



Hybrid warfare and the erosion of state sovereignty in the 21st century: An analysis

Sangeet Singh

Department of Political Science, Guru Nanak Dev University, Punjab, India

DOI: <https://doi.org/10.66856/ijssh.2026.8.3.8121>

Abstract

The nature of armed conflict has been transformed since the turn of the twenty-first century by the emergence of hybrid warfare, a mode of confrontation that fuses conventional military power with irregular tactics, cyber operations, economic coercion, disinformation, and proxy violence. Unlike traditional interstate war, hybrid warfare is deliberately calibrated to remain below the threshold that would trigger a decisive military response, exploiting the ambiguity between war and peace to advance strategic objectives while preserving deniability. This paper examines how hybrid warfare challenges the foundational premises of Westphalian sovereignty, namely territorial integrity, political independence, and the state's monopoly over the legitimate use of force. Drawing on case studies from Russia's actions in Ukraine, China's gray-zone operations in the Indo-Pacific, and the global proliferation of disinformation campaigns and cyber intrusions, the paper argues that hybrid warfare erodes sovereignty not through outright conquest but through the incremental hollowing-out of a state's capacity to control its own territory, information space, economy, and political processes. The paper further evaluates institutional and legal responses developed by NATO, the European Union, and individual states, and considers the conceptual debates surrounding the utility of "hybrid warfare" as an analytical category. It concludes that the resilience of sovereignty in the current era depends less on traditional military deterrence than on the capacity of states and societies to withstand sustained, multidimensional pressure across civilian, economic, and informational domains.

Keywords: Hybrid warfare, state sovereignty, gray-zone conflict, disinformation, cyber operations, Westphalian order, resilience

Introduction

Sovereignty has long served as the organizing principle of the international system established after the Peace of Westphalia in 1648, resting on the presumption that states exercise supreme and exclusive authority within their territorial borders and that this authority is immune from external interference. For more than three centuries, this presumption has coexisted uneasily with the reality of power politics, but it has nonetheless functioned as the normative bedrock of international law, diplomacy, and collective security arrangements. In the twenty-first century, however, a new mode of conflict has emerged that does not so much violate this principle outright as quietly dissolve it from within. Hybrid warfare, understood as the coordinated use of military and non-military instruments, conventional and irregular tactics, and overt and covert operations to achieve strategic objectives while avoiding the threshold of open war, has become the dominant idiom through which revisionist and opportunistic actors challenge the territorial, political, and informational integrity of other states.

The significance of hybrid warfare lies not in any single novel weapon or tactic but in the way it recombines familiar instruments of statecraft and irregular conflict into an integrated campaign designed to exploit the seams of an adversary's political, legal, and social order. Cyberattacks on critical infrastructure, disinformation campaigns that manipulate electoral outcomes, the use of paramilitary proxies and "little green men" to seize territory without formal declarations of war, economic coercion through energy dependency or trade restrictions, and the weaponization of migration flows have all become recognizable features of contemporary international friction. What unites these instruments is their capacity to inflict

strategic harm on a target state while remaining sufficiently ambiguous to complicate attribution, forestall collective defense obligations, and avoid the reputational and legal costs associated with conventional aggression.

This paper argues that hybrid warfare represents a distinctive and consequential challenge to state sovereignty in the contemporary era. It does so not primarily through the schoolbook scenario of tanks crossing a border, but through the erosion of four interlocking dimensions of sovereign authority that Stephen Krasner identified as international legal sovereignty, Westphalian sovereignty, domestic sovereignty, and interdependence sovereignty (Krasner, 1999) ^[18]. Each of these dimensions is targeted by different instruments of hybrid conflict: proxy warfare and territorial annexation strike at Westphalian non-interference; cyber intrusions and disinformation corrode domestic sovereignty by undermining the state's monopoly on information and public trust; economic coercion exploits interdependence sovereignty by turning trade and energy relationships into instruments of pressure; and the selective, self-serving invocation of international law by revisionist powers erodes the coherence of international legal sovereignty itself (Krasner, 2001) ^[19].

The paper proceeds in six parts. Section two conceptualizes hybrid warfare, tracing its intellectual origins and surveying the principal scholarly definitions. Section three examines the theory of state sovereignty and identifies the specific dimensions most vulnerable to hybrid pressure. Section four analyzes the principal instruments of hybrid warfare in turn: cyber operations, disinformation and information warfare, economic and energy coercion, proxy and paramilitary forces, and lawfare. Section five presents case studies, focusing primarily on Russia's campaign against Ukraine

since 2014^[2], China's gray-zone activity in the South China Sea and toward Taiwan, and transnational election interference. Section six evaluates the institutional, legal, and normative responses that have been developed by NATO, the European Union, and individual states, before turning to a critical assessment of the conceptual debates surrounding the term "hybrid warfare" itself. The paper concludes by arguing that sovereignty in the twenty-first century is best understood not as a fixed legal status but as a contested and continuously defended capacity, one whose preservation increasingly depends on societal resilience rather than military strength alone.

Conceptualizing Hybrid Warfare

1. Origins of the Concept

The term "hybrid warfare" entered mainstream strategic vocabulary through the work of American defense analyst Frank G. Hoffman, whose influential 2007^[13] monograph *Conflict in the Twenty-First Century: The Rise of Hybrid Wars* described an emerging mode of conflict in which state and non-state adversaries blend conventional capabilities, irregular tactics, terrorism, and criminal activity within the same battlespace to achieve mutually reinforcing effects (Hoffman, 2007)^[13]. Hoffman built on earlier work co-authored with General James Mattis, who had used the term to describe the fusion of regular and irregular warfare witnessed in conflicts such as the 2006 war between Israel and Hezbollah, in which a non-state actor employed sophisticated anti-tank weapons and rocket barrages alongside guerrilla tactics and a dense information campaign (Mattis & Hoffman, 2005)^[21]. For Hoffman, hybrid threats were defined by the deliberate combination of conventional weapons, irregular tactics, terrorism, and criminal behavior within the same time and battlespace, a synthesis that blurred what had previously been treated as distinct categories of conflict (Hoffman, 2009)^[14].

Although Hoffman's formulation was concerned chiefly with the tactical battlespace, the term rapidly migrated into broader strategic and political usage after 2014^[15], when Russia's annexation of Crimea and its covert support for separatist forces in eastern Ukraine prompted Western analysts and policymakers to search for a vocabulary capable of describing a campaign that combined unmarked soldiers, cyberattacks, disinformation, economic pressure, and diplomatic subterfuge without ever crossing into formally declared war (Chivvis, 2017; Renz, 2016)^[3, 26]. In this expanded usage, hybrid warfare came to denote not merely a battlefield tactic but an entire strategic approach to interstate competition, one explicitly designed to operate beneath the threshold that would trigger a unified military or legal response from the target state or its allies (Hoffman, 2014)^[15].

2. The Gerasimov Discourse

Much of the Western discussion of Russian hybrid strategy has referenced a 2013 article published by the Chief of the General Staff of the Russian Armed Forces, General Valery Gerasimov, in the trade publication *Military-Industrial Courier* (Bartles, 2016)^[1]. Gerasimov's article, which reflected on the character of the Arab Spring uprisings and Western-backed interventions such as the one in Libya, argued that non-military means, including political, economic, informational, humanitarian, and other measures, had come to exceed the power of conventional weapons in

achieving strategic and political goals, and that these means were increasingly supplemented by covert military measures, including information warfare and the actions of special operations forces (Thomas, 2016)^[29]. Western commentary popularized this text under the label "the Gerasimov Doctrine," a term that the analyst who coined it, Mark Galeotti, later disavowed as misleading, since Gerasimov's article was as much a description of what he perceived to be Western practice as it was a blueprint for Russian strategy (Galeotti, 2019)^[11]. Nonetheless, the discourse around the article crystallized a Western perception that Russia had adopted a deliberate strategy of "non-linear war" in which the boundary between war and peace had become permanently blurred (Galeotti, 2016; Kofman & Rojansky, 2015)^[10, 17].

3. Defining Features and Scholarly Debate

Despite its wide currency, hybrid warfare remains a contested and imprecisely bounded concept (Wither, 2016)^[32]. Scholars broadly converge on several defining features: the simultaneous employment of conventional and irregular means; the deliberate manipulation of ambiguity to complicate attribution and delay adversary response; the integration of non-military instruments, particularly cyber operations, disinformation, and economic coercion, into a coherent campaign; and calibration below the threshold that would invite an overwhelming, legally sanctioned military response, often referred to as "gray-zone" conflict (Echevarria, 2016)^[6]. Some analysts, however, have criticized the concept as excessively elastic, noting that it has been invoked to describe phenomena as varied as Hezbollah's tactics against Israel, Russian actions in Ukraine, Chinese activity in the South China Sea, and Islamic State's use of propaganda, thereby diluting its explanatory value (Murray & Mansoor, 2012)^[23]. Critics argue that hybrid warfare risks becoming a residual category for any conflict that does not conform to the paradigm of conventional interstate war, and that its widespread adoption in Western policy circles has been driven as much by bureaucratic and political incentives as by rigorous conceptual clarity (Fridman, 2018)^[9]. This paper adopts a working definition that treats hybrid warfare as a strategy, pursued by state or state-sponsored actors, that combines military and non-military instruments in a coordinated and sustained campaign intended to weaken an adversary's sovereignty and strategic position while remaining below the threshold of open interstate war (Cullen & Reichborn-Kjennerud, 2017)^[4].

Sovereignty in the Twenty-First Century

1. The Westphalian Inheritance

The modern concept of state sovereignty is conventionally traced to the Peace of Westphalia, which ended the Thirty Years' War in 1648 and established, at least in principle, a system of formally equal states possessing supreme authority within their territories and immunity from external interference in their internal affairs. This Westphalian model rests on two interlocking premises: territorial integrity, meaning that borders are inviolable except through mutual consent or lawful self-defense, and political independence, meaning that a state's internal governance arrangements are not subject to external dictation. These premises were subsequently codified in the United Nations Charter, whose Article 2(4) prohibits the threat or use of force against the

territorial integrity or political independence of any state, and whose Article 2(7) affirms the principle of non-intervention in matters essentially within the domestic jurisdiction of states (Krasner, 1999) ^[18].

2. Krasner's Fourfold Typology

Stephen Krasner's influential study *Sovereignty: Organized Hypocrisy* complicates the unitary picture of sovereignty by disaggregating the concept into four analytically distinct components (Krasner, 1999) ^[18]. International legal sovereignty refers to the mutual recognition of states as juridically independent actors within the international system. Westphalian sovereignty refers to the principle of non-interference in a state's internal affairs. Domestic sovereignty refers to the formal organization of political authority within a state and its capacity to exercise effective control over activities within its borders. Interdependence sovereignty refers to a state's capacity to regulate and control the flow of information, capital, goods, and people across its borders (Krasner, 2001) ^[19]. Krasner's central argument, that sovereignty has always been more of an "organized hypocrisy" honored in principle and violated in practice than a stable legal fact, provides an especially useful lens for understanding hybrid warfare, because each of its constitutive dimensions is targeted by a distinct set of hybrid instruments. Proxy warfare and territorial annexation are direct assaults on Westphalian sovereignty. Cyberattacks on electoral infrastructure and disinformation campaigns are assaults on domestic sovereignty, since they degrade the state's capacity to maintain public order, informed citizenship, and legitimate governance. Weaponized trade, energy dependency, and strategic corruption are assaults on interdependence sovereignty. And the selective, self-interested invocation of international legal norms, sometimes termed "lawfare," represents an erosion of international legal sovereignty from within the system's own normative vocabulary.

3. Sovereignty as Contested Practice

Contemporary international relations scholarship increasingly treats sovereignty not as a fixed legal status but as a continuously contested and performed practice, one that depends on a state's ongoing capacity to exercise effective authority rather than on formal recognition alone. This reconceptualization is essential for understanding hybrid warfare, because hybrid campaigns rarely seek to overturn a state's juridical status in the international system; Ukraine remained internationally recognized as a sovereign state throughout Russia's covert intervention in Donbas, just as Georgia retained its seat at the United Nations after the 2008 war and the subsequent occupation of Abkhazia and South Ossetia. What hybrid warfare erodes is not recognition but capacity: the practical ability of a government to control its territory, secure its information space, protect its economy from coercive leverage, and conduct free and credible political processes. Sovereignty erosion in the hybrid era is therefore incremental, cumulative, and frequently invisible until a crisis, such as an attempted annexation or a contested election, exposes the extent to which a state's effective authority has already been hollowed out.

Instruments of Hybrid Warfare

1. Cyber Operations

Cyber operations constitute one of the most consequential instruments of hybrid warfare because they allow state and state-sponsored actors to strike at critical infrastructure, financial systems, and government institutions from a

distance while preserving a substantial degree of deniability (Deibert, 2015). The 2007^[5, 13] cyberattacks against Estonia, widely attributed to Russian state or Russian-aligned actors following a diplomatic dispute over the relocation of a Soviet-era war memorial, disabled government, banking, and media websites for days and are frequently cited as an early demonstration of cyber operations used as a coercive instrument against a sovereign state (Giles, 2016). The 2015 and 2016^[12, 29] attacks on Ukraine's power grid, which caused temporary blackouts affecting hundreds of thousands of consumers, demonstrated the capacity of cyber operations to produce physical, kinetic-like effects without a single soldier crossing a border (Jasper, 2020) ^[16]. Because cyberspace lacks clearly demarcated borders and because attribution of cyberattacks is technically and politically fraught, cyber operations are particularly well suited to hybrid strategies: they can degrade a target state's domestic sovereignty, understood as its capacity to guarantee order and provide essential services, without providing the kind of unambiguous evidence of state responsibility that would justify an armed response under international law (Krishnan, 2020) ^[20]. The Tallinn Manual process, an effort by international legal scholars convened under the NATO Cooperative Cyber Defence Centre of Excellence to clarify how existing international law applies to cyber operations, illustrates both the seriousness with which the international community has approached this challenge and the persistent legal ambiguity that surrounds the threshold at which a cyber operation might constitute an unlawful use of force or an armed attack (Schmitt, 2017) ^[27].

2. Disinformation and Information Warfare

Information warfare, encompassing the deliberate production and dissemination of disinformation, the manipulation of social media platforms, and the exploitation of a target society's existing political and social cleavages, represents a second central pillar of hybrid strategy (Snegovaya, 2015) ^[28]. Unlike propaganda in earlier eras of conflict, contemporary disinformation campaigns are amplified by the architecture of social media platforms, which reward emotionally engaging content regardless of its veracity and allow malicious actors to microtarget specific demographic and ideological audiences (Wigell, 2019) ^[31]. The Internet Research Agency's documented interference in the 2016^[29] United States presidential election, which included the creation of thousands of fabricated social media accounts designed to inflame partisan and racial divisions, and subsequent European experiences with coordinated disinformation around elections in France, Germany, and the Netherlands, illustrate how information operations can degrade a target state's domestic sovereignty by corroding public trust in electoral institutions, media, and government itself (Deibert, 2015; Wigell, 2019) ^[5, 31]. Because information warfare exploits constitutional protections for freedom of expression in democratic societies, it presents an especially difficult governance challenge: measures adequate to counter disinformation risk infringing upon the very civil liberties that hybrid adversaries seek to exploit and discredit (Monaghan, 2019) ^[22].

3. Economic and Energy Coercion

Economic interdependence, long regarded by liberal international relations theory as a stabilizing force that

raises the costs of conflict, has instead become a vector of hybrid pressure in the hands of states willing to weaponize trade, investment, and energy relationships. Russia's use of natural gas exports as a coercive instrument against Ukraine and other European states, most visibly during recurring disputes over gas transit and pricing in the 2000s and 2010s and again amid the broader confrontation following its 2022 invasion, illustrates how energy dependency can be converted into leverage over a target state's domestic political choices. China's use of trade restrictions and informal boycotts against states that take positions Beijing regards as contrary to its core interests, such as the suspension of imports from Australia following Canberra's call for an independent inquiry into the origins of COVID-19, similarly demonstrates how economic interdependence can be selectively instrumentalized to punish and deter policy choices without resort to military force. These practices exploit what Krasner termed interdependence sovereignty: the capacity of a state to regulate and buffer itself against externally imposed economic shocks (Krasner, 1999) ^[18]. When that buffering capacity is insufficient, economic coercion becomes a potent, low-cost, and often legally ambiguous instrument of hybrid pressure (Wigell, 2019) ^[31].

4. Proxy and Paramilitary Forces

The use of unmarked or deniable military and paramilitary forces remains a core instrument of hybrid warfare, precisely because it allows an aggressor state to achieve territorial and political objectives while avoiding the unambiguous attribution that would accompany the deployment of regular, uniformed armed forces. Russia's deployment of unmarked soldiers, popularly termed "little green men," during the 2014^[2] annexation of Crimea, and its subsequent sponsorship of separatist militias in the Donbas region, exemplify this approach; the ambiguity surrounding the identity and command responsibility of these forces complicated both Ukraine's immediate military response and the wider international community's capacity to characterize the operation unambiguously as an act of interstate aggression until evidence of direct Russian military involvement became difficult to deny (Bērziņš, 2014) ^[2]. Beyond state proxies of this kind, private military companies, most notably the Wagner Group and its later reorganized successors, have extended hybrid reach into Syria, Libya, the Central African Republic, Mali, and elsewhere, allowing the Russian state to pursue strategic objectives, including resource extraction and the projection of influence, while formally denying responsibility for the actions of ostensibly private contractors (Giles, 2016) ^[12]. Iran's cultivation of an extensive network of allied militias across Lebanon, Iraq, Syria, and Yemen serves a comparable function, projecting Iranian strategic influence deep into neighboring states' domestic political and security affairs while allowing Tehran to maintain formal deniability for many of the network's more provocative actions (Chivvis, 2017) ^[3].

5. Lawfare and the Instrumentalization of International Norms

A final and less frequently discussed instrument of hybrid warfare is the strategic manipulation of international law itself, a practice sometimes termed "lawfare" (Fridman, 2018) ^[9]. This can take the form of citing the principle of the

responsibility to protect or the right to self-determination in a highly selective manner to justify interventions or annexations, as Russia did in citing the protection of ethnic Russians and Russian-speakers to justify its 2014^[2] intervention in Crimea and its broader 2022 invasion of Ukraine, framings that echo, however imperfectly, the humanitarian justifications advanced by Western states in earlier interventions such as Kosovo in 1999 (Renz, 2016) ^[26]. Lawfare can also involve the manipulation of domestic legal and administrative processes in a target state, such as the strategic use of shell companies, non-governmental organizations, and academic partnerships to launder influence, or the exploitation of judicial and electoral procedures in target states to legitimize outcomes favorable to the aggressor, for example through staged referenda of the kind conducted in Crimea in March 2014 and in the four annexed regions of Ukraine in September 2022, both of which were rejected as unlawful by the overwhelming majority of the international community, including the United Nations General Assembly.

Case Studies

1. Russia and Ukraine, 2014^[2] to the Present

The Russian campaign against Ukraine represents the paradigmatic case of hybrid warfare eroding state sovereignty across every dimension identified by Krasner's typology (Krasner, 1999) ^[18]. The 2014 annexation of Crimea combined the covert deployment of unmarked special forces, extensive disinformation about the nature and origin of the intervening troops, cyber operations against Ukrainian government and media infrastructure, and a staged referendum conducted under conditions of military occupation, all executed with sufficient speed and ambiguity to present the international community with a fait accompli before a coordinated response could be organized (Bērziņš, 2014; Chivvis, 2017) ^[2, 3]. The subsequent conflict in the Donbas region combined the covert insertion of Russian personnel and materiel with the mobilization of local separatist proxies, producing a protracted conflict that Russia was able to characterize, for years, as an internal Ukrainian civil conflict rather than an interstate war, thereby complicating both Ukraine's efforts to invoke international support and the West's efforts to calibrate a proportionate response (Kofman & Rojansky, 2015) ^[17]. Although Russia's full-scale invasion in February 2022 marked a return to overt conventional warfare, the preceding eight years illustrate how hybrid methods can achieve significant territorial and political objectives, including the de facto removal of Crimea from Ukrainian control and the entrenchment of separatist statelets in eastern Ukraine, while avoiding the unambiguous characterization as interstate war that would have more readily triggered collective defense obligations or broader international intervention (Renz, 2016) ^[26].

2. China's Gray-Zone Strategy in the Indo-Pacific

China's approach to territorial disputes in the South China Sea and toward Taiwan exemplifies a parallel but distinct hybrid strategy often described by the term "gray-zone" operations (Echevarria, 2016) ^[6]. Beijing has employed a maritime militia composed of ostensibly civilian fishing vessels, backed by coast guard and naval assets held in reserve, to assert control over contested waters and reefs without engaging in overt military confrontation, a strategy

sometimes termed "cabbage" tactics for the way in which layers of vessels are used to encircle and gradually squeeze out rival claimants from disputed features (Treverton *et al.*, 2018) ^[30]. The construction and militarization of artificial islands on reefs in the Spratly archipelago, conducted incrementally and accompanied by official statements emphasizing civilian and scientific purposes, has allowed China to establish substantial military infrastructure in contested waters while diplomatically minimizing the appearance of aggressive intent until the infrastructure was effectively complete (Krishnan, 2020) ^[20]. Toward Taiwan, China has combined near-continuous incursions into Taiwan's air defense identification zone, cyber intrusions against government and critical infrastructure targets, extensive disinformation campaigns designed to shape Taiwanese public opinion ahead of elections, and economic coercion targeting Taiwanese exporters, all calibrated to maintain pressure on Taipei's political autonomy without crossing the threshold that would constitute an unambiguous act of war and invite a decisive international response (Monaghan, 2019) ^[22].

3. Transnational Election Interference and Democratic Backsliding

A third illustrative case concerns the broader pattern of interference in democratic electoral processes across North America and Europe (Wigell, 2019) ^[31]. Beyond the well-documented Russian interference in the 2016^[29] United States presidential election, European states including France, Germany, the Netherlands, and the Baltic states have reported coordinated disinformation campaigns, hacking operations targeting political parties, and the strategic amplification of extremist and separatist political movements designed to polarize domestic politics and weaken the cohesion of the European Union and NATO (Snegovaya, 2015) ^[28]. These campaigns rarely aim to install a specific alternative government; rather, their strategic logic is corrosive rather than substitutive, aiming to degrade public trust in democratic institutions, deepen social polarization, and diminish the diplomatic and military cohesion of transatlantic alliances, thereby indirectly weakening the collective sovereignty-protecting functions those alliances perform for their individual member states (Wigell, 2019; Deibert, 2015) ^[5, 31].

Institutional, Legal, and Normative Responses

1. NATO and the Threshold Problem

The North Atlantic Treaty Organization has confronted a persistent conceptual and legal challenge in adapting its collective defense framework, anchored in Article 5 of the North Atlantic Treaty, to a form of conflict deliberately designed to remain below the threshold of armed attack that would trigger collective defense obligations. NATO's 2014 Wales Summit and subsequent summits acknowledged this challenge explicitly, affirming that a hybrid campaign could, in principle, meet the threshold for invoking Article 5, while leaving considerable strategic ambiguity as to precisely where that threshold lies, a deliberate ambiguity intended to preserve deterrent flexibility but one that also reflects genuine difficulty in codifying a clear legal or political trigger for hybrid aggression (NATO, 2022). NATO has since developed a network of specialized institutions, including the Cooperative Cyber Defence Centre of Excellence in Tallinn and the Strategic Communications

Centre of Excellence in Riga, to build member states' capacity to detect, attribute, and respond to hybrid threats, alongside "counter hybrid support teams" that can be dispatched to assist member states experiencing acute hybrid pressure (NATO, 2024).

2. The European Union and the Hybrid CoE

The European Union has developed a parallel institutional architecture, most prominently through the European Centre of Excellence for Countering Hybrid Threats, established in Helsinki in 2017 through a memorandum of understanding among an initial group of states together with NATO and the European Union, and subsequently expanded to encompass the near totality of EU and NATO member states (European Centre of Excellence for Countering Hybrid Threats, 2021) ^[7]. The Centre functions as an autonomous, network-based hub that conducts strategic analysis, training exercises, and scenario planning intended to strengthen participating states' resilience against hybrid threats spanning disinformation, cyber intrusions, economic coercion, and the instrumentalization of migration (Cullen & Reichborn-Kjennerud, 2017) ^[4]. The European Union has complemented this institutional effort with a broader "hybrid toolbox," combining sanctions regimes, coordinated diplomatic responses, strategic communications initiatives intended to counter disinformation, and legislative measures targeting foreign interference in elections and critical infrastructure protection (European Union External Action Service, 2016) ^[8]. The Union's 2022 Strategic Compass explicitly identified hybrid threats as a central challenge to European security, reflecting a broader shift within European strategic thinking away from an exclusive focus on conventional military deterrence toward a more comprehensive conception of societal and infrastructural resilience (Monaghan, 2019) ^[22].

3. Legal Ambiguity and the Limits of International Law

Despite these institutional developments, international law remains ill-equipped to address hybrid warfare comprehensively. The United Nations Charter's framework for the use of force was drafted with conventional interstate war in mind and provides limited guidance for calibrated, deniable, and multidimensional campaigns that combine cyber intrusions, disinformation, economic coercion, and proxy violence. Legal scholars associated with the Tallinn Manual process have sought to clarify how existing international humanitarian law and the law governing the use of force apply to cyber operations, but persistent disagreement remains over the precise threshold at which a cyber operation might constitute a prohibited use of force or an armed attack justifying self-defense under Article 51 of the UN Charter (Schmitt, 2017) ^[27]. Attribution, both technical and political, remains the central obstacle: even where forensic evidence strongly suggests state responsibility for a cyber intrusion or disinformation campaign, the requirement of a high evidentiary standard for public attribution, combined with the political risks of escalation, frequently deters affected states from pursuing formal legal or military responses, thereby reinforcing the strategic logic that makes hybrid warfare attractive to revisionist actors in the first place (Jasper, 2020) ^[16].

4. Resilience as a Strategic Paradigm

In response to these legal and institutional limitations, both NATO and the European Union have increasingly

emphasized societal and infrastructural "resilience" as the primary strategic response to hybrid threats, on the premise that a hybrid campaign's effectiveness depends fundamentally on the vulnerabilities present within the target society rather than solely on the sophistication of the attacking state's instruments (Treverton *et al.*, 2018) ^[30]. Resilience-based approaches encompass measures such as media literacy education intended to inoculate populations against disinformation, diversification of energy supplies to reduce vulnerability to coercive leverage, hardening of critical infrastructure against cyber intrusion, and reform of electoral and campaign finance laws to limit covert foreign influence (Monaghan, 2019^[22]; European Union External Action Service, 2016) ^[8]. This resilience paradigm represents a significant conceptual shift in thinking about sovereignty protection: whereas traditional sovereignty was defended primarily through military deterrence and diplomatic recognition, resilience-based approaches locate the primary line of defense within the social, economic, and informational fabric of the state itself, implicitly acknowledging that hybrid warfare targets precisely those dimensions of sovereignty that lie beyond the reach of conventional military power.

Critical Perspectives and Conceptual Debates

Notwithstanding its widespread adoption in policy and scholarly discourse, the concept of hybrid warfare continues to attract substantial criticism (Wither, 2016) ^[32]. Some scholars argue that the term obscures more than it illuminate, given that the blending of conventional and irregular tactics, the use of proxies, and the manipulation of information are not genuinely novel phenomena but recurring features of statecraft and conflict throughout history, from ancient stratagems of subterfuge to Cold War-era covert action and proxy conflict (Murray & Mansoor, 2012) ^[23]. From this perspective, the popularity of "hybrid warfare" as a concept reflects less a fundamentally new mode of conflict than a rebranding of familiar practices, driven in part by the institutional and budgetary incentives of Western defense establishments seeking to justify new capabilities and organizational structures in the aftermath of the counterinsurgency campaigns in Iraq and Afghanistan (Fridman, 2018) ^[9].

A related critique holds that the concept has been applied asymmetrically, with far greater analytical and moral scrutiny directed at the hybrid activities of adversarial states such as Russia, China, and Iran than at comparable practices, including covert action, economic sanctions, and information operations, conducted by Western states themselves (Galeotti, 2019) ^[11]. Scholars associated with this critique caution that securitizing a broad range of ambiguous or contested behaviors under the rubric of hybrid warfare risks justifying disproportionate or illiberal domestic responses, including expanded surveillance powers and restrictions on freedom of expression, in the name of countering foreign interference (Deibert, 2015) ^[5]. A further practical criticism concerns the risk of false attribution and escalation: because hybrid campaigns are deliberately designed to be ambiguous, the pressure to identify and publicly name a responsible state actor can produce premature or politically motivated attributions that themselves contribute to the erosion of a rules-based international order, even as they are undertaken in its defense.

These critiques do not negate the practical significance of the phenomena described under the hybrid warfare label, but they do counsel analytical caution. This paper's use of the term hybrid warfare is intended as a heuristic device for organizing an otherwise disparate set of coercive practices around their shared strategic logic, namely the deliberate exploitation of ambiguity to erode a target state's sovereignty while avoiding the costs associated with unambiguous interstate war, rather than as a claim that these practices constitute an entirely unprecedented category of conflict.

Conclusion

Hybrid warfare has become one of the defining features of interstate competition in the twenty-first century precisely because it exploits the structural weaknesses of a Westphalian international order that was designed to regulate overt, formally declared war between clearly identifiable state actors. By combining conventional military capability with cyber operations, disinformation, economic coercion, proxy violence, and the selective manipulation of international legal norms, hybrid strategies allow revisionist and opportunistic actors to erode a target state's territorial integrity, political autonomy, informational coherence, and economic self-determination without ever crossing the threshold that would unambiguously trigger collective defense obligations or decisive international censure. The cases examined in this paper, spanning Russia's protracted campaign against Ukraine, China's gray-zone assertiveness in the Indo-Pacific, and the broader pattern of interference in democratic electoral processes across North America and Europe, illustrate how each dimension of Krasner's fourfold typology of sovereignty, international legal, Westphalian, domestic, and interdependence sovereignty, has become a distinct target of calibrated hybrid pressure.

The institutional and legal responses developed by NATO, the European Union, and individual states over the past decade reflect a growing recognition that traditional conceptions of sovereignty protection, centered on military deterrence and formal diplomatic recognition, are insufficient to address a mode of conflict that operates chiefly through the exploitation of societal, economic, and informational vulnerabilities. The emerging emphasis on resilience, understood as the capacity of societies and infrastructures to detect, absorb, and recover from sustained hybrid pressure, represents a significant and arguably overdue evolution in strategic thinking, one that locates the defense of sovereignty not solely in the armed forces of the state but in the underlying cohesion of its economy, information ecosystem, and democratic institutions.

At the same time, the conceptual and legal ambiguity that makes hybrid warfare an attractive instrument for revisionist powers also poses a genuine dilemma for democratic societies seeking to respond without compromising the civil liberties and open information environments that hybrid adversaries frequently seek to exploit. Future scholarship and policy will need to grapple with the difficult balance between building societal resilience against hybrid threats and preserving the pluralistic, rights-respecting character of the societies being defended. What is clear, however, is that sovereignty in the twenty-first century can no longer be understood as a static legal condition secured primarily through military deterrence at the border. It must instead be understood as a dynamic and continuously contested

capacity, one that is tested daily across cyberspace, information ecosystems, economic networks, and the proxy battlefields where hybrid warfare has become the defining mode of contemporary interstate rivalry.

References

1. Bartles CK. Getting Gerasimov right. *Military Review*,2016;96(1):30–38.
2. Bērziņš J. Russia's new generation warfare in Ukraine: Implications for Latvian defense policy. National Defence Academy of Latvia, Center for Security and Strategic Research, 2014.
3. Chivvis CS. Understanding Russian "hybrid warfare" and what can be done about it. RAND Corporation, 2017.
4. Cullen PJ, Reichborn-Kjennerud E. Understanding hybrid warfare. Multinational Capability Development Campaign (MCDC), 2017.
5. Deibert RJ. Cyberspace under siege. *Journal of Democracy*,2015;26(3):64–78.
6. Echevarria AJ II. Operating in the gray zone: An alternative paradigm for U.S. military strategy. U.S. Army War College Press, 2016.
7. European Centre of Excellence for Countering Hybrid Threats. Landscaping the hybrid threat. Hybrid CoE, 2021.
8. European Union External Action Service. Joint framework on countering hybrid threats: A European Union response. European Commission, 2016.
9. Fridman O. Russian "hybrid warfare": Resurgence and politicisation. Oxford University Press, 2018.
10. Galeotti M. Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? *Small Wars & Insurgencies*,2016;27(2):282–301.
11. Galeotti M. The mythical "Gerasimov Doctrine" and the language of threat. *Critical Studies on Security*, 2019.
12. Giles K. Russia's "new" tools for confronting the West: Continuity and innovation in Moscow's exercise of power. Chatham House, 2016.
13. Hoffman FG. Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies, 2007.
14. Hoffman FG. Hybrid warfare and challenges. *Joint Force Quarterly*,2009;52(1):34–39.
15. Hoffman FG. On not-so-new warfare: Political warfare vs hybrid threats. War on the Rocks, 2014.
16. Jasper S. Russian cyber operations: Coding the boundaries of conflict. Georgetown University Press, 2020.
17. Kofman M, Rojansky M. A closer look at Russia's "hybrid war." Kennan Cable, Woodrow Wilson International Center for Scholars, 2015, 7.
18. Krasner SD. Sovereignty: Organized hypocrisy. Princeton University Press, 1999.
19. Krasner SD. Abiding sovereignty. *International Political Science Review*,2001;22(3):229–251.
20. Krishnan A. Enter the cyber dragon: Understanding Chinese intelligence agencies' cyber operations. *Comparative Strategy*,2020;39(5):469–488.
21. Mattis JN, Hoffman FG. Future warfare: The rise of hybrid wars. *Proceedings*,2005;131(11):18–19.
22. Monaghan S. Countering hybrid warfare: So what for the future joint force? *PRISM*,2019;8(2):82–98.
23. Murray W, Mansoor PR (Eds.). Hybrid warfare: Fighting complex opponents from the ancient world to the present. Cambridge University Press, 2012.
24. NATO. NATO 2022 strategic concept. North Atlantic Treaty Organization, 2022.
25. NATO. Countering hybrid threats. North Atlantic Treaty Organization Topics, 2024.
26. Renz B. Russia and "hybrid warfare." *Contemporary Politics*,2016;22(3):283–300.
27. Schmitt MN (Ed.). Tallinn manual 2.0 on the international law applicable to cyber operations (2nd ed.). Cambridge University Press, 2017.
28. Snegovaya M. Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare. Institute for the Study of War, 2015.
29. Thomas TL. The evolving nature of Russia's way of war. *Military Review*,2016;96(4):34–42.
30. Treverton GF, Thvedt A, Chen AR, Lee K, McCue M. Addressing hybrid threats. RAND Corporation and Swedish Defence University, 2018.
31. Wigell M. Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. *International Affairs*,2019;95(2):255–275.
32. Wither JK. Making sense of hybrid warfare. *Connections: The Quarterly Journal*,2016;15(2):73–87.