

The Shivapuri

Volume: XXVII, 2026

DOI: <https://doi.org/10.3126/shivapuri.v27i1.90946>

Army Command and Staff College, Nepali Army

Shivapuri, Kathmandu, Nepal

The Gerasimov Doctrine and the Emerging Challenges for the Nepali Army

- ***Brig Gen Madhab Thapa*** (*thapamadhab9@gmail.com*)

Abstract

This article examines the relevance of the Gerasimov Doctrine as an analytical lens for understanding hybrid warfare and its implications for the Nepali Army. Although the concept emerged from a Russian strategic context, its emphasis on the integrated use of non-military instruments, information dominance, and indirect coercion offers useful insights into contemporary conflict dynamics confronting vulnerable states. Twenty-first-century warfare increasingly extends beyond conventional military confrontation, unfolding across informational, cyber, economic, and psychological domains. For small, non-aligned states such as Nepal, these multidimensional threats present complex challenges that traditional defense frameworks are often ill-equipped to address. Through a qualitative analysis of Nepal's security environment, institutional arrangements, and recent crisis experiences, based on government policy documents, military and security reports, and other secondary sources, the study offers a Nepal-specific analysis of hybrid threats - defined as the coordinated use of military and non-military means by state or non-state actors to exploit vulnerabilities below the threshold of open conflict - that has received limited attention in existing literature. The analysis shows that Nepal's experiences with disinformation campaigns, cyber incidents, economic pressure, and contested narratives are not isolated occurrences but part of broader patterns of hybrid conflict. Drawing on comparative security literature and Nepal's own strategic constraints, the article proposes context-specific reforms, including the formulation of a hybrid warfare doctrine, strengthening of cyber and information operations capacity, improved intelligence integration, reform of officer education, and initiatives to enhance societal resilience. The study concludes that protecting Nepal's sovereignty in the evolving security environment requires a strategic shift toward anticipatory, multi-domain defense grounded in whole-of-government coordination and strengthened civil-military synergy.

Keywords

Gerasimov Doctrine, hybrid warfare, Nepali Army, cyber operations, information warfare, national resilience, small state security

Introduction

The character of conflict in the twenty-first century has evolved significantly, with the distinction between war and peace increasingly blurred. Contemporary conflicts combine conventional force with irregular, informational, cyber, and economic instruments, enabling actors to pursue strategic objectives without overt military confrontation (Hoffman, 2007; Coker, 2015). Such multidimensional approaches pose acute challenges for small, non-aligned militaries operating in complex geopolitical environments, including Nepal (McAllister & Miklaucic, 2016).

Gerasimov's analysis of modern warfare underscores the growing primacy of non-military means - political influence, information manipulation, and economic pressure - over direct kinetic force (Gerasimov, 2013). While the concept emerged from a Russian strategic context and is often associated with Moscow's operations in Ukraine and beyond, its value lies less in doctrinal replication than in its analytical utility for understanding indirect, multi-domain coercion (Giles, 2016; Renz, 2016). For smaller states, such pressures may manifest without crossing the threshold of armed conflict, yet still erode national cohesion, institutional stability, and decision-making autonomy.

Hybrid warfare, understood as the coordinated employment of military and non-military instruments across multiple domains to achieve strategic effects, is not exclusive to any single actor or region; historical and contemporary studies demonstrate its reliance on the coordinated use of political, psychological, cyber, and limited conventional tools across multiple domains (Lia, 2019). Nepal's geopolitical position between two major powers, coupled with internal political volatility and growing information exposure, increases its vulnerability to such forms of influence. Disinformation, economic leverage, cyber incidents, and contested narratives can challenge governance and military effectiveness by distorting public trust and strategic judgment.

This article argues that a Gerasimov-informed analytical lens can help the Nepali Army better understand and respond to emerging hybrid threats without adopting foreign doctrines wholesale. It contends that strengthening institutional resilience requires context-specific adaptation in doctrine, leadership development, mission command practices, and multi-domain preparedness. By integrating policy, professional military education, and whole-of-government coordination, the Nepali Army can enhance its

capacity to safeguard national sovereignty in an increasingly contested security environment.

Literature Review: Understanding the Gerasimov Doctrine

The term “Gerasimov Doctrine” originates from a 2013 article by the Russian Chief of the General Staff, General Valery Gerasimov, titled *The Value of Science in Prediction*, published in *Voennaya Mysl*. The concept gained prominence in Western strategic discourse following Mark Galeotti’s English translation and analysis in 2014 (Gerasimov, 2013; Galeotti, 2014). Galeotti later clarified that the label “doctrine” reflects a Western interpretive construct rather than a formally articulated Russian strategic doctrine (Galeotti, 2018). Despite this clarification, the ideas attributed to Gerasimov have remained influential in scholarly and policy debates on contemporary and hybrid warfare.

Gerasimov argued that modern conflicts increasingly rely on non-military instruments to shape strategic outcomes prior to the outbreak of overt hostilities, emphasizing that political, informational, and economic means may prove more effective than direct military force (Gerasimov, 2013). This emphasis reflects a broader strategic tradition in which indirect methods such as psychological pressure, information control, and political manipulation, play decisive roles in statecraft. Classical strategic texts, including Chanakya Niti, similarly emphasize intelligence, subversion, and perception management as critical instruments of power, despite differences in historical and cultural context (Kautilya, trans. 1992).

Contemporary scholars conceptualize the so-called Gerasimov Doctrine as the coordinated application of political, economic, informational, cyber, and military tools to achieve strategic objectives while avoiding large-scale conventional conflict (Bartles, 2016; Fridman, 2018). These methods may include disinformation campaigns, manipulation of traditional and social media, economic coercion, cyber operations, and the selective use of deniable or proxy forces (Giles, 2016; Renz, 2016). The emphasis on narrative shaping and societal mobilization parallels Mao Zedong’s concept of prolonged, politically driven struggle, in which conflict extends beyond the battlefield into informational and psychological domains (Mao, 1967).

The widely cited Gerasimov framework suggests that a substantial proportion of contemporary conflict activity occurs below the threshold of open armed violence (Gerasimov, 2013; Bartles, 2016). While often illustrated through the case of Crimea, the framework is best understood as a conceptual representation of emphasis rather than a

quantitative or prescriptive model of warfare. Its central insight lies in demonstrating how rapid, ambiguous, and non-kinetic pressures can compress decision-making timelines and blur the distinction between war and peace, particularly for small and medium states (Giles, 2016).

The application of these ideas is frequently identified in Russia's annexation of Crimea in 2014, where coordinated information operations, cyber activities, diplomatic pressure, and limited military force shaped political conditions faster than effective resistance could be organized (Giles, 2016; Marten, 2017). Similar, though context-specific, patterns have been observed in other Russian operations, reinforcing scholarly arguments that speed, narrative control, and political influence can be as decisive as conventional military power.

For states such as Nepal, situated between major powers and characterized by periodic internal political volatility, the literature on the Gerasimov framework underscores the growing importance of preparedness against hybrid threats. Scholars note that vulnerabilities may emerge through disinformation, cyber intrusions, societal polarization, or economic pressure rather than direct military aggression (Ghale, 2020; Kattel, 2021; Adhikari, 2022). Policy-oriented studies by NATO Allied Command Transformation (2014) and U.S. Army TRADOC (2017) further emphasize the necessity of adapting military and institutional structures to address multidimensional, non-traditional challenges in contemporary security environments.

Methodology

This study employed a qualitative, interpretive approach based on a focused review of primary and secondary sources. Primary material includes Russian military writings, particularly General Valery Gerasimov's 2013 article *The Value of Science in Prediction*. Secondary sources consist of peer-reviewed scholarship, academic books, and policy documents from established defense and security institutions. Relevant literature was identified through targeted searches of academic databases using keywords related to hybrid warfare and gray-zone conflict. The analysis follows a thematic approach, examining recurring ideas on non-military instruments of power and their implications for small-state security, with specific reference to Nepal.

Strategic Relevance of Gerasimov Doctrine for Small States

The strategic principles commonly associated with the Gerasimov framework extend beyond Russia's experience and hold particular relevance for small states with limited conventional capabilities. Nepal's geographic position between two major regional

powers; India and China exposes it to a complex spectrum of hybrid pressures that exploit institutional vulnerabilities, political volatility, and socio-economic dependencies (Galeotti, 2014; Ghale, 2020). Even in the absence of armed conflict, such pressures operate through non-kinetic means that target political decision-making, information environments, and economic stability (Hoffman, 2007).

At the core of the Gerasimov framework is the recognition that modern conflict increasingly relies on non-military instruments to achieve strategic effects. For Nepal, this presents distinct challenges, as national institutions remain in transition and coordination gaps persist across civil, military, and security sectors (Coker, 2015). Cyber operations, disinformation, and economic coercion can generate strategic outcomes without crossing the threshold of war, making them particularly consequential for small states with constrained response options.

Evidence of information operations affecting Nepal is already visible. Disinformation campaigns and external influence efforts have emerged during politically sensitive periods, including constitutional debates, episodes of instability, and border-related tensions (Adhikari, 2022). Such activities can erode public trust, distort narratives, and strain civil-military relations while avoiding overt confrontation (Giles, 2016).

From a Gerasimov perspective, the information domain functions as a battlespace in its own right. For Nepal, weaknesses in strategic communication and narrative coordination increase susceptibility to cognitive influence, complicating decision-making and undermining social cohesion before any kinetic escalation occurs.

Economic dependencies further intensify Nepal's exposure to hybrid tactics. Heavy reliance on remittances, cross-border trade, and foreign-financed infrastructure projects creates potential leverage points for external actors to influence domestic policy and strategic choices (Renz, 2016). When combined with regulatory and institutional gaps, these dependencies may gradually constrain policy autonomy and limit strategic flexibility.

Similarly, civil society also represents a potential vector for indirect influence. Nepal hosts a large number of NGOs and INGOs, many of which operate with limited transparency regarding funding sources and objectives (Karkee & Comfort, 2016). While these organizations contribute significantly to development and governance, gaps in oversight and inter-agency coordination can create opportunities for narrative shaping and policy influence aligned with external interests (The Kathmandu Post, 2019; myRepublica, 2025). The challenge lies not in civil society engagement itself, but in

ensuring transparency and regulatory coherence to protect national resilience while preserving democratic space.

Cyber defense and strategic communication capacities in Nepal remain underdeveloped. The absence of integrated mechanisms to detect, assess, and respond to hybrid threats has produced coordination gaps across military, civilian, intelligence, and diplomatic institutions (Kattel, 2021). These shortcomings reduce situational awareness and slow decision-making, allowing hybrid activities to shape perceptions and political conditions faster than coordinated responses can be mobilized.

For a force traditionally oriented toward territorial defense, this shift toward cognitive, informational, and cyber domains complicates conventional threat assessment. The Gerasimov framework highlights how such institutional lag can be exploited to achieve strategic outcomes without the use of force.

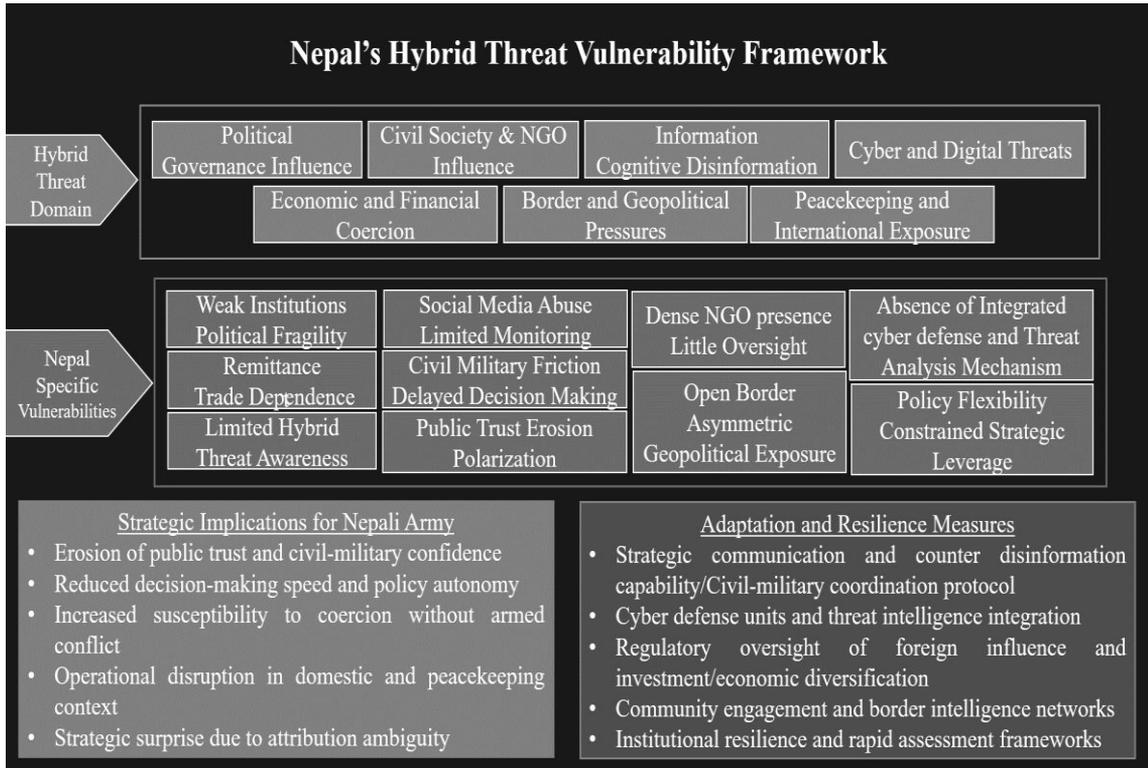
Collectively, these dynamics illustrate a central lesson of the Gerasimov framework: national security can be undermined through non-kinetic means without a single shot being fired. For Nepal, this underscores the need to strengthen whole-of-government resilience, improve cross-sector coordination, and invest in cyber and information defense capabilities alongside conventional preparedness (Lia, 2019).

In this context, Nepal and the Nepali Army exhibit limited adaptive capacity to anticipate, detect, and mitigate hybrid threats while maintaining its non-aligned posture. Deficiencies in strategic communication, civil-military coordination, and regulatory oversight of foreign influence constrain policy autonomy and reduce strategic flexibility. As influence, perception, and digital ecosystems increasingly shape the operational environment, the relative neglect of non-kinetic domains within Nepal's security strategy reveals a persistent imbalance between traditional defense planning and the contemporary character of conflict.

To conceptualize Nepal's exposure and strategic options, Figure 1 presents a four-layer hybrid vulnerability framework, illustrating how multidimensional hybrid threats interact with Nepal-specific vulnerabilities to generate operational, institutional, and societal pressures requiring proactive military and national responses.

Figure 1

Nepal's Hybrid Threat Vulnerability Framework (Prepared by the author)



Institutional Challenges for the Nepali Army

The Nepali Army has historically operated within a conventional defense paradigm, emphasizing border security, counterinsurgency, international peacekeeping, and disaster response. While these roles remain essential, the emergence of hybrid threat environments has exposed institutional stresses that conventional force structures alone are insufficient to address, particularly for small, non-aligned militaries such as Nepal (Hoffman, 2007; Galeotti, 2014).

Case evidence from the 2015 unofficial blockade, cross-border information campaigns, and documented cyber incidents illustrates how influence-based coercion has shaped Nepal's strategic environment without direct military confrontation (International Crisis Group, 2016; Ghale, 2020). These episodes, examined through official statements, crisis reports, and media documentation, reveal a widening gap between Nepal's traditional defense orientation and the institutional demands imposed by hybrid conflict dynamics.

Structural and Doctrinal Limitations

Analysis of Nepal's defense doctrines and national security policy documents indicates a continued emphasis on territorial security and clearly demarcated operational phases. Hybrid threats, however, operate in the ambiguous space between war and peace, requiring adaptive institutional responses beyond traditional deployment models (Giles, 2016; Lia, 2019).

A review of the National Security Policy (2016) and related defense planning documents confirms the absence of a formal hybrid warfare doctrine or an integrated national framework that synchronizes cyber operations, information warfare, and psychological defense across civilian and military institutions (Kattel, 2021). The strategic implications of this doctrinal gap became evident during the 2015 blockade, where official crisis assessments and external analyses highlight Nepal's limited capacity to attribute, assess, and respond coherently to sustained non-kinetic coercion (International Crisis Group, 2016).

Cyber and Information Operations Capability

Data from government cyber incident reports and publicly acknowledged breaches indicate that Nepal's cyber security investment and institutional capacity have not kept pace with the evolving threat landscape. Content analysis of Ministry of Communication and Information Technology reports confirms that the Nepali Army does not yet possess a dedicated cyber or information warfare structure, capabilities increasingly regarded as essential for countering disinformation and digital sabotage (Renz, 2016; Adhikari, 2022).

Event-based analysis of coordinated misinformation campaigns during constitutional debates, federal restructuring, and border-related tensions shows how digital platforms were used to shape public perception and institutional legitimacy (Shrestha, 2020). Additionally, documented cyber incidents including the 2020 breach of multiple government websites, demonstrate how low-cost cyber actions disrupted governance functions and eroded public trust in the absence of robust defensive capacity (Ministry of Communication and Information Technology, 2021).

Intelligence Fusion and Interagency Coordination

Hybrid warfare literature emphasizes the integration of political, economic, social, informational, and cyber intelligence through agile interagency coordination mechanisms (McAllister & Miklaucic, 2016). However, analysis of Nepal's intelligence architecture

based on institutional mandates, organizational structures, and crisis response records, shows that intelligence collection remains largely military-centric and does not systematically incorporate non-traditional indicators commonly exploited in hybrid campaigns (Baral, 2020).

During recent crises, including the 2015 blockade and the September 2025 Gen Z movement, timelines reconstructed from official responses and media reporting indicate that fragmented intelligence assessments and weak cross-agency coordination delayed coherent state action. The absence of an institutionalized intelligence-sharing mechanism among the Nepali Army, National Investigation Department, Nepal Police, Armed Police Force, and civil authorities continues to limit shared situational awareness of hybrid threats.

Legal and Strategic Ambiguity

Nepal's legal and policy frameworks remain insufficiently equipped to address hybrid conflict dynamics. The National Security Policy (2016) provides limited guidance on hybrid warfare, cognitive threats, digital sovereignty, or hostile information operations (Kattel, 2021). As a result, institutional roles often become ambiguous during crises, generating hesitation and delayed responses. Jurisdictional uncertainty during foreign-origin information campaigns surrounding the 2015 constitution and Madhes protests illustrates how legal gaps can inhibit timely action (Human Rights Watch, 2015).

Human Capital and Training Gaps

Human capital development represents a critical vulnerability in Nepal's preparedness for hybrid threats. In the absence of a formal hybrid warfare doctrine, professional military education remains largely focused on kinetic operations, with limited emphasis on strategic communication, cyber defense, media literacy, and information operations (Lia, 2019; Ghale, 2020). During periods of heightened disinformation related to border tensions in 2020, Nepal's limited pool of trained personnel constrained effective counter-messaging and narrative assessment (Shrestha, 2020). As future conflicts increasingly target cognitive and digital domains, operational effectiveness will depend on cultivating officers capable of operating across these non-physical battlefields.

Collectively, these institutional challenges highlight the widening gap between Nepal's traditional defense orientation and the demands of hybrid conflict. Without timely doctrinal, structural, technological, and educational adaptation, the Nepali Army risks strategic unpreparedness in conflicts where influence, perception, and information

increasingly shape outcomes. Addressing these gaps is therefore essential to safeguarding Nepal's sovereignty and strengthening institutional resilience in an evolving security environment.

Strategic Recommendations for Nepal against Hybrid Threats

In light of the institutional challenges outlined above, Nepal's largely state-centric and conventionally oriented security posture requires adjustment to meet the demands of an increasingly hybrid threat environment confronting small, non-aligned states. Although analytical insights associated with the Gerasimov framework emerged from a distinct strategic culture, its core observation that contemporary conflict is shaped as much by non-military, informational, and psychological instruments as by overt force, retains relevance for Nepal's security planning. Rather than adopting external doctrines in a prescriptive manner, the following strategic recommendations emphasize interpretation and adaptation, prioritizing institutional resilience, civil-military coordination, and capability development grounded in Nepal's own geopolitical constraints, constitutional mandates, and organizational capacities.

Develop a Hybrid Warfare Doctrine

Nepal should formulate a hybrid warfare doctrine tailored to its strategic constraints, non-aligned posture, and institutional realities. This doctrine should integrate cyber security, information operations, psychological defense, and civil-military coordination within a unified national framework. Rather than mirroring foreign models, the doctrine should clarify roles, thresholds, and response mechanisms for non-kinetic coercion across civilian and military institutions. The absence of such a framework during the 2015 unofficial blockade highlighted the risks of fragmented assessment and delayed response to hybrid pressure (International Crisis Group, 2016).

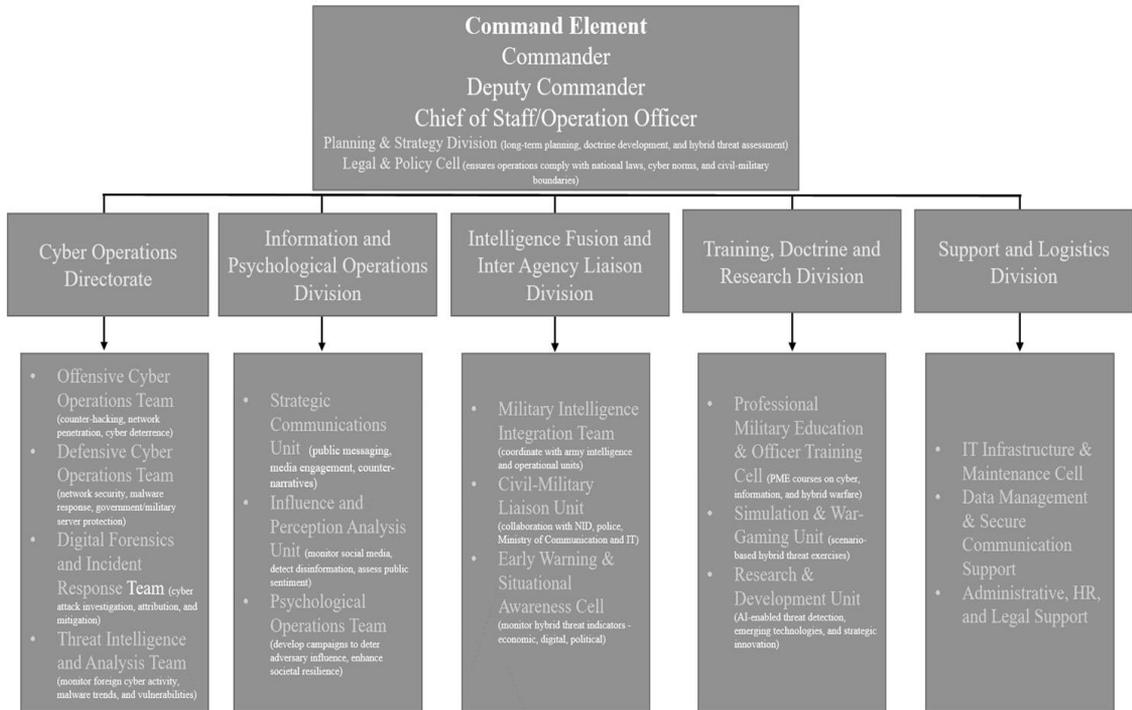
Establish Cyber and Info-Operations Command

Information dominance has become a defining feature of contemporary conflict. The Nepali Army should establish a dedicated Cyber and Information Operations capability (Figure 2) in close coordination with national cyber authorities and intelligence agencies. Within existing structures, this could involve integrating the Cyber Directorate, Directorate of Public Relations, Information Operations elements, and relevant intelligence units into a coherent operational framework. The primary focus should be defensive and protecting military and national digital infrastructure, detecting and countering disinformation, coordinating strategic military communication, and providing early warning of cognitive and psychological operations. This capability should operate

in support of civilian authorities and explicitly avoid roles related to censorship or narrative control.

Figure 2

Cyber and Info-Operations Command (Prepared by the Author)



Reform PME and Officer Training Systems

Professional Military Education must evolve to reflect the realities of hybrid conflict. PME curricula should incorporate information warfare theory, media and data literacy, cyber defense fundamentals, social psychology, and hybrid threat war-gaming alongside conventional military studies. These competencies should complement, not replace, traditional operational skills. Strengthening hybrid literacy among mid- and senior-level officers will enhance the Army’s ability to manage crises that combine political, informational, and military pressures, conditions increasingly relevant to Nepal’s security environment.

Strengthen Interagency Intelligence and Crisis Coordination

Hybrid threats blur institutional boundaries and complicate attribution, making interagency coordination essential. Nepal should establish a whole-of-government early

warning and crisis coordination mechanism involving the Ministry of Home Affairs, Ministry of Foreign Affairs, National Investigation Department, Ministry of Communication and Information Technology, Nepali Army, Nepal Police, and Armed Police Force. This mechanism should facilitate shared situational awareness by monitoring indicators such as economic pressure, cyber anomalies, information flows, and diplomatic signaling, enabling coordinated responses before hybrid pressures escalate. The emphasis should be on cooperation and information-sharing rather than centralized control.

Build Public and Societal Resilience

Hybrid threats exploit societal vulnerabilities as much as institutional weaknesses. Within the framework of civilian oversight, the Nepali Army should support national resilience efforts by promoting awareness of disinformation, collaborating with academic institutions including the under-construction proposed National Defence University, on the study of influence operations, engaging media organizations to strengthen verified information ecosystems, and participating in civil-society partnerships that enhance psychological resilience. Public trust and societal cohesion are critical, as hybrid campaigns often seek to weaken confidence and legitimacy before targeting formal security institutions.

In sum, preparing for hybrid threats requires a whole-of-nation approach. Future security challenges are likely to be shaped less by massed troop movements and more by influence operations, narrative competition, and strategic ambiguity. For Nepal, this necessitates targeted institutional adaptation by the Nepali Army, grounded in doctrine, education, coordination, and resilience to safeguard sovereignty while remaining consistent with the country's non-aligned strategic posture.

Conclusion

Analysis of hybrid conflict demonstrates that contemporary threats often target informational, cyber, economic, and psychological domains well before the use of military force. In Nepal, these dynamics expose vulnerabilities that conventional defense measures alone cannot address, underscoring the need for multi-domain preparedness.

Although the Nepali Army is widely respected for its professionalism, operational experience, and contributions to national stability and international peacekeeping, conventional strengths are insufficient to counter non-kinetic threats that exploit gaps in information security, cyber preparedness, and perception management. The absence of a formal hybrid-threat doctrine, limited interagency intelligence integration, and

underdeveloped strategic communication mechanisms continue to constrain Nepal's national security architecture.

Addressing these challenges requires more than incremental technological upgrades. As contemporary conflicts are increasingly shaped by influence, disruption, and narrative competition rather than direct military confrontation, Nepal must pursue a strategic shift toward anticipatory, multi-domain defense grounded in whole-of-government coordination and strengthened civil–military collaboration. Such an approach places institutional coherence, legal clarity, and societal preparedness alongside conventional military capability.

Future conflicts may begin not with gunfire but with a tweet, digital intrusions, coordinated disinformation campaigns, or the manipulation of public narratives. Preparing for this reality through context-specific doctrine development, coordinated institutional reform under civilian guidance, and sustained societal resilience is therefore essential to safeguarding Nepal's sovereignty, security, and strategic autonomy. For a force historically structured around territorial defense, these hybrid dynamics complicate traditional threat assessment and demand adaptive operational planning.

By examining hybrid warfare through a Gerasimov-informed analytical lens and applying it to the context of a small, non-aligned state, this article contributes to contemporary security studies by demonstrating how institutional adaptation, civil–military coordination, and societal resilience intersect in shaping effective responses to hybrid threats.

References

- Adhikari, A. (2022). *Cybersecurity challenges in Nepal's security sector*. Centre for Security Studies.
- Adhikari, A. (2022). *Disinformation and national security: Emerging risks in Nepal's digital space*. Policy Lab Nepal.
- Adhikari, R. (2022). *Information disorder in Nepal: Disinformation, political communication, and social media dynamics*. Kathmandu Policy Review.
- Baral, B. (2020). *Intelligence reform and security governance in Nepal*. Nepal Institute for Policy Research.
- Baral, B. (2020). Civil-military coordination and intelligence challenges in Nepal. *Nepal Strategic Review*, 6(1), 27–39.
- Bartles, C. K. (2016). Getting Gerasimov right. *Military Review*, 96(1), 30–38.

- Coker, C. (2015). *The future of war: A history*. Oxford University Press.
- Fridman, O. (2018). *Russian “hybrid warfare”: Resurgence and politicisation*. Hurst & Company.
- Galeotti, M. (2014, July 6). The “Gerasimov Doctrine” and Russian non-linear war. In *Moscow’s Shadows*. <https://inmoscowsshadows.wordpress.com/>
- Gerasimov, V. (2013). The value of science in prediction: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military-Industrial Courier*. (English translation by M. Galeotti, 2014.)
- Ghale, S. (2020). Hybrid threats and small-state vulnerabilities: The case of Nepal. *Journal of South Asian Security Studies*, 5(2), 44–59.
- Ghale, S. (2020). Nepal’s geopolitical dilemma: Between India and China. *South Asian Journal of Strategic Studies*, 5(1), 23–36.
- Giles, K. (2016). *Russia’s “New” Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power*. Chatham House.
- Government of Nepal. (2016). *National security policy of Nepal*. Office of the National Security Council.
- Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
- Human Rights Watch. (2015). *Like we are not Nepali: Protest and repression in the Terai region of Nepal*. Human Rights Watch.
- International Crisis Group. (2016). *Nepal’s divisive new constitution: An existential crisis* (Asia Report No. 276).
- Karkee, R., & Comfort, J. (2016). NGOs, foreign aid, and development in Nepal. *Frontiers in Public Health*, 4(177). <https://doi.org/10.3389/fpubh.2016.00177>
- Kattel, S. (2021). Cybersecurity challenges in Nepal: State capacity, governance gaps, and policy imperatives. *Nepal Public Policy Review*, 3(1), 77–92.
- Kattel, S. (2021). Hybrid warfare and Nepal’s national security strategy: Gaps and imperatives. *Journal of Strategic Affairs*, 8(1), 33–52.
- Kattel, S. (2021). Hybrid warfare and small state vulnerabilities: The case of Nepal. *Nepal Defence Review*, 9(2), 18–29.
- Kautilya. (1992). *The Arthashastra* (L. N. Rangarajan, Trans.). Penguin Classics.
- Lia, B. (2019). *Hybrid warfare: Fighting complex opponents from the ancient world to the present*. Cambridge University Press.

- Lia, B. (2019). *Understanding hybrid warfare*. Norwegian Defence University College.
- Mao, Z. (1967). *Selected works of Mao Tse-tung: Volume II* (pp. 113–194). Foreign Languages Press. (Original work published 1938)
- Marten, K. (2017). Hybrid war and the Ukraine crisis: Implications for NATO and the United States. *The Washington Quarterly*, 37(1), 7–26. <https://doi.org/10.1080/0163660X.2014.1002160>
- Marten, K. (2017). Russia’s use of semi-state security forces: The case of the Wagner Group. *Post-Soviet Affairs*, 33(3), 181–204. <https://doi.org/10.1080/1060586X.2017.1293395>
- McAllister, K., & Miklaucic, M. (Eds.). (2016). *Hybrid warfare: Fighting complex opponents from the ancient world to the present*. Georgetown University Press.
- Ministry of Communication and Information Technology. (2021). *Annual cybersecurity incident report*. Government of Nepal.
- myRepublica. (2025, November 20). *50,000 NGOs in Nepal and growing*. myRepublica. <https://myrepublica.nagariknetwork.com>
- NATO Allied Command Transformation. (2014). *Hybrid warfare: A challenge for NATO*.
- NATO Allied Command Transformation. (2014). *Strategic foresight analysis*.
- Renz, B. (2016). Russia and “hybrid warfare.” *Contemporary Politics*, 22(3), 283–300. <https://doi.org/10.1080/13569775.2016.1201316>
- Shrestha, N. (2020). *Information disorder and political narratives in Nepal*. Nepal Media Research Forum.
- The Kathmandu Post. (2019, August 29). More than half of Nepal’s total NGOs are in Province 3 and most are in the capital. <https://kathmandupost.com>
- U.S. Army Training and Doctrine Command. (2017). *Multi-domain operations concept*.
- U.S. Army Training and Doctrine Command (TRADOC). (2017). *The Operational Environment and the Changing Character of Future Warfare*.