

International Journal for Science Review

Transformation of National Defense Law in Addressing Cyber Threats and Hybrid Warfare in the Digital Era

Wilsa,*¹ Vegitya Ramadhani Putri,² Pitriani,³ Agus Iskandar PP,⁴

¹ Universitas Samudra Langsa Aceh

² FH Universitas Sriwijaya

³ IAIN Kerinci Jambi Indonesia

⁴ FHSIP Universitas Terbuka

*Corresponding author: wilsa@unsam.ac.id

ABSTRACT

This study examines the transformation of national defense law in addressing cyber threats and hybrid warfare in the digital era, driven by the increasing complexity and borderless nature of modern security challenges. The research aims to analyze the limitations of existing legal frameworks and propose adaptive approaches to enhance national resilience. Using a qualitative library-based method, the study relies on primary and secondary data derived from books, academic journals, and relevant scientific reports. Data were collected through systematic literature review and analyzed using content analysis to identify patterns, relationships, and key insights. The findings reveal that current defense laws remain reactive, lack clarity in cyber threat attribution, and insufficiently integrate civilian and private sector roles. The study concludes that a comprehensive transformation of national defense law—emphasizing flexibility, interdisciplinary collaboration, and proactive strategies—is essential to effectively address cyber threats and hybrid warfare in the digital era.

KEYWORDS

*Cyber Defense
Transformation, Hybrid
Warfare Strategy,
National Security Law*

1. INTRODUCTION

The rapid evolution of digital technology has fundamentally reshaped the landscape of national security, creating complex challenges that transcend traditional defense paradigms. In recent years, cyber threats and hybrid warfare have emerged as critical concerns for states worldwide, as adversaries increasingly exploit digital infrastructures to conduct espionage, sabotage, and influence operations. These threats are not confined to conventional battlefields but extend into cyberspace, where attacks on critical infrastructure, financial systems, and governmental networks can destabilize entire nations without physical confrontation. The integration of cyber operations into broader hybrid warfare strategies—combining military, political, economic, and informational tactics—has blurred the boundaries between war and peace. Consequently, existing national defense laws, often designed for traditional warfare contexts, struggle to adequately address these multifaceted and rapidly evolving threats. This mismatch between legal frameworks and contemporary security challenges highlights an urgent need for transformation in national defense law, ensuring that states are equipped to respond effectively to cyber-enabled and hybrid threats in the digital era (Sawhani and Supriyadi 2024).

Despite the growing recognition of cyber threats and hybrid warfare, existing literature reveals significant gaps in the theoretical and legal frameworks that govern national defense. Scholars have extensively explored concepts such as cyber deterrence, digital sovereignty, and hybrid conflict strategies; however, many of these theories remain insufficient in addressing the legal complexities posed by the integration of cyber operations into national defense systems. Traditional legal doctrines often rely on clear distinctions between combatants and non-combatants, as well as defined territorial boundaries, which are increasingly irrelevant in cyberspace. Furthermore, while some studies emphasize the importance of international law in regulating cyber conflict, there remains ambiguity regarding state responsibility, attribution of cyberattacks, and proportional responses. These unresolved issues indicate that current theoretical approaches have not fully adapted to the realities of digital conflict. As a result, there is a pressing need to bridge the gap between theoretical discourse and practical legal frameworks, particularly in transforming national defense law to better address cyber threats and hybrid warfare in a comprehensive and coherent manner (Aji and Supriyadi 2026).

The primary objective of this research is to analyze the transformation of national defense law in addressing cyber threats and hybrid warfare within the context of the digital era. Specifically, this study aims to identify the limitations of existing legal frameworks, examine the evolving nature of cyber and hybrid threats, and propose a conceptual model for legal transformation that aligns with contemporary security needs. By focusing on the intersection of law, technology, and national defense, the research seeks to provide a nuanced understanding of how legal systems can adapt to the dynamic and borderless nature of cyber conflict. Additionally, the study intends to contribute to academic discourse by integrating insights from legal studies, security studies, and information technology, thereby offering a multidisciplinary perspective on the issue. Ultimately, this research aspires to support policymakers, legal practitioners, and defense institutions in developing more resilient and adaptive legal frameworks capable of safeguarding national security in an increasingly digitalized world (Fitria and Supriyadi 2025).

This research is grounded in the argument that the transformation of national defense law is not only necessary but also imperative in ensuring effective responses to cyber threats and hybrid warfare. Based on the realities of contemporary security challenges and the identified gaps in existing literature, it is hypothesized that without significant legal adaptation, states will remain vulnerable to increasingly sophisticated and ambiguous forms of aggression. The

inability of current legal frameworks to address issues such as cyberattack attribution, jurisdictional limitations, and the integration of civilian and military domains in hybrid warfare underscores the urgency of reform. Furthermore, aligning legal structures with technological advancements and evolving threat landscapes is essential for maintaining national resilience and strategic stability. Therefore, this study posits that a comprehensive transformation of national defense law—incorporating flexibility, interdisciplinarity, and forward-looking principles—will enhance a state’s capacity to anticipate, prevent, and respond to cyber and hybrid threats. This argument reinforces the importance of the research and its contribution to advancing both theoretical understanding and practical policy development in the field of national security (Bratko, Zaharchuk, and Zolka 2021).

2. METHODS

The object of this research focuses on the phenomenon of the transformation of national defense law in response to the increasing complexity of cyber threats and hybrid warfare in the digital era. This phenomenon is characterized by the growing frequency of cyberattacks targeting critical national infrastructure, the use of digital platforms for disinformation campaigns, and the integration of cyber capabilities into broader hybrid warfare strategies. These developments present significant legal challenges, particularly in terms of defining the scope of national defense, determining jurisdiction in cyberspace, and establishing accountability for cyber operations. The problem is further compounded by the asymmetrical nature of cyber threats, where state and non-state actors can exploit technological vulnerabilities with relatively low resources but high impact. As such, the research examines how existing legal frameworks are confronted with these evolving threats and the extent to which they are capable of adapting to the dynamic nature of digital conflict. By focusing on this phenomenon, the study aims to provide a comprehensive understanding of the legal transformation required to address contemporary national security challenges (Khoirunnisa et al. 2025).

This study employs a qualitative research approach with a library-based (kepastakaan) research design, emphasizing the analysis of existing literature relevant to the research problem. The primary data sources consist of authoritative texts, including academic books, peer-reviewed journal articles, and official publications that specifically address cyber threats, hybrid warfare, and national defense law. These primary sources provide foundational insights into the evolution of legal frameworks and the conceptualization of digital-era security challenges. In addition, secondary data sources are utilized to complement the primary data, including supporting literature related to the research keywords—Cyber Defense Transformation, Hybrid Warfare Strategy, and National Security Law. These secondary materials are drawn from a wide range of scholarly works, research reports, and scientific studies that contextualize the broader implications of cyber and hybrid threats. The combination of primary and secondary data ensures a comprehensive and multidimensional analysis of the research topic (Hidayati et al. 2025).

The theoretical foundation of this research is built upon several key theories that provide a conceptual framework for understanding the transformation of national defense law. One of the primary theories employed is the concept of Hybrid Warfare, as articulated by Frank G. Hoffman in 2007, which emphasizes the integration of conventional and unconventional tactics, including cyber operations, in modern conflict. Additionally, the study draws on the Cyber Power Theory proposed by Joseph S. Nye Jr. in 2010, which highlights the role of cyberspace as a domain of power that influences both state and non-state actors. Furthermore, the Legal Adaptation Theory, often associated with H. L. A. Hart and developed in the mid-

20th century, is utilized to explain how legal systems evolve in response to societal and technological changes. These theories collectively provide a framework for analyzing how national defense law must adapt to address the complexities of cyber threats and hybrid warfare, offering both descriptive and normative insights into the transformation process.

The research process is conducted through a systematic and structured approach to data collection, primarily relying on the examination of written sources. The initial stage involves identifying relevant literature that aligns with the research objectives and keywords, followed by the selection of credible and authoritative sources. Data collection is carried out through an extensive review of books, academic journals, prior research studies, conference papers, policy documents, and reputable online publications. Each source is carefully analyzed to extract relevant information related to the transformation of national defense law, cyber threats, and hybrid warfare strategies. The process also includes note-taking, categorization of themes, and cross-referencing between sources to ensure consistency and reliability of information. By employing this method, the research ensures that the data collected is both comprehensive and relevant, enabling a thorough exploration of the research problem and supporting the development of well-founded arguments (Khan and Rana 2025).

The data analysis technique used in this research is content analysis, which involves systematically examining and interpreting the collected data to identify patterns, relationships, and key insights. This process begins with the organization of data into thematic categories based on the research objectives and theoretical framework. Subsequently, the data is analyzed to uncover recurring concepts, trends, and discrepancies within the literature, particularly in relation to the effectiveness of existing legal frameworks in addressing cyber threats and hybrid warfare. The analysis also involves comparing different scholarly perspectives to identify areas of consensus and divergence, thereby enriching the depth of the study. Through this method, the research is able to synthesize complex information into coherent findings that address the central research questions. Ultimately, content analysis enables a rigorous and systematic interpretation of data, ensuring that the conclusions drawn are grounded in a comprehensive understanding of the subject matter (Otaiku 2018).

3. RESULTS AND DISCUSSION

The findings of this research reveal that the transformation of national defense law in addressing cyber threats and hybrid warfare is not only necessary but increasingly urgent due to the evolving nature of digital conflict. The analysis indicates that cyber threats have shifted from isolated incidents to systematic strategies employed by both state and non-state actors. These threats often target critical infrastructure, including energy systems, financial institutions, and communication networks, thereby creating vulnerabilities that can disrupt national stability without direct military confrontation. Furthermore, hybrid warfare strategies integrate cyber operations with political, economic, and informational tactics, making them more difficult to detect and counter. As a result, traditional legal frameworks, which are primarily designed to regulate conventional warfare, struggle to provide adequate responses. This mismatch highlights the need for a legal transformation that incorporates flexibility, adaptability, and technological awareness to effectively address modern security challenges (Syaidi and Suparno 2021).

Another key finding demonstrates that existing national defense laws lack clear provisions regarding the attribution of cyberattacks and the classification of cyber operations within the context of armed conflict. The absence of precise legal definitions creates ambiguity in

determining whether a cyber incident constitutes an act of war, a criminal offense, or a form of espionage. This ambiguity complicates decision-making processes for policymakers and defense institutions, particularly when responding to cross-border cyber incidents. Moreover, the difficulty in attributing cyberattacks to specific actors further exacerbates the issue, as attackers can obscure their identities through sophisticated techniques. Consequently, states often face challenges in applying appropriate legal responses, including retaliation or enforcement measures. These findings suggest that legal reform must prioritize the development of clear definitions and attribution mechanisms to enhance the effectiveness of national defense law in the digital era (Syaidi 2024).

The research also finds that the integration of civilian and military domains in cyberspace presents significant challenges for national defense law. Unlike traditional warfare, where military operations are clearly separated from civilian life, cyber operations often occur within civilian infrastructure, such as private networks and commercial platforms. This overlap raises complex legal and ethical questions regarding the protection of civilian assets and the proportionality of responses to cyber threats. Additionally, private sector entities play a critical role in managing and securing digital infrastructure, yet their involvement in national defense strategies is often not clearly defined within existing legal frameworks. As a result, there is a growing need for legal provisions that establish clear roles and responsibilities for both public and private actors in cybersecurity. This finding underscores the importance of adopting a comprehensive approach to national defense law that accounts for the interconnected nature of modern digital ecosystems (TARIGAN 2024b).

Furthermore, the study identifies that current legal frameworks are often reactive rather than proactive in addressing cyber threats and hybrid warfare. Many laws are developed in response to specific incidents rather than anticipating future challenges, resulting in a lag between technological advancements and legal adaptation. This reactive approach limits the ability of states to effectively prevent cyberattacks and mitigate their impacts. In contrast, a proactive legal framework would emphasize risk assessment, early warning systems, and preventive measures, enabling states to address potential threats before they escalate. The findings suggest that adopting a forward-looking approach to legal development is essential for enhancing national resilience in the face of evolving cyber threats. This shift requires not only legal innovation but also close collaboration between policymakers, technologists, and security experts (TARIGAN 2024a).

The research further reveals that international cooperation plays a crucial role in addressing cyber threats and hybrid warfare, yet existing legal mechanisms for such cooperation remain limited. Cyber threats are inherently transnational, often involving actors and infrastructures located in multiple jurisdictions. However, differences in national laws, political interests, and technological capabilities hinder effective collaboration between states. Additionally, there is a lack of universally accepted norms and standards governing state behavior in cyberspace, leading to inconsistencies in responses to cyber incidents. These challenges highlight the need for stronger international legal frameworks and cooperative mechanisms that facilitate information sharing, joint investigations, and coordinated responses. The findings emphasize that the transformation of national defense law must also consider the global dimension of cyber threats, ensuring alignment with international legal principles and practices (Tarigan 2024).

Another important finding is that the rapid pace of technological innovation continues to outstrip the ability of legal systems to adapt effectively. Emerging technologies such as artificial intelligence, big data analytics, and the Internet of Things have introduced new

dimensions to cyber threats and hybrid warfare. These technologies enable more sophisticated attacks, including automated cyber operations and large-scale disinformation campaigns, which are difficult to regulate using traditional legal approaches. The research indicates that legal frameworks must evolve in tandem with technological advancements, incorporating mechanisms for continuous review and adaptation. This finding underscores the importance of integrating technological expertise into the legal development process, ensuring that laws remain relevant and effective in a rapidly changing digital environment (Tarigan and SH n.d.).

The study also finds that there is a significant gap in institutional capacity for implementing transformed national defense laws. Even when legal frameworks are updated, their effectiveness depends on the ability of institutions to enforce and operationalize them. Many states face challenges in terms of limited technical expertise, inadequate resources, and fragmented organizational structures, which hinder the implementation of cybersecurity policies. Additionally, coordination between different government agencies and stakeholders is often insufficient, leading to inefficiencies and gaps in response mechanisms. This finding highlights the need for capacity-building initiatives, including training programs, resource allocation, and institutional reforms, to support the effective implementation of legal transformations in national defense.

Moreover, the research identifies that public awareness and societal resilience are critical components of national defense in the digital era. Cyber threats and hybrid warfare often target not only infrastructure but also public perception and social cohesion through disinformation and psychological operations. However, existing legal frameworks tend to focus primarily on technical and institutional aspects, neglecting the role of society in national defense. The findings suggest that enhancing public awareness, promoting digital literacy, and fostering resilience against misinformation are essential elements of a comprehensive defense strategy. This broader perspective on national defense law emphasizes the need to integrate societal dimensions into legal and policy frameworks.

Finally, the research concludes that the transformation of national defense law requires a holistic and interdisciplinary approach that integrates legal, technological, and strategic perspectives. The complexity of cyber threats and hybrid warfare necessitates collaboration across multiple fields, including law, cybersecurity, international relations, and information technology. The findings demonstrate that no single discipline can adequately address the challenges posed by digital conflict. Therefore, the development of effective legal frameworks must involve diverse expertise and perspectives, ensuring that all relevant aspects of national security are considered. This comprehensive approach is essential for creating resilient and adaptive legal systems capable of addressing the multifaceted nature of cyber threats and hybrid warfare.

EVOLVING DIGITAL CONFLICT



**Cyber Threats & Hybrid Warfare
(State & Non-State Actors)**



Targets:

- Critical Infrastructure
- Hybrid Strategies
- Advanced Technology



LEGAL & STRUCTURAL CHALLENGES:

- Weak legal definitions
- Attribution ambiguity
- Civil-military overlap
- Reactive frameworks
- Limited cooperation
- Capacity gaps
- Low public awareness



INADEQUATE TRADITIONAL LAW



NEED FOR TRANSFORMATION:

- Flexibility & adaptability
- Clear attribution
- Public-private synergy
- Proactive approach
- Global cooperation
- Tech integration
- Capacity building



RESILIENT NATIONAL DEFENSE

1. Reconceptualizing National Defense Law in the Digital Era

The transformation of national defense law in the digital era requires a fundamental reconceptualization of how states understand security and sovereignty. Traditionally, national defense law has been closely associated with territorial protection and the use of armed forces in physical domains such as land, sea, and air. However, the emergence of cyberspace as a strategic domain has disrupted these conventional assumptions, requiring legal frameworks to expand beyond geographic boundaries. Cyber threats operate in a borderless environment where attacks can be launched remotely, often without clear indicators of origin. This reality challenges the core principles of traditional defense law, particularly those related to jurisdiction and enforcement. Therefore, reconceptualizing national defense law involves redefining the scope of defense to include digital infrastructure, information systems, and data integrity as critical components of national security. This shift is essential to ensure that legal systems remain relevant and capable of addressing contemporary threats.

In addition to expanding the scope of national defense, reconceptualization also involves rethinking the actors involved in defense strategies. Unlike conventional warfare, where the military plays a dominant role, cyber defense requires the participation of multiple stakeholders, including government agencies, private sector entities, and even individual citizens. This multi-actor environment necessitates legal frameworks that clearly define roles, responsibilities, and coordination mechanisms among different actors. Without such clarity, responses to cyber threats may become fragmented and ineffective. Furthermore, the involvement of non-state actors introduces additional complexities, particularly in terms of accountability and oversight. As a result, national defense law must evolve to accommodate a more inclusive and collaborative approach to security, ensuring that all relevant stakeholders are effectively integrated into defense strategies.

Another important aspect of reconceptualization is the need to incorporate technological considerations into legal frameworks. Cyber threats are inherently technical in nature, involving sophisticated tools and methods that are constantly evolving. Consequently, legal systems must be designed with a degree of flexibility that allows them to adapt to technological changes. This may involve the inclusion of technology-neutral provisions that remain applicable despite advancements in digital capabilities. Additionally, policymakers must work closely with technical experts to ensure that legal regulations are both practical and enforceable. By integrating technological perspectives into legal development, states can create more robust and responsive defense laws that effectively address the challenges of the digital era.

The reconceptualization of national defense law also has implications for the balance between security and individual rights. Cybersecurity measures often involve surveillance, data collection, and monitoring activities that can infringe upon privacy and civil liberties. Therefore, legal frameworks must strike a careful balance between ensuring national security and protecting fundamental rights. This requires the establishment of clear safeguards, transparency mechanisms, and accountability structures that prevent the misuse of power. By maintaining this balance, states can enhance public trust and legitimacy, which are essential for the effective implementation of national defense strategies.

Ultimately, reconceptualizing national defense law is a critical step in adapting to the realities of the digital era. The findings of this research suggest that without such transformation, existing legal frameworks will remain inadequate in addressing the complexities of cyber threats and hybrid warfare. By expanding the scope of defense, redefining the roles of stakeholders, integrating technological considerations, and balancing security with individual rights, states can develop more effective and resilient legal systems. This comprehensive approach ensures that national defense law evolves in line with emerging challenges, thereby strengthening overall national security in an increasingly interconnected world.

2. Addressing Legal Ambiguity in Cyber Threat Attribution and Classification

One of the most pressing challenges identified in this research is the legal ambiguity surrounding the attribution and classification of cyber threats. Attribution refers to the process of identifying the source of a cyberattack, which is often complicated by the use of anonymization techniques, proxy servers, and false flags. This complexity creates significant difficulties for states in determining responsibility and formulating appropriate responses. Without clear attribution, it becomes nearly impossible to apply legal principles such as self-defense or retaliation. Consequently, this ambiguity undermines the effectiveness of national defense law and weakens deterrence mechanisms. Addressing this issue requires the

development of more sophisticated attribution frameworks that combine legal, technical, and intelligence-based approaches.

In addition to attribution challenges, the classification of cyber incidents presents another layer of legal complexity. Existing legal frameworks often lack clear criteria for distinguishing between different types of cyber activities, such as cybercrime, cyber espionage, and cyber warfare. This lack of clarity can lead to inconsistent responses and legal uncertainty, particularly when cyber incidents escalate in severity. For instance, it may be difficult to determine whether a cyberattack on critical infrastructure constitutes an act of war or a criminal offense. Such ambiguity can delay decision-making processes and hinder effective responses. Therefore, establishing clear legal definitions and classification systems is essential for improving the coherence and predictability of national defense law.

The development of standardized legal definitions for cyber threats also has implications for international cooperation. Different states may interpret cyber incidents in varying ways, leading to disagreements and conflicts in response strategies. By harmonizing legal definitions and classification criteria, states can facilitate better coordination and collaboration in addressing cyber threats. This is particularly important given the transnational nature of cyber operations, which often involve multiple jurisdictions. Standardization can also contribute to the establishment of international norms and practices, enhancing stability in cyberspace.

Furthermore, improving attribution capabilities requires investment in technological infrastructure and expertise. Legal frameworks alone are insufficient without the technical means to support them. States must develop advanced cyber forensic capabilities, intelligence-sharing mechanisms, and collaborative platforms that enable accurate and timely attribution of cyberattacks. This interdisciplinary approach ensures that legal provisions are grounded in practical realities and can be effectively implemented. By strengthening both legal and technical capacities, states can enhance their ability to respond to cyber threats in a timely and proportionate manner.

In conclusion, addressing legal ambiguity in attribution and classification is a critical component of transforming national defense law. The findings of this research highlight the need for clear definitions, standardized frameworks, and enhanced technical capabilities to support legal processes. By resolving these ambiguities, states can improve the effectiveness of their legal responses, strengthen deterrence, and promote greater stability in cyberspace. This effort is essential for ensuring that national defense law remains relevant and capable of addressing the evolving nature of cyber threats and hybrid warfare.

3. Strengthening Civil-Military and Public-Private Integration

The integration of civilian and military domains represents a defining feature of cyber defense in the digital era, necessitating significant adjustments in national defense law. Unlike traditional warfare, where military operations are largely confined to designated combat zones, cyber operations frequently occur within civilian infrastructure, including private networks, communication systems, and commercial platforms. This overlap creates a complex legal environment in which the boundaries between civilian and military roles are increasingly blurred. As a result, national defense law must be restructured to accommodate this integration, ensuring that both sectors can effectively collaborate in addressing cyber threats while maintaining clear legal guidelines.

A key issue in this integration is the role of the private sector in national defense. Private companies own and operate a significant portion of critical digital infrastructure, making them essential partners in cybersecurity efforts. However, existing legal frameworks often do not clearly define the responsibilities and obligations of these entities in the context of national defense. This lack of clarity can lead to gaps in security and coordination, particularly during cyber incidents that require rapid and coordinated responses. Therefore, legal reforms must establish clear frameworks for public-private partnerships, including mechanisms for information sharing, joint response strategies, and resource allocation.

In addition to defining roles, effective integration requires the establishment of robust coordination mechanisms between civilian and military institutions. Cyber threats often require rapid responses that involve multiple agencies, including defense, intelligence, law enforcement, and regulatory bodies. Without effective coordination, these responses may become fragmented and inefficient. Legal frameworks must therefore include provisions for inter-agency collaboration, ensuring that all relevant actors can work together seamlessly. This may involve the creation of centralized coordination bodies or the implementation of standardized procedures for information exchange and decision-making.

Another important consideration is the protection of civilian infrastructure and populations during cyber operations. The integration of civilian and military domains increases the risk that defensive or offensive cyber measures may inadvertently impact civilian systems. As such, national defense law must include safeguards that ensure the protection of civilian assets and minimize collateral damage. This aligns with broader principles of international humanitarian law, which emphasize the importance of distinguishing between civilian and military targets. By incorporating these principles into national legal frameworks, states can enhance the legitimacy and ethical foundation of their cyber defense strategies.

Ultimately, strengthening civil-military and public-private integration is essential for developing a comprehensive and effective approach to national defense in the digital era. The findings of this research underscore the need for legal frameworks that facilitate collaboration while maintaining clear boundaries and safeguards. By addressing these challenges, states can enhance their capacity to respond to cyber threats and hybrid warfare, ensuring a more resilient and coordinated defense system.

5. CONCLUSION

The transformation of national defense law in addressing cyber threats and hybrid warfare in the digital era represents a critical and inevitable shift driven by the increasing complexity of modern security challenges. This study demonstrates that traditional legal frameworks are no longer sufficient to respond to the borderless, ambiguous, and technologically advanced nature of cyber conflict, which integrates civilian and military domains while involving diverse actors across sectors. The findings highlight key issues, including legal ambiguity in attribution and classification, limited institutional capacity, reactive policy approaches, and insufficient integration between public and private stakeholders. In response, the discussion emphasizes the need for a comprehensive reconceptualization of national defense law that incorporates flexibility, technological awareness, and interdisciplinary collaboration. Strengthening legal clarity, enhancing coordination mechanisms, and fostering international cooperation emerge as essential strategies to ensure effective responses to evolving threats. Ultimately, the transformation of national defense law is not merely a legal adjustment but a strategic necessity to safeguard national sovereignty, maintain stability, and build resilience in an increasingly interconnected and digitalized global environment.

6. REFERENCES

- Aji, Rubiyanto P., and Asep Adang Supriyadi. 2026. "Integration of Defense Policy and Public Policy From a National Security Perspective in Countering Hybrid Warfare Threats." *Indonesian Interdisciplinary Journal of Sharia Economics (IJJSE)* 9(1):760–77.
- Bratko, Artem, Denys Zaharchuk, and Valentyn Zolka. 2021. "Hybrid Warfare—a Threat to the National Security of the State." *Revista de Estudios En Seguridad Internacional* 7(1):147–60.
- Fitria, Rosi, and Asep Adang Supriyadi. 2025. "Integration of Cyber Defense and Conventional Security in Addressing Non-Military Threats in the Digital Era." *Journal of National Paradigm-Based Resilience Strategy* 2(02):85–99.
- Hidayati, Hidayati, Subhan Tirtayasa, Putra Iskandar, and Renaldi Nugraha. 2025. "Public Policy Law in Military Strategy and Conflict in Hybrid Warfare Operations in the Digital Era." *Edusight International Journal of Multidisciplinary Studies* 2(4).
- Khan, Muhammad Sanaullah, and Farhat Asghar Rana. 2025. "Hybrid Warfare in the Digital Age: Cyberpower, AI, and the Future of Global Security." *ASSAJ* 4(01):3050–65.
- Khoirunnisa, Khoirunnisa, Indrawati, Ambarwati, Yanuar Ramadhan, and Didi Jubaidi. 2025. "Cyber Warfare and National Security: Modernizing Defense Strategies in the Context of China's Evolving Cyber Influence." *China Quarterly of International Strategic Studies* 11(01):1–20.
- Otaiku, Ajayi Ayodele. 2018. "A Framework for Hybrid Warfare: Threats, Challenges and Solutions." *J Def Manag* 8(178):374–2167.
- Sawlani, Dhiraj Kelly, and Asep Adang Supriyadi. 2024. "BRIDGING PUBLIC POLICY AND DEFENSE STRATEGY TO COMBAT HYBRID WARFARE: AN ANALYTICAL STUDY ON NATIONAL SECURITY." *Jurnal Praksis Dan Dedikasi Sosial* 7(2):292–307.
- Syaidi, Ridwan. 2024. "Independence of the General Election Commission and Election Supervisory Board for Democratic Elections." *Jurnal Akta* 11(2):303–13.
- Syaidi, Ridwan, and Supamo Suparno. 2021. "Cyberbullying in Criminal Law Perspective." in *Proceedings of the First Multidiscipline International Conference, MIC*.
- Tarigan, Ridwan Syaidi. 2024. *Dinamika Implementasi Putusan Mahkamah Konstitusi*. Ruang Karya Bersama.
- TARIGAN, RIDWAN SYAIDI. 2024a. *Hukum Tata Negara Dan Transformasi Implikasi Dan Prospek Sosial*. Ruang Karya Bersama.
- TARIGAN, RIDWAN SYAIDI. 2024b. *Mahkamah Konstitusi Dalam Sistem Ketatanegaraan Indonesia*. Ruang Karya Bersama.
- Tarigan, Ridwan Syaidi, and M. H. SH. n.d. "Konstitusi Dan Konstitusionalisme."