fail-safes in AI systems that could be repurposed for malware. Mechanisms such as mandatory vulnerability disclosure, secure coding guidelines for AI integration in software, and oversight of dual-use AI tools (e.g., penetration-testing agents) can reduce misuse.[6][13][22][7]

Critical infrastructure operators should be required or strongly encouraged to implement AI-based behavioral monitoring and anomaly detection, recognizing that autonomous malware may attempt to compromise industrial control systems, transportation, energy grids and healthcare networks. Shared threat intelligence platforms, combining state and private-sector data on AI-driven incidents, can help identify emerging patterns and support rapid mitigation.[24][4][12][6]

D. Enhancing Cooperation and Evidence Sharing

Given the transnational nature of AI-driven cybercrime, enhanced mechanisms for cross-border cooperation in electronic evidence are crucial.

The Hanoi Convention already establishes a 24/7 cooperation network and standardized processes for sharing electronic evidence of serious crimes, including cyber-dependent and cyber-enabled offences, which should be leveraged and expanded to cover AI-related incidents.[[20][17][[22][23][^26]

States should negotiate bilateral and multilateral agreements to facilitate joint investigation of AI-driven attacks, including provisions for sharing forensic tools, expertise and AI models used for detection and attribution. Harmonizing evidentiary standards, particularly regarding the admissibility and reliability of AI-generated forensic analysis, will support mutual legal assistance and reduce friction in cross-border prosecutions.[[22][27][[25][21]

VII. CONCLUSION

AI-driven cybercrime and autonomous malware present a qualitatively new class of technological threats, characterized by independent decision-making, adaptive behavior and scalable automation that challenge traditional cybersecurity paradigms. Existing legal frameworks, while technology-neutral and capable of applying general doctrines of criminal responsibility and cooperation, lack explicit and robust provisions tailored to AI-enabled threats, leading to gaps in attribution, liability and preventive obligations.

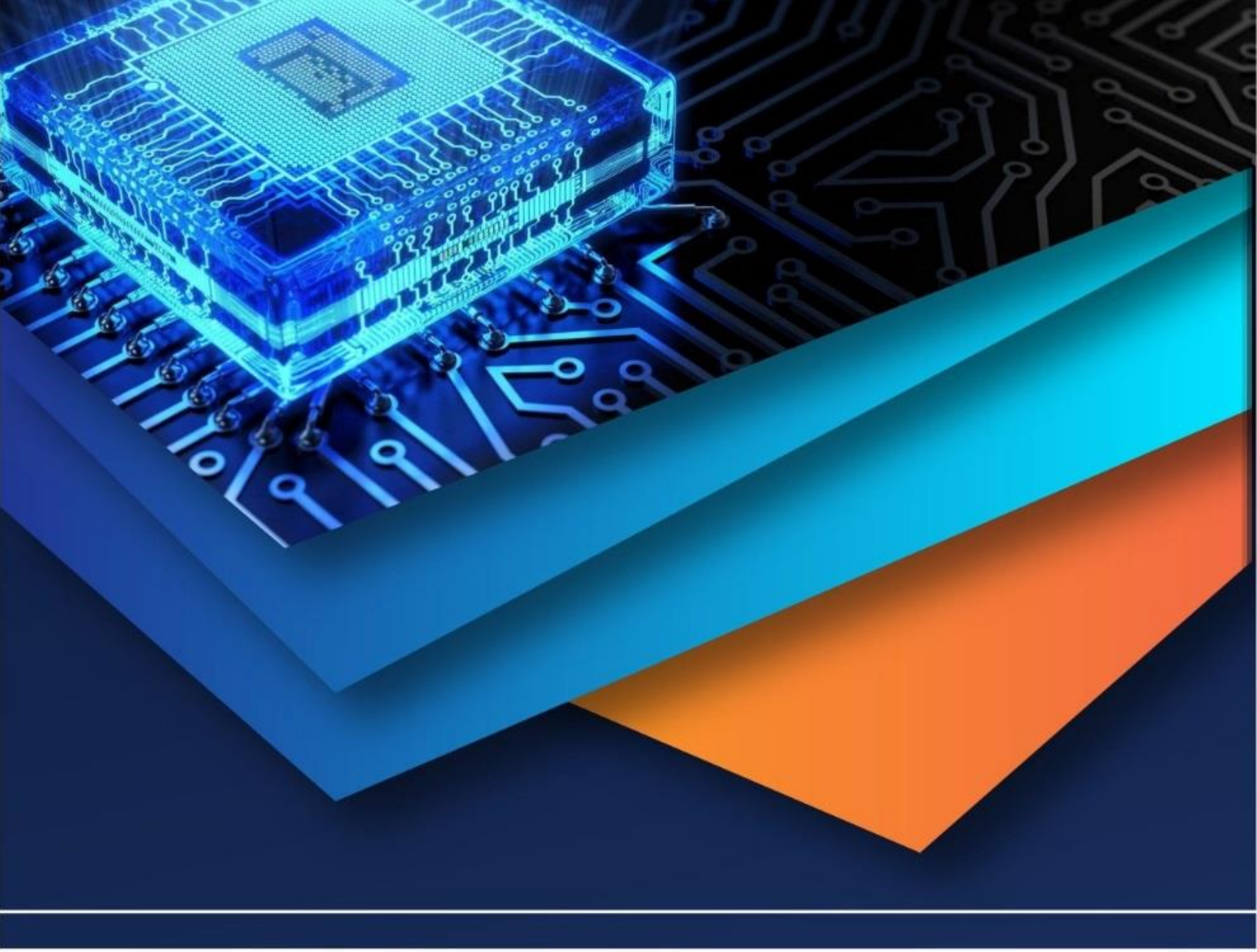
Case law on autonomous worms and botnets confirms that responsibility remains with human actors who design, deploy or control these systems, but emerging forms of autonomous malware make it harder to define foreseeability and control thresholds. As AI continues to transform the cybercrime landscape, a new cybersecurity framework—comprising updated international treaties, domestic law reforms, technical standards and capacity-building—is necessary to ensure that legal norms keep pace with technological realities and that states and private actors can effectively deter, detect and respond to AI-driven threats.

Such a framework must balance technology-neutral principles with AI-specific risk governance, reinforcing accountability chains, enhancing cross-border cooperation, and integrating advanced AI-based defensive tools to safeguard digital infrastructure and human rights in an era of autonomous malware.

REFERENCES

[1] What Is AI-powered malware? Definition & Examples - Malware that consults a model during execution to generate instructions, adapt behaviour, or choose ...
[2] Cybersecurity and AI: The Role of International Law in ...
[3] Modes of Liability for AI-Enabled Crimes in International ...
[4] What Makes Autonomous Malware a New Category of Cyber Threat? - Discover why autonomous malware represents a fundamentally new category of cyber threat in 2025. Thi...
[5] Legal framework in criminal liability for crimes involving ...
[6] Autonomous attacks ushered cybercrime into AI era in 2025 - AI is making cyberattacks faster and more effective through deepfakes, vulnerability discovery, auto...
[7] [PDF] AI-driven malware: The next cybersecurity crisis
[8] AI-driven malware: The next cybersecurity crisis
[9] What Is Autonomous Malware? - Lazarus Alliance, Inc. - We're reaching the end of 2025, and looking ahead to 2026, most experts are discussing the latest th...
[10] What Is AI-Powered Malware? Adaptive Threats - AI-powered malware uses AI techniques to improve targeting, evasion, or automation. Learn examples, ...
[11] The Rise of AI-Powered Malware: How Autonomous Cyber Threats ... - The cyber threat landscape is evolving faster than ever, and AI-powered malware has now become one o...
[12] Addressing AI-Driven Cyber-Terrorism Within the Framework of International Law - Global Journal of Politics and Law Research (GJPLR) - AI has introduced new dimensions to cyberterrorism, enabling more sophisticated, automated, and pote...
[13] [PDF] International Criminal Law Challenges Regarding The Misuse of ...
[14] Adapting the Budapest Convention to address emerging ...
[15] cybersecurity-and-ai-the-role-of-international-law-in- ...
[16] Addressing AI-Driven Cyber-Terrorism Within the Framework of ...
[17] United Nations Convention against Cybercrime - Wikipedia
[18] Malware and Cyber Attack Analysis Using Machine Learning - machine learning techniques are a crucial part of modern malware detection and more so in detecting ...
[19] Case Law On Criminal Responsibility For Autonomous Ai ... - Case 1: United States v. Morris (1991)Facts:Robert Tappan Morris released the “Morris Worm,” one of ...
[20] United Nations Convention against Cybercrime - Unodc - Convention at a glance. The United Nations Convention against Cybercrime; Strengthening Internationa...
[21] Case Law On Forensic Analysis Of Automated Cyber-Attack ... - Analytical OverviewBefore the cases, here are key themes and legal issues that recur when forensic a...
[22] The UN cybercrime treaty and AI: Navigating the intersection ...
[23] Homepage - The United Nations Convention - It sets legal standards for addressing offenses such as illegal access, cyber fraud, and online chil...
[24] 251025 UN Cybercrime Convention Signing Ceremony - 251025 UN Cybercrime Convention Signing Ceremony

[25] [PDF] Securing justice for cyber-enabled international crimes
[26] Sixty-five nations sign first UN treaty to fight cybercrime, in milestone ... - 25 October 2025 Law and Crime Prevention. Sixty-five nations have signed a landmark United Nations t...
[27] CCPCJ35: Meeting 5 – 4 June 2026
[28] EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)
[29] PowerPoint Presentation



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY