CONTRARIUS INSTITUTE

Original Article

Legal Challenges of Swarm Intelligence Exploitation in Cybercrime across Distributed Systems

Naeem AllahRakha [1,*]

[1] Department of Law and Technology, Tashkent State University of Law, Tashkent, Uzbekistan.

*Corresponding author: chaudharynaeem133@gmail.com

Abstract

Cybercrime continues to evolve at a pace that challenges the adaptability of existing legal frameworks, particularly with the emergence of swarm intelligence as a tool for coordinating autonomous and distributed cyberattacks. This study aims to analyse the adequacy of contemporary international cybercrime law in addressing the exploitation of swarm intelligence, with specific reference to recent global regulatory developments. The research employs a doctrinal legal method, combining normative analysis of treaty provisions with a qualitative review of recent enforcement practices. The findings reveal four principal deficiencies: the ambiguity of legal liability in decentralized systems lacking identifiable control; jurisdictional fragmentation that enables regulatory evasion; inherent limitations in detecting multi-agent coordinated attacks; and a structural mismatch between legal norms and states' technical enforcement capacities. These gaps demonstrate that existing frameworks remain insufficient to respond effectively to technologically sophisticated cyber threats. The study concludes that without targeted legal reform, including the development of specialized regulatory instruments, enhanced international cooperation mechanisms, and improved technical capacity, the enforcement of cybercrime law will remain reactive and fragmented. Strengthening the integration between legal doctrine and technological realities is therefore essential to ensure effective governance and protection in the evolving digital landscape.

Keywords: Autonomous System; Cybercrimes; Legal; Swarm Intelligence;

Introduction

Cybercrime is evolving faster than laws can keep pace with technological change. Swarm intelligence, which is based on collective behavior observed in nature, is now being misused in distributed systems.[1] Criminals can coordinate multiple devices to attack networks in ways traditional security cannot easily detect. In 2025, Europol coordinated a multinational operation that dismantled IoT-based botnets responsible for large-scale distributed attacks across various jurisdictions. This operation highlighted significant challenges in attribution and enforcement. Similarly, the Federal Bureau of Investigation in the USA reported disrupting AI-assisted phishing systems running through decentralized cloud nodes.[2]

This situation shows how autonomous coordination makes it harder to assess liability and conduct prosecutions across borders. Current laws often do not clearly define who is responsible for coordinated, automated cyber attacks. Scholars and policymakers have looked at cybercrime and distributed systems separately, but few have studied their intersection with swarm intelligence.[3] Understanding how these systems are exploited can help lawmakers fill legal gaps and protect digital infrastructure. This issue is urgent because

[1] Dukka Karun Kumar Reddy and others, 'A Systematic Literature Review on Swarm Intelligence Based Intrusion Detection System: Past, Present and Future', *Archives of Computational Methods in Engineering*, 31.5 (2024), 2717–84 <https://doi.org/10.1007/s11831-023-10059-2>.

[2] Dhanasak Bhumichai and others, 'The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead', *Information*, 15.5 (2024), 268 <https://doi.org/10.3390/info15050268>.

[3] Yuchong Li and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments', *Energy Reports*, 7 (2021), 8176–86 <https://doi.org/10.1016/j.egyr.2021.08.126>.

Contrarius, P-ISSN: 3090-9309, E-ISSN: 3109-0931

Received: December 15, 2025 - Revised: March 20, 2026 - Accepted: March 25, 2026

attacks are becoming more sophisticated and widespread, putting critical data and services at risk. This research will clarify the legal uncertainties and suggest frameworks to tackle swarm-based cybercrime effectively, aiding both law enforcement and lawmakers.[4]

This study intends to investigate how current cybercrime laws handle or fall short of addressing such coordinated attacks, as well as the legal ramifications of swarm intelligence exploitation in distributed systems. It also aims to create workable suggestions for bolstering legal frameworks to successfully stop and control swarm-based cybercrime. The study's main goals are to identify the ambiguities and gaps in the law as it stands today and investigate ways to improve legal responses. Large-scale distributed attacks continued to occur throughout 2025 and into 2026, indicating that current international frameworks are still reactive to decentralized autonomous threats rather than adapting to them. Central to this research is the question: *how can existing cyber laws be adapted or improved to effectively address and regulate swarm intelligence exploitation in distributed systems*? By answering this question, the study intends to provide both theoretical insights and practical guidance for lawmakers and law enforcement.

Research on swarm intelligence and cybercrime has grown considerably in recent years, yet it remains largely divided between technical and legal domains, with few studies bridging both effectively. On the technical side, coordinated multi-agent behavior substantially reduces detection probability relative to single-source attacks.[5] The analysis has been extended to fog-enabled networks, where intrusion detection rates exceeding 89% are reported when swarm intelligence algorithms are applied, illustrating the same techniques' offensive potential when used by adversaries.[6] Similarly, swarm-optimized machine learning approaches can identify complex threats with high accuracy in industrial control systems, achieving anomaly detection rates above 97%.[7] Collectively, these technical studies provide compelling empirical evidence of the scalability and sophistication of swarm-based threats. However, they address legal accountability only peripherally, if at all.[8]

On the legal side, persistent enforcement gaps in existing cybercrime law have been identified, particularly the inability of current liability frameworks to address attacks where no single human actor retains continuous control over the operation.[9] Comparative analyses further conclude that most international cybercrime instruments were designed for identifiable human perpetrators and are structurally unsuited to algorithmic agency.[10] In addition, the technology-neutral drafting approach adopted by major regulatory bodies has been critiqued for inadvertently permitting autonomous systems to operate without

[4] N. Satheesh Kumar and others, 'Swarm-Based Intelligent Models for Developing Cybersecurity Frameworks with IDS', *Scientific Reports*, 16.1 (2026), 3492 <https://doi.org/10.1038/s41598-025-30223-x>.

[5] Lizzy Ofusori, Tebogo Bokaba and Siyabonga Mhlongo, 'Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction', *Applied Artificial Intelligence*, 38.1 (2024) <https://doi.org/10.1080/08839514.2024.2439609>.

[6] Laura Bartoli, 'Cybersecurity and the Fight against Cybercrime: Partners or Competitors?', *European Journal of Risk Regulation*, 16.2 (2025), 498–513 <https://doi.org/10.1017/err.2025.31>.

[7] Laith Abualigah, Deborah Falcone and Agostino Forestiero, 'Swarm Intelligence to Face IoT Challenges', ed. by Abdul Rehman Javed, *Computational Intelligence and Neuroscience*, 2023.1 (2023) <https://doi.org/10.1155/2023/4254194>.

[8] Muhammad Hanif and others, 'Orchestrating Machine Learning Models in a Swarm Architecture for IoT Inline Malware Detection', *Scientific Reports*, 16.1 (2025), 187 <https://doi.org/10.1038/s41598-025-28859-w>.

[9] Muhammad Hassan Nasir and others, 'Swarm Intelligence Inspired Intrusion Detection Systems — A Systematic Literature Review', *Computer Networks*, 205 (2022), 108708 <https://doi.org/10.1016/j.comnet.2021.108708>.

[10] Muaadh Mukred and others, 'The Roots of Digital Aggression: Exploring Cyber-Violence through a Systematic Literature Review', *International Journal of Information Management Data Insights*, 4.2 (2024), 100281 <https://doi.org/10.1016/j.jjimei.2024.100281>.

meaningful legal oversight.[11] While these analyses map the normative landscape, they focus primarily on general AI governance rather than the specific hybrid challenge of swarm intelligence deployed for criminal purposes.[12] The closest prior studies to this paper's scope focusing on the legal implications of autonomous swarms and task allocation under swarm attack stop short of proposing operationalizable legal frameworks tailored to swarm-based cybercrime.[13]

Research acknowledges the attribution challenges of multi-agent systems but does not analyze specific treaty provisions in depth, while foundational work in swarm robotics reflects a threat landscape that has since evolved substantially. Several studies demonstrate significant advancements from a technical perspective. For instance, George Hatzivasilis et al. (2024) show that swarm intelligence solutions have been applied in incident handling and response through the integration of Cyber Threat Intelligence (CTI) into systems such as MISP, CVEs, and STIX, alongside the incorporation of Artificial Intelligence (AI) and Machine Learning (ML) in risk assessment processes.[14] Research by Minghai Xu et al. (2023) explains that swarm intelligence algorithms are intelligent computational methods inspired by the evolutionary patterns and collective behavior of biological entities such as insects and birds.[15] Chao Wang et al. (2025) emphasize that swarm intelligence emerges from the collective interactions among individuals within a group.[16] Furthermore, Rashid A. Saeed et al. (2022) demonstrate the application of swarm optimization algorithms in intelligent drone path planning.[17] Mengqing Mei et al. (2026) highlight the importance of swarm-based metaheuristic algorithms in feature selection to reduce dimensionality and improve model accuracy in high-dimensional datasets.[18] This study addresses these gaps directly by conducting a focused legal analysis of two key international instruments, the UN Convention against Cybercrime (2024) and the Council of Europe Framework Convention on AI (2024) against the specific operational characteristics of swarm intelligence exploitation, and by deriving targeted, actionable legal recommendations from that analysis.

Method

This study adopts a qualitative, doctrinal legal research design. The primary methodological approach is systematic document analysis, encompassing academic literature, international legal instruments, and official policy documents.[19] Academic sources were identified through searches of Google Scholar and Scopus using the following search

[11] Damian Copeland, Philip Sammons and Lauren Sanders, 'An Approach to the Legal Review of Autonomous Swarms', in *Thinking Swarms* (Cham: Springer Nature Switzerland, 2025), pp. 171–86 <https://doi.org/10.1007/978-3-031-82790-7_10>.

[12] Danqing Shen and others, 'Task Allocation for UAV Swarms under Communication Attacks: An Approach Based on Game Theory and Negotiation Mechanism', *Journal of the Franklin Institute*, 362.1 (2025), 107417 <https://doi.org/10.1016/j.jfranklin.2024.107417>.

[13] Shen and others, 'Task Allocation for UAV Swarms under Communication Attacks'.

[14] George Hatzivasilis and others, 'Swarm-Intelligence for the Modern ICT Ecosystems', *International Journal of Information Security*, 23.4 (2024), 2951–75 <https://doi.org/10.1007/s10207-024-00869-1>.

[15] Minghai Xu and others, 'Application of Swarm Intelligence Optimization Algorithms in Image Processing: A Comprehensive Review of Analysis, Synthesis, and Optimization', *Biomimetics*, 8.2 (2023), 235 <https://doi.org/10.3390/biomimetics8020235>.

[16] Chao WANG and others, 'Swarm Intelligence: A Survey of Model Classification and Applications', *Chinese Journal of Aeronautics*, 38.3 (2025), 102982 <https://doi.org/10.1016/j.cja.2024.03.019>.

[17] Rashid A. Saeed and others, 'Optimal Path Planning for Drones Based on Swarm Intelligence Algorithm', *Neural Computing and Applications*, 34.12 (2022), 10133–55 <https://doi.org/10.1007/s00521-022-06998-9>.

[18] Mengqing Mei and others, 'A Cooperative Hybrid Breeding Swarm Intelligence Algorithm for Feature Selection', *Pattern Recognition*, 169 (2026), 111901 <https://doi.org/10.1016/j.patcog.2025.111901>.

[19] Khusniati Rofi'ah, Martha Eri Safira and Muhammad Ikhlas Rosele, 'The Effectiveness of Accelerating Halal Product Certification: Regulations and Companions', *Journal of Human Rights, Culture and Legal System*, 4.2 (2024), 449–76 <https://doi.org/10.53955/jhcls.v4i2.203>.

terms: swarm intelligence, cybercrime, distributed systems, autonomous agents, legal attribution, and cybercrime law. Only peer-reviewed journal articles indexed in Scopus were included to ensure source quality. Legal and policy materials were drawn exclusively from official government or organizational publications and are publicly accessible. The search covered literature published between 2013 and 2025, with priority given to studies from 2020 onward to reflect the current threat environment. An initial pool of sources was screened against three inclusion criteria are first, direct relevance to swarm intelligence, cybercrime, or AI governance; second, engagement with either technical or legal dimensions of autonomous distributed systems; and third, availability in English. Sources addressing only general cybersecurity without legal or AI-specific analysis were excluded. Legal analysis focused on the substantive provisions of the United Nations Convention against Cybercrime (2024) and the Council of Europe Framework Convention on AI (2024), with particular attention to articles governing attribution, jurisdiction, accountability, and enforcement. Thematic analysis was applied to identify convergences and gaps across academic and legal sources. The study proceeds inductively, deriving legal categories and reform recommendations from the patterns identified across the analyzed materials. This research received no external funding. All data sources are publicly available, and proper attribution is provided throughout.[20]

Results and Discussions

Unclear Legal Liability for Swarm Attacks

Swarm intelligence derives from the study of collective behaviour in biological systems, including ants, bees, and birds, in which simple agents solve complex problems through decentralized, self-organized coordination rather than central direction.[21] In the context of cybercrime, this principle enables networks of compromised devices or bots to coordinate attacks collectively, each unit operating according to shared algorithms while producing behaviour that appears organized and deliberate. Such attacks propagate rapidly, adapt their tactics in real time, and are designed to evade detection, making attribution and interdiction significantly more difficult. The decentralized and autonomous nature of swarm intelligence fundamentally challenges the liability frameworks on which law enforcement and courts traditionally rely. Existing legal rules, constructed around identifiable human actors, are poorly suited to scenarios in which hundreds or thousands of bots act in concert without any single controller.[22]

The exploitation of swarm intelligence in cybercrime poses severe and growing challenges for legal systems globally. When criminals launch coordinated attacks using distributed networks, identifying the responsible parties presents a formidable legal and technical challenge.[23] The United Nations adopted the Convention against Cybercrime in December 2024 in response to these escalating threats. However, the Convention faces significant limitations when confronting swarm-based attacks in which thousands of devices operate

[20] Abdul Kadir Jaelani, Anila Rabbani and Muhammad Jihadul Hayat, 'Land Reform Policy in Determining Abandoned Land for Halal Tourism Destination Management Based on Fiqh Siyasah', *El-Mashlahah*, 14.1 (2024), 211–38 <https://doi.org/10.23971/el-mashlahah.v14i1.8051>.

[21] Fatima Ezzahra Zaizi, Sara Qassimi and Said Rakrak, 'Multi-Objective Optimization with Recommender Systems: A Systematic Review', *Information Systems*, 117 (2023), 102233 <https://doi.org/10.1016/j.is.2023.102233>.

[22] Noble Anumbe, Clint Saidy and Ramy Harik, 'A Primer on the Factories of the Future', *Sensors*, 22.15 (2022), 5834 <https://doi.org/10.3390/s22155834>.

[23] Shai Farber, 'The Evolving Nexus of Cybercrime and Terrorism: A Systematic Review of Convergence and Policy Implications', *Security Journal*, 38.1 (2025), 29 <https://doi.org/10.1057/s41284-025-00471-7>.

Contrarius, P-ISSN: **3090-9309**, E-ISSN: **3109-0931**

collectively and automatically.[24] The Convention obliges states to criminalize a defined set of computer-related offences. Articles 6 through 9 specifically require the criminalization of illegal access, interception, data interference, and system interference. A central challenge arises from the fact that swarm attacks distribute malicious activity across thousands of compromised devices, whose owners are typically unaware of their devices' involvement. Consequently, even where an attack satisfies the criteria for system interference under Article 9, establishing criminal intent attributable to a specific individual becomes legally untenable, particularly when conduct is orchestrated by algorithms with no identifiable central controller.[25]

The decentralized architecture of swarm attacks renders conventional legal frameworks for individual accountability structurally inadequate.[26] States face significant difficulty in identifying the actors responsible for these coordinated operations. Network traffic associated with swarm attacks traverses multiple jurisdictions simultaneously, making linear investigative tracing legally and technically unreliable. The Council of Europe Framework Convention on AI introduces an additional layer of complexity. Adopted in September 2024, this landmark treaty, the first of its kind internationally, establishes binding obligations governing AI throughout its entire lifecycle, from design through deployment to decommissioning, and requires states to ensure that accountability is maintained when AI systems cause harm.[27]

Swarm intelligence operates differently from the conventional AI systems that the Convention primarily addresses. In swarm attacks, multiple autonomous agents each make independent decisions without any central coordinating authority. While the Convention emphasizes human oversight and individual accountability, it provides no clear guidance on responsibility attribution when AI systems execute attacks through collective, autonomous coordination. Article 5 of the Convention mandates meaningful human oversight of AI systems. However, swarm intelligence is architecturally designed to circumvent centralized control; these systems are built precisely for agents to coordinate autonomously and directly with one another. This creates a substantial compliance problem: when no human actor maintains operational control now the system acts, it is legally unclear whether the oversight requirement can be satisfied at all. This remains an unresolved area of international law.[28]

Both conventions recognize the importance of international cooperation, yet they fall short on swarm-specific provisions. The UN Cybercrime Convention promotes information sharing and mutual legal assistance between countries and establishes national contact points for rapid cooperation during investigations. However, swarm attacks exploit the very speed and scale that make international cooperation difficult. Attacks can originate from multiple countries simultaneously, with each jurisdiction seeing only a small part of the overall

[24] Wael Hadi and others, 'Swarm AI for Distributed Cyber Defense and Autonomous Threat Detection' (IGI Global, 2025), pp. 185–208 <https://doi.org/10.4018/979-8-3373-0954-5.ch007>.

[25] Stefan Schäferling, 'The Case for a Right Against Automated Decision-Making', in *Governmental Automated Decision-Making and Human Rights. Law, Governance and Technology Serie* (Springer Charm, 2023), pp. 231–83 <https://doi.org/10.1007/978-3-031-48125-3_7>.

[26] Dalia Kadry Ahmed Abdelaziz, 'Criminal Liability for the Misuse and Crimes Committed by AI: A Comparative Analysis of Legislation and International Conventions', *Journal of Infrastructure Policy and Development*, 9.1 (2025), 10722 <https://doi.org/10.24294/jipd10722>.

[27] Maikel Leon, 'Lifecycle-Based Governance to Build Reliable Ethical AI Systems', *Systems Research and Behavioral Science*, 2026 <https://doi.org/10.1002/sres.70014>.

[28] Josephine Bhavani Rajendra and Ambikai S. Thuraisingam, 'The Role of Explainability and Human Intervention in AI Decisions: Jurisdictional and Regulatory Aspects', *Information & Communications Technology Law*, 2025, 1–32 <https://doi.org/10.1080/13600834.2025.2537514>.

threat.[29] The Convention assigns jurisdictional responsibility to states where crimes occur on their territory or are committed by their nationals. Articles 23 to 27 govern jurisdiction based on territory and nationality. However, swarm attacks simultaneously involve thousands of compromised devices distributed across multiple countries, meaning that each jurisdiction observes only a fragment of the overall attack. The result is frequent enforcement paralysis, where no single state assumes lead responsibility and the collective response collapses.[30]

The UN Convention extends criminal liability to both individuals and legal entities. Article 12 requires states to ensure that companies can be held accountable when offences are committed for their benefit, including by persons acting under their authority.[31] However, contemporary swarm-based cyber-attacks rely on distributed cloud infrastructure, commercial botnet services, and decentralized networks with no identifiable central authority. When operations are algorithmically fragmented and geographically dispersed, establishing that a specific corporate entity benefited from the criminal conduct becomes legally untenable.[32] The Convention also extends criminal liability to accomplices, assistants, and instigators. However, in many swarm attacks, ordinary individuals are effectively victims: their devices are compromised and incorporated into criminal activity without their knowledge or consent.[33] When malware autonomously organizes and executes the attack, establishing criminal intent attributable to any individual becomes legally impracticable.[34] Furthermore, the Convention's reservation mechanisms permit states to opt out of certain provisions, creating additional inconsistencies in enforcement across jurisdictions. The Council of Europe's AI Convention requires states to conduct risk assessments and impact evaluations for AI systems and mandates transparency and comprehensive documentation throughout the full lifecycle of AI operations.[35]

Hidden Loopholes in Cybercrimes Regulation

Despite the existence of international legal frameworks, significant regulatory gaps persist, particularly with respect to the exploitation of distributed systems. Swarm attacks, in which adversaries coordinate across multiple countries and strike simultaneously from numerous vectors, operate at a speed that severely limits the capacity of law enforcement to mount an effective real-time response. Established mechanisms for cross-border investigation, including mutual legal assistance treaties and national contact points, operate too slowly to intercept these attacks in real time. Criminal actors exploit this vulnerability by operating from jurisdictions where regulatory standards are minimal, enforcement capacity is weak, or

[29] Ying Tan and Zhong-yang Zheng, 'Research Advance in Swarm Robotics', *Defence Technology*, 9.1 (2013), 18–39 <https://doi.org/10.1016/j.dt.2013.03.001>.

[30] Zaid Mustafa and others, 'Intrusion Detection Systems for Software-Defined Networks: A Comprehensive Study on Machine Learning-Based Techniques', *Cluster Computing*, 27.7 (2024), 9635–61 <https://doi.org/10.1007/s10586-024-04430-6>.

[31] Mahrus Ali, Andi Muliyono and Syarif Nurhidayat, 'The Application of a Human Rights Approach toward Crimes of Corruption: Analyzing Anti-Corruption Regulations and Judicial Decisions', *Laws*, 12.4 (2023), 68 <https://doi.org/10.3390/laws12040068>.

[32] Akhat Bakirov and Ibragim Suleimenov, 'Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare', *Computers*, 14.10 (2025), 410 <https://doi.org/10.3390/computers14100410>.

[33] Santosh Kumar Birthriya, Priyanka Ahlawat and Ankit Kumar Jain, 'A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies', *Journal of Applied Security Research*, 20.2 (2025), 244–92 <https://doi.org/10.1080/19361610.2024.2372986>.

[34] Giuseppe Primiero and others, 'Swarm Attack: A Self-Organized Model to Recover from Malicious Communication Manipulation in a Swarm of Simple Simulated Agents' (Springer Charm, 2018), pp. 213–24 <https://doi.org/10.1007/978-3-030-00533-7_17>.

[35] Tamas Szadeczky and Zsolt Bederna, 'Risk, Regulation, and Governance: Evaluating Artificial Intelligence across Diverse Application Scenarios', *Security Journal*, 38.1 (2025), 35 <https://doi.org/10.1057/s41284-025-00495-z>.

international cooperation mechanisms are underdeveloped. The absence of clear technical standards for detecting, blocking, and countering swarm-based attacks creates additional enforcement gaps that offenders can exploit. Consequently, law enforcement agencies face compounded difficulties not only in identifying attack origins and responsible actors, but also in collecting evidence that meets evidentiary standards in court.[36]

Broad exemptions for private companies, combined with permissive regulatory standards, substantially undermine enforcement effectiveness. Where broad exemptions apply to national security or research activities, AI and distributed systems may operate with minimal oversight, creating conditions that are readily exploited by criminal actors.[37] The technology-neutral drafting approach, while intended to promote innovation, fails to establish concrete technical standards, allowing companies to deploy distributed systems that can be incorporated into criminal activity with minimal clear legal accountability.[38] Criminal actors deliberately exploit this gap by constructing systems without any central point of control, making it effectively impossible to assign liability to developers, deployers, or platform operators. In decentralized, self-organizing swarm systems, where machines make decisions autonomously across distributed nodes, establishing intent and legal responsibility becomes exceptionally complex, and legal proceedings frequently stall as a result.[39]

Contemporary cybercrime has evolved well beyond isolated individual actors; it now operates as a structured, commercialized ecosystem. Botnet-as-a-service platforms, automated attack tools, and ransomware marketplaces operate as commercialized criminal enterprises largely beyond the reach of law enforcement. As a result, individuals with limited technical expertise can execute large-scale attacks by accessing commercially available criminal infrastructure. This places considerable pressure on legal systems, which consistently struggle to keep pace with the speed of technological change. Proving criminal intent is equally challenging, particularly when malware autonomously handles coordination and device owners are unwitting participants whose equipment has been compromised without their knowledge. Criminal actors systematically target legacy devices that no longer receive security updates, a class of vulnerable hardware that existing legal frameworks largely fail to address.[40]

High-profile cybercrime cases illustrate the scale and complexity that swarm-based threats have reached. The 911 S5 botnet, dismantled in 2024, had silently compromised 19 million devices across 190 countries and operated for years before an effective international law enforcement response could be coordinated. The Integrity Technology Group botnet, as of June 2024, retained control over more than 260,000 compromised devices, demonstrating the persistent ability of criminal actors to exploit legacy hardware and outdated infrastructure. State-sponsored threat actors, including Volt Typhoon and Fancy Bear, exploit distributed network architectures to evade attribution while targeting critical infrastructure, further complicating the enforcement landscape. When law enforcement does step in, they sometimes must use sweeping nationwide warrants just to reach and clean up

[36] Haibin Duan, Mengzhen Huo and Yanming Fan, 'From Animal Collective Behaviors to Swarm Robotic Cooperation', *National Science Review*, 10.5 (2023) <https://doi.org/10.1093/nsr/nwad040>.
[37] Rowena Rodrigues, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities', *Journal of Responsible Technology*, 4 (2020), 100005 <https://doi.org/10.1016/j.jrt.2020.100005>.
[38] Monika Simmler, Giulia Canova and Kuno Schedler, 'Smart Criminal Justice: Phenomena and Normative Requirements', *International Review of Administrative Sciences*, 89.2 (2023), 415–32 <https://doi.org/10.1177/00208523211039740>.
[39] Jonas D Hasbach and Maren Bennewitz, 'The Design of Self-Organizing Human–Swarm Intelligence', *Adaptive Behavior*, 30.4 (2022), 361–86 <https://doi.org/10.1177/10597123211017550>.
[40] Nilufer Tuptuk and Stephen Hailes, 'Security of Smart Manufacturing Systems', *Journal of Manufacturing Systems*, 47 (2018), 93–106 <https://doi.org/10.1016/j.jmsy.2018.04.007>.

Contrarius, P-ISSN: **3090-9389**, E-ISSN: **3109-0931**

infected devices. Such measures, however, raise significant legal and ethical questions concerning privacy rights, national sovereignty, and the scope of law enforcement authority.[41]

The widespread commercialization of cybercrime tools and the pervasiveness of automation have further complicated enforcement.[42] Criminal marketplaces extend well beyond the sale of stolen data, offering access to compromised devices, pre-packaged attack toolkits, and automated attack platforms that operate across borders with minimal friction. The UN Cybercrime Convention prohibits the possession and distribution of tools designed for criminal use. Nevertheless, establishing criminal intent remains extremely difficult, particularly when attacks execute autonomously with minimal human intervention. Regulatory frameworks presuppose the ability to identify those who built or deployed criminal tools; this assumption becomes untenable in swarm-based attacks where control is deliberately distributed.[43] Compounding this problem, many distributed attack platforms incorporate self-deletion or origin-concealment mechanisms designed to frustrate forensic investigation. This combination of factors makes it effectively impossible to hold accountable those responsible whether developers, operators, or end users. A fundamental and growing gap therefore exists between what current law is capable of enforcing and what technology makes operationally possible for criminal actors.[44]

Current legal frameworks are structurally ill-equipped to address threats emanating from distributed systems.[45] They fail to account for the speed, decentralization, and autonomy that define swarm intelligence attacks. Private companies, technology platforms, and developers are not meaningfully compelled to implement robust safeguards, and the rapid evolution of criminal tools means that every unaddressed legal gap becomes an exploitable vulnerability. Governments, businesses, and individuals alike remain exposed consequently.[46] What is required is substantive legal reform not incremental adjustment. This means genuinely harmonized international standards, unambiguous liability rules, and mandatory security requirements. Without such reform, cross-border law enforcement will remain structurally incapable of keeping pace with swarm-based cybercrime.[47]

Detection Challenges of Multi-Agent Attack

Multi-agent attacks employing swarm intelligence present a qualitatively distinct set of investigative challenges that existing legal frameworks are not equipped to address.[48] The

[41] Saman Iftikhar, 'Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures', *PeerJ Computer Science*, 10 (2024), e1772 <https://doi.org/10.7717/peerj-cs.1772>.

[42] Amr Adel and Mohammad Norouzifard, 'Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application', *Big Data and Cognitive Computing*, 8.8 (2024), 91 <https://doi.org/10.3390/bdcc8080091>.

[43] Yan Wang, Hao Wang and Yanghuang Cao, 'Comprehensive Review of Storage Optimization Techniques in Blockchain Systems', *Applied Sciences*, 15.1 (2024), 243 <https://doi.org/10.3390/app15010243>.

[44] Anri Nishnianidze, 'Some New Challenges of Cybercrime and the Reason for Its Outdated Regulations', *European Scientific Journal, ESJ*, 19.39 (2023), 92 <https://doi.org/10.19044/esj.2023.v19n39p92>.

[45] Jean Paul A. Yaacoub and others, 'Toward Secure Smart Grid Systems: Risks, Threats, Challenges, and Future Directions', *Future Internet*, 17.7 (2025), 318 <https://doi.org/10.3390/fi17070318>.

[46] Wasyihun Sema Admass, Yirga Yayeh Munaye and Abebe Abeshu Diro, 'Cyber Security: State of the Art, Challenges and Future Directions', *Cyber Security and Applications*, 2 (2024), 100031 <https://doi.org/10.1016/j.csa.2023.100031>.

[47] Mahipal Lather, Sachin Bhardwaj and Vandana Ajay Kumar, 'Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms', *Productivity*, 65.1 (2024), 1–10 <https://doi.org/10.32381/PROD.2024.65.01.1>.

[48] Deafallah Alsadie, 'Cybersecurity and Artificial Intelligence in Unmanned Aerial Vehicles: Emerging Challenges and Advanced Countermeasures', ed. by Jiwei Tian, *IET Information Security*, 2025.1 (2025) <https://doi.org/10.1049/ise2/2046868>.

UN Convention against Cybercrime requires states to collect and preserve electronic evidence and to establish systems for real-time traffic monitoring and content interception. These provisions, however, were designed around conventional attack models in which conduct can generally be traced to an identifiable individual or organization. Swarm attacks operate by distributing malicious activity across thousands of independent agents, each of which may appear individually innocuous while collectively causing substantial harm. The Convention requires that computer data be preserved for ninety days; however, this provision proves inadequate in practice, as swarm attacks typically complete their operations within hours and leave minimal forensic evidence. States are also required to maintain legal mechanisms for the search and seizure of stored data during criminal investigations.[49] In practice, however, this capacity is rendered ineffective when attackers distribute their infrastructure across multiple jurisdictions and coordinate operations autonomously, making targeted seizure nearly impossible.

The Convention requires AI systems to be transparent and subject to meaningful oversight throughout their entire operational lifecycle. States are required to ensure that individuals are informed when interacting with AI systems, and that clear records of AI decision-making processes are maintained to support accountability. Swarm intelligence systems are, however, architecturally designed to resist this form of oversight. The absence of a central control node means that transparency requirements have no effective point of application. Criminal actors exploit this structural gap, deploying swarm-based systems in ways that preclude meaningful pre-deployment risk or impact assessment. Unlike compliant actors, cybercriminals operating with swarm intelligence disregard risk management and safety obligations entirely.[50] Furthermore, the Convention's national security exemptions provide additional opportunities for exploitation. The Convention also fails to establish concrete technical standards for identifying coordinated attacks across decentralized autonomous systems, a gap that significantly limits its practical enforcement value.

AI agents can conceal inter-agent communications through steganographic techniques, enabling covert coordination that evades conventional security monitoring. Swarm intelligence amplifies this capability by allowing agents to exchange information and collectively converge on optimal attack vectors. This distributed architecture confers substantially greater scalability and resilience compared to single-agent attacks. Research on countering UAV swarms confirms this challenge: when hundreds of autonomous agents coordinate simultaneously, tracking their individual actions becomes operationally infeasible. Legacy security systems are not designed for threats that scale and distribute in this manner. The UN Convention promotes inter-state cooperation primarily through accelerated information-sharing mechanisms and expedited mutual legal assistance. Nevertheless, the scale and velocity of cyberattacks continue to grow. A 2024 global operation dismantled more than 134,000 malicious infrastructures within two months, yet even this significant enforcement effort illustrated how the sheer volume of swarm-based activity continues to exceed the capacity of current security tools.[51]

A fundamental challenge is the attribution problem inherent in multi-agent swarm attacks. The UN Convention grants jurisdictional authority to states when an attack occurs on their

[49] Issa Qiqieh and others, 'An Intelligent Cyber Threat Detection: A Swarm-Optimized Machine Learning Approach', *Alexandria Engineering Journal*, 115 (2025), 553–63 <https://doi.org/10.1016/j.aej.2024.12.039>.
[50] Hasbach and Bennewitz.
[51] Mikhail Baranchuk and others, 'Secret Collusion among AI Agents: Multi-Agent Deception via Steganography', in *Advances in Neural Information Processing Systems 37* (San Diego, California, USA: Neural Information Processing Systems Foundation, Inc. (NeurIPS), 2024), pp. 73439–86 <https://doi.org/10.52202/079017-2336>.

territory or is carried out by their nationals. However, when attacks are executed through compromised devices whose owners have no awareness of their involvement, this jurisdictional basis becomes legally unsustainable. This renders conventional attribution approaches legally and technically inadequate. The Convention prohibits the possession of hacking tools with criminal intent; however, establishing intent in the context of autonomous attack systems whose developers may claim general-purpose applications presents formidable legal obstacles. The Council of Europe's AI Convention requires that accountability be maintained for harm caused by AI systems and mandates comprehensive records of AI decision-making to enable retrospective review and legal challenge. Swarm attacks are, however, deliberately architected to minimize forensic traceability. Control is distributed among numerous independent agents, making it impossible to reconstruct a coherent decision chain. Article 8 requires systems capable of identifying accountability from beginning to end of an operation. Swarm intelligence renders this requirement operationally unworkable, because the system's behaviour emerges from collective interaction rather than from any individual actor or traceable sequence of decisions. Conventional mechanisms for assigning legal blame are therefore inapplicable: responsibility is diffused across algorithms rather than located in identifiable persons, fundamentally undermining the accountability architecture on which both Conventions depend.[52]

The UN Convention should be strengthened to require states to develop forensic capabilities specifically designed to address distributed autonomous attacks. States must also establish targeted training programs equipping personnel to detect and respond to coordinated multi-agent criminal activity. Siloed national responses are insufficient; internationally harmonized standards for real-time threat intelligence sharing are essential when swarm attacks occur. Law enforcement agencies require operational access to AI-driven detection systems capable of identifying coordinated behavioural patterns and anomalous activity across large-scale distributed networks.[53] The Council of Europe AI Convention should add extra protocols to cover decentralized autonomous systems that criminals use.[54] States must establish legal mechanisms enabling proactive disruption of swarm attacks during their formation phase, rather than limiting responses to post-incident enforcement.[55] Courts require clear and workable guidelines for attribution in cases involving thousands of simultaneously hijacked devices acting in coordination. International cooperation mechanisms must operate at a tempo commensurate with the speed of modern swarm attacks, rather than following the slower cadence of traditional diplomatic processes. Technical specialists must be embedded in the drafting and revision of these protocols to ensure that legal rules remain practically aligned with evolving attack methodologies.[56]

Without significant improvements to detection capability, swarm intelligence will continue to power sophisticated attacks that evade both technical defences and legal

[52] Yunes Alqudsi and Murat Makaraci, 'UAV Swarms: Research, Challenges, and Future Directions', *Journal of Engineering and Applied Science*, 72.1 (2025), 12 <https://doi.org/10.1186/s44147-025-00582-3>.
[53] Serhii Vladov and others, 'Method for Detecting Low-Intensity DDoS Attacks Based on a Combined Neural Network and Its Application in Law Enforcement Activities', *Data*, 10.11 (2025), 173 <https://doi.org/10.3390/data10110173>.
[54] Salvatore Luciano Furnari and Chiara Villani, 'Regulation of Financial Protocol DAOs: Addressing the Problems of Decentralization and AI Governance', in *Decentralized Autonomous Organizations—Governance, Technology, and Legal Perspectives. DAWO 2025. Springer Proceedings in Business and Economics* (Springer Charm, 2026), pp. 115–34 <https://doi.org/10.1007/978-3-032-03273-7_7>.
[55] Kubra Kose, Nuri Alperen Kose and Fan Liang, 'Securing Unmanned Devices in Critical Infrastructure: A Survey of Hardware, Network, and Swarm Intelligence', *Electronics*, 15.6 (2026), 1204 <https://doi.org/10.3390/electronics15061204>.
[56] Šarūnas Grigaliūnas and others, 'Holistic Information Security Management and Compliance Framework', *Electronics*, 13.19 (2024), 3955 <https://doi.org/10.3390/electronics13193955>.

enforcement. Enhanced forensic tools, advanced AI-driven monitoring, and consistent cross-jurisdictional legal standards are indispensable to addressing the dangers posed by multi-agent distributed attacks. Addressing this challenge requires a genuinely integrated effort one in which law, technology, and global cooperation function as a unified system rather than independent domains.[57]

The Fragmented Relationship between Legal Frameworks and Technical Realities

The collection of electronic evidence, preservation of data, and interception of real-time traffic all depend on robust technical infrastructure, a resource that is frequently absent or unreliable across many jurisdictions.[58] Law enforcement agencies frequently lack the specialized tools necessary to detect distributed attacks, particularly where adversaries deploy swarm intelligence to evade conventional monitoring systems. Resource-constrained states face difficulty in acquiring and maintaining the surveillance infrastructure, forensic software, and AI-driven monitoring capabilities necessary for effective enforcement. The result is a fragmented and uneven enforcement landscape.[59] Existing laws compound this problem by articulating broad normative principles without specifying the technical standards or methodologies necessary to detect and counter swarm-based attacks in practice. This gap impedes cross-border cooperation, weakens enforcement effectiveness, and undermines the global community's capacity to respond to continuously evolving threats.[60]

Risk assessments, impact evaluations, and transparency requirements are sound in principle, but their practical implementation is frequently inadequate. While the law requires ongoing monitoring and documentation of AI systems, it provides minimal practical guidance on how these obligations are to be fulfilled in decentralized or multi-agent environments. Criminal actors exploit these implementation gaps by deploying autonomous agents that obscure decision-making processes, making accountability effectively unenforceable. Regulatory sandboxes and controlled testing environments are intended to allow safe experimentation with AI systems, but their effectiveness depends on governments possessing the technical capacity to administer and supervise them, a prerequisite that many states lack. Monitoring is consequently inconsistent, and compliance with legal obligations is frequently unsupervised. The absence of standardized auditing, logging, and analysis protocols for complex autonomous systems further limits the feasibility of meaningful oversight.[61]

The exponential growth of digital data exacerbates these difficulties. Swarm intelligence attacks generate vast volumes of data produced by millions of devices operating across multiple jurisdictions.[62] Although the law requires agencies to collect this data, most lack the technological infrastructure to store, process, or analyze it at the required scale and security standard. The absence of standardized data formats, adequate encryption requirements, and

[57] Bo Nørregaard Jørgensen and Zheng Grace Ma, 'Digital Twin of the European Electricity Grid: A Review of Regulatory Barriers, Technological Challenges, and Economic Opportunities', *Applied Sciences*, 15.12 (2025), 6475 <https://doi.org/10.3390/app15126475>.

[58] Valsamis Mitsilegas and others, 'Data Retention and the Future of Large-scale Surveillance: The Evolution and Contestation of Judicial Benchmarks', *European Law Journal*, 29.1–2 (2023), 176–211 <https://doi.org/10.1111/eulj.12417>.

[59] Jessica Shurson, 'The Balance of Efficiency and Fundamental Rights in the EU E-Evidence Regulation', *New Journal of European Criminal Law*, 16.3 (2025), 278–99 <https://doi.org/10.1177/20322844251357090>.

[60] Emmanuel Brunet-Jailly, 'Cross-Border Cooperation: A Global Overview', *Alternatives: Global, Local, Political*, 47.1 (2022), 3–17 <https://doi.org/10.1177/03043754211073463>.

[61] Henrik Hassel and Alexander Cedergren, 'Integrating Risk Assessment and Business Impact Assessment in the Public Crisis Management Sector', *International Journal of Disaster Risk Reduction*, 56 (2021), 102136 <https://doi.org/10.1016/j.ijdrr.2021.102136>.

[62] Abualigah, Falcone and Forestiero.

consistent evidence-handling procedures prolongs forensic investigations and introduces errors, particularly in multi-jurisdictional cases.[63] Criminal actors exploit these institutional limitations, operating at speed and scale that allows them to disperse evidence and relocate infrastructure before it can be preserved. Furthermore, legal frameworks do not mandate ongoing training in advanced areas such as network forensics, distributed systems analysis, or AI-driven anomaly detection, leaving investigators inadequately equipped and enforcement correspondingly slow or ineffective.[64]

Divergent regulatory standards and uneven technical capacity across jurisdictions produce an inconsistent enforcement environment.[65] While some states employ advanced AI-driven threat detection, others continue to rely on manual log review. Criminal actors identify and systematically exploit these disparities. Regulatory bodies tasked with AI oversight frequently lack the specialized expertise required to assess complex, decentralized systems. As a result, some systems operate with minimal scrutiny and limited transparency. Developers of swarm-based criminal systems exploit this institutional gap deliberately, designing their architectures to evade centralized oversight. Taken together, these conditions create an enforcement environment in which criminal actors can systematically exploit institutional and regulatory gaps.[66]

Addressing these challenges requires genuine integration of legal standards with technical expertise. Establishing clear global technical standards is a necessary foundation that every state must possess at minimum the baseline capacity to detect, analyze, and counter distributed attacks.[67] International support programs must move beyond declaratory commitments to deliver concrete technology transfers, provide access to forensic tools, and assist in establishing advanced AI monitoring systems.[68] Law enforcement training must be substantive and practical, equipping officers with applied competencies in network forensics, the analysis of distributed attacks, and AI-assisted anomaly detection.[69] Universal adoption of harmonized standards for data formats, encryption, logging, and evidence preservation is essential to ensuring consistent and reliable outcomes across jurisdictions. Regulatory frameworks must also provide for continuous oversight rather than point-in-time compliance checks, establishing clear procedures for ongoing monitoring of decentralized systems to detect both legal violations and criminal exploitation.[70]

---

[63] Munirah Maher Alshabibi, Alanood Khaled Bu dookhi and M. M. Hafizur Rahman, 'Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review', *Computers*, 13.8 (2024), 213 <https://doi.org/10.3390/computers13080213>.

[64] Adil S. Al-Busaidi and others, 'Redefining Boundaries in Innovation and Knowledge Domains: Investigating the Impact of Generative Artificial Intelligence on Copyright and Intellectual Property Rights', *Journal of Innovation & Knowledge*, 9.4 (2024), 100630 <https://doi.org/10.1016/j.jik.2024.100630>.

[65] William Walter Finch and Marya Butt, 'Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Systematic Review', *Journal of Cybersecurity and Privacy*, 5.4 (2025), 101 <https://doi.org/10.3390/jcp5040101>.

[66] Seumas Miller and Terry Bossomaier, *Cybersecurity, Ethics, and Collective Responsibility* (Oxford University PressNew York, 2024) <https://doi.org/10.1093/oso/9780190058135.001.0001>.

[67] Vasiliki Demertzi, Stavros Demertzis and Konstantinos Demertzis, 'An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities', *Applied Sciences*, 13.2 (2023), 790 <https://doi.org/10.3390/app13020790>.

[68] Athina Sachoulidou, 'Going beyond the "Common Suspects": To Be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence', *Artificial Intelligence and Law*, 2023 <https://doi.org/10.1007/s10506-023-09347-w>.

[69] Partha Pratim Ray, 'A Review of <scp>TRiSM</Scp> Frameworks in Artificial Intelligence Systems: Fundamentals, Taxonomy, Use Cases, Key Challenges and Future Directions', *Expert Systems*, 43.3 (2026) <https://doi.org/10.1111/exsy.70213>.

[70] Dorian Knoblauch and Jürgen Großmann, 'Automating Lifecycle Compliance: A Continuous Assessment Framework for High-Risk and GPAI Obligations in the EU AI Act', in *Risikoanalyse Künstliche Intelligenz* (Berlin,

Closing the gap between abstract legal obligations and technical reality requires a proactive rather than reactive approach.[71] States must establish interoperable cross-border monitoring systems, particularly for the surveillance of autonomous systems with potential for criminal exploitation.[72] Legal requirements for risk assessments and impact evaluations must be accompanied by precise technical guidance rather than remaining at the level of general principle. This means providing explicit procedural specifications for scenarios involving decentralized control and swarm-based coordination, rather than treating them as edge cases. This also requires genuine collaborative governance: legal experts and technical specialists must jointly develop and regularly revise protocols, rather than working in disciplinary silos.[73] Only through this sustained interdisciplinary engagement can legal rules remain aligned with rapidly evolving cyber threats. Where states fail to align legal frameworks with technical realities, they create conditions in which increasingly sophisticated swarm intelligence attacks can evade both detection and enforcement. The only viable solution to this fragmented enforcement landscape is coordinated action across all relevant domains. This requires harmonizing technical standards, building investigative capacity, delivering concrete technical assistance, and maintaining ongoing training to prevent capability gaps from emerging.[74] When legal frameworks are grounded in technical reality, states are better positioned to trace threats, collaborate effectively across borders, and ensure that accountability is meaningfully enforced when cybercrimes occur. Without these changes, legal frameworks will remain declaratory rather than operational, while swarm-based attacks continue to identify and exploit every available gap.[75]

Opportunity for Innovative Legal Frameworks

Swarm intelligence presents a dual challenge: while it constitutes a genuine and growing threat, it simultaneously creates an impetus for the reform and strengthening of legal and regulatory systems globally.[76] When confronting coordinated multi-agent attacks, states cannot rely on conventional enforcement methods alone. Effective responses must integrate legal, technical, and operational strategies. Cross-border cooperation is not merely beneficial, it is operationally necessary. Rapid, coordinated responses supported by centralized information-sharing mechanisms and dedicated rapid-response teams are critical to disrupting attacks before they cause widespread harm. These mechanisms enable authorities to identify threats at an early stage and intervene before attacks reach full operational scale. Expedited evidence preservation and real-time digital traffic monitoring are equally essential, enabling investigators to trace coordinated swarm attacks even where criminal actors

Heidelberg: Springer Berlin Heidelberg, 2026), pp. 279–301 <https://doi.org/10.1007/978-3-662-72661-7_11>.

[71] Stuart Weinstein, 'Preventive Legal Technology for Micro-Entities: Improving Access to Justice in Commercial Contract Analysis', *International Review of Law, Computers & Technology*, 2025, 1–21 <https://doi.org/10.1080/13600869.2025.2602106>.

[72] Bhupinder Singh, 'Unmanned Aircraft Systems (UAS), Surveillance, Risk Management to Cybersecurity and Legal Regulation Landscape', in *Unmanned Aircraft Systems* (Wiley, 2024), pp. 313–54 <https://doi.org/10.1002/9781394230648.ch8>.

[73] Claudio Novelli and others, 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act', *Digital Society*, 3.1 (2024), 13 <https://doi.org/10.1007/s44206-024-00095-1>.

[74] Deanna House, Michelle Black and Lana Obradovic, 'Closing the Tech Gap: Updating Cyber and Technology Curriculum for Homeland Security Professionals', *Journal of Policing, Intelligence and Counter Terrorism*, 21.1 (2026), 1–21 <https://doi.org/10.1080/18335330.2025.2538880>.

[75] Chirag Ganguli and others, 'Nature-Inspired Swarm Optimization Paradigms for Securing Semantic Web Frameworks against DDoS Attacks: A Computational Approach', *Scientific Reports*, 15.1 (2025), 39020 <https://doi.org/10.1038/s41598-025-26058-1>.

[76] Anton Klarin and others, 'Understanding the Roots of Swarm Intelligence in Defence to Find the Path Forward', in *Thinking Swarms* (Cham: Springer Nature Switzerland, 2025), pp. 21–37 <https://doi.org/10.1007/978-3-031-82790-7_2>.

deliberately obscure their activities across jurisdictions.[77] The effectiveness of these measures is also contingent on the independence of oversight mechanisms. Depoliticized, independent regulatory bodies are better positioned to ensure impartial accountability and to provide victims of swarm attacks with meaningful access to legal redress.[78]

Regulatory frameworks must create structured pathways for safe innovation, ensuring that security standards keep pace with technological advancement.[79] Controlled testing environments and regulatory sandboxes enable authorities to observe the real-world behavior of autonomous systems, identify anomalous or high-risk patterns, and detect potential vectors of criminal exploitation before deployment.[80] Risk-based regulatory approaches enable states to concentrate enforcement resources where the probability or potential impact of a swarm attack is greatest. For systems assessed as presenting high risk, targeted regulations ensure that the most significant threats are addressed without disproportionately restricting the beneficial applications of AI. Clear transparency and documentation requirements enable post-incident investigation by allowing investigators to reconstruct the sequence of automated decisions, even when thousands of devices have operated in coordination.[81]

Embedding proactive technical standards within legal frameworks substantially strengthens enforcement effectiveness. Security-by-design obligations require developers to incorporate protective mechanisms at the architectural level, eliminating categories of vulnerability before they can be exploited. Streamlined information-sharing protocols between law enforcement agencies and service providers accelerate investigations and reduce dependence on slow traditional mutual legal assistance procedures.[82] The effectiveness of this integrated approach is demonstrated by large-scale multinational operations in which coordinated teams have dismantled extensive malicious networks with significantly greater speed. Multinational botnet disruption operations have succeeded in neutralizing hundreds of thousands of infected machines within days, demonstrating what is achievable when robust legal authority, technical capability, and coordinated international action are combined.[83]

Sustained capacity-building is essential to mounting an effective global response to complex multi-agent attacks. Investigators require applied, practical training not merely theoretical instruction in network forensics, distributed systems analysis, and AI-assisted

[77] Ranul Deelaka Thantilage, Gerry Buttner and Ray Genoe, 'Drone Forensics in Law Enforcement: Assessing Utilisation, Challenges, and Emerging Necessities', *Forensic Science International: Digital Investigation*, 55 (2025), 302003 <https://doi.org/10.1016/j.fsidi.2025.302003>.

[78] Muhammad Tayyab and others, 'Swarm Security: Tackling Threats in the Age of Drone Swarms', in Advances in Information Security, Privacy, and Ethics', ed. by Imdad Ali Shah and Noor Zaman Jhanjhi (IGI Global, 2024), pp. 324–42 <https://doi.org/10.4018/979-8-3693-0774-8.ch013>.

[79] Liron Pantanowitz and others, 'Regulatory Aspects of Artificial Intelligence and Machine Learning', *Modern Pathology*, 37.12 (2024), 100609 <https://doi.org/10.1016/j.modpat.2024.100609>.

[80] Birupaksha Biswas and Suhena Sarkar, 'Responsible Agentic Artificial Intelligence Governance: Risk, Safety, and Ethical Challenges in Autonomous Systems', *International Journal of Applied Resilience and Sustainability*, 2.2 (2026), 142–67 <https://doi.org/10.70593/deepsci.0202005>.

[81] Daniel Oliveira Cajueiro and Victor Rafael Rezende Celestino, 'A Comprehensive Review of Artificial Intelligence Regulation: Weighing Ethical Principles and Innovation', *Journal of Economy and Technology*, 4 (2026), 77–91 <https://doi.org/10.1016/j.ject.2025.07.001>.

[82] Rebecca Phythian, Stuart Kirby and Lauren Swan-Keig, 'Understanding How Law Enforcement Agencies Share Information in an Intelligence-Led Environment: How Operational Context Influences Different Approaches', *Policing: An International Journal*, 47.1 (2024), 112–25 <https://doi.org/10.1108/PIJPSM-06-2023-0073>.

[83] Thomas Nygren and others, 'The Seven Roles of Generative AI: Potential & Pitfalls in Combatting Misinformation', *Behavioral Science & Policy*, 2026 <https://doi.org/10.1177/23794607261417815>.

Contrarius, P-ISSN: **3090-9389**, E-ISSN: **3109-0931**

threat identification.[84] Harmonized technical standards for logging, evidence preservation, and anomaly detection further strengthen cross-jurisdictional investigative cooperation. This enables states to conduct joint investigations without being impeded by incompatible systems or inconsistent evidential standards. Providing resource-constrained states with technical assistance and access to appropriate investigative tools closes the enforcement gaps that criminal actors routinely exploit. Technology transfer and knowledge-sharing raise the baseline capacity of all participating states. When capabilities are aligned across jurisdictions, legal enforcement becomes more consistent, and criminal actors lose the asymmetric advantage they currently derive from uneven international cooperation.[85]

Legal systems must confront the inherent complexity of swarm intelligence attacks: establishing accountability in decentralized, multi-agent environments is not amenable to straightforward resolution.[86] When numerous autonomous agents operate in a decentralized manner, identifying which agent made which decision, and attributing responsibility for the collective outcome, poses fundamental legal and evidential challenges. Clear rules for tracking coordinated actions and rigorous evidence documentation procedures are therefore indispensable. Such rules support effective prosecution and provide courts with the structured evidentiary basis needed for fair adjudication. Individuals harmed by swarm-based cyber-attacks are entitled to genuine and accessible legal remedies, not merely declaratory commitments. Effective governance in this domain requires more than formal rules. It demands continuous vulnerability assessment, regular law enforcement training, and sustained dialogue between technical experts and policymakers.[87]

The integration of technical, legal, and operational strategies produces a substantially more resilient overall response to swarm-based cybercrime. Where high security standards, real-time threat monitoring, structured investigative procedures, and rapid international coordination are combined, the resulting system can respond to swarm attacks effectively. Laws that are genuinely grounded in transparency, accountability, and risk proportionality translate into operational tools that enable authorities to detect, trace, and neutralize complex swarm-based attacks. Effective governance in this domain, however, extends beyond formal legal rules. It requires continuous vulnerability assessment, regular law enforcement training, and sustained structured dialogue between technical experts and policymakers, the only means by which legal frameworks can remain aligned with the pace of technological change. When legal rules are grounded in operational reality, states can more effectively deter swarm intelligence attacks, provide meaningful protection to victims, and foster responsible technological development.[88]

Ultimately, when legal, technical, and operational strategies function in genuine alignment, the regulatory vulnerabilities that criminal actors depend upon can be

[84] Kwaku Gyamfi Boamah and others, 'Artificial Intelligence Integration in Cyber Incident Response Teams to Enable Faster Containment, Forensic Accuracy, and Resilient Business Continuity', *International Journal of Science and Research Archive*, 17.1 (2025), 1263–80 <https://doi.org/10.30574/ijsra.2025.17.1.2933>.

[85] Ke Li and others, 'Unified Multi-Agent Recovery Framework via Multi-Scale Diffusion and Dependency-Aware Hierarchical PPO for Resilience Enhancement', *Journal of Big Data*, 12.1 (2025), 226 <https://doi.org/10.1186/s40537-025-01285-5>.

[86] Ijaz Ahmed and others, 'Distributed Computing in Multi-Agent Systems: A Survey of Decentralized Machine Learning Approaches', *Computing*, 107.1 (2025), 2 <https://doi.org/10.1007/s00607-024-01356-0>.

[87] Michael Y. Lee, 'Enacting Decentralized Authority: The Practices and Limits of Moving Beyond Hierarchy', *Administrative Science Quarterly*, 69.3 (2024), 791–833 <https://doi.org/10.1177/00018392241257372>.

[88] Adnan Bin Amanat Ali and others, 'Cybersecurity Infrastructure Compliance Key Factors to Detect and Mitigate Malware Attacks in SMEs: A Systematic Literature Review', *Sage Open*, 15.1 (2025) <https://doi.org/10.1177/21582440251314671>.

systematically closed.[89] Active monitoring, clear technical standards, rigorous training, and robust accountability mechanisms collectively establish an environment capable of responding to the novel threats that swarm intelligence presents.[90] When these elements are effectively integrated, authorities are positioned to respond to coordinated attacks with speed and legal confidence, without compromising innovation or human rights protections. Aligning legal, technical, and enforcement dimensions enables a coordinated and enforceable response to swarm-based cybercrime. The result is a meaningful reduction in exploitable vulnerabilities and a substantially more resilient global cybersecurity posture.[91]

Implementation and Recommendations: Legal Guidelines

The effective domestic implementation of international legal obligations requires states to urgently develop targeted strategies for countering the exploitation of swarm intelligence in cybercrime and AI-related criminal activity. To this end, states should create specialized units within national law enforcement organizations that have access to the latest digital forensic technologies to analyze attacks that involve many autonomous agents or participants.[92] The specialized cyber units must develop protocols and procedures by which real-time traffic can be monitored, electronic evidence can be preserved quickly, and data can be exchanged with other countries in a reasonable amount of time. Law enforcement personnel should be well trained and have experience in the areas of detection, investigation, and attribution of crimes committed by distributed (i.e., many participants in a coordinated effort) autonomous (i.e., individuals who act or produce results without human support) agents and be able to respond to crimes committed across several jurisdictions at the same time. These new approaches will challenge traditional theories of criminal culpability because they assign liability or criminal responsibility based on the actions of groups or collective entities rather than on individual actors. To ensure that the new swarming-based crimes can be prosecuted effectively, law enforcement and courts must adapt their prosecutorial models to allow them to hold accountable those who acted as part of a swarm, while also reflecting the most current understanding of how to interpret the developing concepts of the law.[93]

Clear harmonization rules are required to align domestic practices across jurisdictions. States should adopt common technical procedures for logging, encryption, and evidence handling. Harmonized technical standards substantially facilitate cross-border cooperation. Manufacturers must be legally required to provide security updates throughout the operational lifespan of their products; the failure to do so creates the conditions in which devices are recruited into botnets.[94] Security-by-design principles must be embedded in

[89] Niloufar Bagherifam and others, 'Digital Regulatory Governance: The Role of RegTech and SupTech in Transforming Financial Oversight and Administrative Capacity', *International Journal of Financial Studies*, 13.4 (2025), 217 <https://doi.org/10.3390/ijfs13040217>.

[90] Yunes Alqudsi and Murat Makaraci, 'Exploring Advancements and Emerging Trends in Robotic Swarm Coordination and Control of Swarm Flying Robots: A Review', *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, 239.1 (2025), 180–204 <https://doi.org/10.1177/09544062241275359>.

[91] Muhammad Fakhrul Safitra, Muharman Lubis and Hanif Fakhrurroja, 'Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity', *Sustainability*, 15.18 (2023), 13369 <https://doi.org/10.3390/su151813369>.

[92] Shashwata Sahu and Saurabh Chandra, 'AI Applications in Global Counterterrorism Efforts: Challenges, Compliance, and Regulatory Gaps', in *Artificial Intelligence for Global Counter-Terrorism* (Springer Charm, 2025), pp. 17–35 <https://doi.org/10.1007/978-3-031-99235-3_2>.

[93] Suleman Lazarus, Adebayo Benedict Soares and Mark Button, 'Pathways, Pressure, and Profit: Adaptive Innovation and Strain in a Convicted Cybercrime Academy Called Hustle Kingdom', *Deviant Behavior*, 2025, 1–25 <https://doi.org/10.1080/01639625.2025.2551790>.

[94] Alana Maurushat and Kathy Nguyen, 'The Legal Obligation to Provide Timely Security Patching and Automatic Updates', *International Cybersecurity Law Review*, 3.2 (2022), 437–65 <https://doi.org/10.1365/s43439-022-00059-6>.

regulatory policy as a mandatory requirement, not treated as an optional feature. Regulatory sandboxes also serve an important function, providing supervised environments for testing AI systems against risk and transparency requirements prior to deployment. Collectively, these measures reduce exploitable vulnerabilities, strengthen accountability mechanisms, and improve protections for victims. However, inconsistent enforcement across states undermines the integrity of the entire framework. This underscores the necessity of binding international standards and enforceable inter-state agreements. Policy adaptation is not a one-time exercise; it requires sustained, structured collaboration among technical experts, legislators, and the judiciary.[95]

In practice, harmonized frameworks facilitate the rapid detection and disruption of swarm-based cybercrime, providing meaningful protection for critical infrastructure such as power grids and banking systems, as well as individuals' personal data.[96] Victims gain clearer pathways to legal assistance. Law enforcement can apply well-defined investigative procedures when handling complex distributed attacks.[97] Legislators can employ harmonized frameworks to respond promptly and update legal instruments in step with technological developments.[98] However, significant challenges remain resource and capability disparities across states persist, and attribution in decentralized networks continues to present fundamental legal and technical difficulties. Furthermore, the rapid pace of AI and swarm technology development means those legal rules can lag, creating temporary but exploitable enforcement gaps.[99]

The recommended measures include the establishment of international rapid-response teams combining law enforcement officers, cybersecurity professionals, and AI specialists, enabling swift intervention in cross-border swarm attacks. Additionally, existing regulatory systems should be modified to integrate technical standards with legal accountability mechanisms, ensuring that autonomous systems cannot evade meaningful oversight.[100] The proposed guidelines call for continuous auditing and regular impact assessments for AI systems operating in critical sectors. Future research should develop methodologies for tracing distributed attacks, establish standardized forensic tools, and construct risk assessment frameworks specifically calibrated to decentralized autonomous systems. Research into both the social and technical dimensions of swarm-based cybercrime, including organizational behavior and human factors will inform more effective policy design and improve operational outcomes.[101]

[95] Patrizio Monfardini, Silvia Macchia and Davide Eltrudis, 'Reforming Resistant KIPOs to Achieve Justice: Can the Judiciary System Hybridise?', *Journal of Public Budgeting, Accounting & Financial Management*, 36.5 (2024), 580–96 <https://doi.org/10.1108/JPBAFM-07-2023-0132>.

[96] Memoona Sadaf and others, 'Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects', *Technologies*, 11.5 (2023), 117 <https://doi.org/10.3390/technologies11050117>.

[97] Vladov and others.

[98] Qiang REN and Jing DU, 'Harmonizing Innovation and Regulation: The EU Artificial Intelligence Act in the International Trade Context', *Computer Law & Security Review*, 54 (2024), 106028 <https://doi.org/10.1016/j.clsr.2024.106028>.

[99] Mohamad Sheikho Al Jasem, Trevor De Clark and Ajay Kumar Shrestha, 'Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems', *Information*, 16.9 (2025), 765 <https://doi.org/10.3390/info16090765>.

[100] Dharmendra Chauhan and others, 'Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies', *IEEE Access*, 13 (2025), 53476–505 <https://doi.org/10.1109/ACCESS.2025.3550338>.

[101] Sangita Baruah, Dhruba Jyoti Borah and Vaskar Deka, 'Reviewing Various Feature Selection Techniques in Machine Learning-based Botnet Detection', *Concurrency and Computation: Practice and Experience*, 36.12 (2024) <https://doi.org/10.1002/cpe.8076>.

The combination of technical tools with legal mechanisms produces effective strategies for preventing, detecting, and prosecuting swarm intelligence attacks. This comprehensive approach not only strengthens global cybersecurity resilience but also enhances inter-state cooperation and extends protection to individuals and organizations facing threats from coordinated autonomous agent systems. When states adopt common standards, invest in threat-specific training, and develop their defensive capabilities in coordination, the foundation for durable, effective enforcement is established, one that accommodates innovation while preserving meaningful accountability. Without these targeted interventions, criminal actors will continue to identify and exploit emerging legal gaps. This is why continuous policy updating, the reassessment of outdated legal models, and sustained research investment are indispensable to maintaining effective legal responses to swarm intelligence in distributed systems.[102]

Conclusion

This study concludes that, *first,* the development of swarm intelligence has generated highly complex and distributed forms of cybercrime, creating significant challenges for legal attribution as operations are carried out by autonomous agents across multiple jurisdictions without clearly identifiable perpetrators. *Second,* existing detection technologies and law enforcement capacities lag the speed and scale of swarm-based attacks, which can be executed rapidly and leave minimal forensic traces. *Third,* there is a structural gap between current legal frameworks and technical realities, reflected in the absence of standardized technical protocols, limited cybersecurity capacity in certain states, and the inadequacy of existing international cooperation mechanisms. Therefore, this study underscores the urgent need for technically grounded legal reform, emphasizing stronger collaboration between policymakers, law enforcement authorities, and technical experts to develop more adaptive and effective regulatory frameworks for addressing swarm-based cyber threats. These recommendations have direct practical consequences for the protection of critical infrastructure, financial systems, and personal data against large-scale, coordinated cyber-attacks. When states adopt harmonized technical procedures and investigative methods and actively support the capacity-building of partner nations, collective resilience is substantially strengthened. The integration of legal frameworks with technical tools enables authorities to detect and disrupt multi-agent attacks more effectively, while also improving victims' access to legal recourse. Looking ahead, emerging developments such as quantum computing will further complicate forensic attribution and investigative tracing. Researchers must investigate decentralized governance models and novel legal frameworks capable of addressing threats driven by swarm intelligence. The immediate priorities are clear: existing international agreements must be updated, technical standards must be harmonized across jurisdictions, and international rapid-response teams combining legal expertise, technical knowledge, and operational capacity must be established. There remains a genuine opportunity to strengthen the international legal architecture before swarm intelligence capabilities advance beyond the reach of effective legal and technical countermeasures.

References

Abdelaziz, Dalia Kadry Ahmed, 'Criminal Liability for the Misuse and Crimes Committed by AI: A Comparative Analysis of Legislation and International Conventions', *Journal of Infrastructure Policy and Development*, 9 (2025), 10722 <https://doi.org/10.24294/jipd10722>

Abualigah, Laith, Deborah Falcone and Agostino Forestiero, 'Swarm Intelligence to Face IoT Challenges', ed. by Abdul Rehman Javed, *Computational Intelligence and Neuroscience*, 2023 (2023) <https://doi.org/10.1155/2023/4254194>

[102] Petar Radanliev, 'Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing', *Journal of Cyber Security Technology*, 9.1 (2025), 28–78 <https://doi.org/10.1080/23742917.2024.2312671>.

Contrarius, P-ISSN: **3090-9309**, E-ISSN: **3109-0931**

Adel, Amr and Mohammad Norouzifard, 'Weaponization of the Growing Cybercrimes inside the Dark Net: The Question of Detection and Application', *Big Data and Cognitive Computing*, 8 (2024), 91 <https://doi.org/10.3390/bdcc8080091>

Admass, Wasyihun Sema, Yirga Yayeh Munaye and Abebe Abeshu Diro, 'Cyber Security: State of the Art, Challenges and Future Directions', *Cyber Security and Applications*, 2 (2024), 100031 <https://doi.org/10.1016/j.csa.2023.100031>

Ahmed, Ijaz, Miswar Akhtar Syed, Muhammad Maaruf and Muhammad Khalid, 'Distributed Computing in Multi-Agent Systems: A Survey of Decentralized Machine Learning Approaches', *Computing*, 107 (2025), 2 <https://doi.org/10.1007/s00607-024-01356-0>

Al-Busaidi, Adil S, Raghu Raman, Laurie Hughes, Mousa Ahmed Albashrawi, Tegwen Malik, Yogesh K Dwivedi, and others, 'Redefining Boundaries in Innovation and Knowledge Domains: Investigating the Impact of Generative Artificial Intelligence on Copyright and Intellectual Property Rights', *Journal of Innovation & Knowledge*, 9 (2024), 100630 <https://doi.org/10.1016/j.jik.2024.100630>

Ali, Adnan Bin Amanat, Ramesh Kumar Ayyasamy, Rehan Akbar, Abdulkarim Kanaan Jebna and Kiran Adnan, 'Cybersecurity Infrastructure Compliance Key Factors to Detect and Mitigate Malware Attacks in SMEs: A Systematic Literature Review', *Sage Open*, 15 (2025) <https://doi.org/10.1177/21582440251314671>

Ali, Mahrus, Andi Muliyono and Syarif Nurhidayat, 'The Application of a Human Rights Approach toward Crimes of Corruption: Analyzing Anti-Corruption Regulations and Judicial Decisions', *Laws*, 12 (2023), 68 <https://doi.org/10.3390/laws12040068>

Alqudsi, Yunes and Murat Makaraci, 'Exploring Advancements and Emerging Trends in Robotic Swarm Coordination and Control of Swarm Flying Robots: A Review', *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, 239 (2025), 180–204 <https://doi.org/10.1177/09544062241275359>

———, 'UAV Swarms: Research, Challenges, and Future Directions', *Journal of Engineering and Applied Science*, 72 (2025), 12 <https://doi.org/10.1186/s44147-025-00582-3>

Alsadie, Deafallah, 'Cybersecurity and Artificial Intelligence in Unmanned Aerial Vehicles: Emerging Challenges and Advanced Countermeasures', ed. by Jiwei Tian, *IET Information Security*, 2025 (2025) <https://doi.org/10.1049/ise2/2046868>

Alshabibi, Munirah Maher, Alanood Khaled Bu dookhi and MM Hafizur Rahman, 'Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review', *Computers*, 13 (2024), 213 <https://doi.org/10.3390/computers13080213>

Anumbe, Noble, Clint Saidy and Ramy Harik, 'A Primer on the Factories of the Future', *Sensors*, 22 (2022), 5834 <https://doi.org/10.3390/s22155834>

Bagherifam, Niloufar, Sajjad Naghdi, Vahid Ahmadian, Alireza Fazlzadeh and Milad Baghalzadeh Shishehgarkhaneh, 'Digital Regulatory Governance: The Role of RegTech and SupTech in Transforming Financial Oversight and Administrative Capacity', *International Journal of Financial Studies*, 13 (2025), 217 <https://doi.org/10.3390/ijfs13040217>

Bakirov, Akhat and Ibragim Suleimenov, 'Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare', *Computers*, 14 (2025), 410 <https://doi.org/10.3390/computers14100410>

Baranchuk, Mikhail, Vijay Bolina, Christian de Witt, Lewis Hammond, Sumeet Motwani, Martin Strohmeier, and others, 'Secret Collusion among AI Agents: Multi-Agent Deception via Steganography', in *Advances in Neural Information Processing Systems 37* (San Diego, California, USA: Neural Information Processing Systems Foundation, Inc. (NeurIPS), 2024), pp. 73439–86 <https://doi.org/10.52202/079017-2336>

Bartoli, Laura, 'Cybersecurity and the Fight against Cybercrime: Partners or Competitors?', *European Journal of Risk Regulation*, 16 (2025), 498–513 <https://doi.org/10.1017/err.2025.31>

Baruah, Sangita, Dhruba Jyoti Borah and Vaskar Deka, 'Reviewing Various Feature Selection Techniques in Machine Learning-based Botnet Detection', *Concurrency and Computation: Practice and*

Experience, 36 (2024) <https://doi.org/10.1002/cpe.8076>

Bhumichai, Dhanasak, Christos Smiliotopoulos, Ryan Benton, Georgios Kambourakis and Dimitrios Damopoulos, 'The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead', *Information*, 15 (2024), 268 <https://doi.org/10.3390/info15050268>

Birthriya, Santosh Kumar, Priyanka Ahlawat and Ankit Kumar Jain, 'A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies', *Journal of Applied Security Research*, 20 (2025), 244–92 <https://doi.org/10.1080/19361610.2024.2372986>

Biswas, Birupaksha and Suhena Sarkar, 'Responsible Agentic Artificial Intelligence Governance: Risk, Safety, and Ethical Challenges in Autonomous Systems', *International Journal of Applied Resilience and Sustainability*, 2 (2026), 142–67 <https://doi.org/10.70593/deepsci.0202005>

Boamah, Kwaku Gyamfi, AFUA Asante, Ashley Timean and Kwadwo Fening Okai, 'Artificial Intelligence Integration in Cyber Incident Response Teams to Enable Faster Containment, Forensic Accuracy, and Resilient Business Continuity', *International Journal of Science and Research Archive*, 17 (2025), 1263–80 <https://doi.org/10.30574/ijsra.2025.17.1.2933>

Brunet-Jailly, Emmanuel, 'Cross-Border Cooperation: A Global Overview', *Alternatives: Global, Local, Political*, 47 (2022), 3–17 <https://doi.org/10.1177/03043754211073463>

Cajueiro, Daniel Oliveira and Victor Rafael Rezende Celestino, 'A Comprehensive Review of Artificial Intelligence Regulation: Weighing Ethical Principles and Innovation', *Journal of Economy and Technology*, 4 (2026), 77–91 <https://doi.org/10.1016/j.ject.2025.07.001>

Chauhan, Dharmendra, Harshil Kagathara, Hiren Mewada, Sagar Patel, Sagar Kavaiya and Gordana Barb, 'Nation's Defense: A Comprehensive Review of Anti-Drone Systems and Strategies', *IEEE Access*, 13 (2025), 53476–505 <https://doi.org/10.1109/ACCESS.2025.3550338>

Copeland, Damian, Philip Sammons and Lauren Sanders, 'An Approach to the Legal Review of Autonomous Swarms', in *Thinking Swarms* (Cham: Springer Nature Switzerland, 2025), pp. 171–86 <https://doi.org/10.1007/978-3-031-82790-7_10>

Demertzi, Vasiliki, Stavros Demertzis and Konstantinos Demertzis, 'An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities', *Applied Sciences*, 13 (2023), 790 <https://doi.org/10.3390/app13020790>

Duan, Haibin, Mengzhen Huo and Yanming Fan, 'From Animal Collective Behaviors to Swarm Robotic Cooperation', *National Science Review*, 10 (2023) <https://doi.org/10.1093/nsr/nwad040>

Farber, Shai, 'The Evolving Nexus of Cybercrime and Terrorism: A Systematic Review of Convergence and Policy Implications', *Security Journal*, 38 (2025), 29 <https://doi.org/10.1057/s41284-025-00471-7>

Finch, William Walter and Marya Butt, 'Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Systematic Review', *Journal of Cybersecurity and Privacy*, 5 (2025), 101 <https://doi.org/10.3390/jcp5040101>

Furnari, Salvatore Luciano and Chiara Villani, 'Regulation of Financial Protocol DAOs: Addressing the Problems of Decentralization and AI Governance', in *Decentralized Autonomous Organizations—Governance, Technology, and Legal Perspectives. DAWO 2025. Springer Proceedings in Business and Economics* (Springer Charm, 2026), pp. 115–34 <https://doi.org/10.1007/978-3-032-03273-7_7>

Ganguli, Chirag, Shishir Kumar Shandilya, Ivan Izonin and Lesia Hentosh, 'Nature-Inspired Swarm Optimization Paradigms for Securing Semantic Web Frameworks against DDoS Attacks: A Computational Approach', *Scientific Reports*, 15 (2025), 39020 <https://doi.org/10.1038/s41598-025-26058-1>

Grigaliūnas, Šarūnas, Michael Schmidt, Rasa Brūzgienė, Panayiota Smyrli, Stephanos Andreou and Audrius Lopata, 'Holistic Information Security Management and Compliance Framework', *Electronics*, 13 (2024), 3955 <https://doi.org/10.3390/electronics13193955>

Hadi, Wael, Ala Hamarsheh, Ahmad Al-Qerem and Amjad Aldweesh, 'Swarm AI for Distributed Cyber Defense and Autonomous Threat Detection' (IGI Global, 2025), pp. 185–208 <https://doi.org/10.4018/979-8-3373-0954-5.ch007>

Hanif, Muhammad, Ehsan Ullah Munir, Muhammad Maaz Rehan, Saima Gulzar Ahmad, Kashif Ayyub and Naeem Ramzan, 'Orchestrating Machine Learning Models in a Swarm Architecture for IoT Inline Malware Detection', *Scientific Reports*, 16 (2025), 187 <https://doi.org/10.1038/s41598-025-28859-w>

Hasbach, Jonas D and Maren Bennewitz, 'The Design of Self-Organizing Human–Swarm Intelligence', *Adaptive Behavior*, 30 (2022), 361–86 <https://doi.org/10.1177/10597123211017550>

Hassel, Henrik and Alexander Cedergren, 'Integrating Risk Assessment and Business Impact Assessment in the Public Crisis Management Sector', *International Journal of Disaster Risk Reduction*, 56 (2021), 102136 <https://doi.org/10.1016/j.ijdrr.2021.102136>

Hatzivasilis, George, Eftychia Lakka, Manos Athanatos, Sotiris Ioannidis, Grigoris Kalogiannis, Manolis Chatzimpyrros, and others, 'Swarm-Intelligence for the Modern ICT Ecosystems', *International Journal of Information Security*, 23 (2024), 2951–75 <https://doi.org/10.1007/s10207-024-00869-1>

House, Deanna, Michelle Black and Lana Obradovic, 'Closing the Tech Gap: Updating Cyber and Technology Curriculum for Homeland Security Professionals', *Journal of Policing, Intelligence and Counter Terrorism*, 21 (2026), 1–21 <https://doi.org/10.1080/18335330.2025.2538880>

Iftikhar, Saman, 'Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures', *PeerJ Computer Science*, 10 (2024), e1772 <https://doi.org/10.7717/peerj-cs.1772>

Jaelani, Abdul Kadir, Anila Rabbani and Muhammad Jihadul Hayat, 'Land Reform Policy in Determining Abandoned Land for Halal Tourism Destination Management Based on Fiqh Siyasah', *El-Mashlahah*, 14 (2024), 211–38 <https://doi.org/10.23971/el-mashlahah.v14i1.8051>

Al Jasem, Mohamad Sheikho, Trevor De Clark and Ajay Kumar Shrestha, 'Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems', *Information*, 16 (2025), 765 <https://doi.org/10.3390/info16090765>

Jørgensen, Bo Nørregaard and Zheng Grace Ma, 'Digital Twin of the European Electricity Grid: A Review of Regulatory Barriers, Technological Challenges, and Economic Opportunities', *Applied Sciences*, 15 (2025), 6475 <https://doi.org/10.3390/app15126475>

Klarin, Anton, Pi-Shen Seet, Janice Jones, Michael N Johnstone, Helen Cripps, Jalleh Sharafizad, and others, 'Understanding the Roots of Swarm Intelligence in Defence to Find the Path Forward', in *Thinking Swarms* (Cham: Springer Nature Switzerland, 2025), pp. 21–37 <https://doi.org/10.1007/978-3-031-82790-7_2>

Knoblauch, Dorian and Jürgen Großmann, 'Automating Lifecycle Compliance: A Continuous Assessment Framework for High-Risk and GPAI Obligations in the EU AI Act', in *Risikoanalyse Künstliche Intelligenz* (Berlin, Heidelberg: Springer Berlin Heidelberg, 2026), pp. 279–301 <https://doi.org/10.1007/978-3-662-72661-7_11>

Kose, Kubra, Nuri Alperen Kose and Fan Liang, 'Securing Unmanned Devices in Critical Infrastructure: A Survey of Hardware, Network, and Swarm Intelligence', *Electronics*, 15 (2026), 1204 <https://doi.org/10.3390/electronics15061204>

Kumar, N Satheesh, V Ramakrishna, M V. Kamal, K Sathish Kumar, V Shiva Narayana Reddy and Perumalla Janaki Ramulu, 'Swarm-Based Intelligent Models for Developing Cybersecurity Frameworks with IDS', *Scientific Reports*, 16 (2026), 3492 <https://doi.org/10.1038/s41598-025-30223-x>

Lather, Mahipal, Sachin Bhardwaj and Vandana Ajay Kumar, 'Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms', *Productivity*, 65 (2024), 1–10 <https://doi.org/10.32381/PROD.2024.65.01.1>

Lazarus, Suleman, Adebayo Benedict Soares and Mark Button, 'Pathways, Pressure, and Profit:

Adaptive Innovation and Strain in a Convicted Cybercrime Academy Called Hustle Kingdom', *Deviant Behavior*, 2025, 1–25 <https://doi.org/10.1080/01639625.2025.2551790>

Lee, Michael Y, 'Enacting Decentralized Authority: The Practices and Limits of Moving Beyond Hierarchy', *Administrative Science Quarterly*, 69 (2024), 791–833 <https://doi.org/10.1177/00018392241257372>

Leon, Maikel, 'Lifecycle-Based Governance to Build Reliable Ethical AI Systems', *Systems Research and Behavioral Science*, 2026 <https://doi.org/10.1002/sres.70014>

Li, Ke, Yuqing Lin, Xiaolong Su, Aifeng Liu, Jiancheng Liu, Wanlong Qi, and others, 'Unified Multi-Agent Recovery Framework via Multi-Scale Diffusion and Dependency-Aware Hierarchical PPO for Resilience Enhancement', *Journal of Big Data*, 12 (2025), 226 <https://doi.org/10.1186/s40537-025-01285-5>

Li, Yuchong and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments', *Energy Reports*, 7 (2021), 8176–86 <https://doi.org/10.1016/j.egyr.2021.08.126>

Maurushat, Alana and Kathy Nguyen, 'The Legal Obligation to Provide Timely Security Patching and Automatic Updates', *International Cybersecurity Law Review*, 3 (2022), 437–65 <https://doi.org/10.1365/s43439-022-00059-6>

Mei, Mengqing, Songsong Zhang, Zhiwei Ye, Mingwei Wang, Wen Zhou, Jia Yang, and others, 'A Cooperative Hybrid Breeding Swarm Intelligence Algorithm for Feature Selection', *Pattern Recognition*, 169 (2026), 111901 <https://doi.org/10.1016/j.patcog.2025.111901>

Miller, Seumas, Terry Bossomaier, *Cybersecurity, Ethics, and Collective Responsibility* (Oxford University PressNew York, 2024) <https://doi.org/10.1093/oso/9780190058135.001.0001>

Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz and Niovi Vavoula, 'Data Retention and the Future of Large-scale Surveillance: The Evolution and Contestation of Judicial Benchmarks', *European Law Journal*, 29 (2023), 176–211 <https://doi.org/10.1111/eulj.12417>

Monfardini, Patrizio, Silvia Macchia and Davide Eltrudis, 'Reforming Resistant KIPOs to Achieve Justice: Can the Judiciary System Hybridise?', *Journal of Public Budgeting, Accounting & Financial Management*, 36 (2024), 580–96 <https://doi.org/10.1108/JPBAFM-07-2023-0132>

Mukred, Muaadh, Umi Asma' Mokhtar, Fahad Abdullah Moafa, Abdu Gumaei, Ali Safaa Sadiq and Abdulaleem Al-Othmani, 'The Roots of Digital Aggression: Exploring Cyber-Violence through a Systematic Literature Review', *International Journal of Information Management Data Insights*, 4 (2024), 100281 <https://doi.org/10.1016/j.jjimei.2024.100281>

Mustafa, Zaid, Rashid Amin, Hamza Aldabbas and Naeem Ahmed, 'Intrusion Detection Systems for Software-Defined Networks: A Comprehensive Study on Machine Learning-Based Techniques', *Cluster Computing*, 27 (2024), 9635–61 <https://doi.org/10.1007/s10586-024-04430-6>

Nasir, Muhammad Hassan, Salman A Khan, Muhammad Mubashir Khan and Mahawish Fatima, 'Swarm Intelligence Inspired Intrusion Detection Systems — A Systematic Literature Review', *Computer Networks*, 205 (2022), 108708 <https://doi.org/10.1016/j.comnet.2021.108708>

Nishnianidze, Anri, 'Some New Challenges of Cybercrime and the Reason for Its Outdated Regulations', *European Scientific Journal, ESJ*, 19 (2023), 92 <https://doi.org/10.19044/esj.2023.v19n39p92>

Novelli, Claudio, Federico Casolari, Antonino Rotolo, Mariarosaria Taddeo and Luciano Floridi, 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act', *Digital Society*, 3 (2024), 13 <https://doi.org/10.1007/s44206-024-00095-1>

Nygren, Thomas, Emily R Spearing, Nicolas Fay, Davide Vega, Isabella I Hardwick, Jon Roozenbeek, and others, 'The Seven Roles of Generative AI: Potential & Pitfalls in Combatting Misinformation', *Behavioral Science & Policy*, 2026 <https://doi.org/10.1177/23794607261417815>

Ofusori, Lizzy, Tebogo Bokaba and Siyabonga Mhlongo, 'Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction', *Applied Artificial Intelligence*, 38 (2024)

<https://doi.org/10.1080/08839514.2024.2439609>

Pantanowitz, Liron, Matthew Hanna, Joshua Pantanowitz, Joe Lennerz, Walter H Henricks, Peter Shen, and others, 'Regulatory Aspects of Artificial Intelligence and Machine Learning', *Modern Pathology*, 37 (2024), 100609 <https://doi.org/10.1016/j.modpat.2024.100609>

Phythian, Rebecca, Stuart Kirby and Lauren Swan-Keig, 'Understanding How Law Enforcement Agencies Share Information in an Intelligence-Led Environment: How Operational Context Influences Different Approaches', *Policing: An International Journal*, 47 (2024), 112–25 <https://doi.org/10.1108/PIJPSM-06-2023-0073>

Primiero, Giuseppe, Elio Tuci, Jacopo Tagliabue and Eliseo Ferrante, 'Swarm Attack: A Self-Organized Model to Recover from Malicious Communication Manipulation in a Swarm of Simple Simulated Agents' (Springer Charm, 2018), pp. 213–24 <https://doi.org/10.1007/978-3-030-00533-7_17>

Qiqieh, Issa, Omar Alzubi, Jafar Alzubi, KC Sreedhar and Ala' M Al-Zoubi, 'An Intelligent Cyber Threat Detection: A Swarm-Optimized Machine Learning Approach', *Alexandria Engineering Journal*, 115 (2025), 553–63 <https://doi.org/10.1016/j.aej.2024.12.039>

Radanliev, Petar, 'Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing', *Journal of Cyber Security Technology*, 9 (2025), 28–78 <https://doi.org/10.1080/23742917.2024.2312671>

Rajendra, Josephine Bhavani and Ambikai S Thuraisingam, 'The Role of Explainability and Human Intervention in AI Decisions: Jurisdictional and Regulatory Aspects', *Information & Communications Technology Law*, 2025, 1–32 <https://doi.org/10.1080/13600834.2025.2537514>

Ray, Partha Pratim, 'A Review of <scp>TRiSM</Scp> Frameworks in Artificial Intelligence Systems: Fundamentals, Taxonomy, Use Cases, Key Challenges and Future Directions', *Expert Systems*, 43 (2026) <https://doi.org/10.1111/exsy.70213>

Reddy, Dukka Karun Kumar, Janmenjoy Nayak, HS Behera, Vimal Shanmuganathan, Wattana Viriyasitavat and Gaurav Dhiman, 'A Systematic Literature Review on Swarm Intelligence Based Intrusion Detection System: Past, Present and Future', *Archives of Computational Methods in Engineering*, 31 (2024), 2717–84 <https://doi.org/10.1007/s11831-023-10059-2>

REN, Qiang and Jing DU, 'Harmonizing Innovation and Regulation: The EU Artificial Intelligence Act in the International Trade Context', *Computer Law & Security Review*, 54 (2024), 106028 <https://doi.org/10.1016/j.clsr.2024.106028>

Rodrigues, Rowena, 'Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities', *Journal of Responsible Technology*, 4 (2020), 100005 <https://doi.org/10.1016/j.jrt.2020.100005>

Rofi'ah, Khusniati, Martha Eri Safira and Muhammad Ikhlas Rosele, 'The Effectiveness of Accelerating Halal Product Certification: Regulations and Companions', *Journal of Human Rights, Culture and Legal System*, 4 (2024), 449–76 <https://doi.org/10.53955/jhcls.v4i2.203>

Sachoulidou, Athina, 'Going beyond the "Common Suspects": To Be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence', *Artificial Intelligence and Law*, 2023 <https://doi.org/10.1007/s10506-023-09347-w>

Sadaf, Memoona, Zafar Iqbal, Abdul Javed, Irum Saba, Moez Krichen, Sajid Majeed, and others, 'Connected and Automated Vehicles: Infrastructure, Applications, Security, Critical Challenges, and Future Aspects', *Technologies*, 11 (2023), 117 <https://doi.org/10.3390/technologies11050117>

Saeed, Rashid A, Mohamed Omri, S Abdel-Khalek, Elmustafa Sayed Ali and Maged Faihan Alotaibi, 'Optimal Path Planning for Drones Based on Swarm Intelligence Algorithm', *Neural Computing and Applications*, 34 (2022), 10133–55 <https://doi.org/10.1007/s00521-022-06998-9>

Safitra, Muhammad Fakhrul, Muharman Lubis and Hanif Fakhrurroja, 'Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity', *Sustainability*, 15 (2023), 13369 <https://doi.org/10.3390/su151813369>

Sahu, Shashwata and Saurabh Chandra, 'AI Applications in Global Counterterrorism Efforts:

Contrarius, P-ISSN: **3090-9309**, E-ISSN: **3109-0931**

Challenges, Compliance, and Regulatory Gaps', in *Artificial Intelligence for Global Counter-Terrorism* (Springer Charm, 2025), pp. 17–35 <https://doi.org/10.1007/978-3-031-99235-3_2>

Schäferling, Stefan, 'The Case for a Right Against Automated Decision-Making', in *Governmental Automated Decision-Making and Human Rights. Law, Governance and Technology Serie* (Springer Charm, 2023), pp. 231–83 <https://doi.org/10.1007/978-3-031-48125-3_7>

Shen, Danqing, Xiaoming Chen, Wenhai Qi and Lisha Meng, 'Task Allocation for UAV Swarms under Communication Attacks: An Approach Based on Game Theory and Negotiation Mechanism', *Journal of the Franklin Institute*, 362 (2025), 107417 <https://doi.org/10.1016/j.jfranklin.2024.107417>

Shurson, Jessica, 'The Balance of Efficiency and Fundamental Rights in the EU E-Evidence Regulation', *New Journal of European Criminal Law*, 16 (2025), 278–99 <https://doi.org/10.1177/20322844251357090>

Simmler, Monika, Giulia Canova and Kuno Schedler, 'Smart Criminal Justice: Phenomena and Normative Requirements', *International Review of Administrative Sciences*, 89 (2023), 415–32 <https://doi.org/10.1177/00208523211039740>

Singh, Bhupinder, 'Unmanned Aircraft Systems (UAS), Surveillance, Risk Management to Cybersecurity and Legal Regulation Landscape', in *Unmanned Aircraft Systems* (Wiley, 2024), pp. 313–54 <https://doi.org/10.1002/9781394230648.ch8>

Szadeczky, Tamas and Zsolt Bederna, 'Risk, Regulation, and Governance: Evaluating Artificial Intelligence across Diverse Application Scenarios', *Security Journal*, 38 (2025), 35 <https://doi.org/10.1057/s41284-025-00495-z>

Tan, Ying and Zhong-yang Zheng, 'Research Advance in Swarm Robotics', *Defence Technology*, 9 (2013), 18–39 <https://doi.org/10.1016/j.dt.2013.03.001>

Tayyab, Muhammad, Majid Mumtaz, Syeda Mariam Muzammal, Noor Zaman Jhanjhi and Fatimah-Tuz-Zahra, 'Swarm Security: Tackling Threats in the Age of Drone Swarms', in Advances in Information Security, Privacy, and Ethics', ed. by Imdad Ali Shah and Noor Zaman Jhanjhi (IGI Global, 2024), pp. 324–42 <https://doi.org/10.4018/979-8-3693-0774-8.ch013>

Thantilage, Ranul Deelaka, Gerry Buttner and Ray Genoe, 'Drone Forensics in Law Enforcement: Assessing Utilisation, Challenges, and Emerging Necessities', *Forensic Science International: Digital Investigation*, 55 (2025), 302003 <https://doi.org/10.1016/j.fsidi.2025.302003>

Tuptuk, Nilufer and Stephen Hailes, 'Security of Smart Manufacturing Systems', *Journal of Manufacturing Systems*, 47 (2018), 93–106 <https://doi.org/10.1016/j.jmsy.2018.04.007>

Vladov, Serhii, Oksana Mulesa, Victoria Vysotska, Petro Horvat, Nataliia Paziura, Oleksandra Kolobylina, and others, 'Method for Detecting Low-Intensity DDoS Attacks Based on a Combined Neural Network and Its Application in Law Enforcement Activities', *Data*, 10 (2025), 173 <https://doi.org/10.3390/data10110173>

WANG, Chao, Shuyuan ZHANG, Tianhang MA, Yuetong XIAO, Michael Zhiqiang CHEN and Lei WANG, 'Swarm Intelligence: A Survey of Model Classification and Applications', *Chinese Journal of Aeronautics*, 38 (2025), 102982 <https://doi.org/10.1016/j.cja.2024.03.019>

Wang, Yan, Hao Wang and Yanghuang Cao, 'Comprehensive Review of Storage Optimization Techniques in Blockchain Systems', *Applied Sciences*, 15 (2024), 243 <https://doi.org/10.3390/app15010243>

Weinstein, Stuart, 'Preventive Legal Technology for Micro-Entities: Improving Access to Justice in Commercial Contract Analysis', *International Review of Law, Computers & Technology*, 2025, 1–21 <https://doi.org/10.1080/13600869.2025.2602106>

Xu, Minghai, Li Cao, Dongwan Lu, Zhongyi Hu and Yinggao Yue, 'Application of Swarm Intelligence Optimization Algorithms in Image Processing: A Comprehensive Review of Analysis, Synthesis, and Optimization', *Biomimetics*, 8 (2023), 235 <https://doi.org/10.3390/biomimetics8020235>

Yaacoub, Jean Paul A, Hassan N Noura, Ola Salman and Khaled Chahine, 'Toward Secure Smart

Grid Systems: Risks, Threats, Challenges, and Future Directions', *Future Internet*, 17 (2025), 318 <https://doi.org/10.3390/fi17070318>

Zaizi, Fatima Ezzahra, Sara Qassimi and Said Rakrak, 'Multi-Objective Optimization with Recommender Systems: A Systematic Review', *Information Systems*, 117 (2023), 102233 <https://doi.org/10.1016/j.is.2023.102233>

Contrarius, P-ISSN: **3090-9309**, E-ISSN: **3109-0931**