

Hybrid Warfare And Asymmetric Conflict Repositioning The Counterinsurgency Doctrine In The Context Of 21st Century Defense Operations

Nopiyani¹

¹Indonesian National Defense University, Ministry of Defense of the Republic of Indonesia

Priyanto²

²Indonesian National Defense University, Ministry of Defense of the Republic of Indonesia

Sulistyono Reksoprodjo³

³Indonesian National Defense University, Ministry of Defense of the Republic of Indonesia

Corresponding Author: noviyani567@gmail.com

Abstract

Modern counterinsurgency (COIN) operations face increasingly complex challenges due to the changing nature of conflict and the growing involvement of local communities in security dynamics. Success in COIN is no longer determined solely by military power but by the state's capacity to build political legitimacy and community trust within conflict zones. This article analyzes the strategic role of local intelligence and civil and military partnerships in enhancing COIN effectiveness through trust-based community engagement. Drawing on a systematic review of scholarly works published between 2020 and 2025, the study finds that (1) local intelligence contributes by providing contextual understanding of social, cultural, and political networks; (2) civil and military cooperation strengthens legitimacy through communication and public service delivery; and (3) operational success depends on accountability, transparency, and the alignment between rhetoric and practice. Building community trust is thus identified as the foundation of sustainable stability and legitimacy in post-conflict governance.

Keywords: Counterinsurgency, Local Intelligence, Civil And Military, Community Trust, Legitimacy



INTRODUCTION

The transformation of the global battlefield over the past two decades has been marked by the emergence of forms of conflict that are increasingly difficult to distinguish clearly between conventional and unconventional warfare. The practice of hybrid warfare and asymmetric conflict has developed alongside advances in information technology, the globalization of data flows, and the increasing role of non-state actors in the international security landscape (Shvydanenko et al., 2022). The combination of overt military operations with non-military instruments such as cyberattacks, disinformation campaigns, economic pressure, and exploitation of social vulnerabilities has resulted in a pattern of conflict that operates in the gray zone between war and peace, often referred to as the gray zone. In this context, defense doctrines designed to deal with conventional warfare and classic insurgency are under pressure to adapt in order to remain relevant and effective (Kyselyova, 2022).

Hybrid warfare is generally understood as the simultaneous and integrated use of military, political, economic, information, and cyber instruments of power to achieve strategic objectives without triggering a formal declaration of war. This strategy relies heavily on ambiguity, plausible deniability, and the exploitation of loopholes in the international legal regime to avoid direct attribution while simultaneously undermining the legitimacy of the opponent in the eyes of the international community (Kyselyova, 2022). On the other hand, asymmetric conflicts refer to situations where the militarily weaker party adopts asymmetrical tactics to exploit the structural, political, or social vulnerabilities of the stronger party, including through guerrilla warfare, terrorism, proxy warfare, and the use of cyberspace as a medium for attack and mobilization of support (Siahaan & Risman, 2021). These two forms of conflict intersect and produce a threat configuration that is far more complex than the insurgency model that formed the basis for the birth of the classic counterinsurgency (COIN) doctrine.

The impact of hybrid warfare and asymmetric conflict is not limited to the military and political spheres, but also extends to the humanitarian, civil governance, and public health dimensions. The increasingly digitized and data-driven battlefield creates new risks for civilian populations, ranging from attacks on critical infrastructure such as energy, communications, and health services, to sabotage of public services and manipulation of information that affects perceptions, behavior, and social polarization (Fitz-Gerald & Hennebry, 2024). In the context of Russia's invasion of Ukraine, for example, the combination of conventional military operations, cyber attacks on healthcare systems and vital infrastructure, and cross-border disinformation



campaigns has had a direct impact on the physical safety of citizens, the continuity of medical services, and the social resilience of civil society (Khorram-Manesh & Burkle, 2023). Recent studies show that civilian victims in hybrid conflicts tend to suffer multiple losses, including loss of life, health problems, psychosocial vulnerability, and the destruction of public services needed for long-term recovery (Khorram-Manesh & Burkle, 2022).

Historically, the COIN doctrine was developed to deal with forms of insurgency that were relatively clear in terms of geographical area, actors, and patterns of violence. This approach emphasizes a combination of military operations, political efforts, and socio-economic programs to win the support of the local population, known as the hearts and minds strategy. The doctrine essentially assumes that insurgents and the government compete for the loyalty of the population in a more or less defined territory, with identifiable authority structures and lines of command (Asmoro et al., 2021). However, in the era of hybrid warfare, such assumptions are no longer adequate. The boundaries between combatants and non-combatants are increasingly blurred, the conflict space extends to the cyber and information domains that are cross-border in nature, and the actors involved are often not within a single jurisdiction or even a single region (Kyselyova, 2022). This situation raises fundamental questions about the extent to which existing COIN conceptual and operational frameworks are capable of responding to the demands of defense operations that are now multidomain, distributed, and fraught with ambiguity.

Advances in military and security technology have added a new layer of complexity to COIN doctrine. Artificial intelligence, autonomous weapons systems, armed drones, high-resolution satellite surveillance, and big data analytics and pattern recognition capabilities have changed the way military operations are planned and executed, including operations claimed to be COIN (Duchêne et al., 2022). On the one hand, this technology enables early detection, broader surveillance, and more precise targeting, which in theory can reduce civilian casualties. On the other hand, the use of algorithms in military decision-making raises new ethical and legal issues: who is responsible in the event of a misfire, how to measure proportionality and military necessity in the context of autonomous systems, and to what extent the use of such technology is in line with the principles of international humanitarian law (Kavanagh & Lindsay, 2024). This tension between operational efficiency and the protection of civilians demands a paradigm shift in COIN so that it is not only militarily effective, but also legally and morally legitimate and accountable.



In this context, studies on the protection of civilians in digitized conflict zones are becoming increasingly important. Technological infrastructure that supports military operations and is also the backbone of civilian services, such as electricity networks, communication systems, and health data platforms, makes the line between military targets and civilian objects increasingly fragile (Fitz-Gerald & Hennebry, 2024). Attacks on digital infrastructure not only cause technical disruptions, but can also lead to the failure of health care systems, disruption of humanitarian aid distribution, and increased mortality and morbidity among vulnerable populations (Khorram-Manesh & Burkle, 2022). This is where 21st-century COIN needs to be understood not only as an instrument for suppressing insurgencies, but also as an operational framework that must be able to protect, maintain, and restore vital community functions amid the pressures of hybrid warfare.

The Ukraine case is often referred to as a contemporary laboratory for hybrid warfare practices and is an important reference for assessing the relevance and limitations of existing COIN doctrines (Shvydanenko et al., 2022). There, we witness how conventional military operations are combined with the use of proxy actors, coordinated cyber attacks, exploitation of social media, and manipulation of narratives targeting domestic and international public opinion (Khorram-Manesh & Burkle, 2023). The response of the international community, which includes economic sanctions, military support, and efforts to document violations of humanitarian law, shows that hybrid warfare forces not only the countries directly involved, but also international organizations and coalitions of countries, to review their collective tools and mechanisms in facing this new spectrum of threats (Kyselyova, 2022). This experience reinforces the urgency of repositioning the COIN doctrine to be more sensitive to the legal, technological, and humanitarian dimensions of contemporary conflicts.

Although literature on hybrid warfare and asymmetric conflicts has grown rapidly, there is still a gap in research on how COIN needs to be reformulated more systematically amid the changing conflict landscape. Most discussions still focus on tactical descriptions and case studies, while theoretical elaborations on the integration of COIN with the concepts of multi-domain operations, the framework of lawfare, and civilian protection in the digital domain are not yet fully developed (Hoijtink, 2022). In addition, there is a need to review organizational structures, civil-military coordination mechanisms, and the culture of innovation within defense institutions in order to respond to the volatility and uncertainty of hybrid threats (Hoijtink, 2022).



Based on this background, this article aims to analyze the repositioning of counterinsurgency doctrine in the context of hybrid warfare and 21st-century asymmetric conflict. The analysis is conducted through a literature review of the development of the concept of hybrid warfare, the dynamics of international law and norms, and a case study of Ukraine as an illustration of contemporary practice. The main focus is on three dimensions, namely the conceptual adjustment of COIN within the framework of multi-domain operations, the legal and humanitarian implications of hybrid warfare practices, and the need for organizational innovation and defense governance in facing a new spectrum of threats (Kavanagh & Lindsay, 2024). Thus, this article is expected to provide theoretical and practical contributions to the development of more adaptive, responsive, and human-centered defense doctrines and policies in the era of hybrid warfare.

Research Method

This study uses a qualitative approach with a descriptive-analytical library research design. This approach was chosen because the main objective of the article is to thoroughly examine the repositioning of the counterinsurgency doctrine in the context of hybrid warfare and asymmetric conflict through tracing concepts, arguments, and empirical findings that are already available in scientific literature (Hoijtink, 2022). The qualitative approach allows the author to interpret the relationships between concepts, rather than simply measuring variables, making it more suitable for answering conceptual and normative questions related to COIN, civilian protection, and multidomain operations (Kyselyova, 2022).

The main data sources are indexed journal articles, academic books, research reports, and policy documents relevant to the themes of hybrid warfare, asymmetric conflicts, COIN doctrine, international humanitarian law, civilian protection, and developments in military and cyber technology. Literature searches were conducted through online scientific databases using structured keywords, including “hybrid warfare,” “asymmetric conflict,” “counterinsurgency,” “civilian protection,” “multi-domain operations,” “autonomous weapons,” and “AI-enabled cyber operations.” From the search results, priority was given to literature published in the last ten years or so, with particular attention to recent publications on the impact of hybrid warfare on civilian populations and health systems, as well as the risk of escalation in cyberspace (Kavanagh & Lindsay, 2024).



Source selection was conducted using several inclusion criteria. First, the work must be directly relevant to the concepts of hybrid warfare and/or COIN, both theoretically and empirically (Shvydanenko et al., 2022). Second, the literature must contain discussions on the legal, humanitarian, or normative implications of hybrid conflict practices, including issues of lawfare, attribution, and civilian protection (Kyselyova, 2022). Third, as far as possible, articles presenting concrete case studies such as the conflict in Ukraine were selected so that the analysis would not only be abstract but also connected to the dynamics on the ground (Khorram-Manesh & Burkle, 2023). Sources that only discussed narrow technical aspects without a clear connection to COIN or civilian protection were excluded from the main corpus of the analysis.

The collected data was analyzed using qualitative content analysis techniques. The first stage was a comprehensive reading to identify core concepts, such as the definition of hybrid warfare, the characteristics of asymmetric conflict, the population-centric COIN approach, the issue of lawfare, and the role of artificial intelligence and autonomous systems in military operations (Duchêne et al., 2022). The next stage was thematic categorization by grouping the literature findings into several major themes, including changes in the conflict landscape and their implications for COIN, the legal and humanitarian dimensions of hybrid warfare, and the need for organizational and doctrinal innovation. Each theme was then synthesized to formulate arguments regarding the necessary repositioning of COIN doctrine in the era of hybrid warfare (Hoijsink, 2022).

This study acknowledges its limitations, particularly because all data is secondary and highly dependent on the availability and quality of existing literature. The rapidly changing dynamics of technology and the conflict environment also have the potential to render some findings obsolete (Kavanagh & Lindsay, 2024). However, through the selection of up-to-date sources and systematic thematic analysis, it is hoped that this method will still be able to provide a strong basis for conceptual understanding and normative recommendations related to the repositioning of counterinsurgency doctrine in the context of 21st-century defense operations.

RESULTS AND DISCUSSION

1. Conceptual Repositioning of the COIN Doctrine in the Hybrid Warfare Environment

Based on a review of the literature, one of the main findings is that the classic counterinsurgency doctrine rooted in colonial and Cold War experiences is no longer adequate to explain and guide operations in the contemporary hybrid warfare environment (Shvydanenko



et al., 2022). Traditional COIN is based on the assumption that insurgents have a relatively clear identity, area of operation, and organizational structure, and that there is direct competition between the state and rebel groups for the support of the local population. In the practice of hybrid warfare, this pattern has shifted to a constellation of threats involving a combination of state and non-state actors, overt and covert military operations, and the use of the cyber and information domains as the primary medium of operations (Kyselyova, 2022).

The conceptual repositioning that emerged from this study shows that COIN needs to be understood as part of a multidomain operational framework that integrates the land, sea, air, cyber, and space dimensions into a single campaign (Hojtink, 2022). Within this framework, COIN operations are no longer limited to the physical suppression of insurgents in a region, but also include countering disinformation campaigns, securing digital infrastructure, and protecting the community's information ecosystem. The population-centric approach remains relevant, but its manifestation has shifted from merely physical development programs and basic services to strengthening digital literacy, information resilience, and public trust in state institutions (Fitz-Gerald & Hennebry, 2024).

Other findings indicate that modern COIN must integrate human security perspectives more explicitly. The protection of civilians is no longer viewed merely as an ethical consequence of military operations, but as a center of gravity that determines the legitimacy and long-term success of operations (Khorram-Manesh & Burkle, 2022). Thus, the conceptual repositioning of COIN requires a shift in focus from simply defeating the enemy to maintaining the sustainability of social and institutional functions of society amid the pressures of hybrid warfare. This expands COIN from a purely military doctrine framework to a policy framework that involves civilian actors, international institutions, and local communities in a broader security architecture (Hojtink, 2022).

2. Legal and Humanitarian Dimensions in COIN Practices in the Hybrid Era

Another important finding relates to the increasing role of international law and the dynamics of lawfare in the context of hybrid warfare. A review of the literature shows that both state and non-state actors actively exploit the complexity and loopholes in the international legal regime, both humanitarian law and human rights law, to strengthen their own position or weaken the legitimacy of their opponents (Kyselyova, 2022). In this context, COIN operations no longer face only kinetic threats, but also the risk of delegitimization through allegations of legal



violations, the digital documentation of war crimes, and the framing of narratives in the global public sphere (Khorram-Manesh & Burkle, 2022).

Hybrid warfare in Ukraine illustrates how physical, cyber, and information attacks have a direct impact on civilians and health systems (Khorram-Manesh & Burkle, 2023). Attacks on health infrastructure, power outages, disruption of hospital information systems, and disinformation targeting the civilian population have caused significant humanitarian burdens, ranging from increased mortality and morbidity to disruption of basic health services (Fitz-Gerald & Hennebry, 2024). A systematic review shows that in a hybrid context, the victimization of civilians occurs not only through direct violence, but also through systemic disruption of public services, logistics chains, and community health ecosystems (Khorram-Manesh & Burkle, 2022). This reinforces the argument that civilian protection must be a key parameter in reformulating COIN practices.

Within the framework of modern COIN, commanders and policymakers need to consider that every operational decision has legal and humanitarian implications that are digitally documented and can be reviewed in the long term (Khorram-Manesh & Burkle, 2022). The use of autonomous weapons, cyber operations against civilian infrastructure, and the use of population data for military purposes, for example, raise new questions about proportionality, the distinction between combatants and non-combatants, and accountability in decision-making (Kavanagh & Lindsay, 2024). Thus, the repositioning of COIN cannot be separated from strengthening legal analysis capacity within the command structure, developing specific rules of engagement for the cyber domain and information space, and closer collaboration with humanitarian actors and international institutions (Kyselyova, 2022).

Overall, the results of the study show that legal and humanitarian dimensions are no longer additional elements, but have become an integral part of the design, implementation, and evaluation of COIN operations in the era of hybrid warfare. Failure to integrate these dimensions risks long-term consequences in the form of erosion of legitimacy, international sanctions, and a cycle of violence that is increasingly difficult to end (Khorram-Manesh & Burkle, 2022).

3. Organizational, Technological, and Defense Governance Innovation

The third dimension that emerged strongly from the study results was the need for organizational and defense governance innovation in order to adapt to the experimental and rapidly changing nature of conflict. The concept of prototype warfare shows that the military and



defense institutions are increasingly driven to adopt iterative, trial-based innovation patterns and be ready to continuously adjust doctrine and structure (Hoijtink, 2022). In the context of COIN, this means that approaches, tactics, and even unit structures can no longer be treated as fixed packages, but must be viewed as prototypes that are tested in various hybrid environments and continuously refined.

Advances in artificial intelligence, autonomous systems, drones, and big data analytics provide significant opportunities to improve the effectiveness of threat detection, mapping of insurgent networks and hybrid actors, and faster, data-driven decision-making (Duchêne et al., 2022). However, the literature also highlights considerable risks, particularly related to algorithmic bias, lack of transparency in automated decision-making processes, and the potential for unexpected escalation when artificial intelligence systems are used in offensive cyber operations (Kavanagh & Lindsay, 2024). In this context, COIN that relies on advanced technology without being balanced by strong governance mechanisms has the potential to accelerate conflict escalation and expand the impact on civilians.

The findings of the study emphasize the importance of building organizational resilience that does not only rely on technological superiority, but also on institutional learning capacity, a culture of critical reflection, and cross-sector coordination (Hoijtink, 2022). A whole-of-government and even whole-of-society approach is becoming increasingly important as hybrid threats transcend traditional boundaries between the military and civilian spheres. Data integration and policy coordination between the ministries of defense and foreign affairs, health agencies, cyber agencies, and domestic security authorities are prerequisites for effective and legitimate COIN in this era (Khorram-Manesh & Burkle, 2023).

Thus, the results and discussion show that COIN repositioning in the era of hybrid warfare cannot be done partially. Conceptual adjustments, strengthening of legal and humanitarian dimensions, and organizational and technological innovations must be viewed as a single process. 21st-century COIN is required to be more adaptive, integrated, and human-centered, while maintaining military effectiveness in facing an increasingly complex spectrum of threats (Kyselyova, 2022).



CONCLUSION

This paper demonstrates that the emergence of hybrid warfare and asymmetric conflict has fundamentally changed the landscape of defense operations and challenged the relevance of classic counterinsurgency doctrine. The boundaries between war and peace, combatants and non-combatants, and the physical and cyber domains are becoming increasingly blurred, so that COIN can no longer be understood solely as counterinsurgency operations at the tactical level, but as part of a much broader and more complex multidomain security architecture.

In this situation, the protection of civilians, humanitarian governance, and compliance with the international legal framework need to be placed at the center of gravity in the reformulation of COIN. Hybrid warfare not only produces direct violence, but also disrupts critical infrastructure, health services, and the information ecosystem that supports social life. Therefore, the success of COIN cannot be measured solely by the weakening of the opponent's capacity, but rather by the ability to maintain social functions, minimize civilian casualties, and maintain the legitimacy of the state in the eyes of the public.

In addition to conceptual repositioning and strengthening the legal-humanitarian dimension, organizational and technological innovation are essential prerequisites. 21st-century COIN requires institutional learning capacity, responsible integration of technology, and a collaborative, cross-sectoral approach. Only in this way can the COIN doctrine evolve into an adaptive, human-centered defense instrument that remains effective in the face of an ever-evolving spectrum of hybrid threats.

References

- Asmoro, N., Widodo, P., Putro, R. W., Hidayat, C., & Putri, R. M. (2021). Terrorism threat in doctrine formulating of military campaign scenario to achieve national security: On estimative methodology review. *Humanities and Social Science Research*, 4(3), 25–33. <https://doi.org/10.30560/hssr.v4n3p25>
- Duchêne, C., Bouhlel, M. A., & others. (2022). Recent advances in artificial intelligence and tactical autonomy: Current status, challenges, and perspectives. *Sensors*, 22(24), 9916. <https://doi.org/10.3390/s22249916>
- Fitz-Gerald, A., & Hennebry, J. (2024). Protecting civilians in a data-driven and digitalized battlespace: Toward a baseline humanitarian technology infrastructure. *Frontiers in*



- Human Dynamics, 6, 1465594. Retrieved from <https://www.frontiersin.org/articles/10.3389/fhumd.2024.1465594/full>
- Hoijsink, M. (2022). Prototype warfare: Innovation, optimisation and the experimental way of warfare. *European Journal of International Security*, 7(3), 322–336. <https://doi.org/10.1017/eis.2022.12>
- Kavanagh, C., & Lindsay, J. R. (2024). Escalation risks in cyberspace: How AI-enabled cyber operations shape crisis stability. *arXiv preprint arXiv:2406.08963*. Retrieved from <http://arxiv.org/pdf/2406.08963.pdf>
- Khorram-Manesh, A., & Burkle, F. M. (2022). Civilian population victimization: A systematic review comparing humanitarian and health outcomes in conventional and hybrid warfare. *Disaster Medicine and Public Health Preparedness*, 17, e192. <https://doi.org/10.1017/dmp.2022.96>
- Khorram-Manesh, A., & Burkle, F. M. (2023). Social and healthcare impacts of the Russian-led hybrid war in Ukraine: A conflict with unique global consequences. *Disaster Medicine and Public Health Preparedness*, 17, eXXX (ahead-of-print).
- Kyselyova, N. (2022). Civilian population victimization: Legal and political dimensions of hybrid warfare in Ukraine. *Kyiv-Mohyla Law and Politics Journal*, 8, 71–92. Accessed from <http://kmlpj.ukma.edu.ua/article/download/220732/220352>
- Shvydanenko, O., Duginets, G., Tkachenko, O., Kotenok, A., & Busarieva, T. (2022). Analysis of crisis strategies in the conditions of modern hybrid war. *Financial and Credit Activity: Problems of Theory and Practice*, 6(41), 250–257. <https://doi.org/10.18371/fcaptp.v6i41.251447>
(Full text: <http://fkd1.ubs.edu.ua/article/download/251447/249087>)
- Siahaan, S., & Risman, H. (2021). Contemporary irregular warfare: Defense strategy. *Journal of Social and Political Sciences*, 4(1), 55–63. <https://doi.org/10.31014/aior.1991.04.01.249>
(Full text: <https://zenodo.org/record/4436765/files/jsp0771%20sotardodo.pdf>)

