

Journal of legal and social studies

Issn: 2507-7333

Eissn: 2676-1742

## **Hybrid Threats and the Future of Modern Warfare: Examining Transformations in the International Security Environment**

**Saliha Kouidri\***

Lecturer at The University of Ziane Achour a Djelfa Algeria

|                              |                                |                                 |
|------------------------------|--------------------------------|---------------------------------|
| Date of send: 01 / 06 / 2026 | date of acceptance: 01/07/2026 | Date of Publication: 01/09/2026 |
|------------------------------|--------------------------------|---------------------------------|

**Corresponding author\***

**Abstract :**

Hybrid warfare has emerged as one of the defining characteristics of the contemporary international security environment. Combining conventional military force with cyber operations, disinformation campaigns, economic coercion, proxy warfare, and political subversion, hybrid strategies deliberately exploit the gray zone between peace and open conflict. This article argues that hybrid warfare represents a fundamental transformation in modern conflict paradigms by eroding traditional distinctions between state and non-state actors, military and civilian domains, and war and peace itself. Drawing on qualitative case study analysis and comparative process tracing, the study examines the evolution of hybrid warfare theory and analyzes Russia's operations in Ukraine and China's gray zone activities in the South China Sea and Taiwan Strait. The article situates hybrid threats within broader international relations theory while assessing how technological disruption, geopolitical rivalry, and institutional fragmentation have intensified hybrid competition. The analysis demonstrates that hybrid threats challenge existing deterrence frameworks, complicate attribution, and expose vulnerabilities within democratic societies and global governance institutions. The article concludes that future security competition will increasingly depend on societal resilience, integrated deterrence, and the capacity of states and alliances to adapt to multi-domain conflict environments.

**Keywords :** Hybrid threats; International Security; Modern Warfare; Cyber Operations; Strategic politic; Weaponization .

**Introduction**

The international security environment of the twenty-first century has undergone profound transformation. Traditional interstate warfare has not disappeared, but it increasingly coexists with forms of conflict that operate below the threshold of conventional war. These methods include cyberattacks, disinformation campaigns, proxy warfare, economic coercion, political interference, and lawfare. Collectively, these practices are often described under the concept of hybrid warfare or hybrid threats.

Hybrid warfare generally refers to the coordinated use of military and non-military instruments by state or non-state actors to achieve strategic objectives while avoiding formal escalation into conventional war (Hoffman 2007). Unlike traditional military conflict, hybrid strategies are designed to exploit ambiguity, deny attribution, and target societal vulnerabilities rather than solely battlefield outcomes. Hybrid threats

therefore challenge the conceptual boundaries separating war and peace, domestic and international politics, and civilian and military domains.

The contemporary relevance of hybrid warfare became especially visible after Russia's annexation of Crimea in 2014. Russian operations integrated special forces, information warfare, cyberattacks, economic pressure, and local proxies in a coordinated campaign that destabilized Ukraine while complicating Western responses. Since then, hybrid methods have become central features of strategic competition among major powers. China's gray zone operations in the South China Sea and Taiwan Strait, Iran's use of regional proxy networks, and North Korea's cyber-enabled coercion further illustrate the growing prominence of hybrid strategies.

This article argues that hybrid warfare represents a fundamental transformation in conflict paradigms. Hybrid threats blur the distinction between conventional and irregular warfare while integrating military and non-military tools into continuous strategic competition. The article further contends that hybrid warfare reflects deeper structural changes in the international system, including technological disruption, the erosion of the post-Cold War order, and renewed great power rivalry.

Methodologically, the article employs qualitative case study analysis and comparative process tracing to examine how hybrid strategies operate in practice. Russia's actions in Ukraine and China's gray zone operations provide primary empirical cases through which broader theoretical and strategic dynamics are explored.

The article proceeds in six sections. First, it outlines the conceptual and theoretical foundations of hybrid warfare. Second, it examines the changing character of hybrid threats across multiple domains. Third, it analyzes selected case studies. Fourth, it explores the broader transformation of the international security environment. Fifth, it assesses implications for defense and deterrence. Finally, the article offers policy recommendations and concluding reflections on the future trajectory of modern warfare.

## **TOPIC 1 : Conceptual Framework and Theoretical Foundations**

### **Requieurement 1 : The Evolution of Hybrid Warfare Theory**

The concept of hybrid warfare emerged in response to the changing operational environment of the post- Cold War era. Although military theorists have long recognized the interaction between conventional and irregular forms of conflict, the term “hybrid warfare” gained prominence through the work of Frank Hoffman in the mid-2000s. Hoffman argued that future adversaries would increasingly blend conventional military capabilities with irregular tactics, terrorism, cyber operations, and criminal activity within unified operational campaigns (Hoffman 2007).

Earlier strategic thinkers had anticipated aspects of hybrid conflict. Colin Gray (2005) emphasized that future warfare would involve the integration of multiple forms of violence rather than the replacement of conventional war. Similarly, Mary Kaldor's theory of “new wars” highlighted how globalization, identity politics, and transnational networks blurred distinctions between state and non-state violence (Kaldor 2012).

Hybrid warfare theory evolved substantially after 2014. Initially treated as a primarily military concept, hybrid warfare increasingly became understood as a comprehensive strategy encompassing political, economic, informational, legal, and cyber dimensions. Analysts began emphasizing “gray zone conflict,” referring to coercive activities conducted below the threshold likely to trigger full-scale military responses.

Subsequent scholarship expanded the concept considerably. Some analysts interpreted hybrid warfare primarily as a military-operational phenomenon focused on battlefield convergence, while others broadened it into a grand-strategic framework encompassing political warfare, economic coercion, cyber operations, and societal manipulation. This conceptual expansion generated significant debate regarding the analytical utility and coherence of the term.

Nevertheless, proponents of the concept maintain that contemporary hybrid threats differ qualitatively due to technological acceleration, globalization, digital interconnectedness, and the unprecedented integration of military and non-military tools in real time. Advances in cyber capabilities, social media platforms, artificial intelligence, and data analytics have dramatically expanded opportunities for influence operations and strategic disruption below the threshold of open conflict.

## **Requirement 2 : Competing Definitions and Strategic Traditions**

Different institutions and strategic cultures conceptualize hybrid warfare in distinct ways

NATO defines hybrid threats as “activities, conducted by state or non-state actors, that are coordinated and synchronized to deliberately target democratic states’ and institutions’ vulnerabilities through a wide range of means” (NATO 2022). NATO’s definition emphasizes societal resilience, coordinated defense, and the challenge of attribution.

The European Union similarly stresses the multidimensional nature of hybrid threats, particularly in relation to critical infrastructure, disinformation, and economic coercion. EU approaches tend to emphasize civilian preparedness, institutional coordination, and legal resilience.

Russian strategic discourse differs significantly. Western analysts frequently associate Russian hybrid warfare with the so-called “Gerasimov Doctrine,” derived from General Valery Gerasimov’s 2013 article emphasizing non-military means in modern conflict. However, scholars such as Mark Galeotti (2014) and Ofer Fridman (2018) caution against oversimplifying Russian strategy into a singular doctrine. Russian strategic thinking instead reflects a broader understanding of “new generation warfare,” in which informational, psychological, and political operations are integrated with military force.

Chinese strategic thought offers another important perspective. Liang Qiao and Wang Xiangsui’s concept of “unrestricted warfare” argued that future conflict would transcend conventional military domains and include economic, technological, legal, informational, and financial dimensions (Liang and Wang 1999).

Contemporary Chinese gray zone operations in maritime disputes reflect this broader strategic logic.

## **Requirement 3 : Hybrid Warfare and International Relations Theory**

Hybrid warfare intersects with multiple theoretical traditions in international relations. Realist perspectives interpret hybrid warfare primarily as an adaptive instrument of state power under conditions of renewed great power competition. States employ hybrid methods to maximize strategic advantage while minimizing escalation risks. From this perspective, hybrid warfare reflects continuity in power politics rather than a revolutionary break.

Liberal theories emphasize how globalization, interdependence, and institutional vulnerability create opportunities for hybrid coercion. Open societies and interconnected economies may be especially susceptible to cyberattacks, information manipulation, and economic pressure.

Constructivist approaches focus on the role of narratives, identities, and information in shaping conflict dynamics. Information warfare and cognitive operations seek not merely physical effects but also the manipulation of perceptions, legitimacy, and political identity.

Hybrid warfare therefore cannot be understood solely through military analysis. It represents a convergence of military force, political influence, technological disruption, and societal vulnerability.

## **TOPIC 2 : The Changing Character Of Hybrid Threats**

Contemporary hybrid threats operate across multiple interconnected domains. Understanding their dynamics requires treating these domains as components of an

integrated system rather than isolated phenomena. The following subsections analyze each domain while emphasizing points of intersection and mutual reinforcement.

### **Requirement 1 : Cyber Operations and Digital Infrastructure Attacks**

Cyberspace has become the central operational domain of hybrid conflict, offering states an unprecedented combination of reach, precision, deniability, and scalability. State-sponsored cyber operations range from espionage and intelligence collection to disruptive attacks on critical infrastructure and destructive operations targeting industrial control systems (Singer and Friedman 2014). The Russian cyberattacks on Ukrainian power grids in 2015 and 2016—attributed to the Sandworm unit of Russian military intelligence (GRU)—demonstrated for the first time the capacity to cause physical effects through cyber means, temporarily disabling electricity supply for hundreds of thousands of civilians. The NotPetya malware campaign of 2017, also attributed to Russian state actors, caused an estimated ten billion dollars in global economic damage while targeting Ukrainian financial institutions (Greenberg 2019).

Chinese cyber operations have focused primarily on long-term espionage and intellectual property theft, with the Office of Personnel Management breach of 2015—in which records of approximately 22 million U.S. government employees were compromised—representing a landmark strategic intelligence achievement. Beyond espionage, Chinese actors have pre-positioned malware within U.S. critical infrastructure, including power grids and water systems, in what U.S. Cyber Command characterizes as preparation for potential coercive action in a crisis scenario. The integration of cyber operations with conventional and informational instruments—as demonstrated in Russia's Ukraine campaign and China's approach to Taiwan contingency planning—suggests that cyber is not a standalone domain but a force multiplier across all other operational environments (Nye 2017).

### **Requirement 2 : Information Warfare, Disinformation, and Cognitive Warfare**

Information warfare has undergone a structural transformation driven by the proliferation of social media platforms, which have dramatically lowered the cost and increased the reach of influence operations. Contemporary information warfare encompasses strategic communication, narrative shaping, disinformation campaigns, deepfake production, the amplification of social divisions, and the undermining of epistemic trust in democratic institutions. NATO StratCom has documented systematic Russian information operations targeting European audiences, which have employed networks of fake accounts, state media outlets (RT and Sputnik), and algorithmically optimized content to promote narratives favorable to Russian strategic interests (NATO StratCom COE 2019).

The concept of 'cognitive warfare'—the deliberate targeting of adversary decision-making processes and societal cohesion—has emerged as an extension of information warfare that emphasizes psychological and neuroscientific dimensions. Bernard (2020) and others have argued that cognitive warfare represents the ultimate evolution of non-kinetic conflict, aiming not to destroy the adversary's physical capabilities but to paralyze their will and capacity for collective action. Chinese military doctrine's emphasis on 'winning without fighting' (sheng bu zhan er ren zhi bing), derived from Sun Tzu's strategic principles, reflects a sophisticated understanding of cognitive dimensions of conflict that Western deterrence theory has historically underappreciated. The challenge for democratic societies is that the openness and pluralism that

characterize liberal polities simultaneously create the social fabric that makes them resilient and the vulnerabilities that information warfare seeks to exploit.

### **Requirement 3 : Economic Coercion and Energy Weaponization**

Economic instruments have become central tools of hybrid coercion, operationalized through trade restrictions, investment screening manipulation, sanctions evasion, debt-trap diplomacy, and the weaponization of energy dependencies. Russia's exploitation of European natural gas dependence—encapsulated in the Nord Stream pipeline projects and repeated gas supply disruptions to Ukraine and broader European markets—represents a paradigmatic case of energy as a coercive instrument. The European Union's belated recognition of this vulnerability, accelerated by the 2022 full-scale invasion, prompted emergency diversification measures and long-term strategic investments in alternative supply chains (Giles 2016).

China's deployment of economic coercion is more sophisticated and structurally embedded, leveraging trade dependencies, technological supply chains, and financial interconnections to exercise leverage over smaller states. The economic campaign against Australia following Canberra's calls for an independent investigation into COVID-19 origins—which included tariffs on barley, wine, beef, and coal—demonstrated a willingness to weaponize bilateral economic relationships in response to perceived political slights. The Belt and Road Initiative (BRI), while genuinely serving infrastructure development objectives, simultaneously creates dependencies that can be instrumentalized for political leverage, as illustrated in Sri Lanka's Hambantota port concession and Malaysian debt renegotiation episodes (Fravel 2020; U.S. Department of Defense 2023).

### **Requirement 4: Proxy Warfare, Private Military Companies, and Deniable Actors**

The instrumentalization of proxy forces represents a time-honored instrument of state competition that has been significantly enhanced by the privatization of military force and the emergence of sophisticated private military companies (PMCs). Russia's Wagner Group—subsequently reorganized following the June 2023 mutiny and Prigozhin's death—demonstrated the utility of PMCs as a tool of strategic deniability, enabling Russian military intervention in Syria, Libya, Mali, the Central African Republic, Sudan, and Ukraine while maintaining official distance (Galeotti 2018). Wagner's deployment created what Galeotti has termed a 'geopolitical mercenary' force capable of projecting Russian influence across multiple theaters simultaneously without the political costs of formal military engagement.

Iran's proxy network—comprising Hezbollah, Hamas, the Houthi movement in Yemen, and various Iraqi militias—represents the most sophisticated and geographically extensive proxy architecture in the contemporary Middle East. This network enables Tehran to pursue strategic objectives—deterring Israeli military action, pressuring Gulf states, projecting influence across the Arab world—while maintaining a degree of deniability and limiting the risk of direct conventional conflict with superior adversaries. The operational integration of this proxy network, demonstrated in the coordinated multi-front pressure campaign following the October 7, 2023 Hamas attacks, illustrates the strategic coherence that can be achieved through proxy architectures even without direct command-and-control (Cronin 2015).

### **Requirement 5 : Political Interference and Influence Operations**

Political interference operations—encompassing electoral manipulation, the financing of extremist political movements, the cultivation of political allies, and the exploitation

of democratic processes—constitute a systematic component of hybrid strategies directed against liberal democracies. The U.S. intelligence community's assessment of Russian interference in the 2016 presidential election, the French investigation into Russian support for Marine Le Pen's National Rally, and documented Russian financial flows to European far-right parties collectively illustrate a strategic pattern of exploiting democratic openness to shape the political environments of adversary states (Mueller 2019). These operations do not require success in achieving specific electoral outcomes; the disruption of trust in democratic institutions is itself a strategic objective.

Chinese political influence operations, analyzed extensively by Clive Hamilton (2018) and others, employ different instruments—United Front Work Department activities, Confucius Institutes, business community networks, and elite capture—to shape political discourse and limit criticism of Chinese policies in targeted countries. The Australian, Canadian, and New Zealand parliamentary inquiries into Chinese political interference from 2018 onward have documented systematic efforts to penetrate political donor networks, shape academic discourse, and cultivate officials whose career trajectories might create durable channels of influence. These operations reflect a long-term strategic patience that contrasts with the more acute, election-cycle-focused interventions characteristic of Russian practice.

### **Requirement 6 : Lawfare and Exploitation of Legal Ambiguity**

Lawfare—the strategic exploitation and manipulation of legal frameworks to achieve operational objectives—has emerged as a sophisticated component of hybrid strategies. The concept encompasses both the misuse of international law to justify aggression and the deliberate creation of legal ambiguity to complicate adversary responses. Russia's invocation of the Responsibility to Protect (R2P) doctrine in Crimea, its claims of protecting Russian speakers under humanitarian law, and its legal arguments regarding Kosovo precedent were not intended to persuade but to create sufficient legal murkiness to complicate Western political and legal responses (Giles 2016). China's claim to 'historical rights' over the South China Sea—rejected by the Permanent Court of Arbitration in its 2016 award—similarly functions as a form of lawfare, providing legal language for domestic and international audiences while contesting the legal framework established by the United Nations Convention on the Law of the Sea (UNCLOS).

### **Requirement 7: Instrumentalization of Migration and Demographic Pressures**

The weaponization of migration flows as a coercive instrument represents one of the more contentious and morally complex dimensions of hybrid strategy. Belarus's deliberate facilitation of irregular migration flows to the Polish, Lithuanian, and Latvian borders in 2021—widely characterized as a hybrid attack on EU member states in retaliation for sanctions imposed following the Lukashenko government's fraudulent 2020 election—demonstrated that migration can be instrumentalized as a tool of political coercion without the legal and institutional clarity that characterizes more conventional threats. Turkey has similarly employed the implicit threat of permitting large-scale migration flows as leverage in negotiations with the European Union over financial support and political concessions. These episodes highlight a domain in which the hybrid threat literature has been less well-developed, partly reflecting the political sensitivity of migration issues in European democracies.

### **TOPIC 3 : Policy Recommendations**

The analysis above generates a set of analytically grounded policy recommendations organized across institutional levels from national to multilateral.

**Requirement 1: Strengthening Integrated Deterrence**

Effective deterrence of hybrid threats requires an integrated approach that combines military credibility with economic, diplomatic, and informational instruments. The U.S. National Defense Strategy's concept of 'integrated deterrence' represents a promising framework, but requires fuller operationalization across alliance structures and bureaucratic silos. Specifically, NATO should develop and exercise 'hybrid response protocols' that pre-authorize graduated response options for identified hybrid attack signatures, reducing the decision-action gap that adversaries currently exploit. These protocols should include pre-agreed thresholds and responses for cyber attacks on critical infrastructure, political interference operations, and proxy provocations, developed through robust alliance consultation that maintains political legitimacy while enabling rapid response.

**Requirement 2 : Enhancing Cyber and Information Resilience**

Building resilience in the cyber and information domains requires investment in both technical infrastructure and human capacity. Governments should mandate minimum cyber security standards for critical infrastructure operators, develop sovereign capacity in key technology sectors (semiconductors, cloud computing, satellite communications), and invest in the media literacy and digital hygiene education of their populations. The development of 'prebunking' strategies—which inoculate populations against disinformation by exposing them to the techniques of manipulation before specific campaigns are encountered—has shown promising experimental results and deserves systematic investment and evaluation. International cooperation on cyber norms and attribution mechanisms, while hampered by great-power rivalry, should be pursued through minilateral formats (groupings of like-minded democracies) where multilateral consensus is unavailable.

**Requirement 3: Improving Alliance Coordination**

The multi-domain character of hybrid threats requires alliance coordination mechanisms that span not merely defense ministries but the full range of government functions implicated in hybrid conflict. The establishment of an enhanced NATO Hybrid Center of Excellence, with a dedicated analytical and planning capability for cross-domain hybrid scenarios, would improve collective situational awareness and response coordination. Bilateral and multilateral information-sharing agreements should be deepened to enable real-time sharing of threat intelligence across hybrid domains, including economic intelligence regarding state-backed coercive economic measures that is not currently well-integrated into security frameworks.

**Requirement 4: Reforming Legal Frameworks**

Existing international legal frameworks require systematic review and, where possible, reform or reinterpretation to address the ambiguities that hybrid strategies exploit. The development of clearer legal standards for the attribution of cyber attacks, the definition of armed attack in hybrid contexts, and the application of international humanitarian law to information operations should be pursued through international legal forums and bilateral treaty mechanisms. States should also invest in their own legal and lawfare capabilities, developing the capacity to contest adversary legal manipulations in international forums with equal sophistication. The Tallinn Manual process, which has developed expert analysis of international law applicable to cyber operations, provides a model that could be extended to other hybrid domains.

**Requirement 5: Investing in Emerging Technologies and Whole-of-Government Approaches**

Effective adaptation to the hybrid threat environment requires sustained investment in the emerging technologies—AI-enabled analysis, autonomous systems, quantum-resistant encryption, advanced sensor networks—that will define the next generation of both hybrid threats and responses. These investments must be accompanied by doctrinal and organizational adaptation that enables the integration of new capabilities into coherent operational concepts. Perhaps most fundamentally, the whole-of-government approaches required for hybrid defense demand institutional reform: the creation of cross-cutting coordination mechanisms, the breaking down of bureaucratic silos between defense, intelligence, law enforcement, economic, and communications functions, and the development of personnel with the cross-domain expertise to operate effectively in the hybrid environment.

## **TOPIC 4 : Comparative Case Study Analysis**

### **Requirement 1 : Russia in Ukraine, 2014–2024**

#### **Section 1 : Strategic Objectives**

Russia's hybrid campaign in Ukraine, initiated in 2014 and escalating to full-scale conventional invasion in February 2022, represents the most extensively documented and analytically significant case of hybrid warfare in the contemporary era. Russian strategic objectives evolved over this decade but centered on several consistent priorities: preventing Ukraine's integration into Western political, economic, and security structures (NATO, EU); maintaining influence over Ukrainian domestic politics; securing access to the Black Sea and strategically valuable Crimean territory; and, by 2022, achieving decisive influence over or control of Ukraine as a whole. These objectives reflected both a maximalist revisionist agenda—the reversal of what Vladimir Putin has characterized as the greatest geopolitical catastrophe of the twentieth century—and more immediate security concerns about Western military infrastructure approaching Russian borders (Mearsheimer 2014; Kofman and Rojansky 2015).

#### **Section 2: Operational Methods and Hybrid Instruments**

The 2014 Crimean operation demonstrated an unprecedented degree of hybrid integration. Special operations forces, operating without insignia, rapidly secured key infrastructure, government buildings, and communication nodes before a referendum could be meaningfully organized or contested. Simultaneously, information operations promoted narratives of popular Crimean enthusiasm for Russian reincorporation and the threat posed to Russian speakers by Ukrainian 'fascists.' Economic leverage over the Ukrainian energy sector, cultivated through years of gas pricing arrangements and Gazprom supply contracts, provided additional coercive pressure. The speed and coordination of these instruments—achieving a *fait accompli* before NATO could meaningfully consider a collective response—illustrated the strategic logic of hybrid approaches: they exploit the decision-action gap in deliberative institutions.

The subsequent conflict in Donbas from April 2014 onward demonstrated the sustained integration of hybrid instruments over a longer time horizon. Russian military intelligence (GRU) personnel organized, directed, and embedded with local separatist formations that provided the political fiction of a popular uprising against the Kiev government. Russian cyber operations—including the BlackEnergy malware attacks on Ukrainian power infrastructure in December 2015 and 2016—were timed to coincide with periods of maximum political pressure. Disinformation operations, conducted

through RT, social media networks, and cultivated domestic Ukrainian actors, promoted narratives designed to undermine public trust in the Ukrainian government and fracture domestic political cohesion.

The 2022 full-scale invasion, paradoxically, revealed both the capabilities and the limitations of hybrid approaches. While the initial assault combined conventional armored advances with cyberattacks (the Viasat satellite hack in the hours before the invasion), information operations (claiming denazification objectives), and electronic warfare, the anticipated rapid capitulation of Ukrainian political institutions did not occur. Ukraine's societal resilience—partly a product of the preceding eight years of hybrid conflict, which had inoculated Ukrainian institutions and civil society against Russian information operations—proved more robust than Russian planners apparently anticipated. The failure of the initial hybrid-conventional integration underscored that hybrid strategies, while powerful in achieving limited revisionist objectives, face significant limitations against determined, resilient, and increasingly Western-supported opponents.

### **Section 3: Strategic Assessment**

Russia's Ukraine campaign yields several important analytical conclusions. First, hybrid instruments proved highly effective in achieving limited territorial revisionism (Crimea) under conditions of adversary unpreparedness and international disunity, but proved insufficient to achieve maximalist objectives against a resilient and externally supported opponent. Second, the combination of hybrid and conventional instruments is not inherently contradictory; the two modes are complementary and can be employed sequentially or simultaneously depending on operational context. Third, the campaign accelerated NATO's adaptation—the 2022 Strategic Concept explicitly identified Russia as the 'most significant and direct threat' and prompted significant force posture changes in Eastern Europe—demonstrating that hybrid strategies carry the risk of strategic blowback by galvanizing adversary responses (NATO 2022). Fourth, the Russian case highlights the critical role of societal resilience as a determinant of hybrid warfare outcomes: populations and institutions that have developed awareness of hybrid tactics, practiced information hygiene, and strengthened civil society networks have proven significantly more resistant to Russian hybrid pressure.

## **Requirement 2 : China's Gray-Zone Operations in the South China Sea and Taiwan Strait**

### **Section 1: Strategic Objectives**

China's gray-zone strategy in the Indo-Pacific reflects objectives fundamentally different from Russia's more acute revisionism, yet equally consequential for international order. Beijing's core strategic objectives include the consolidation of territorial claims in the South China Sea (including the Paracel and Spratly Islands and the contested Scarborough Shoal), the deterrence of Taiwan independence and maintenance of the conditions for eventual unification, the erosion of U.S. alliance credibility and forward presence in the region, and the establishment of a regional order consistent with Chinese definitions of sovereignty and hierarchy. These objectives are pursued through a strategy of deliberate gradualism—the 'salami-slicing' approach that advances positions incrementally in ways that individually fall below the threshold of triggering formal deterrence responses while cumulatively achieving significant strategic gains (Fravel 2020; U.S. Department of Defense 2023).

## Section 2 : Operational Methods and Gray-Zone Instruments

China's gray-zone toolkit in the South China Sea encompasses a diverse set of instruments carefully calibrated to maintain deniability and avoid crossing established redlines. The People's Liberation Army Navy (PLAN), China Coast Guard (CCG), and the maritime militia—a force of ostensibly civilian fishing vessels that can be rapidly organized into paramilitary formations—operate in a layered system that allows Beijing to escalate or de-escalate presence and coercion without formal military engagement. The CCG's deployment of water cannons against Philippine resupply missions to the BRP Sierra Madre at Second Thomas Shoal, documented throughout 2023 and 2024, illustrates this graduated coercion: the action is provocative and operationally significant but falls below the threshold of armed attack under Article 2(4) of the UN Charter, complicating legal and alliance responses.

The construction of artificial islands in the Spratly archipelago—involving the dredging and fortification of seven features between 2013 and 2016—represents the paradigmatic case of gray-zone fait accompli. By moving rapidly, using civilian construction equipment, and framing the activity as infrastructure development on Chinese sovereign territory, Beijing presented the international community with a strategic reality that could not be reversed without the threat or use of force. The subsequent militarization of these features—with runways, radar installations, and eventually weapons systems—proceeded under similar informational cover, leveraging the domestic and international credibility of the narrative of Chinese sovereignty while systematically altering the operational military environment.

In the Taiwan Strait, China's gray-zone operations encompass regular incursions into Taiwan's Air Defense Identification Zone (ADIZ) by PLAN Air Force aircraft—which numbered in the hundreds annually by 2023—maritime operations around Taiwan's outer islands, economic coercion through trade restrictions and tourism limitations, and comprehensive information operations targeting Taiwanese domestic politics. Chinese cyber operations against Taiwanese government systems, financial institutions, and critical infrastructure have been documented extensively. The combination of military coercion, economic pressure, and information operations constitutes an integrated campaign designed to erode Taiwanese societal confidence in the viability of resistance, complicate U.S. and allied planning, and progressively normalize Chinese military activity in the Taiwan Strait (Wuthnow 2022).

## Section 3 : Strategic Assessment

China's gray-zone strategy yields distinct but complementary insights to the Russian case. First, patient incrementalism can achieve durable strategic gains—China's position in the South China Sea has been fundamentally altered without triggering the conventional conflict that more acute revisionism would risk. Second, the maritime and aviation domains offer particular opportunities for gray-zone exploitation because the legal frameworks governing them contain significant ambiguities that sophisticated actors can exploit without unambiguous legal violation. Third, the integration of state and nominally non-state actors (the maritime militia) creates attribution challenges that complicate alliance responses; determining the appropriate collective defense obligation when a 'fishing vessel' engages in coercive action against a treaty ally's resupply mission requires legal and political determinations for which existing frameworks were not designed. Fourth, the Chinese case highlights the importance of economic interdependence as both a source of coercive leverage and a constraint on escalation: the

deep integration of Chinese and U.S. and allied economies creates mutual vulnerabilities that deter both sides from rapid escalation but also complicate the imposition of meaningful costs for gray-zone behavior.

## CONCLUSION

Hybrid warfare represents one of the most significant transformations in the contemporary international security environment. By integrating conventional military force with cyber operations, information warfare, economic coercion, political subversion, and proxy networks, hybrid strategies deliberately exploit the ambiguities of modern interconnected societies.

This article has argued that hybrid warfare represents not merely a tactical evolution but a structural transformation in the character of conflict—one in which the erosion of the war-peace distinction, the convergence of military and non-military instruments, and the growing centrality of the information, cyber, and cognitive domains have fundamentally altered the strategic environment. The comparative analysis of Russia's Ukraine campaign and China's gray-zone operations demonstrates that contemporary great-power revisionism increasingly operates in the hybrid space, exploiting legal ambiguity, information asymmetries, and institutional gaps to advance strategic objectives while managing escalation risk.

The implications of this transformation for the international security environment are deeply consequential. The rules-based order that emerged from post-World War II and post-Cold War settlements is under systematic pressure from hybrid strategies that target its normative foundations rather than confronting it through conventional military force. Strategic stability, undermined by the integration of cyber capabilities into nuclear architectures and the collapse of arms control regimes, faces new and poorly understood risks. Democratic societies, whose openness is simultaneously their greatest strength and their most significant vulnerability in hybrid conflict, confront the difficult challenge of building resilience without sacrificing the values that make them worth defending.

The analytical framework developed here has its limitations. The hybrid warfare concept remains contested, and the article's focus on great-power competition necessarily underplays the dynamics of hybrid conflict in regional and sub-state contexts. The rapidly evolving technological landscape means that analytical frameworks developed today may require significant revision as AI, autonomous systems, and quantum technologies mature. Future research should address the determinants of hybrid strategy choice—the conditions under which states select hybrid rather than conventional or diplomatic instruments—and the effectiveness of different deterrence and resilience strategies across varied political and institutional contexts.

What does seem clear is that the future of warfare will be characterized by continued blurring of the distinctions that organized twentieth-century strategic thought: war and peace, military and civilian, state and non-state, kinetic and non-kinetic. States and institutions that adapt their strategic frameworks, legal architectures, and organizational cultures to this reality will be better positioned to navigate the hybrid threat environment. Those that cling to inherited frameworks designed for a world of conventional interstate conflict will face mounting strategic surprises and institutional failures. The fundamental challenge is not merely technical or military but political: building the democratic consensus, institutional capacity, and strategic culture required to compete effectively in a world where conflict is increasingly continuous, diffuse, and ambiguous. Meeting this challenge is the defining strategic task of the current era.

Ultimately, navigating the hybrid threat era will require not only military modernization but also societal preparedness, democratic resilience, institutional innovation, and sustained international cooperation. States that successfully integrate these dimensions will be better positioned to manage the uncertainties and complexities of twenty-first-century conflict.

## **BIBLIOGRAPHY**

- 1 - Bernard, Alix. 2020. "Cognitive Warfare: The Newest Military Domain." NATO Review, November 20, 2020.
- 2 - Cronin, Audrey Kurth. 2015. "ISIS Is Not a Terrorist Group: Why Counterterrorism Won't Stop the Islamic State." *Foreign Affairs* 94 (2): 87–98.
- 3 - European Commission. 2016. *Joint Framework on Countering Hybrid Threats: A European Union Response*. Brussels: European Commission.
- 4 - Fravel, M. Taylor. 2020. *Active Defense: China's Military Strategy since 1949*. Princeton: Princeton University Press.
- 5 - Fridman, Ofer. 2018. *Russian 'Hybrid Warfare': Resurgence and Politicisation*. London: Hurst.
- 6 - Galeotti, Mark. 2016. "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?" *Small Wars and Insurgencies* 27 (2): 282–301.
- 7 - Galeotti, Mark. 2018. *The Vory: Russia's Super Mafia*. New Haven: Yale University Press.
- 8 - Giles, Keir. 2016. *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House.
- 10 - Gray, Colin S. 2006. *Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?* Carlisle: Strategic Studies Institute.
- 11 - Greenberg, Andy. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday.
- 12 - Hamilton, Clive. 2018. *Silent Invasion: China's Influence in Australia*. Melbourne: Hardie Grant Books.
- 13 - Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Research.
- 14 - Kaldor, Mary. 2012. *New and Old Wars: Organised Violence in a Global Era*. 3rd ed. Cambridge: Polity.
- 15 - Kofman, Michael, and Matthew Rojansky. 2015. "A Closer Look at Russia's 'Hybrid War'." Kennan Cable, no. 7. Washington, DC: Wilson Center.
- 16 - Liang, Qiao, and Wang Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.
- 17 - Mattis, James N., and Frank Hoffman. 2005. "Future Warfare: The Rise of Hybrid Wars." *Proceedings* 132 (11): 18–19.
- 18 - Mazarr, Michael J. 2015. "Mastering the Gray Zone: Understanding a Changing Era of Conflict." Carlisle: Strategic Studies Institute.
- 19 - Mearsheimer, John J. 2014. "Why the Ukraine Crisis Is the West's Fault." *Foreign Affairs* 93 (5): 77–89.
- 20 - Mueller, Robert S. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. 2 vols. Washington, DC: U.S. Department of Justice.
- 21 - NATO. 2022. *NATO 2022 Strategic Concept*. Brussels: North Atlantic Treaty Organization.
- 22 - NATO StratCom COE. 2019. *Social Media as a Tool of Hybrid Warfare*. Riga: NATO Strategic Communications Centre of Excellence.
- 23 - Nye, Joseph S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71.

- 24 - Rid, Thomas. 2013. Cyber War Will Not Take Place. London: Hurst.
- 25 - Singer, P. W., and Allan Friedman. 2014. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press.
- 26 - U.S. Department of Defense. 2022. 2022 National Defense Strategy of the United States of America. Washington, DC: DoD.
- 27 -U.S. Department of Defense. 2023. Military and Security Developments Involving the People's Republic of China 2023. Washington, DC: DoD.
- 28 - Votel, Joseph L., Charles T. Cleveland, Charles T. Connett, and Will Irwin. 2016. "Unconventional Warfare in the Gray Zone." Joint Force Quarterly 80 (1): 101–9.
- 29 - Wuthnow, Joel. 2022. "PLA Perspectives on Gray Zone Challenges in the Taiwan Strait." Journal of Strategic Studies 45 (5): 633–57.