SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

Borders, Business, and Biases: The Ripple Effects of Hybrid Warfare on Future Society

Parhlad Singh Ahluwalia, Academician, Dr. Bhimrao Ambedkar Law University, Jaipur, Rajasthan, India

Abstract

Hybrid warfare — the deliberate, coordinated blending of conventional force, irregular tactics, cyber operations, economic coercion, and disinformation below the threshold of declared war — has moved from a niche military concept to a defining feature of twenty-first-century geopolitics. This paper examines the ripple effects of hybrid warfare across three interlocking domains: borders (territorial sovereignty and critical infrastructure), business (corporate, financial, and macroeconomic systems), and biases (the cognitive and informational ecosystems that shape public perception). Drawing on a structured review of peer-reviewed literature, international financial institution reports, and recent case evidence from the Baltic Sea, the Taiwan Strait, and Eastern Europe, the paper triangulates quantitative estimates of economic loss with qualitative analysis of institutional and psychological effects. Findings indicate that hybrid campaigns generate compounding, cross-domain costs: gross domestic product (GDP) losses of up to 15.1 percent in directly affected regions, global cybercrime damages approaching USD 10.5 trillion annually, corporate deepfake-enabled fraud losses averaging nearly USD 450,000 per incident, and measurable, if uneven, erosion of institutional trust. The paper further shows that hybrid warfare is contested as an analytical category, with several scholars arguing it functions more as a political framing device than a precise doctrine. A multi-perspective analysis — political-strategic, economic, and socio-psychological — is offered, followed by implications for future governance, corporate risk management, and media literacy. The paper concludes that societies which fail to build cross-sectoral resilience across borders, business, and belief systems simultaneously will remain structurally vulnerable to sub-threshold aggression.

Keywords: *hybrid warfare; gray-zone conflict; disinformation; geoeconomic fragmentation; critical infrastructure; cognitive bias; economic security*

1. Introduction

War no longer announces itself. For most of the industrial age, armed conflict was demarcated by declarations, fronts, and treaties; today, the most consequential confrontations between states unfold in the ambiguous space between peace and war, where a cyberattack on a hospital network, a disinformation campaign timed to an election, a severed undersea cable, and a currency-market shock can all originate from the same strategic playbook. This blended approach — encompassing military, economic, informational, and technological instruments deployed simultaneously and often deniably — has come to be known as hybrid warfare [1,2].

The term gained conceptual traction after the U.S. Marine Corps strategist Frank Hoffman

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

described the fusion of conventional capability, irregular tactics, terrorism, and criminality "coordinated within the main battlespace to achieve synergistic effects" in his 2007 monograph on twenty-first-century conflict [1]. It was subsequently adopted, redefined, and institutionalized by the North Atlantic Treaty Organization (NATO) after 2014, when Russia's annexation of Crimea combined denials, irregular fighters, propaganda, and economic pressure in a manner that defied existing military taxonomy [2]. NATO now defines hybrid threats as those that combine military and non-military, covert and overt means — including disinformation, cyberattacks, economic pressure, irregular armed groups, and regular forces — in a manner deliberately designed to blur the line between war and peace and to sow doubt in target populations [2].

What began as a niche strategic-studies term has since become a lens through which governments, corporations, and citizens are asked to interpret an extraordinary range of phenomena: an oil tanker allegedly dragging its anchor across a Baltic power cable [20], a Hong Kong-registered freighter suspected of severing a Taiwan Strait data line [19], a finance employee wiring USD 25 million after a video call with a deepfaked chief financial officer [17], and coordinated social media accounts amplifying electoral distrust [28]. Each of these episodes sits at the intersection of the paper's three organizing themes.

Borders are no longer solely lines defended by armies; they are digital chokepoints, undersea cable landing stations, energy interconnectors, and migration corridors that can be probed, congested, or severed without a single soldier crossing a land frontier [18,19]. **Business** has become both a target and, involuntarily, a battlespace: firms absorb the costs of cybercrime, sanctions-driven decoupling, and reputational sabotage, while simultaneously serving as unwitting vectors for geopolitical competition through supply chains and critical technology [7,11,12]. **Biases** — the cognitive shortcuts, partisan identities, and trust heuristics through which citizens process information — are the terrain on which the informational dimension of hybrid warfare is fought, since disinformation succeeds not by inventing belief from nothing but by exploiting pre-existing psychological and social fault lines [24,25].

This paper argues that these three domains cannot be understood in isolation. A cyberattack on a logistics firm is simultaneously a business event, a border-security event (if it disrupts customs or port systems), and a bias event (if it is accompanied by narrative manipulation about who is responsible). The central contribution of this paper is to integrate economic, security, and communication scholarship into a single analytical account of hybrid warfare's societal ripple effects, supported by quantitative data, comparative case evidence, and a critical discussion of the concept's own contested status in the academic literature [3,5].

The paper is structured as follows. Section 2 defines hybrid warfare and traces its conceptual evolution. Section 3 reviews the relevant literature across security studies, economics, and communication research. Section 4 outlines the methodology. Sections 5 through 7 present findings organized around borders, business, and biases, respectively, supported by tables and figures. Section 8 offers comparative case studies. Section 9 synthesizes multiple disciplinary perspectives. Section 10 discusses implications for future society, Section 11 notes limitations, and Section 12 concludes with recommendations.

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

2. Conceptual Framework: Defining Hybrid Warfare

2.1 Origins and Evolution

The term "hybrid" entered strategic vocabulary in the early 2000s, but it was Hoffman's 2007 monograph that gave it analytical shape, describing hybrid threats as actors that blend conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder within a unified campaign [1]. The concept drew initial empirical grounding from Hezbollah's 2006 confrontation with Israel, in which a non-state actor combined guerrilla tactics with sophisticated anti-tank weaponry, media operations, and rocket barrages [2].

The concept's decisive institutional moment came in 2014. When Russia annexed Crimea and supported separatist movements in the Donbas region using unmarked soldiers, denial operations, economic leverage over energy supplies, and an extensive disinformation campaign, NATO adopted "hybrid warfare" as its interpretive frame for a form of aggression that did not fit the alliance's existing conflict spectrum [2,4]. The U.S. Army's 2011 doctrinal definition described a hybrid threat as the diverse and dynamic combination of regular forces, irregular forces, and criminal elements unified to achieve mutually benefiting effects, while the European Centre of Excellence for Countering Hybrid Threats, established in 2017, defines hybrid threats more broadly as methods and activities targeted towards vulnerabilities of the opponent across a wide range of domains [2].

2.2 A Contested Concept

Despite — or perhaps because of — its rapid institutional adoption, hybrid warfare remains a contested analytical category. Libiseller's 2023 study in the *Journal of Strategic Studies* argues that hybrid warfare became an "academic fashion" specifically because NATO's post-2014 framing diffused into scholarship, meaning that much of the literature reproduces an institutional and political interpretation rather than an independently derived analytical one [3]. Caliskan's interview-based study with NATO officials similarly concludes that the concept is ambiguous and risks leading the alliance to conflate the difference between war and peace, a finding echoed by practitioners who note the term functions partly as a communicative warning signal within NATO and the European Union rather than a precise doctrinal category [5,2]. A related strand of scholarship frames hybrid warfare as, in essence, the continuation of strategic ambiguity by other means, suggesting the concept's primary utility may be as much rhetorical and political as descriptive [30].

This paper adopts a pragmatic position: while acknowledging the concept's definitional looseness, hybrid warfare remains analytically useful as a label for campaigns that deliberately integrate multiple instruments of power — military, economic, cyber, and informational — to achieve strategic effects while remaining below the threshold that would trigger a conventional military or legal response [6,9]. This ambiguity is not incidental; it is the mechanism. Genini's 2025 documentary analysis of NATO strategic communications shows that hybrid methods are calibrated specifically to avoid clear attribution and to exploit the gap between what is legally actionable and what is strategically damaging [4].

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

2.3 A Three-Domain Framework

Building on this definition, the paper proposes a three-domain framework — **borders, business, and biases** — to organize the study of hybrid warfare's societal effects (Table 1). This framework departs from purely military taxonomies by foregrounding the civilian and economic institutions that absorb the majority of hybrid warfare's costs.

Table 1. A Three-Domain Framework for Analyzing Hybrid Warfare's Ripple Effects

Domain	Primary Targets	Illustrative Instruments	Primary Discipline of Analysis
Borders	Territorial sovereignty, critical infrastructure, migration corridors, undersea cables and pipelines	Gray-zone maritime operations, proxy forces, infrastructure sabotage, weaponized migration	Security studies, international law
Business	Firms, financial markets, supply chains, critical technology sectors	Cyberattacks, ransomware, sanctions and counter-sanctions, deepfake-enabled fraud, trade and technology decoupling	Economics, corporate risk management
Biases	Public opinion, institutional trust, electoral processes, social cohesion	Disinformation, computational propaganda, narrative laundering, algorithmic amplification	Communication studies, political psychology

3. Literature Review

3.1 Security and Strategic Studies Literature

The security studies literature on hybrid warfare can be grouped into several broad streams. The first, exemplified by Hoffman's foundational work, treats hybrid warfare as an emergent and genuinely novel mode of conflict requiring new doctrine [1]. The second stream is critical and constructivist, arguing that the concept is less a description of a new reality than a political and institutional artifact. Libiseller's discourse analysis of NATO and academic publications found striking similarities between the two bodies of literature, suggesting that scholarly interest followed institutional framing rather than preceding it [3]. Caliskan's interview data from NATO officials reinforces this reading, with several officials themselves expressing discomfort with the term's imprecision [5]. Sanz-Caballero's 2023 legal analysis adds a third stream, examining how existing international law — on the use of force, sovereignty, and countermeasures — struggles to accommodate hybrid activities precisely because they are designed to remain below legal thresholds of "armed attack" [6].

A fourth, more recent stream examines specific sub-domains of hybrid activity. Balcaen, Bois, and Buts apply game theory to model the strategic incentives facing a state weighing hybrid aggression against conventional deterrence, finding that ambiguity itself has strategic value because it complicates the target's response calculus [9]. Wijnja's comparative study of strategic culture finds that a state's institutional and historical disposition significantly shapes

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

how it perceives and responds to hybrid threats, meaning that a uniform "hybrid warfare doctrine" is unlikely to be equally effective across different national contexts [8].

3.2 Economic Literature

Economic scholarship on hybrid warfare has concentrated on quantifying the costs of conflict that does not resemble conventional interstate war. Bluszcz and Valente's synthetic control study of the Donbas conflict is the most methodologically rigorous example: using cross-country panel data from 1995 to 2017, they estimate that Ukraine's per-capita GDP loss attributable to the war averaged 15.1 percent for 2013 to 2017, rising to 47 percent in the directly affected Donetsk and Luhansk regions for 2013 to 2016 [7,10]. Their analysis also documents that foreign direct investment into the Donbas region stagnated near 1 percent of GDP between 2014 and 2018, reflecting the broader tendency of capital to retreat from ambiguous-conflict environments even when full-scale war has not been declared [10].

At the macro level, the International Monetary Fund's 2023 staff discussion note on geoeconomic fragmentation estimates that policy-driven fragmentation of the global economy — a phenomenon closely linked to, though broader than, hybrid warfare — could reduce global output by up to 7 percent under a severe-fragmentation scenario, rising to 8 to 12 percent in the most exposed countries if technological decoupling accompanies trade restrictions [11,12,13]. A related illustrative scenario in which the world splits into a United States-European Union bloc and a China-Russia bloc estimates permanent global GDP losses of 2.3 percent, equivalent in size to the French economy, with low-income countries losing more than 4 percent of GDP [12].

3.3 Cybersecurity and Corporate Risk Literature

A distinct but overlapping literature quantifies the corporate and cyber dimension of hybrid conflict. Industry projections put global cybercrime damages at approximately USD 10.5 trillion annually by 2025, up from USD 3 trillion in 2015 — a figure the authors describe as representing one of the greatest transfers of economic wealth in history [14]. Complementary industry data show the average global data breach cost falling slightly to USD 4.4 million in 2025 from USD 4.88 million in 2024, even as healthcare breaches remain the costliest at close to USD 10 million per incident [15]. A World Bank literature review cautions, however, that many headline cost estimates cannot be independently verified because they lack transparent methodology, and calls instead for closer attention to peer-reviewed studies of stock market reactions, production-chain disruption, and systemic spillover risk from cyber incidents [16].

The World Economic Forum's 2025 analysis of disinformation's corporate cost adds a further empirical layer: half of surveyed businesses reported being victims of deepfake-enabled attacks in 2024, with average losses of nearly USD 450,000 per incident, and eight in ten executives expressing concern about AI-driven reputational risk even as over a third admitted their organizations were inadequately prepared [17].

3.4 Communication and Political Psychology Literature

The communication and political psychology literature is more cautious than popular discourse about the direct causal power of disinformation. A mixed-methods thesis examining the 2020

U.S. election, the Rohingya crisis, and Russian denial narratives around the invasion of Ukraine found only a weak, non-significant direct correlation between exposure to false content and declining institutional trust, suggesting that erosion operates indirectly and cumulatively through polarization and media ecosystem effects rather than through simple exposure [23]. This nuance is echoed by the Carnegie Endowment's evidence-based policy review, which finds that domestic disinformation is typically far more prolific and influential than foreign influence operations, and that no single intervention — cyber operations, sanctions, indictments, or platform bans — has demonstrated durable strategic deterrence against foreign disinformation campaigns [24].

A Swedish randomized controlled experiment (n = 1,054) further complicates the picture: media literacy interventions that named a foreign adversary (Russia) as the source of disinformation performed differently from source-criticism training that made no such attribution, with implications for how governments calibrate public warnings without inadvertently fuelling excessive suspicion of legitimate media [25]. Harvard Kennedy School's Misinformation Review similarly finds that exposure to fake news is associated with lower trust in media generally, but higher trust in government specifically when a person's preferred political side holds power, indicating that partisan motivated reasoning, not simple exposure, mediates the trust effect [26]. A 2024 review from Japan's Institute of Geoeconomics documents that over 30,000 accounts linked to Russia's Internet Research Agency were active around the U.S. 2016 election, contributing to measurable declines in liberal-democracy index scores, even as the review stresses that domestic polarization created the conditions for foreign narratives to take hold [28]. Recent comparative work extends this by showing that in several democracies, incumbent political elites now spread disinformation openly and explicitly as part of official communication rather than relying solely on covert foreign operations, reframing disinformation as a domestic elite strategy embedded within evolving media systems rather than an externally imposed phenomenon alone [27].

3.5 Infrastructure and Maritime Security Literature

A rapidly growing literature addresses hybrid threats to physical infrastructure. Analyses of the 2024 to 2025 period document a marked rise in undersea cable disruptions in the Baltic Sea, the Taiwan Strait, and the Red Sea, several linked to vessels with obscured ownership or state-aligned crews [18,19]. One assessment identifies 44 cable-damage incidents across 2024 to 2025 alone, while another places total annual submarine cable incidents, including accidental damage, above 100 [20,21]. Given that more than 95 to 99 percent of international data traffic transits undersea cables, these incidents illustrate how physical border infrastructure has become a primary vector of hybrid pressure even though, technically, no territorial boundary is crossed by an anchor dragged across a seabed [22,34].

3.6 The Global South and Developing-Economy Perspective

Much of the literature reviewed above is produced by, and concerned with, institutions and states in North America, Europe, and East Asia. This is not incidental: NATO's conceptual leadership on hybrid warfare, the IMF's institutional vantage point on geoeconomic fragmentation, and the concentration of undersea cable ownership among four firms based in the United States, France, Japan, and China all reflect a research and policy geography

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

weighted toward advanced and major emerging economies [2,11,22]. Yet the IMF's own fragmentation modelling explicitly finds that low-income countries are likely to bear a disproportionate share of the costs of geoeconomic fragmentation, losing more than 4 percent of GDP in illustrative bloc-split scenarios compared with 2 to 3 percent for advanced and other emerging economies, precisely because such countries have the least capacity to diversify trading partners, substitute technology sources, or absorb knowledge-diffusion losses [12]. This asymmetry matters for the paper's argument because it suggests that the societal ripple effects of hybrid warfare are unlikely to be evenly distributed: states with the least involvement in triggering hybrid competition between major powers may nonetheless absorb some of its largest relative economic costs, a pattern that echoes long-standing findings in the conflict-economics literature regarding the disproportionate exposure of smaller and lower-income states to great-power rivalry.

4. Methodology

This paper employs a structured, integrative literature review methodology combined with secondary quantitative data synthesis. The approach is appropriate given the paper's aim: to integrate dispersed, discipline-specific findings — from security studies, economics, cybersecurity risk research, and political psychology — into a single, coherent account of hybrid warfare's societal ripple effects, rather than to generate new primary data.

Source selection. Peer-reviewed journal articles (in outlets such as *Defence and Peace Economics*, the *Journal of Strategic Studies*, *Small Wars & Insurgencies*, and *Humanities and Social Sciences Communications*), International Monetary Fund and World Bank staff publications, and specialist security and cybersecurity industry reports were prioritized. Sources were retrieved through targeted searches combining terms such as "hybrid warfare," "geoeconomic fragmentation," "disinformation trust," "undersea cable sabotage," and "cybercrime cost," restricted primarily to material published or substantively updated between 2020 and 2026 to ensure currency, while foundational conceptual works (notably Hoffman, 2007) were retained regardless of date for their doctrinal significance.

Analytical procedure. Sources were coded thematically according to the three-domain framework (borders, business, biases) developed in Section 2.3. Quantitative estimates — GDP effects, cybercrime costs, fragmentation losses, and trust-erosion metrics — were extracted and cross-tabulated to identify convergence and divergence across studies (Section 6, Table 2; Section 7, Table 3). Qualitative findings on institutional ambiguity, strategic communication, and psychological mechanisms were synthesized narratively.

Limitations of method. As an integrative review rather than a primary empirical study, the paper is necessarily dependent on the methodological quality of its underlying sources, several of which — as the World Bank review itself notes regarding cybercrime cost estimates — lack fully transparent methodology [16]. Where this is the case, the paper flags the estimate as indicative rather than definitive. This limitation is discussed further in Section 11.

5. Borders: Territorial and Sovereignty Effects

5.1 The Blurring of the Border Concept

Hybrid warfare reconfigures what a "border" means. Traditionally, borders demarcated the limits of sovereign jurisdiction defended by conventional military force. In the hybrid

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

paradigm, the contested perimeter extends to undersea cables, energy interconnectors, satellite links, and even the algorithms that shape a population's information diet, none of which correspond neatly to a line on a map [22]. The maritime "gray zone" is the clearest illustration: activities such as anchor-dragging, vessel harassment, and ambiguous survey operations are calibrated specifically to remain below the threshold that would justify a military response, while still degrading an adversary's infrastructure, economy, or resolve [19].

5.2 Undersea Infrastructure as the New Frontier

Between 2024 and 2025, undersea cables in the Baltic Sea, the Taiwan Strait, and the Red Sea were damaged or sabotaged in a pattern that analysts increasingly attribute to state-aligned or state-tolerated activity [18]. On Christmas Day 2024, the Estlink-2 power cable connecting Finland and Estonia, along with two adjacent data cables, was severed; Finnish authorities intercepted the tanker Eagle S, a vessel linked to Russia's sanctions-evading "shadow fleet," illustrating how illicit commercial shipping and strategic sabotage capability have converged [20]. In January and February 2025, two separate incidents damaged cables linking Taiwan to the Penghu Islands and to the wider Trans-Pacific network; in both cases, vessels flagged in third countries but linked to Chinese ownership or crewing were implicated, and in one case a Chinese national captain received a three-year prison sentence from a Taiwanese court [19]. Analysts characterize this as a deliberate extension of gray-zone pressure — alongside routine incursions by Chinese vessels and aircraft — intended to erode Taiwan's stability while preserving plausible deniability [19].

> The scale of the phenomenon is significant: one industry assessment identified 44 cable-damage incidents across 2024 to 2025 with several linked to state-aligned vessels, while a separate threat-intelligence review documented four incidents involving eight distinct cable faults in the Baltic Sea and five incidents involving five distinct faults around Taiwan across the same period [20,21]. Since more than 95 to 99 percent of international data and financial traffic transits these cables, owned overwhelmingly by four companies (U.S.-based SubCom, France's Alcatel Submarine Networks, Japan's NEC, and China's HMN Technologies), even localized sabotage carries disproportionate systemic risk [22].

5.3 Governance Gaps

A recurring theme across the infrastructure-security literature is the mismatch between the transnational nature of undersea assets and the fragmented, largely voluntary architecture of their governance. Repair capacity is concentrated and slow, redundancy is uneven across regions, and there is limited legal accountability for damage inflicted in international waters, particularly when attribution is deliberately obscured through flags of convenience and transponder shutdowns [21,33]. NATO's 2025 launch of Operation Baltic Sentry, along with a coordinated 2024 statement subsequently endorsed by the European Union, Japan, and several other states at the United Nations General Assembly, indicates growing recognition of the problem, though concrete multilateral enforcement mechanisms remain underdeveloped [33].

5.4 Borders as Economic Chokepoints

Border effects are not confined to sabotage; they also include the weaponization of legitimate cross-border flows. Sanctions regimes, export controls on strategically sensitive technologies

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

(notably semiconductors), and restrictions on medical and food exports during crises all transform the border into an instrument of coercive economic pressure, a dynamic the literature terms "geoeconomic fragmentation," discussed further in Section 6 [11,13].

5.5 Weaponized Migration and Human Mobility

A further, less technical but equally consequential border effect concerns the instrumentalization of human mobility itself. States engaged in hybrid competition have, in a number of documented instances, facilitated or encouraged the movement of migrants toward a rival's border in order to generate internal political strain, overwhelm processing capacity, and manufacture domestic division over asylum policy, effectively converting a humanitarian phenomenon into a coercive lever. Because such flows are difficult to distinguish definitively from ordinary migration pressure, they share the same core property as undersea cable incidents and gray-zone maritime probes: plausible deniability combined with genuine, tangible strain on the target state's institutions. This dimension of border security illustrates why the "borders" domain of the paper's framework cannot be reduced to physical infrastructure alone; it also encompasses the administrative and political capacity of a state to process, absorb, and respond to cross-border flows of people without those flows becoming a vector for externally engineered instability.

5.6 Energy Interdependence as a Border-Adjacent Vulnerability

Energy infrastructure sits at the intersection of physical borders and economic coercion, and the Donbas case illustrates this convergence directly: Ukraine's pre-war dependence on Russian gas transit, and the subsequent disruption of energy and coal supply chains discussed in Section 6.1, functioned as a border-adjacent instrument of pressure even where no formal territorial line was crossed [10]. Pipelines, cross-border electricity interconnectors, and liquefied natural gas terminals are, in this sense, functionally equivalent to undersea data cables: they are physical assets whose ownership and routing cross sovereign boundaries, whose disruption can be engineered to appear accidental or commercially motivated, and whose loss imposes costs disproportionate to the physical scale of the damage inflicted. Analysts increasingly treat energy security and undersea infrastructure security as a single integrated category of critical infrastructure protection precisely because the same maritime and gray-zone tactics — anchor-dragging, ambiguous vessel activity, and slow multilateral attribution processes — apply equally to both [21,22].

6. Business: Economic and Corporate Ripple Effects

6.1 Macroeconomic Costs of Hybrid Conflict

The most methodologically rigorous macroeconomic estimate of hybrid warfare's cost comes from the Donbas conflict. Using a synthetic control method applied to cross-country panel data (1995 to 2017), Bluszcz and Valente calculate that Ukraine's foregone per-capita GDP averaged 15.1 percent across 2013 to 2017, escalating from 5.23 percent in 2013 to 21.67 percent by 2017; in the directly affected Donetsk and Luhansk regions, the average causal effect over 2013 to 2016 reached 47 percent [7,10]. The study attributes part of this effect to capital flight: real foreign direct investment into the region stagnated near 1 percent of GDP between 2014 and 2018, and a 2017 blockade of anthracite coal transport by pro-Russian

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

separatists caused production breaks that rippled through interconnected supply chains on both sides of the front line [10].

6.2 Geoeconomic Fragmentation

At the systemic level, the International Monetary Fund's Staff Discussion Note *Geoeconomic Fragmentation and the Future of Multilateralism* estimates that a limited-fragmentation, low-cost-adjustment scenario could reduce global output by roughly 0.2 percent, while a severe-fragmentation, high-cost-adjustment scenario could cost up to 7 percent of global GDP [11,13]. When technological decoupling is layered onto trade restriction, losses in the most exposed countries could reach 8 to 12 percent [11,12]. An illustrative bifurcated-bloc scenario, in which the world splits between a U.S.-EU axis and a China-Russia axis, projects permanent global output losses of 2.3 percent, comparable to the size of the French economy, with emerging markets losing 2 to 3 percent and low-income countries more than 4 percent [12]. Figure 2 summarizes these ranges.

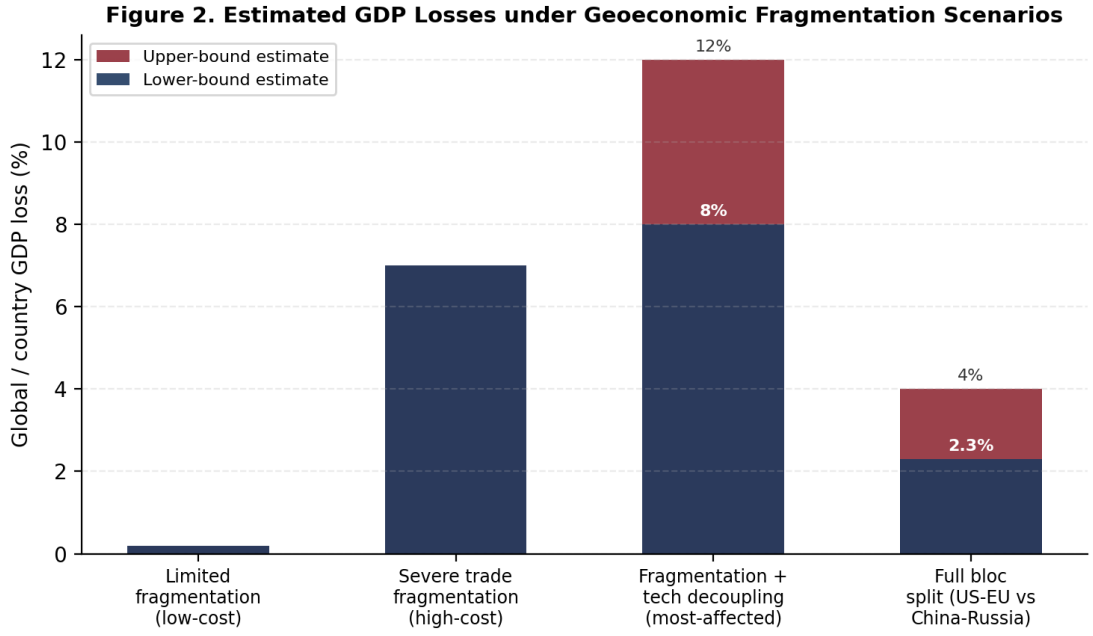


Figure 2. Estimated GDP losses under geoeconomic fragmentation scenarios

Table 2. Estimated Economic Costs Associated with Hybrid and Fragmentation-Related Conflict

Metric	Estimate	Source
Ukraine per-capita GDP loss, 2013-2017 (national average)	15.1%	[10]
Donetsk/Luhansk per-capita GDP loss, 2013-2016	47%	[10]
FDI into Donbas as share of GDP, 2014-2018	~1% (stagnant)	[10]
Global GDP loss, severe trade fragmentation	up to 7%	[11,13]
GDP loss, fragmentation plus technological decoupling (most-exposed countries)	8-12%	[11,12]

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

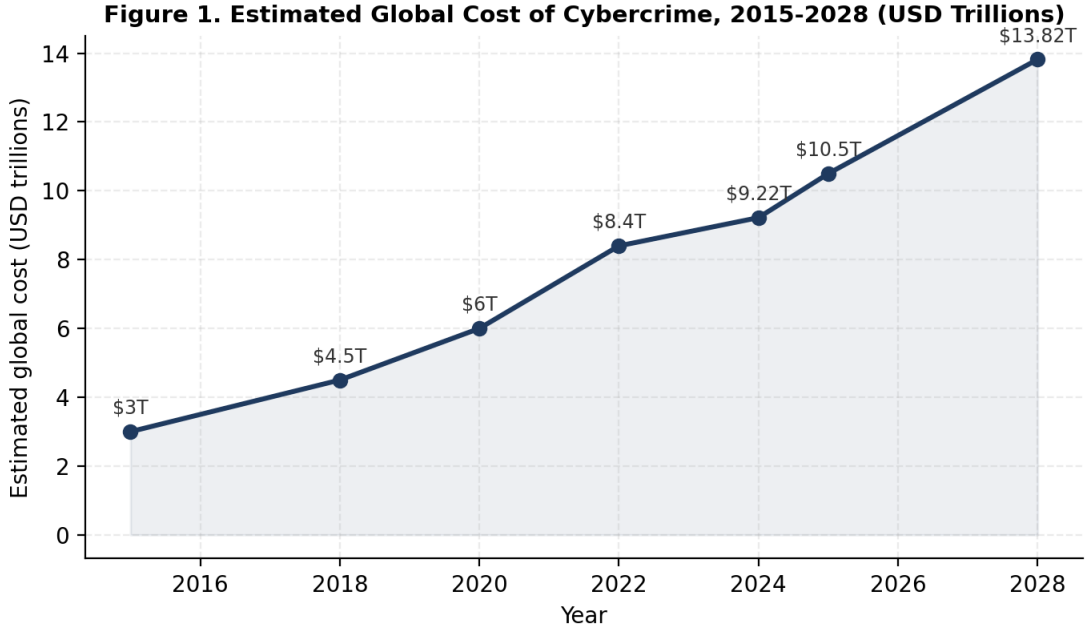
Metric	Estimate	Source
Global GDP loss, illustrative bloc-split scenario	2.3%	[12]
Global cybercrime cost, 2025 (industry projection)	~USD 10.5 trillion	[14]
Global cybercrime cost, 2024-2028 (alternative projection)	USD 9.22T to USD 13.82T	[15]
Average global data breach cost, 2025	USD 4.4 million	[15]
Average healthcare data breach cost, 2024-2025	~USD 9.8-10 million	[15]
Average corporate loss per deepfake-enabled fraud incident, 2024	~USD 450,000	[17]
Businesses reporting deepfake attacks, 2024	~50%	[17]

Note: figures are drawn from diverse sources with differing methodologies; several industry-derived cybercrime cost estimates lack fully transparent methodology and should be read as indicative orders of magnitude rather than precise measurements [16].

6.3 Cybercrime as a Business-Facing Instrument of Hybrid Pressure

Cyber operations occupy a central place in the business dimension of hybrid warfare precisely because they can be deniable, scalable, and calibrated in intensity. Industry projections estimate global cybercrime costs reaching approximately USD 10.5 trillion in 2025, a figure that, if treated as a national economy, would rank third globally behind only the United States and China, up from roughly USD 3 trillion in 2015 [14]. Independent industry data project a rise from USD 9.22 trillion in 2024 to USD 13.82 trillion by 2028 (Figure 1) [15].

Figure 1. Estimated Global Cost of Cybercrime, 2015-2028 (USD Trillions)



While a World Bank review cautions that such aggregate figures often rest on unverifiable methodology, the same review confirms convergent, better-supported evidence on indirect costs, including adverse stock market reactions, reputational damage, production-chain

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

disruption, and systemic spillover risk following major cyber incidents [16].

Individual corporate incidents illustrate the scale at the firm level. A major 2024 ransomware attack on a healthcare claims processor forced a subsidiary of a large insurer to pay a substantial ransom and absorb well over a billion dollars in recorded breach-related costs once recovery, vendor support, and emergency capital are included [15]. A major UK retailer's 2025 breach, attributed to a third-party supplier compromise, halted online ordering for weeks and cost an estimated GBP 300 million in lost sales, remediation, and insurance shortfalls [15].

6.4 Disinformation as a Corporate Risk Vector

A less examined but rapidly growing business-facing dimension of hybrid warfare is synthetic-media-enabled fraud and reputational sabotage. The World Economic Forum's 2025 analysis reports that half of surveyed businesses were victims of deepfake attacks in 2024, with average losses of nearly USD 450,000 per incident, and that 42 percent of surveyed companies identified identity theft as the greatest deepfake-related risk [17]. The starkest illustration is a 2024 case in which a finance employee authorized a USD 25 million transfer after a video call with what he believed to be his company's chief financial officer, but which was in fact an artificial intelligence-generated deepfake [17]. Eight in ten executives surveyed reported concern about AI-driven reputational damage, yet more than a third of companies admitted inadequate preparedness, a gap that is itself a form of systemic vulnerability that hybrid actors can exploit [17].

6.5 Supply Chain and Technology Decoupling

Beyond direct attack, hybrid pressure reshapes business strategy through the slower, structural channel of supply chain reconfiguration. Firms increasingly practice "friend-shoring," relocating production according to political alignment rather than pure cost efficiency, in response to national security-justified trade and technology restrictions [13]. The ratio of global goods trade to GDP has risen from roughly 16 percent at the start of the Cold War to approximately 45 percent today, meaning that contemporary fragmentation is considerably more economically costly than historical precedent might suggest, even before accounting for the deeper integration of financial and technological systems [13]. "Connector" economies such as Mexico and Vietnam have partially cushioned the impact of direct decoupling between major powers, though whether this genuinely diversifies risk or merely relocates it remains an open empirical question [13].

7. Biases: Cognitive, Informational, and Societal Effects

7.1 The Psychological Terrain of Hybrid Warfare

If borders and business represent the physical and economic battlespace of hybrid conflict, biases represent its cognitive battlespace. Disinformation, propaganda, and computational amplification do not implant belief in a vacuum; they succeed by exploiting pre-existing psychological tendencies, including motivated reasoning, in-group loyalty, confirmation bias, and heuristic trust in familiar sources [26,27]. This distinction matters analytically: it shifts the unit of concern from the content of false information to the structural and psychological conditions that make populations receptive to it.

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

7.2 Evidence on Trust Erosion

The empirical picture here is more nuanced than popular discourse suggests. A mixed-methods study combining survey data with case analysis of the 2020 U.S. "Stop the Steal" movement, the Rohingya crisis, and Russian wartime denial narratives found only a weak, non-significant direct correlation between exposure to disinformation and declining institutional trust, concluding that erosion is indirect, cumulative, and mediated by external factors such as pre-existing polarization [23]. This is corroborated by Harvard Kennedy School's Misinformation Review, which found that exposure to fake news correlates with lower general media trust but, counter-intuitively, higher trust in government among those whose preferred party currently holds power, indicating that partisanship, not mere exposure, mediates the relationship between disinformation and institutional trust [26].

A comparative six-country study spanning the United States, United Kingdom, France, Germany, Belgium, and Switzerland (n = 7,006) similarly found that citizens satisfied with the functioning of democracy were generally less vulnerable to disinformation, with the notable exception of the United States, suggesting that baseline democratic satisfaction operates as a protective factor against, rather than a target of, disinformation in most contexts studied [29]. A 2024 review from Japan's Institute of Geoeconomics documents that over 30,000 accounts linked to Russia's Internet Research Agency were active in discourse around the 2016 U.S. presidential election, and situates this activity alongside a measurable dip in that year's liberal-democracy index score, while cautioning that domestic conditions of distrust created the receptive environment foreign narratives exploited rather than being solely created by them [28].

7.3 Domestic versus Foreign Disinformation

A consistent finding across the literature is that domestic disinformation is generally more consequential than foreign-originated disinformation. The Carnegie Endowment's evidence-based policy review states plainly that domestic disinformation is far more prolific and influential than foreign influence operations in most democracies, and finds no strong evidence that cyber operations, sanctions, or indictments achieve durable strategic deterrence against foreign influence campaigns, though preemptive public education shows the most promise among available tools [24]. Recent comparative research extends this insight further, documenting that in several democracies, incumbent political elites now spread disinformation openly and explicitly as an instrument of official communication and campaigning, rather than relying on covert operations alone, a shift that reframes democratic backsliding as substantially a function of domestic elite strategy operating within an evolving media ecosystem [27].

7.4 Calibrating Public Warnings

A Swedish randomized controlled experiment (n = 1,054) offers a methodologically important finding for policy design: media literacy interventions that explicitly named a foreign adversary as a disinformation source produced different effects from source-criticism training that made no external attribution, raising the possibility that naming foreign threats too aggressively risks generating excessive vigilance toward legitimate media rather than more discerning judgment [25]. This finding is significant because it cautions against counter-disinformation strategies

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

that, however well-intentioned, might themselves damage the broader information ecosystem they are meant to protect.

Table 3. Comparative Findings on Disinformation and Institutional Trust

Study / Source	Method	Key Finding
Mixed-methods thesis on 2020 U.S. election, Rohingya crisis, and Ukraine war denial [23]	Survey plus case study analysis	Weak, non-significant direct correlation between exposure and trust decline; erosion is indirect and cumulative
HKS Misinformation Review [26]	Survey analysis of fake-news exposure	Lower trust in media generally, but higher trust in government when the respondent's party is in power
Six-country comparative study, n = 7,006 [29]	Cross-national survey	Satisfaction with democracy reduces vulnerability to disinformation in most countries studied, except the United States
Institute of Geoeconomics review [28]	Documentary and historical review	Foreign-linked accounts (over 30,000, 2016 U.S. election) coincided with measurable liberal-democracy index decline
Carnegie Endowment policy review [24]	Evidence synthesis	Domestic disinformation more influential than foreign operations; no tool shows durable strategic deterrence
Swedish RCT, n = 1,054 [25]	Randomized controlled experiment	Naming a foreign adversary in media literacy training shapes outcomes differently than source-neutral training
Comparative democratic backsliding study [27]	Cross-national analysis	Incumbent elites increasingly spread disinformation openly, shifting the locus from covert foreign operations to domestic elite strategy

7.5 Algorithmic Amplification and Artificial Intelligence

A further and rapidly intensifying dimension of the biases domain concerns the role of algorithmic recommendation systems and generative artificial intelligence in scaling the informational component of hybrid warfare. Where earlier propaganda campaigns required substantial human labor to produce and disseminate persuasive content, generative AI tools now allow a small team, or even a single actor, to produce large volumes of tailored text, images, audio, and video at negligible marginal cost. The corporate deepfake fraud cases discussed in Sections 6.4 and 8.3 are a direct illustration of this shift in the cost structure of deception: what previously required a skilled forger or an elaborate social-engineering operation can now be approximated by widely available synthetic-media tools [17]. Recommendation algorithms on major social platforms compound this effect by optimizing for

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

engagement rather than accuracy, meaning that emotionally charged or identity-affirming content, whether organically produced or synthetically generated, tends to receive disproportionate distribution regardless of its truth value. This combination, cheap production plus algorithmically amplified distribution, means that the "biases" domain of hybrid warfare is likely to become more, not less, significant over the coming decade, even as attribution of any specific piece of synthetic content to a state actor becomes correspondingly more difficult.

7.6 Bias as a Two-Way Vulnerability

An important, if under-examined, implication of this literature is that "bias" in the hybrid warfare context cuts in two directions. On one hand, cognitive and partisan biases make populations susceptible to manipulation. On the other, the analytical and policy discourse about hybrid warfare is itself subject to bias and politicization, a point developed by the "academic fashion" critique discussed in Section 2.2, which shows how institutional framing can shape scholarly and public perception of what counts as a hybrid threat in the first place [3]. This dual vulnerability, susceptibility to manipulation and susceptibility to conceptual over-securitization, is a defining feature of the informational dimension of hybrid conflict.

8. Comparative Case Studies

8.1 Case One: The Donbas War as Prototype Hybrid Conflict (2014-present)

The conflict in eastern Ukraine's Donbas region is widely treated as the paradigmatic case that catalyzed NATO's adoption of the hybrid warfare concept [2,4]. It combined unmarked regular forces, local separatist proxies, extensive denial and disinformation, and economic pressure through energy dependencies and, later, a 2017 transport blockade of anthracite coal that disrupted integrated production cycles across the front line [10]. The rigorously estimated economic toll, a 15.1 percent average per-capita GDP loss nationally and 47 percent regionally, demonstrates that hybrid conflict, even without full-scale conventional invasion, can inflict costs comparable to significant civil conflict [7,10]. The case is also instructive methodologically: because Ukraine avoided formally declaring war for years, the conflict's costs were for a long period difficult to isolate econometrically from ordinary economic volatility, illustrating the broader challenge that ambiguity poses to both policymakers and researchers [10].

8.2 Case Two: Baltic and Taiwan Strait Undersea Cable Incidents (2024-2025)

The near-simultaneous emergence of undersea cable incidents in the Baltic Sea and the Taiwan Strait during 2024 to 2025 illustrates the geographically dispersed but strategically coordinated character of contemporary gray-zone activity. In the Baltic, the Estlink-2 power cable and adjacent data cables were severed on Christmas Day 2024, with Finnish authorities intercepting the tanker Eagle S, part of Russia's sanctions-evading shadow fleet [20]. In the Taiwan Strait, at least two separate incidents in January and February 2025 damaged cables linking Taiwan to regional and transpacific networks, with vessels registered under flags of convenience but linked to Chinese ownership implicated in both [19]. These parallel cases show a common operational signature: use of ambiguously flagged commercial vessels, exploitation of legal gaps in international waters, and reliance on the slow, fragmented nature of multilateral maritime governance to avoid attribution and consequence [21,33]. NATO's response through

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

Operation Baltic Sentry, and Taiwan's shift toward treating cable protection as a national defense priority, illustrate the beginnings of an institutional adaptation, though enforcement capacity still lags the scale of the threat [33].

8.3 Case Three: Corporate Deepfake Fraud as a Business-Facing Hybrid Vector

The 2024 case of a finance employee who authorized a USD 25 million transfer following a deepfake video call impersonating his chief financial officer exemplifies how synthetic media collapses the boundary between cybercrime, corporate fraud, and information warfare [17]. While this incident does not appear to have been state-directed, it demonstrates the capability now available to any actor, state or non-state, willing to combine artificial intelligence tools with social engineering, and it foreshadows a plausible future in which state or state-tolerated actors use identical techniques against strategically significant firms, such as defense contractors, energy operators, and financial clearinghouses, as a deniable instrument of economic coercion [17].

8.4 Case Four: Domestic Disinformation and Democratic Backsliding

Comparative research on informational pathways to electoral distrust in multiple democracies shows a shift from covert foreign interference toward open, elite-driven disinformation as an instrument of domestic political strategy, with the countries examined in one comparative study experiencing attempts to challenge election outcomes motivated in part by disinformation-fuelled beliefs of fraud [27]. This case matters for the paper's argument because it demonstrates that the "biases" dimension of hybrid warfare need not originate from a foreign adversary at all; domestic actors can adopt functionally identical tactics, which complicates both the analytical boundaries of the concept and the design of effective countermeasures [24,27].

8.5 Case Five: Sanctions, Shadow Fleets, and the Convergence of Crime and Statecraft

A final illustrative case concerns the emergence of sanctions-evading "shadow fleets," oil tankers and cargo vessels reflagged under third-country registries, often with obscured beneficial ownership, that were originally developed to circumvent energy sanctions but have since been implicated in suspected infrastructure sabotage, as in the Baltic Estlink-2 incident discussed in Section 8.2 [20]. This case is analytically significant because it demonstrates how instruments developed for one purpose, namely sanctions evasion in the economic domain, can be repurposed for another, namely infrastructure disruption in the border domain, without requiring any new institutional investment. The same vessel, crew, and ownership structure that allow a state to sell sanctioned oil can, with minimal adaptation, also serve as a deniable platform for cable-severing operations. This convergence illustrates why the paper's three-domain framework should be read as interdependent rather than as three separate silos: an asset created for business-domain sanctions evasion becomes, without significant modification, a border-domain coercive instrument, and its use is then interpreted and contested through the biases domain as competing narratives emerge over whether any given incident was accidental or deliberate.

9. Analysis: Multiple Disciplinary Perspectives

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

9.1 The Political-Strategic Perspective

From a political-strategic standpoint, hybrid warfare represents a rational adaptation to the constraints of a nuclear-armed, economically interdependent, and legally regulated international order. States facing high costs and risks associated with overt conventional aggression have strong incentives to pursue objectives through means that remain below thresholds triggering formal alliance responses, such as NATO's Article 5, or unambiguous violations of international law [6,9]. Game-theoretic modelling suggests that the resulting strategic ambiguity is not a side effect but a deliberate feature: it complicates the target state's decision calculus regarding proportional response, and it can be sustained indefinitely at relatively low cost to the aggressor compared to conventional warfare [9]. From this perspective, the Baltic and Taiwan Strait cable incidents and the Donbas conflict are not separate categories of phenomena but points along the same strategic continuum [2,4].

9.2 The Economic Perspective

Economists analyzing hybrid conflict tend to emphasize measurable output losses and capital flight as the primary transmission mechanisms of harm, an approach exemplified by the synthetic control methodology applied to the Donbas conflict [7,10]. This perspective foregrounds an important asymmetry: hybrid conflict's costs are often more diffuse and harder to attribute than conventional war's, which paradoxically can make them politically easier for target governments to underreport or underprioritize, even as their cumulative macroeconomic impact, as the IMF's geoeconomic fragmentation estimates suggest, can rival or exceed the costs of historically significant global shocks in a severe fragmentation scenario [12]. The economic perspective is also notably more skeptical of unverified aggregate cost figures, such as some cybercrime cost projections, preferring methodologically transparent, peer-reviewed estimation over headline industry statistics [16].

9.3 The Socio-Psychological and Communication Perspective

Communication scholars and political psychologists offer a perspective that complicates both the political-strategic and economic accounts by emphasizing that the informational dimension of hybrid warfare cannot be fully understood through a purely instrumental, state-versus-state lens. Their research consistently shows that domestic conditions, including polarization, partisan identity, and pre-existing distrust, mediate whether disinformation succeeds, meaning that foreign hybrid actors are, in an important sense, borrowing the vulnerability that domestic social and political conditions have already created [23,26,29]. This perspective also raises an uncomfortable normative implication: since incumbent domestic political actors have shown a willingness to deploy disinformation tactics functionally identical to those associated with foreign hybrid warfare, drawing a firm analytical line between hybrid warfare attributed to hostile foreign states and ordinary, if corrosive, domestic political competition becomes genuinely difficult [27].

9.4 The Critical-Constructivist Perspective

A fourth, more skeptical perspective, represented by the "academic fashion" critique, cautions against treating hybrid warfare as a stable, objectively bounded phenomenon at all [3]. On this view, the concept's rapid diffusion after 2014 reflects NATO's institutional need for a unifying

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 4, ISSUE 3, SEPTEMBER 2026
Available Online : https://shodhprakashan.in/

interpretive frame as much as it reflects a genuinely novel form of conflict, and its continued use risks encouraging threat inflation, in which ordinary criminal, commercial, or accidental phenomena, such as a cargo ship's anchor drag, a lone hacker's ransomware attack, or a partisan blogger's exaggeration, are reflexively read through a securitized lens [3,5]. This perspective does not deny that states engage in coordinated, multi-domain coercion; rather, it insists that analysts and policymakers must maintain rigorous, case-by-case standards of evidence and attribution before applying the "hybrid warfare" label, precisely because the label itself carries escalatory and legitimizing power [5,6].

9.5 The Corporate Governance Perspective

A fifth perspective, drawn from corporate risk management and business ethics scholarship rather than security studies proper, treats hybrid warfare primarily as an exogenous shock to enterprise risk models that were not originally designed to accommodate state-level adversaries. From this vantage point, the central analytical puzzle is not why states behave ambiguously, but why firms, particularly those in critical sectors such as energy, telecommunications, logistics, and finance, have historically under-invested in resilience against low-probability, high-impact, state-linked disruption relative to their investment in more familiar categories of risk such as market volatility or conventional crime [16,17]. This perspective helps explain a pattern visible across the case studies in Section 8: in the Baltic and Taiwan Strait cable incidents, in the healthcare ransomware case, and in the corporate deepfake fraud case, private firms rather than governments bore the immediate operational and financial consequences of state-linked or state-tolerated hybrid activity, even though the strategic objective of the activity was plausibly geopolitical rather than commercial. The corporate governance perspective therefore argues for treating hybrid-warfare exposure as a distinct category within enterprise risk frameworks, subject to board-level oversight, rather than folding it into generic cybersecurity or business-continuity planning.

9.6 Synthesis

Taken together, these five perspectives are not fully reconcilable, and this paper does not attempt to resolve their tension artificially. Instead, it treats their disagreement as analytically productive: the political-strategic and economic perspectives are most useful for quantifying and anticipating the material costs of hybrid activity (Sections 5 and 6), the communication and psychological perspective is indispensable for understanding why populations are differentially vulnerable to the informational dimension (Section 7), the corporate governance perspective clarifies why private firms rather than governments so often absorb the immediate costs of state-linked disruption, and the critical-constructivist perspective functions as a necessary check against overextending the concept to phenomena that may be better explained by ordinary crime, market dynamics, or domestic political dysfunction [3,5,16,23,27].

10. Implications for Future Society

10.1 Governance and Institutional Adaptation

The evidence reviewed suggests that future societal resilience against hybrid pressure will depend on institutional adaptation across at least three fronts. First, infrastructure governance must evolve from a largely voluntary, fragmented model toward binding multilateral frameworks for undersea cable protection, given that current mechanisms lag well behind the scale and pace of incidents documented since 2024 [21,33]. Second, economic policy will need to balance the legitimate goal of supply chain resilience against the risk that overly aggressive "de-risking" itself accelerates the fragmentation costs it seeks to avoid, since IMF modelling shows that the deepest losses occur precisely when countries are forced into exclusive trading blocs rather than retaining diversified partners [12,13]. Third, information governance will require calibrated rather than blanket interventions; the Swedish RCT evidence suggests that poorly designed public warnings about foreign disinformation can themselves erode trust in legitimate media, meaning transparency and proportionality should guide counter-disinformation communication [25].

10.2 Business and Corporate Risk Management

For the corporate sector, hybrid warfare implies that risk management can no longer treat cybersecurity, geopolitical risk, and reputation management as separate functions. The convergence of ransomware, sanctions exposure, and deepfake-enabled fraud into a single incident type, as illustrated by the USD 25 million deepfake fraud case, suggests firms operating in strategically sensitive sectors such as energy, finance, logistics, and defense-adjacent technology should integrate scenario planning across these domains rather than maintaining siloed departments [17]. Boards and executives, eight in ten of whom already report concern about AI-driven reputational risk, will need to close the preparedness gap identified in current surveys, given that over a third of firms admit inadequate readiness [17].

10.3 Media Literacy and Civic Resilience

The communication literature's most consistent policy-relevant finding is that strengthening baseline democratic satisfaction and general media literacy is likely to be more durable than narrowly targeted counter-foreign-influence campaigns, given the evidence that domestic disinformation dynamics are often more consequential than foreign ones and that poorly calibrated foreign-attribution warnings can backfire [24,25,29]. Future civic education strategies may therefore benefit from emphasizing general epistemic skills, such as source evaluation, understanding of motivated reasoning, and recognition of synthetic media, over campaigns organized primarily around naming specific foreign adversaries.

10.4 The Risk of Conceptual Overreach

Finally, the critical-constructivist literature's caution against "hybrid warfare" as an overextended, securitizing label carries an important implication for future society: institutions, media, and publics should resist the temptation to interpret every ambiguous disruption, such as a shipping accident, a criminal ransomware attack, or a partisan falsehood, as evidence of coordinated state aggression [3,5]. Indiscriminate application of the hybrid warfare frame risks two failure modes simultaneously: desensitizing publics to genuine threats through overuse,

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

and providing hostile actors a ready-made narrative of victimization or plausible deniability whenever they are, in fact, responsible.

11. Limitations

This paper has several limitations. First, as an integrative literature review rather than a primary empirical study, its conclusions are only as reliable as the underlying sources, several of which, particularly industry-derived cybercrime cost estimates, lack fully transparent methodology, a limitation explicitly acknowledged by the World Bank's own review of this literature [16]. Second, the paper's case studies (Donbas, Baltic and Taiwan Strait cables, corporate deepfake fraud) were selected for their prominence and data availability rather than through a systematic, exhaustive sampling procedure, which may introduce selection bias toward well-documented, internationally covered incidents. Third, attribution in gray-zone incidents is frequently contested by design; several of the infrastructure incidents discussed remain formally unresolved or disputed by the states allegedly responsible, meaning the paper's characterizations should be read as reflecting the balance of open-source analytical opinion rather than adjudicated fact [19,33]. Finally, because hybrid warfare itself is a contested concept, this paper's three-domain framework of borders, business, and biases represents one useful heuristic organization among several plausible alternatives, and should not be read as a claim to a single, universally agreed taxonomy [3,5].

12. Conclusion and Recommendations

Hybrid warfare, whatever its precise conceptual boundaries, describes a real and consequential pattern: the coordinated use of military, economic, cyber, and informational instruments to achieve strategic effects while remaining below thresholds that would trigger conventional military or legal responses. This paper has shown that the ripple effects of this pattern are neither confined to the battlefield nor to any single domain of society. Borders now include undersea cables and energy interconnectors as much as land frontiers; businesses absorb trillions of dollars in cyber-related losses and increasingly serve as unwitting fronts in geoeconomic competition; and the cognitive biases of ordinary citizens have become contested terrain in a struggle over institutional trust that implicates domestic political actors nearly as much as foreign adversaries.

The quantitative evidence assembled here, including a 15.1 percent regional GDP loss in the Donbas, global cybercrime costs approaching USD 10.5 trillion, potential fragmentation-related GDP losses of up to 12 percent in the most exposed countries, and corporate deepfake fraud losses averaging USD 450,000 per incident, indicates that the cumulative economic burden of hybrid-style conflict is already substantial and likely to grow as artificial intelligence lowers the cost of both cyberattacks and synthetic disinformation [7,10,11,12,14,17]. At the same time, the communication and critical-constructivist literatures caution against treating every disruption as proof of coordinated hostile design, and against countermeasures so aggressive that they damage the very institutions of trust they intend to protect [3,5,25].

Building future societal resilience will therefore require simultaneous action across all three domains examined in this paper: binding, well-resourced multilateral governance for shared critical infrastructure; integrated corporate risk management that treats cyber, geopolitical,

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 4, Issue 3, September 2026
Available Online : https://shodhprakashan.in/

and reputational threats as a single risk category rather than separate silos; and civic and media literacy strategies grounded in general epistemic skills rather than narrowly targeted foreign-threat messaging. No single domain, whether border security, corporate cybersecurity, or media literacy, can address hybrid warfare's effects in isolation; it is precisely the coordinated, cross-domain nature of the threat that necessitates an equally coordinated, cross-domain societal response. Table 4 summarizes concrete, domain-specific recommendations arising from the analysis above, directed respectively at governments, firms, and civil society and media institutions.

Table 4. Summary of Domain-Specific Recommendations

Domain	Primary Actor	Recommendation	Supporting Evidence
Borders	National governments and multilateral bodies	Establish binding, jointly funded rapid-repair and attribution mechanisms for undersea cables and cross-border energy infrastructure, rather than relying on voluntary coordination	[21,33]
Borders	Regional alliances	Extend maritime domain-awareness programs (e.g., Operation Baltic Sentry) to cover a wider range of gray-zone tactics, including weaponized migration and shadow-fleet activity	[20,33]
Business	Corporate boards and executives	Integrate cyber, geopolitical, and synthetic-media fraud risk into a single enterprise risk category with direct board-level reporting, rather than siloed IT or compliance functions	[16,17]
Business	Governments and international financial institutions	Pursue supply chain resilience through diversification rather than exclusive bloc formation, given that the latter carries substantially higher modelled GDP costs	[12,13]
Biases	Educators and civil society organizations	Prioritize general epistemic and media-literacy skills over narrowly targeted foreign-adversary messaging, to avoid triggering excessive vigilance toward legitimate media	[24,25]
Biases	Platforms and policymakers	Increase transparency around algorithmic amplification of synthetic and emotionally charged content, given the declining cost of AI-generated disinformation	[17,27]
Cross-cutting	Researchers and analysts	Maintain rigorous, case-specific attribution standards before applying the "hybrid warfare" label, to avoid both threat inflation and the provision of ready-made deniability narratives to genuine aggressors	[3,5]

References

1. Hoffman FG. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington (VA): Potomac Institute for Policy Studies; 2007.
2. Radin A. What is "Hybrid Warfare," Really? Washington (DC): Center for European Policy Analysis (CEPA); 2022 Oct 19.
3. Libiseller C. 'Hybrid warfare' as an academic fashion. Journal of Strategic Studies. 2023.
4. Genini D. Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. Journal of European Security and Defence Studies (Sage). 2025.
5. Caliskan M. The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials. Small Wars & Insurgencies. 2021;32(2).
6. Sanz-Caballero S. The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanities and Social Sciences Communications. 2023.
7. Bluszcz J, Valente M. The economic costs of hybrid wars: the case of Ukraine. Defence and Peace Economics. 2022;33(1):1-25.
8. Wijnja K. Countering hybrid threats: does strategic culture matter? Defence Studies. 2022.
9. Balcaen P, Bois C, Buts C. A game-theoretic analysis of hybrid threats. Defence and Peace Economics. 2022.
10. Bluszcz J, Valente M. The economic costs of hybrid wars: the case of Ukraine [full article]. Defence and Peace Economics. 2022;33(1):1-25.
11. Aiyar S, Ilyina A, et al. Geoeconomic Fragmentation and the Future of Multilateralism. Washington (DC): International Monetary Fund; 2023. Staff Discussion Note No. SDN/2023/001.
12. Bolhuis M, Chen J, Kett B. The Costs of Geoeconomic Fragmentation. Finance & Development. Washington (DC): International Monetary Fund; 2023.
13. Gopinath G. Geopolitics and its Impact on Global Trade and the Dollar [speech]. Washington (DC): International Monetary Fund; 2024 May 7.
14. Cybersecurity Ventures. Official Cybercrime Report 2025: Cybercrime to cost the world $12.2 trillion annually by 2031. 2025 May 30.
15. Infinum. The Cost of Cyberattack in 2025. 2026 Apr 29.
16. World Bank Group. A Review of the Economic Costs of Cyber Incidents. Washington (DC): World Bank; 2024.
17. World Economic Forum. What's the real cost of disinformation for corporations? 2025.
18. Georgetown Journal of International Affairs. Critical Undersea Infrastructures: A Framework to Address Threats in a Post-Physical Context. Washington (DC): Georgetown University; 2026 Feb 12.
19. Global Taiwan Institute. China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities. 2025 Jun 4.
20. Windward. What is the Maritime Gray Zone? 2025 Dec 7.

21. Recorded Future (Insikt Group). Submarine Cable Security at Risk Amid Geopolitical Tensions and Limited Repair Capabilities. 2025 Jul 17.
22. Atlas Institute for International Affairs. Weaponized Connectivity: Political Risk and the Security of Global Undersea Cables. 2026 Jul 11.
23. [Author name not disclosed in source metadata]. Misinformation, Disinformation, and the Erosion of Institutional Trust: The Role of Social Media in Democracy [master's thesis]. Chapman University Digital Commons; International Studies Theses, No. 33.
24. Carnegie Endowment for International Peace. Countering Disinformation Effectively: An Evidence-Based Policy Guide. Washington (DC): Carnegie Endowment; 2024 Jan.
25. [Authors not disclosed in source metadata]. Naming the enemy: how to fortify society against foreign disinformation while avoiding excessive vigilance to reliable media. Humanities and Social Sciences Communications. 2025 Jun 11.
26. Harvard Kennedy School Shorenstein Center. Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. HKS Misinformation Review. 2023 Jul 10.
27. [Authors not disclosed in source metadata]. Disrupting democracy: how informational pathways and misinformation shape trust in election results. Journal article. 2026.
28. Institute of Geoeconomics (IOG). Chapter 2: Disinformation in the United States: When Distrust Trumps Facts. Tokyo: IOG News; 2024 Dec 2.
29. [Authors not disclosed in source metadata]. The Role of Trust and Attitudes toward Democracy in the Dissemination of Disinformation: a Comparative Analysis of Six Democracies. Digital Journalism. 2023.
30. Carlucci P, Mumford A. Hybrid Warfare: The Continuation of Ambiguity by Other Means. European Journal of International Security. 2022.
31. 3GIMBALS. Grey Zone Maritime Threats in European Waters and Strategies. 2025 May 8.
32. Global SITU. Global Deep Dive: Undersea Cable Sabotage Underscores Ongoing Threat of Grey Zone Warfare. 2025 Jun 27.
33. Texas National Security Review. Toward Undersea Cable Resilience: The Case for Global Collaboration. 2026 Jun 15.
34. ASIS International. Nation-States Suspected of Cutting the Cords in Emerging Form of Warfare. Security Management Magazine. 2025 Jan 7.