Indonesian Journal of Contemporary Multidisciplinary Research (MODERN)
Vol. 5, No. 2, 2026: 381-388

Cyber Warfare and the Law: Emerging Challenges of Digital Militaries in Indonesia

Arief Fahmi Lubis
Indonesian Military College of Law
Corresponding Author: Arief Fahmi Lubis arieffahmilubis0@gmail.com

A R T I C L E I N F O

Keywords: Cyber Warfare, International Humanitarian Law, Digital Military, Cyber Sovereignty, In-Donesian Defense

Received : 10 January
Revised : 15 February
Accepted: 30 March

A B S T R A C T

The development of information technology has transformed the character of armed conflict from conventional models to the cyber domain, which is non-linear, border-less, and difficult to attribute. Cyber warfare is no longer merely a hypothetical threat but has become a strategic instrument in global geopolitical rivalry. In the context of Indonesia, the digitalization of government systems, critical infrastructure, and the defense sector increases vulnerability to cyberattacks that could disrupt national sovereignty and stability. This article aims to analyze cyber warfare from the per-spectives of international law and Indonesian national law, as well as to identify normative and institutional challenges in the development of a digital military. The study employs a juridical-normative method with legislative, conceptual, and com-parative approaches. The findings indicate that, although the principles of Interna-tional Humanitarian Law (IHL) remain relevant, ambiguities exist in their application to cyber operations—particularly regarding attack attribution, thresholds of armed attacks, and the exercise of the right to self-defense. At the national level, Indone-sian regulations remain sectoral and do not explicitly regulate cyberwar doctrine as part of the national defense system. Therefore, harmonization of regulations, formu-lation of a national cyber military doctrine, and strengthened inter-agency coordina-tion are required to ensure Indonesia's readiness to address the dynamics of digital conflict in the modern era

DOI: https://doi.org/10.55927/modern.v5i2.35
E-ISSN: 2985-6108
https://journalmodern.my.id/index.php/MODERN/index

INTRODUCTION

The development of information and communication technology has fundamentally reshaped the landscape of armed conflict. While the 20th century was dominated by conventional military confrontations based on physical territory, the 21st century is characterized by the emergence of a new domain cyberspace as a strategic arena for national defense and security. This transformation aligns with Mary Kaldor's "new wars" thesis, which asserts that contemporary conflicts are increasingly asymmetric, involve non-state actors, and utilize information technology as a prima-ry instrument of power.

In this context, cyber warfare is not merely a form of digital espionage but can reach a level of disruption capable of affecting critical national infrastructure, such as en-ergy systems, banking, communications, and defense.

From the perspective of international law, fundamental questions arise regarding how the existing regime of International Humanitarian Law (IHL) governs military operations in cyberspace. Classical principles such as distinction, proportionality, and military necessity remain the normative foundation for armed conflict, as dis-cussed by Yoram Dinstein in his work on the conduct of hostilities. However, the unique characteristics of cyber warfare particularly related to attack attribution and the threshold for the use of force generate both academic and practical debates. Mi-chael N. Schmitt argues that existing international law is fundamentally applicable to cyberspace but requires adaptive interpretation in light of digital technology. These ambiguities are further complicated by Articles 2(4) and 51 of the UN Charter regarding the prohibition of the use of force and the right of self-defense.

In Indonesia, the relevance of cyber warfare has increased in parallel with the digi-talization of government systems and national infrastructure. National regulations, such as Law No. 3 of 2002 on National Defense and Law No. 34 of 2004 on the In-donesian National Armed Forces (TNI), do not explicitly recognize cyberspace as a distinct operational domain. Meanwhile, the Electronic Information and Transac-tions Law (UU ITE) primarily addresses cybercrime enforcement rather than the di-mension of digital armed conflict. The absence of comprehensive regulation creates a normative gap in addressing potential escalation of digital conflicts, particularly concerning the role of the military, inter-agency coordination, and the protection of human rights.

Thus, cyber warfare presents multidimensional challenges normative, institutional, and strategic. As a nation with high digital penetration and a strategic geopolitical position in the Indo-Pacific, Indonesia must strengthen its legal framework and cyber defense doctrine to safeguard national sovereignty. This article critically ex-amines how both international and national law respond to the dynamics of digital militarization and assesses Indonesia's preparedness in the era of cyber conflict.

The main research questions addressed in this study are: How is cyber warfare characterized under international law and Indonesian national law? To what extent can the principles of International Humanitarian Law be applied to cyber military operations? And how prepared is Indonesia's regulatory framework to govern the role of digital military forces in national defense?

The study aims to normatively analyze the application of international law to cyber warfare, evaluate Indonesia's national legal framework on cyber defense and secu-rity, and formulate conceptual recommendations to strengthen the regulation and doctrine of digital military operations to protect national sovereignty and stability.

LITERATURE REVIEW

1. Transformation of Modern Warfare and Cyberspace

The development of cyber warfare is inseparable from the transformation of modern conflicts, which have become increasingly decentralized, asymmetric, and technology-driven. Mary Kaldor observes that contemporary conflicts are no longer dominated solely by interstate wars but involve non-state actors, transnational networks, and the use of information technology as instruments of power. In this context, cyberspace has become a new domain that trans-cends traditional geographic and state sovereignty boundaries.

From the perspective of international law, the central discourse concerns whether and to what extent existing law can govern cyber military operations. Yoram Dinstein asserts that the fundamental principles of IHL remain applica-ble in any form of armed conflict, regardless of medium or technology. Similar-ly, Michael N. Schmitt contends that international law does not become obso-lete due to technological advancement; rather, it demands progressive inter-pretation to remain relevant in the context of cyber warfare. However, applying the principles of distinction and proportionality to cyberattacks, which may not cause direct physical damage, remains a normative debate.

2. Legal Sociology and Response to Technological Change

Legal sociology provides a broader perspective by viewing law not merely as a normative text but as a social institution that evolves within society. Roscoe Pound introduced the concept of law as a tool of social engineering, in which law functions as an instrument to balance societal interests. In the context of cyber warfare, law not only regulates state behavior but also manages social risks arising from the digitalization of defense and security.

Eugen Ehrlich's concept of "living law" emphasizes that effective law aligns with actual social practices. In cyberspace, military and security practices evolve far faster than formal state regulations, creating a gap between law in books and law in action, particularly in regulating military cyber operations in Indonesia. As defense institutions develop offensive and defensive cyber ca-pabilities, while national regulations do not explicitly recognize cyberspace as a distinct operational domain, a misalignment arises between socio-technological realities and positive legal norms.

From a social structure perspective, Lawrence M. Friedman argues that a legal system consists of three elements: structure, substance, and legal culture. Ap-plied to Indonesia's cyber warfare context:

1. Legal structure involves institutions such as the TNI and the National Cyber and Crypto Agency (BSSN);
2. Legal substance relates to regulations governing cyber defense and se-curity;

3. Legal culture concerns policymakers' awareness and orientation toward digital threats.

Misalignment among these three elements can hinder the effectiveness of dig-ital military regulation.

3. Militarization of Cyberspace and Power Dynamics

From a critical legal sociology perspective, the development of a digital military is also tied to state power and legitimacy. Law is not neutral but often reflects dominant power configurations. Strengthening military roles in cyberspace po-tentially expands state security into the civilian digital sphere. Therefore, a bal-ance between national security and human rights protection is essential.

A sociological approach enables a more comprehensive analysis of whether Indonesia's cyberwar regulations are security-oriented or rights-oriented. This tension demonstrates that cyber warfare is not merely a technical military issue but also a complex social, political, and legal matter.

4. Theoretical Synthesis

By integrating modern warfare theory, International Humanitarian Law, and le-gal sociology, it can be concluded that cyber warfare is a multidimensional phenomenon. Normatively, international legal principles remain the primary reference. Sociologically, the effectiveness of law depends on institutional ad-aptation, legal culture, and the alignment between norms and technological realities. In Indonesia, the greatest challenge lies not only in regulatory gaps but also in harmonizing structure and legal culture to address the militarization of cyberspace.

METHODOLOGY

This study adopts a juridical-normative approach, complemented by conceptual and comparative analysis, to examine the legal, institutional, and socio-technical dimen-sions of cyber warfare in Indonesia.

1. Juridical-Normative Analysis: Primary and secondary legal sources—including international treaties, UN Charter provisions, International Humanitarian Law (IHL), and Indonesian defense and cyber regulations—are systematically ana-lyzed to assess their applicability to cyber military operations and identify regu-latory gaps.
2. Conceptual Framework: The study synthesizes theoretical constructs from modern warfare, digital militarization, and socio-legal theory to develop a dy-namic legal framework for cyber operations, bridging law in books with law in action.
3. Comparative Perspective: Indonesia's legal and institutional arrangements are compared with international best practices and cyber doctrines of other states, highlighting gaps, challenges, and potential improvements in governance, at-tribution, and operational thresholds.
4. Analytical Method: Qualitative content analysis is employed to examine norma-tive coherence, interpretive ambiguities, and institutional

readiness, enabling a multidimensional understanding of cyber warfare that integrates legal, mili-tary, and socio-political perspectives.

This streamlined methodology ensures rigorous, multidisciplinary insights into cyber warfare, providing both theoretical and policy-relevant contributions for national and international security governance.

RESULTS AND DISCUSSION

1. Normative Gaps and Socio-Technological Realities

The analysis reveals that Indonesia's national regulations do not explicitly recognize cyber warfare as a defense domain on par with the land, sea, and air forces. The National Defense Law and the Indonesian Armed Forces (TNI) Law remain oriented toward conventional conflict paradigms, while cyber se-curity practices are evolving rapidly through the establishment of cyber units and coordination with the National Cyber and Crypto Agency (BSSN). From a legal sociology perspective, this reflects Eugen Ehrlich's distinction between law in books and living law, highlighting a misalignment between written norms and evolving social practices.

In practice, defense institutions have adopted digital security as part of the na-tional strategy, yet normative integration remains incomplete. This indicates that law lags behind social and technological dynamics. The phenomenon al-so demonstrates that social changes driven by digitalization occur faster than legislative processes, creating a grey area in the legitimacy of state cyber oper-ations.

2. Structure, Substance, and Legal Culture in the Digital Military

Using Lawrence M. Friedman's framework of the legal system, the effective-ness of cyber warfare regulation can be analyzed through three elements: structure, substance, and legal culture.

a. Legal Structure: Indonesia has relevant institutions, such as the TNI and BSSN, but coordination of authority in the context of cyber armed conflict is not yet explicitly regulated.
b. Legal Substance: Regulations remain sectoral, focusing primarily on cybercrime rather than cyber warfare.
c. Legal Culture: Policy orientation is still predominantly security-driven, while civil oversight and human rights dimensions of the digital military remain underdeveloped.
d. The imbalance among these three elements may create legitimacy prob-lems, especially if military cyber operations impact civilian digital spaces.

3. Critical Legal Studies Perspective: Law and Power Relations

From the lens of critical legal studies (CLS), law is not neutral but reflects power relations within society. In the context of cyber warfare, regulations granting broad state authority for digital operations may reinforce state domi-nance over the domestic cyber space. This perspective highlights the need for normative limits to prevent the militarization of cyberspace from becoming a justification for excessive control over digital society.

In international relations, applying the principle of self-defense to cyberattacks may also expand the interpretation of the use of force. Michael N. Schmitt em-phasizes that the threshold for armed attacks in cyberspace must be interpret-ed cautiously to prevent disproportionate conflict escalation. From a critical le-gal sociology perspective, the interpretation of international law is often influ-enced by the interests of powerful states with high cyber capabilities.

4. State Legitimacy and Digital Security

The concept of state legitimacy is crucial for understanding cyber warfare as a defense instrument. A state gains legitimacy when the use of force including cyber capabilities is recognized as lawful and socially accepted. In this context, International Humanitarian Law principles, as articulated by Yoram Dinstein, remain the primary normative reference. However, applying the principles of distinction and proportionality to cyberattacks affecting civilian infrastructure such as banking or healthcare systems raises complex ethical and social is-sues.

From a legal sociology perspective, legitimacy is not solely determined by for-mal legality but also by public acceptance (social acceptance). Therefore, transparency in cyber defense policies, mechanisms for civilian oversight, and accountability are essential to maintain the democratic legitimacy of the digital military.

5. Implications for Indonesia

The main challenge for Indonesia lies not merely in normative gaps but in harmonizing the development of digital military technology with legal system updates. Without timely legal adaptation, an imbalance may emerge between technological power and normative control. From a legal sociology standpoint, reforming cyber warfare regulations must consider social dynamics, national legal culture, and the commitment to the rule of law (Rechtsstaat).

Consequently, cyber warfare requires an interdisciplinary approach that inte-grates international law, national law, and sociological analysis of power rela-tions and legitimacy. Without such an approach, digital military regulation risks becoming a mere instrument of state power rather than a tool for safeguarding sovereignty and public interests.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Cyber warfare is a multidimensional phenomenon of modern conflict, involving technology, law, and socio-political dynamics. The analysis indicates that interna-tional law, particularly the principles of International Humanitarian Law (IHL), re-mains a relevant normative foundation; however, its application in cyberspace faces ambiguities, especially regarding attack attribution, the threshold for armed attacks, and states' exercise of the right to self-defense.

At the national level, Indonesia's regulations remain sectoral and partial. The Na-tional Defense Law and the Indonesian Armed Forces (TNI) Law do not explicitly recognize cyberspace as a distinct military operational domain, while the Electronic Information and Transactions Law (UU ITE) primarily addresses cybercrime rather than digital military operations. This imbalance between law

in books and opera-tional practice (living law) generates legitimacy gaps for the state and potential so-cial risks.

From the perspectives of legal sociology and state legitimacy, the effectiveness of cyber warfare regulation depends not only on formal compliance but also on public acceptance and social awareness. Weber's theory emphasizes rational-legal legiti-macy, which must be built through adherence to formal legal procedures, while Ha-bermas highlights the importance of public participation and policy transparency to maintain democratic legitimacy. Accordingly, cyber warfare is not merely a technical-military issue but a social phenomenon that requires legal adaptation, institutional coordination, and ethical and civil rights considerations.

Recommendations

Based on the study's findings, the following strategic recommendations are pro-posed:

1. Harmonization of Cyber Defense Regulations

a. Revise the National Defense Law and the TNI Law to explicitly recognize cyberspace as a military operational domain.
b. Integrate the UU ITE and related regulations to distinguish between cybercrime and military cyber operations.

2. Development of a National Cyber Military Doctrine

a. Formulate a doctrine for cyber operations aligned with IHL principles and ethical considerations.
b. Establish standard procedures for attack attribution, response protocols, and conflict escalation.

3. Strengthening Inter-Agency Coordination

a. Foster synergy among the TNI, BSSN, Ministry of Communication and Information (Kemenkominfo), and other security agencies to establish a unified national cyber command.
b. Implement mechanisms for civilian oversight and transparent accountability.

4. Enhancing Digital Military Human Resource Capacity

a. Recruit and train personnel with expertise in cyber warfare, international law, and cybersecurity.
b. Integrate training on ethics and human rights to maintain operational legitimacy.

5. Sociological and Participatory Approaches

a. Involve the public and stakeholders in cyber policy formulation to strengthen democratic legitimacy (Habermas).
b. Consider social impacts and national legal culture in all digital military strategy development (Ehrlich & Friedman).

By implementing these recommendations, Indonesia can strengthen its digital sov-ereignty, reduce cyber conflict risks, and maintain both legal and social legitimacy in the context of militarizing cyberspace in the modern era.

REFERENCES

Dinstein, Yoram. The Conduct of Hostilities under the Law of International Armed Conflict. 3rd ed. Cambridge: Cambridge University Press, 2016.

Ehrlich, Eugen. Fundamental Principles of the Sociology of Law. Cambridge: Har-vard University Press, 1936.

Friedman, Lawrence M. The Legal System: A Social Science Perspective. New York: Russell Sage Foundation, 1975.

Habermas, Jürgen. The Theory of Communicative Action. Vol. 2. Translated by Thomas McCarthy. Boston: Beacon Press, 1984.

Kaldor, Mary. New and Old Wars: Organized Violence in a Global Era. 3rd ed. Stan-ford: Stanford University Press, 2012.

Pound, Roscoe. An Introduction to the Philosophy of Law. New Haven: Yale Univer-sity Press, 1922.

Republik Indonesia. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Republik Indonesia. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Na-sional Indonesia.

Schmitt, Michael N. "Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance." Virginia Journal of International Law 50, no. 4 (2010): 795–839.

Critical Legal Studies Collective. The Politics of Law: A Progressive Critique. Oxford: Oxford University Press, 1983.

Weber, Max. Economy and Society: An Outline of Interpretive Sociology. Translated by Guenther Roth and Claus Wittich. Berkeley: University of California Press, 1978.