Customary Law Journal, ICLSSEE Special Collection 2026, *Page*: 1-9

Legal Accountability for the Utilization of Autonomous Cyber Defense Systems in Cybersecurity Governance

Yovid*, Marhaeni Ria Siombo

Universitas Borobudur, Jakarta, Indonesia, yovidhalim@gmail.com

Universitas Borobudur, Jakarta, Indonesia, , riasiombo@yahoo.com

DOI:
https://doi.org/10.47134/jcl.v3i3.1.5871

*Correspondence: Yovid

Email: yovidhalim@gmail.com

Received: 29/05/2026
Accepted: 30/06/2026
Published: 30/06/2026

Abstract: *The increasingly complex development of cyber threats has driven the use of artificial intelligence-based cyber defense technology capable of autonomous operation, known as Autonomous Cyber Defense Systems (ACDS). These systems offer high efficiency and speed of response, but also raise new legal issues related to accountability for actions resulting from algorithmic decisions. This study aims to analyze the nature of legal accountability problems in the use of ACDS and examine the limitations of the legal framework that is oriented towards human subjects. The study focuses on the unclear legal subjects responsible, the difficulty of tracing system decisions, and the potential for human rights violations resulting from automated cyber defense actions. The research method employs normative legal research through legislative, conceptual, and comparative approaches. The analysis was conducted on national regulations related to cybersecurity, electronic systems, and personal data protection, as well as international principles and soft law relevant to the governance of artificial intelligence and cybersecurity. The results reveal that conventional legal approaches are inadequate to address accountability challenges in autonomous cyber defense systems due to the limitations of traditional responsibility doctrines. This study proposes the reconstruction of an adaptive and layered legal accountability model by strengthening the principles of human oversight, algorithmic transparency, and the division of responsibility between actors. This model is expected to serve as a normative basis for developing effective, equitable, and human rights-compliant cybersecurity governance in the digital age.*

Keywords: *legal accountability; cybersecurity; autonomous cyber defense systems; artificial intelligence; cyber governance.*

Introduction

Cyber threats in the digital era are increasing in both scale and complexity, including their patterns, techniques, and actors (Ismail, 2025). Cyberattacks are no longer sporadic or individual, but rather organized, cross-jurisdictional, and often utilize artificial intelligence to evade conventional detection (Pramudya, 2025). This situation is pushing state institutions and the private sector to adopt cyber defense systems capable of rapid and adaptive response. Autonomous Cyber Defense Systems (ACDS) are emerging as a technological solution designed to automatically detect, analyze, and respond to cyber threats (Santoso, 2023). The use of these systems marks a significant shift in how humans manage cybersecurity risks.

The transformation from entirely human-controlled defense mechanisms to machine-driven systems raises complex legal issues (Sarjito, 2024). Decision-making, previously under human discretion, is now shifted to autonomous algorithms (Farid, 2023). This situation raises fundamental questions about who should bear legal responsibility for the system's actions. Accountability can no longer be understood linearly, as with traditional legal subject relations. The relationship between humans, technology, and legal consequences has become increasingly blurred.

The use of ACDS also carries serious implications regarding the risk of legal losses that may arise from active defense measures. Automatic blocking, network isolation, or cyber counter-responses have the potential to impact the systems of other parties not actually involved in the attack (Jaeni, 2025). Such actions can violate the rights to privacy, freedom of communication, and even economic interests. Cyber conflict can also escalate if these autonomous responses are perceived as aggressive. These risks position ACDS as a technological entity fraught with legal implications.

The current cybersecurity legal framework still relies on the assumption that humans make all strategic decisions as the primary legal subject. Criminal, civil, and administrative law norms are still oriented towards human will, error, and negligence (Najwa, 2024). This type of normative structure is not fully capable of addressing the challenges arising from algorithmic decisions that operate autonomously and in real time. This regulatory vacuum creates legal uncertainty for system administrators, technology developers, and affected parties (Sudira, 2025). This situation demands a reexamination of the fundamental concept of legal accountability.

Autonomous Cyber Defense Systems can be conceptually understood as cyber defense systems that utilize artificial intelligence to identify threats and respond without direct human intervention (Sinaga, 2024). These systems differ fundamentally from conventional intrusion detection systems or firewalls, which are passive and reactive. ACDS can learn, adapt, and adjust defense strategies based on detected attack patterns. These characteristics make ACDS more effective, but also risky from a legal perspective (Shaimerdenova, 2024). High autonomy increases the potential for actions that are not fully predictable by humans.

The level of autonomy in ACDS demonstrates the varying relationship between humans and machines in the decision-making process. The human-in-the-loop model still places humans as the final controller before actions are executed. The human-on-the-loop scheme allows the system to act autonomously, while humans serve as supervisors (Mosqueira-Rey, 2023). Full autonomy eliminates direct human involvement in operational decision-making (Fathoni, 2025). Each level of autonomy carries different legal implications regarding responsibility and accountability.

Real-time decision-making through algorithms increases legal risks stemming from misidentified threats (Rustiyana, 2025). The system may produce false positives, blocking legitimate services or harming third parties. Algorithmic decision-making processes are often opaque and difficult to explain (Budiyanto, 2025). This complicates the process of proving and establishing legal accountability. These challenges place ACDS as a complex and multidimensional object of legal study.

Legal accountability theoretically holds a crucial position in both public and private law. It serves as a mechanism to ensure that power or authority is exercised legitimately and

responsibly (Andriana, 2025). In public law, accountability is closely related to the principle of the rule of law and oversight of government actions. In private law, accountability relates to responsibility for losses arising from an action (Resmadiktia, 2023). The expanding use of autonomous technology challenges the conceptual boundaries of accountability.

The distinction between responsibility, liability, and accountability is crucial in analyzing the legal issues of ACDS. Responsibility refers to the moral or functional obligation to act appropriately (Anwar, 2023). Liability refers to the legal consequences in the form of an obligation to bear losses or sanctions. Accountability has a broader dimension, encompassing the obligation to explain, monitor, and account for an action (Sadzili, 2026). These three concepts do not always coexist in autonomous systems.

Traditional legal accountability theory is primarily designed to regulate the behavior of human subjects. Non-human systems, such as algorithms and artificial intelligence, lack the will or consciousness of humans. The law's reliance on the concepts of fault and intent becomes problematic when faced with machine decisions (Sadzili, 2026). The relevance of classical accountability theory needs to be reexamined to ensure fairness. Developing new approaches is both an academic and practical necessity.

Autonomous technology creates a responsibility gap, separating system actions from human accountability (Surajiyo, 2023). Algorithmic opacity exacerbates this situation because the system's internal processes are difficult to understand, even for its developers (Yang, 2024). Strict liability is a risk-based approach that eliminates the need to prove fault (Juniarso, 2026). Vicarious liability and product liability are also relevant for ensnaring certain actors in the technology chain. The application of these doctrines remains limited because they are designed for conventional legal relationships.

Cybersecurity governance demands a balance between effective protection and respect for human rights. The principles of good cyber governance emphasize transparency, accountability, proportionality, and oversight. The state, the private sector, and non-state actors have complementary roles in the cybersecurity ecosystem (Anwar, 2025). The absence of a clear accountability framework has the potential to erode public trust in the cyber defense system. Integrating security and rights protection is a crucial prerequisite for developing a responsible ACDS.

Method

This research employs normative legal methodologies that integrate conceptual, legislative, and comparative approaches to systematically investigate the issue of legal responsibility for the deployment of Autonomous Cyber Defense Systems. This study employs a legislative approach to examine regulatory frameworks on cybersecurity, electronic systems, artificial intelligence, and personal data protection at both national and international levels, aiming to identify the limits of existing regulatory capacity. The conceptual framework focuses on examining and advancing the ideas of accountability, legal liability, and legal principles concerning autonomous technology related to the nature of algorithm-driven cyber defense systems. The comparative method is employed to analyze legal practices and principles evolving from international soft law and global doctrine, including principles related to AI governance and cybersecurity, as a basis for critical reflection regarding national legal reform. Primary, secondary, and tertiary legal

resources are examined qualitatively using prescriptive legal reasoning to develop a legal accountability framework that is flexible, multi-faceted, and corresponds with the demands of contemporary cybersecurity governance.

Result and Discussion

Legal Analysis of the Utilization of Autonomous Cyber Defense Systems

National legal regulations regarding cybersecurity in Indonesia are still scattered across various sectoral laws and regulations and have not yet formed a coherent regime. Under Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016, providers are legally required to ensure electronic system security. Article 15 of the ITE Law requires every electronic system provider to operate the system reliably, securely, and responsibly. This norm indicates a legal obligation, but does not specifically address the use of autonomous cyber defense systems. The regulatory orientation still places humans as the primary decision-makers.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions expands the obligations of electronic system providers regarding risk management and data protection. Article 14 of Government Regulation 71 of 2019 emphasizes the obligation to implement risk management against disruptions and threats to electronic systems. This provision provides scope for the use of advanced technology, including artificial intelligence, as a risk mitigation tool. The existence of Autonomous Cyber Defense Systems can be interpreted as fulfilling this obligation. A normative vacuum arises in the aspect of accountability for automated system actions that operate without direct human consent.

The legal standing of electronic system operators and administrators is a central issue in the analysis of ACDS accountability. Electronic system administrators are normatively positioned as legal subjects responsible for the entire operation of their systems. Article 1, number 6 of Government Regulation No. 71 of 2019 defines an administrator as any person, business entity, or agency that provides and operates an electronic system. This definition still assumes human control. Decisions made by autonomous systems have not received clear legal treatment as an extension of the will of the legal subject.

The limitations of national norms are further evident in the absence of specific regulations regarding artificial intelligence in cybersecurity. Indonesia does not yet have a specific law on artificial intelligence that governs standards of responsibility, algorithmic audits, or limits on system autonomy. Existing regulations remain implicit and scattered across sectoral regulations. This situation complicates law enforcement when losses occur due to automated cyber defense measures. Legal uncertainty has the potential to harm victims and create compliance risks for system administrators.

An international legal perspective shows that cybersecurity and artificial intelligence issues are largely regulated through non-binding principles and norms. International legal principles emphasize states' obligations to maintain the stability of cyberspace and prevent transnational harm. The concept of due diligence is often used as the basis for state responsibility for cyber activities within their jurisdiction. This principle remains general and does not explicitly address autonomous cyber defense systems. This wide scope for interpretation leads to variations in application between states.

The Tallinn Manual on the International Law Applicable to Cyber Operations provides important guidance on the application of humanitarian law and general international law to cyber operations. This manual recognizes that cyber actions can have legal consequences equivalent to conventional actions. Discussion of autonomous systems remains limited and interpretative. Automated cyber defense measures have not yet been classified as a separate category within the legal responsibility framework. It reflects the limitations of soft law in responding to developments in cyber defense technology.

The OECD AI Principles emphasize the value of transparency, accountability, and human oversight in the use of artificial intelligence. These principles are recommendatory in nature and do not create binding legal obligations. States and businesses are encouraged to integrate these principles into national policies. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security also emphasized the importance of responsible state behavior. The absence of binding international norms regarding autonomous cyber defense creates a significant regulatory gap.

One of the legal risks of using ACDS stems from misidentification of threats or false positives. The system can classify legitimate activity as a cyberattack and automatically take restrictive action. The impact of these actions can include service interruptions, economic losses, or violations of third parties' legitimate interests. The risk assessment process by algorithms is often difficult to trace transparently. Proving errors becomes problematic in law enforcement.

The potential for privacy violations is also a key issue in the use of ACDS. Law Number 27 of 2022 concerning Personal Data Protection affirms the principle of lawful, fair, and transparent processing of personal data. Automated network traffic monitoring can involve large-scale processing of personal data. Article 20 of the Personal Data Protection Law requires data controllers to ensure processing is for legitimate purposes. The tension between security needs and the protection of individual rights poses a serious challenge in the implementation of autonomous cyber defense systems.

The digital due process aspect also faces challenges from automated cyber defense systems. Blocking access or isolating networks can occur without prior objection or clarification mechanisms. The principle of procedural fairness, the foundation of modern law, is difficult to apply to instant algorithmic decisions. The lack of effective remedial mechanisms has the potential to create substantive injustice. This situation demands strengthening procedural guarantees in cybersecurity governance.

Cross-jurisdictional legal implications arise when ACDS actions impact systems or infrastructure in other countries. Automated counterattacks can be perceived as a violation of another country's digital sovereignty. National laws have limited reach regarding events that cross borders. Jurisdictional conflicts and differing legal standards complicate dispute resolution. The absence of a clear international framework increases the risk of escalating cyber disputes.

Regulatory gaps are further highlighted by the lack of clarity regarding the legal entities responsible for the actions of autonomous systems. Developers, operators, and system owners are all part of a complex technological chain. The absence of mandatory algorithmic audits and technical transparency hampers the accountability assessment

process. The fragmentation of regulations between cyber law, artificial intelligence law, and liability law deepens normative issues. This position highlights the urgency of reconstructing a legal accountability framework capable of addressing the challenges of autonomy-based cyber defense.

Reconstruction of Legal Accountability in Cybersecurity Governance

The principle of accountability in autonomous cyber defense systems rests on the recognition that algorithmic decisions must remain under the normative control of humans. Human oversight cannot be understood simply as a symbolic human presence, but rather as a concrete mechanism for monitoring, evaluating, and correcting system actions. The presence of human oversight bridges the gap between technological efficiency and demands for legal accountability. Without meaningful oversight, autonomous system actions have the potential to lose legal legitimacy. This principle emphasizes that technology should not exist outside the framework of legal accountability.

Human oversight is also closely related to the distribution of authority and responsibility within electronic system management organizations. Human oversight must be designed from the system design stage, not just during the operational phase. System designs that allow for proportional human intervention reflect legal prudence in the use of high-risk technology. The absence of intervention mechanisms can be viewed as a form of structural negligence. Placing humans as the final oversight ensures continuity between innovation and legal certainty.

The principles of proportionality and necessity serve as the ethical and legal foundations for autonomous cyber defense. Any automated response to a cyber threat must be commensurate with the level of risk faced. Excessive action has the potential to cause harm disproportionate to the protection objective. Assessing response needs presents a particular challenge for autonomous systems that operate rapidly. This principle requires the design of algorithms that are sensitive to legal and social impacts.

The need for proportionality also relates to protecting the interests of third parties not directly involved in a cyber incident. An overly aggressive automated response could disrupt public services or legitimate economic activity. The principle of necessity requires the system to choose the minimal but effective action. It aligns with the principle of limiting power in a state governed by the rule of law. Implementing this principle strengthens the legitimacy of ACDS use.

Algorithmic explainability and traceability serve as key prerequisites for legal accountability. Decisions by autonomous systems must be rationally explained, and their decision-making process traced. Without traceability, the legal process of proof will face serious obstacles. Technical transparency does not mean disclosing all source code, but rather providing an auditable decision trail. This principle reconciles cybersecurity needs with the interests of justice.

Traceability also relates to the obligation to document and record every action of a cyber defense system. These records serve as a crucial tool in post-incident evaluations. This mechanism allows for the identification of actors involved in the decision chain. The lack of documentation can obscure responsibility and harm victims. Strengthening this principle clarifies the relationship between technology and legal accountability.

The multi-actor accountability model reflects the complexity of the cyberdefense technology ecosystem. System developers are responsible for the design and algorithmic logic used. Operators are responsible for the configuration, oversight, and operational use of the system. System owners are responsible for usage policies and legal compliance. This division of roles requires contractual and normative clarity.

The concept of shared responsibility recognizes that harm cannot always be traced to a single actor. Layered accountability offers a multi-layered approach that aligns the level of responsibility with each actor's role. This approach avoids oversimplification in determining fault. Layered accountability also encourages each actor to exercise heightened standards of care. This structure is more realistic when dealing with complex technological systems.

The role of the state remains central to the accountability model for autonomous cyberdefense systems. The state serves as a regulator, setting minimum standards for the use of high-risk technology. The state also acts as a guarantor, ensuring the protection of the public interest. Failure by the state to provide an oversight framework can result in a loss of public trust. The state's responsibility does not diminish even if the system is operated by the private sector.

Integrating accountability into cybersecurity governance requires mandatory legal and technical audits. Audits not only verify formal compliance but also assess the system's impact on legal rights and interests. The audit process serves as a risk prevention tool. The involvement of independent auditors strengthens the objectivity of assessments. This mechanism creates room for corrections before serious violations occur.

Operational standards and oversight mechanisms must be clearly formulated and enforceable. These standards include usage procedures, limitations on automated actions, and incident reporting mechanisms. Effective oversight requires coordination across agencies and sectors. The lack of uniform standards has the potential to lead to inconsistent practices. Consistent oversight is key to sustainable cybersecurity governance.

The link between accountability and human rights protection is inseparable from cybersecurity governance. Personal data protection, freedom of expression, and the right to procedural fairness must remain intact in the use of ACDS. Strengthening accountability serves as an instrument for rights protection. This principle aligns with Law Number 27 of 2022 concerning Personal Data Protection, which emphasizes the responsibility of data controllers. The integration of human rights values strengthens the legitimacy of the use of cyber defense technology.

Normative implications for legal formation demonstrate the need for policy direction that adapts to technological developments. Legal regulations for cybersecurity and artificial intelligence need to be designed in a complementary manner to avoid overlap. Harmonization across legal regimes is crucial to ensure certainty and fairness. Developing countries face the dual challenge of security needs and limited regulatory capacity. The reconstruction of legal accountability offers a normative foundation for responsibly addressing the dynamics of global cyber threats.

Conclusion

The use of Autonomous Cyber Defense Systems presents a structural, not merely technical, legal accountability problem, as key cybersecurity decisions have shifted from human control to autonomous algorithmic mechanisms. The central characteristic of this problem lies in the unclear legal entity responsible for the system's actions, given the involvement of multiple actors, from developers and operators to system owners. Conventional legal approaches, which rely on human error, intent, and negligence, demonstrate significant limitations when faced with autonomous decisions based on artificial intelligence. Existing legal structures are not fully capable of addressing the challenges of transparency, decision traceability, and ensuring procedural fairness for affected parties. This situation underscores the urgency of developing a legal accountability model that is adaptive, multi-layered, and aligned with the complexity of modern cyber defense technology.

Normative suggestions target policymakers and lawmakers to develop a legal structure that clearly governs the deployment of autonomous cyber defense systems, encompassing guidelines for human oversight, required algorithmic evaluations, and the distribution of responsibilities among involved parties. Such policies must be designed in harmony with the legal regimes for personal data protection, cybersecurity, and artificial intelligence to avoid normative fragmentation. System administrators and law enforcement officials are encouraged to develop operational guidelines that emphasize caution, proportionality, and clear accountability mechanisms. Strengthening institutional capacity is a crucial prerequisite for law enforcement to keep pace with technological dynamics. Further research is expected to deepen the study of the relationship between algorithmic accountability, human rights, and global cybersecurity governance as a foundation for developing equitable cyber law.

References

Andriana, D. (2025). *Akuntabilitas publik*. Yogyakarta: Deepublish.

Anwar, R. (2023). Pemaknaan aliran dualistis perspektif hukum pidana dalam KUHP nasional. *ASY SYAR'IYYAH: Jurnal Ilmu Syari'ah dan Perbankan Islam, 8*(1), 64–83.

Anwar, S., & (penulis tidak lengkap). (2025). Harmonisasi hukum digital: Tantangan global dan strategi adaptif Indonesia dalam era kedaulatan siber. *Hutanasyah: Jurnal Hukum Tata Negara, 4*(1), 69–88.

Budiyanto. (2025). *Pengantar cybercrime dalam sistem hukum pidana di Indonesia*. Serang: Sada Kurnia Pustaka.

Farid, I. R. (2023). Pemanfaatan artificial intelligence dalam pertahanan siber. *Nusantara: Jurnal Ilmu Pengetahuan Sosial, 10*(2), 779–788.

Fathoni, F. R. (2025). Analisis literatur mengenai peran AI agent dalam efisiensi automasi digital. *JOISIE (Journal of Information Systems and Informatics Engineering), 9*(1), 77–90.

Ismail, M. N. (2025). Pengaruh teknologi AI terhadap evolusi modus kejahatan siber di Indonesia tahun 2024–2025 dan implikasinya terhadap penegakan hukum. *Jurnal Intelek dan Cendikiawan Nusantara, 2*(6), 12647–12665.

Jaeni, A. I. (2025). A literature review on the transformation of defense law in the digital age and advanced technology. *TOFEDU: The Future of Education Journal, 4*(4), 821–829.

Juniarso, D. A. (2026). Reformasi kebijakan pidana nasional terhadap kejahatan siber berbasis AI melalui pendekatan hukum progresif. *Jurnal Impresi Indonesia, 5*(1), 77–88.

Mosqueira-Rey, Eduardo & Hernández-Pereira, Elena & Alonso-Ríos, David & Bobes-Bascarán, José & Fernández-Leal, Ángel. (2022). Human-in-the-loop machine learning: a state of the art. *Artificial Intelligence Review, 56*(4), 3005–3054.

Najwa, F. R. (2024). Analisis hukum terhadap tantangan keamanan siber: Studi kasus penegakan hukum siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, 1*(2), 8–16.

Pramudya, D. W. (2025). Anatomi kriminal siber: Motif, modus, dan penanggulangannya dari perspektif kriminologi. *Jurnal Intelek Insan Cendikia, 2*(8), 14613–14623.

Resmadiktia, N. M. (2023). Pertanggungjawaban pemerintah dalam mewujudkan good governance sesuai hukum administrasi negara. *Jurnal Ilmiah Wahana Pendidikan, 9*(11), 685–697.

Rustiyana, R. J. (2025). *Pemanfaataan AI dalam keamanan siber*. Jambi: PT Sonpedia Publishing Indonesia.

Sadzili, M. Y. (2026). Politik impunitas dan stagnasi akuntabilitas konstitusional di Indonesia: Suatu analisis hukum tata negara. *AKADEMIK: Jurnal Mahasiswa Humanis, 6*(1), 268–282.

Santoso, J. T. (2023). *Teknologi keamanan siber (cyber security)*. Semarang: Penerbit Yayasan Prima Agus Teknik.

Sarjito, I. A. (2024). *Transformasi manajemen pertahanan Indonesia di era modernisasi militer*. Indonesia Emas Group.

Shaimerdenova, G. S. (2024). A review of cyber defense mechanisms in autonomous electrical systems. *Bulletin of Abai KazNPU. Series of Physical and Mathematical Sciences, 88*(4), 188–197.

Sinaga, N. H. (2024). Mengoptimalkan keamanan jaringan memanfaatkan kecerdasan buatan untuk meningkatkan deteksi dan respon ancaman. *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI), 7*(2), 364–369.

Sudira, I. W. (2025). Keadilan digital: Tantangan hukum dalam era disrupsi teknologi. *Kertha Widya, 12*(2), 35–59.

Surajiyo, S. D., & (penulis tidak lengkap). (2023). Teknologi dan masa depan otonomi manusia: Sebuah kajian fenomena gawai dan otonomi manusia. *Prosiding Konferensi Berbahasa Indonesia Universitas Indraprasta PGRI*, 140–147.

Yang, H. L., et al. (2024). Decoding algorithm fatigue: The role of algorithmic literacy, information cocoons, and algorithmic opacity. *Technology in Society, 79*, 102749.