Hybrid Warfare, Grey Zone Conflicts, and the Battle of Narratives: Discourse as a Strategic Weapon

Alizeh khakwani – alizehkhakwani97@gmail.com – Mphil Public Administration, Department of Political Science Bahauddin Zakariya University Multan

Muqadas Saleem – muqadassaleemlaghari@gmail.com – Mphil Public Administration, Office Coordinator Bloomfield Hall School Multan Cantt

Dr. Muhammad Mudabbir Malik – mudabbir.malik@gmail.com – Faculty member Department of Political Science Bahauddin Zakariya University Multan

Abstract

This paper explores the changing nature of warfare in the current environment, which has brought into focus the nature of hybrid warfare and the grey zone of military conflict, including the central role that discourse and narrative play as strategic weapons. Conventional war has changed, state and non-state adversaries are employing Information operations, influence warfare and media control to achieve strategic end states without the use of force of arms. This investigation is based on a qualitative research design with the critical discourse analysis (CDA), and strategic communication theories providing the overall framework for how stories create views, change attitudes and, perhaps, even realign hard geopolitical circumstances. The paper integrates theories from international relations, as well as media and military strategy, to examine case studies such as Russian activities in Ukraine, Chinese influence in Asia and ISIS propaganda. The results illustrate the growing importance of narrative supremacy in current conflict and suggest countermeasures to democratic resilience.

Keywords: Hybrid warfare, grey zone conflict, strategic narratives, information warfare, discourse analysis

1. Introduction

At the dawn of the 21st century, there have been significant changes in the dynamics of conflict, especially as conventional military operations are replaced with more indirect, asymmetric methodologies. Hybrid warfare and grey zone conflict take place underneath the level of traditional war, by mixing military with economic, cyber and information warfare instruments (Hoffman, 2007; Mazarr, 2015). Central to these strategies is the weaponization of discourse— using narratives in ways that sway perceptions, divide societies, and weaken opponents (Pamment, 2020).

This article investigates the way in which discourse is used as a strategic weapon in contemporary warfare, more specifically, in hybrid warfare and grey zone operations. The following research questions guided the study

(1) How do strategic narratives of state and non-state actors emerge and are employed in hybrid warfare?

(2) Which theoretical perspectives or schools of thought offer the best insight regarding the place of discourse in modern warfare?

(3) How can democracies push back against adversarial narrative domination?

2. Literature Review

2.1 Introduction

The comparison is done through qualitative methods, including critical discourse analysis (CDA) and case study comparisons, in order to evaluate the narrative strategies in conflicts of the recent past. Contemporary war is not only about weaponry--it is about information, public perception, and discourse. Hybrid warfare and grey zone conflicts symbolize this shift, with traditional and non-traditional approaches combined to pursue strategic goals short of open warfare (Hoffman, 2007; Mazarr, 2015). An essential component of these conflicts is the weaponization of narratives – or how language in deployed as a tactic to shape public opinion, polarize a society or discredit an opponent (Pamment, 2020).

This literature review discusses the literature concerning hybrid warfare, grey zone conflicts and the use of discourse as a strategic weapon. Taking stock of theoretical, applied and counter perspectives on detoxication and from international relations, media studies, and security studies, this book will interest all students of conflict studies.

2.2 Conceptualizing Hybrid Warfare and Grey Zone Conflicts

Hybrid warfare is considered a new form of conflict, combining elements of traditional warfare with those of irregular warfare, including cyber warfare, economic pressure, and propaganda (Hoffman, 2007). Unlike traditional warfare that requires clear battle fronts, hybrid warfare uses ambiguity, and confounds the enemy so that it cannot attribute actions, and cannot respond with efficacious action (NATO, 2010). In this way, aggressors can exploit strategic effects without provoking all out war, frequently through the manipulation of proxies, covert means, and the psyche (Mazarr, 2015). Hybrid warfare is most readily characterized by its is capacity for adaptation-both state and non-state actors can tay the means that they use to take advantage of a rivals weaknesses, whether that be through interfering in elections, energy blackmail or social media-driven polarization (Pomerantsev, 2014). For instance, Russia's seizure of Crimea in the spring of 2014 showed how hybrid warfare could be used to undermine a neighbor (Ukraine), through a combination of covert forces ("little green men") and propaganda, while allowing deniability (Galeotti, 2019). The fluidity of the hybrid challenge would undermine the hard security of the panzer formations, making necessary a comprehensive approach to the kinetic and non-kinetic conduct of warfare.

Grey zone conflicts occupy the unclear space between war and peace, where actions are deliberately designed to remain below the threshold that would provoke a conventional military response (Mazarr, 2015). These conflicts often involve incremental aggression such as China's salami-slicing tactics in the South China Sea or Iran's use of proxy militias in the Middle East to gradually alter facts on the ground without overt escalation (Mattis & Brazil, 2019). Grey zone strategies thrive in legal and normative gaps, exploiting the slow reaction times of democratic

institutions and the difficulty of mobilizing international consensus against ambiguous threats (Freier, 2015). Unlike hybrid warfare, which may include direct (though deniable) military action, grey zone conflicts prioritize indirect means: economic pressure, law fare, and influence operations aimed at eroding an adversary's cohesion over time (Brands, 2016). The strategic use of narratives is particularly critical in grey zone conflicts, where perception management can shape geopolitical outcomes as decisively as physical force (Pamment, 2020). For instance, China's "Three War fares" doctrine integrates media manipulation, legal justifications, and psychological operations to assert dominance without firing a shot (Shambaugh, 2020). Together, hybrid and grey zone conflicts underscore the growing importance of non-military tools in 21st-century warfare, demanding innovative approaches to deterrence and resilience.

2.3 Grey Zone Conflict: Between War and Peace

Grey zone conflicts represent a strategic middle ground where state and non-state actors deliberately operate below the threshold of conventional warfare to achieve political and military objectives without triggering overt retaliation (Mazarr, 2015). These ambiguous confrontations characterized by incremental aggression, legal warfare, and persistent deniability exploit the inherent constraints of democratic decision-making and international law (Freier, 2015). Unlike traditional warfare, where clear red lines and escalation dynamics apply, grey zone tactics thrive in ambiguity: China's gradual militarization of artificial islands in the South China Sea, Russia's use of unmarked forces in eastern Ukraine, and Iran's proxy warfare through groups like Hezbollah all exemplify how actors manipulate the space between peace and conflict to advance strategic aims (Brands, 2016). The absence of declared hostilities allows aggressors to avoid unified resistance while steadily altering facts on the ground, forcing adversaries into reactive and often fragmented responses (Mattis & Brazil, 2019). This approach is particularly effective against rule-based international systems, where institutional inertia and legalistic debates over attribution create windows of opportunity for grey zone actors to consolidate gains (Pamment, 2020).

The strategic use of narratives is a defining feature of grey zone conflicts, as perception management becomes as critical as physical control of territory (Galeotti, 2019). By framing actions as defensive (e.g., Russia's "protection" of Russian-speaking populations) or legitimate (e.g., China's historical claims in the South China Sea), aggressors shape global and domestic opinion to normalize their encroachments (Shambaugh, 2020). Legal warfare—exploiting international tribunals, bilateral agreements, and sovereignty debates—further blurs the lines between aggression and diplomacy, complicating countermeasures (Pomerantsev, 2014). Meanwhile, economic coercion (e.g., China's trade restrictions on Australia) and cyber operations (e.g., Russian election interference) extend the battlefield into non-military domains, eroding adversary resilience without direct confrontation (Nye, 2021). The result is a "slow-burning wear and tear on the status quo in which there is no one dramatic event to focus attention on, making it difficult to place strategic weight on steady but unremarkable movements forward" (Mazarr et al., 2023). For democracies, the grey zone threat demands a re-imagining of deterrence in terms of constant level of contestation across the legal, economic, and informational spaces—a challenge that involves much more coherent government, private sector and civil society inter-action (Wardle & Derakhshan, 2017).

2.4 The Role of Non-State Actors in Hybrid Warfare

Non-state actors have emerged as pivotal players in hybrid warfare, leveraging their agility, deniability, and ideological networks to amplify the effectiveness of asymmetric strategies (Kilcullen, 2010). Unlike traditional state militaries, these groups—including terrorist organizations, private military companies, and cyber mercenaries—operate outside conventional legal and military frameworks, enabling them to exploit vulnerabilities that rigid state structures cannot address swiftly (Bunker, 2015). For instance, the Islamic State (ISIS) demonstrated how non-state actors could blend guerrilla warfare with sophisticated propaganda, using social media to recruit foreign fighters and incite global terror while controlling territory in Iraq and Syria (Berger, 2018). Similarly, Russian-backed private military contractors like the Wagner Group have executed destabilizing operations in Syria, Libya, and sub-Saharan Africa, providing Moscow with plausible deniability while advancing its geopolitical interests (Galeotti, 2019). The decentralized nature of these actors allows them to adapt rapidly to countermeasures, making them persistent threats in hybrid conflicts where ambiguity and indirect action dominate (Hoffman, 2007). Their ability to weaponize ideology, finance operations through illicit networks, and exploit ungoverned spaces further complicates efforts to neutralize them through conventional military or diplomatic means (Marten, 2019).

Beyond armed groups, cyber collectives and hacktivist networks have expanded the battlefield into the digital domain, where attribution is challenging and attacks can be launched with minimal resources (Rid, 2013). Groups like Anonymous or state-aligned cyber militias (e.g., Russia's "Fancy Bear") conduct disruptive operations—from election interference to critical infrastructure sabotage—without direct state fingerprints, blurring the lines between criminal activity and warfare (Singer & Friedman, 2014). Transnational criminal organizations further exacerbate hybrid threats by trafficking weapons, laundering money, and collaborating with insurgent groups, as seen in Latin America's nexus of cartels and guerrilla movements (Felbab-Brown, 2020). These actors thrive in governance gaps, where weak institutions and corruption allow them to operate with impunity (Williams, 2016). The convergence of non-state violence, digital warfare, and illicit economies creates a layered threat environment, demanding coordinated responses that integrate intelligence-sharing, law enforcement, and community resilience (Kilcullen, 2013). For example, countering ISIS required not only military strikes but also dismantling its online recruitment networks and disrupting financing through cryptocurrency tracking (Awan, 2017). As hybrid warfare evolves, the role of non-state actors will likely grow, necessitating innovative frameworks that address their unique operational and ideological dimensions (Arquilla & Ronfeldt, 2001).

3. Theoretical Framework

3.1 Hybrid Warfare and Grey Zone Conflict

he theoretical framework of hybrid warfare and grey zone conflict provides a critical lens for analyzing the evolving nature of 21st-century strategic competition, where the boundaries between war and peace are deliberately blurred (Hoffman, 2007; Mazarr, 2015). Hybrid warfare theory, as articulated by Frank Hoffman, posits that modern conflicts increasingly integrate conventional military force with irregular tactics such as cyber operations, economic coercion, and information warfare to exploit an adversary's vulnerabilities while avoiding direct attribution (Hoffman, 2009). This framework challenges traditional binary conceptions of war and peace, emphasizing instead a spectrum of conflict where state and non-state actors employ tailored

combinations of kinetic and non-kinetic tools to achieve strategic objectives (Mazarr et al., 2023). Grey zone conflict theory complements this by focusing on operations that remain below the threshold of conventional war, leveraging ambiguity in international law and institutional inertia to gradually alter the status quo (Freier, 2015). Collectively, these theories account for how (non-)state actors such as Russia, China and Islamists leverage perceptions, norms and institutions to achieve strategic goals while avoiding full-blown war—be it the Russian ('little green men') intervention in Crimea, the Chinese salami-slicing in the South China Sea, or IS's digital caliphate (Galeotti, 2019; Shambaugh, 2020; Berger, 2018). The framework also emphasizes the strategic value of narrative control as a force multiplier: that is, how narrative constructing discourse is used to legitimize actions, drive allegiance and discredit enemies (Pamment, 2020). By integrating military strategy, international relations, and communication studies perspectives, this theory provides a comprehensive picture of the current dynamics of conflict, with an increased focus on the integrated response addressing both the physical and cognitive aspects of war (Nye, 2021).

3.2 Strategic Narratives and Discourse Power

The concepts of strategic narratives and discourse power offer valuable explanations of the cognitive aspects of hybrid warfare, drawing attention to the ways in which language, media, and symbolic representations are weaponized to influence perceptions, construct identities and justify conduct in modern conflict (Miskimmon et al., 2013; Pamment, 2020). Based on constructivist IR theory (Wendt, 1999) and CDA (Fairclough, 1995), this approach argues that narratives are not merely descriptive but also constitutive of reality (i.e., they 'do things'—constructing threat, legitimizing intervention, mobilizing population) (Wodak & Meyer, 2016). In hybrid warfare, both state and non-state actors intentionally construct and propagate rival narratives in order to undermine enemies, such as Russia's disinformation campaigns portraying NATO as a menace (Pomerantsev, 2014) and China's "discourse power" posture to normalize its maritime sovereign claims (Shambaugh, 2020). The framework emphasizes the three core purposes of strategic narratives: coercion (e.g., threats articulated through state-led media), persuasion (ChinasBelt and Road Initiativenarratives), and subversion (ISIS leveraging digital propaganda playing on Western grievances) (Berger, 2018; Miskimmon et al., 2017). Examining how stories move in media ecosystems, along social networks, and through institutional discourses, this theoretical approach shows the relationship between material power and symbolic power in hybrid conflicts —where dominating narratives is often as important as having the upper hand over territory (Nye, 2021). The framework further highlights democratic vulnerabilities to narrative warfare, including open societies' tension between commitment to free speech and counter-disinformation efforts (Benkler et al., 2018) while providing avenues for resilience through narratives contested, media literacy, and strategic communication (Wardle & Derakhshan, 2017).

3.3 Constructivism and Soft Power

The conceptual conjuncture between constructivism and soft power offers a strong explanatory edifice for analyzing the ideational and normative dimensions of hybrid warfare, focusing on shared beliefs, identities and cultural attractions that inform conflict behaviour in the 21st century (Wendt, 1999; Nye, 2004). Constructivist theory contests materialist inferences of international relations by claiming that social facts such as threats, alliances, and sovereignty are intersubjectively constituted through discursive argumentation, social practice, and

institutionalization (Katzenstein 1996). When pressed against the insecurities that drive hybrid warfare, this lens also shows us how actors such as Russia and China strategically manipulate norms and identities to legitimate (e.g., in relation to Crimea, this meant framing annexation as the provision of 'protection' to Russian speakers) while delegitimizing adversaries (e.g., NATO expansion seen as imperialist) (Pomerantsev, 2014; Shambaugh, 2020). Soft power theory adds to this understanding by studying how states weaponize attractive and persuasive means like cultural institutions (such as Confucius Institutes), ecosystems of media (such as RT and CGTN), and economic statecraft (such as Belt and Road Initiative narratives) to influence behavior in ways that are promiscuous rather than coercive (Nye, 2011). This framework accounts for hybrid warfare's ccognitive domain where historical narratives, value claims, and symbolic politics convey the meaning- making processes that allow actors to chip away at democratic unity (e.g., Russian election interference) or to make territorial expansion seem normal (e.g., China's "nine gate line") (Miskimmon et al., 2013). Crucially, this model raises democratic vulnerabilities: the pluralism of open societies is manipulable by wedge issues and disinformation, whereas in the authoritarian model, narrative control gets more and more centralized (Benkler et al., 2018). The constructivist-soft power hybrid ultimately requires a reconceptualization of deterrence to feature normative resilience (civil society, media literacy, alternative narratives) at the heart of the 21st century strategic competition (Pamment, 2020).

4. Mechanisms of Narrative Warfare

4.1 Disinformation and Propaganda

Russia's "firehouse of falsehood" model relies on rapid, repetitive, and contradictory messaging to paralyze critical thinking (Paul & Matthews, 2016). Its state media outlets RT, Sputnik serve as vectors of confusion, targeting both domestic and international audiences.

China's narrative strategy is more structured. Its "Wolf Warrior" diplomacy aggressively counters foreign criticism, while initiatives like "mask diplomacy" during COVID-19 seek to present China as a humanitarian leader (Zhao, 2020).

4.2 Victim-Perpetrator Framing

States routinely invert moral roles in conflict. Russia portrays NATO expansion as aggression and its own invasions as defense. China frames itself as a victim of Western containment, painting its regional assertiveness as necessary for survival (Shambaugh, 2020). These roles resonate with audiences primed by historical grievances.

4.3 Semantic Subversion

Lexical warfare involves redefining terms to suit strategic goals. Russia called its 2022 Ukraine invasion a "special military operation." China refers to its militarization of disputed maritime zones as "defensive modernization." Such language obscures true intent and reshapes public discourse (Batongbacal, 2016).

5. Counter-Narrative Strategies

5.1 Defensive Measures

Democracies have begun to recognize the need for resilience. Finland's media literacy programs teach students how to evaluate sources and identify propaganda from an early age (Suoninen, 2020). EUvsDisinfo and similar fact-checking bodies play a vital role in exposing falsehoods before they gain traction.

5.2 Offensive Measures

Proactive storytelling matters. Ukraine's President Zelensky has demonstrated the power of emotional, authentic, and visually engaging communication. His wartime speeches have helped shape global perceptions of the conflict.

Social media companies are beginning to take responsibility. Meta removed coordinated Chinese networks in 2022 and continues to invest in identifying state-linked disinformation campaigns (Meta, 2022).

5.3 Institutional Reforms

NATO has recognized cognitive warfare as a domain of conflict, calling for psychological resilience among member states (NATO, 2022). The EU's Digital Services Act mandates that tech companies monitor and mitigate harmful content, including state-sponsored disinformation.

6. Future Challenges

Artificial intelligence introduces new complexities. AI can produce persuasive deepfakes, clone voices, and flood platforms with synthetic content that mimics real discourse (DiResta, 2023). Blockchain technologies may allow anonymous propaganda networks to emerge, complicating traceability and accountability.

Moreover, non-state actors—from terrorist groups to extremist ideologues—now use gamified narratives and interactive content to radicalize youth. These narratives are often more engaging and immersive than traditional state media (Awan, 2017).

To counter these threats, democracies must forge new alliances with tech firms, invest in adaptive digital education, and establish ethical oversight for AI-generated content.

7. Methodology

This research adopts a qualitative approach, combining:

- **Critical Discourse Analysis (CDA):** To examine how language and media shape power relations (Fairclough, 1995; Wodak & Meyer, 2016).
- **Case Study Analysis:** Focusing on Russian disinformation in Ukraine, China's "Three Warfares" doctrine, and ISIS's digital propaganda.
- **Theoretical Synthesis:** Integrating theories from international relations (e.g., constructivism, soft power) and media studies (e.g., framing theory).

Data sources include government reports, news media, social media content, and academic literature.

8. Analysis

8.1 Russian Hybrid Warfare in Ukraine

Russia's annexation of Crimea (2014) combined military action with disinformation, portraying the intervention as a defense of Russian speakers (Pomerantsev, 2014). State-backed outlets (RT, Sputnik) amplified divisive narratives to weaken Western cohesion.

8.2 China's "Three Warfares" Doctrine

China employs psychological, media, and legal warfare to assert dominance without direct conflict (Mattis & Brazil, 2019). The Belt and Road Initiative (BRI) narratives frame China as a benevolent global leader.

8.3 ISIS and Digital Propaganda

ISIS used social media to recruit followers and spread fear, crafting a narrative of jihadist supremacy (Berger, 2018). Their discourse combined religious rhetoric with modern media tactics.

9. Case Studies

9.1 Russia: Mastering the Grey Zone through Hybrid Warfare and Narrative Control

Russia's media ecosystem reinforces nationalist narratives and suppresses dissent. Domestically, it cultivates the myth of a besieged fortress under Western attack. Abroad, it amplifies social divisions racial tensions in the U.S., Euroscepticism in the EU using bots, memes, and conspiracy theories (Howard et al., 2018; Pomerantsev, 2019).

Russia has emerged as one of the most adept practitioners of hybrid warfare, integrating conventional military capabilities with cyber operations, disinformation campaigns, and proxy forces to achieve strategic objectives below the threshold of open war. The hallmark of Russian hybrid strategy lies in its exploitation of the "grey zone" that ambiguous space between peace and war where attribution is difficult, responses are constrained, and international norms are blurred (Galeotti, 2016).

One of the clearest examples is the 2014 annexation of Crimea. Russian forces, disguised as local militias often referred to as "little green men" seized control without open conflict. Simultaneously, Russian state media and online trolls flooded global and local platforms with narratives justifying the intervention as a defense of ethnic Russians and a response to an illegitimate coup in Ukraine (Pomerantsev& Weiss, 2014).

Cyber operations and information warfare are central to Russia's approach. The 2016 U.S. presidential elections marked a watershed moment, with Russian-linked entities using social media to polarize American society (Mueller, 2019). Troll farms like the Internet Research Agency leveraged fake personas, both networks, and targeted advertisements to sow discord and undermine trust in democratic institutions.

At the heart of this strategy is Russia's mastery of narrative warfare. The Kremlin views discourse not merely as an adjunct to military power but as a strategic weapon in its own right. Russian media outlets

such as RT and Sputnik craft and export alternative narratives that challenge Western norms and values, often promoting relativism and conspiracy theories to erode the credibility of objective truth (Paul & Matthews, 2016).

Russia also uses historical revisionism to justify aggressive policies. By invoking a narrative of Western encirclement and historical grievance, Moscow seeks to legitimize its actions domestically and to some extent internationally.

In sum, Russia exemplifies how hybrid warfare and grey zone tactics can be harmonized with a sophisticated information strategy to achieve strategic ends without triggering conventional military responses. The country's emphasis on narrative as a weapon of war underscores the changing nature of conflict in the 21st century where controlling the story can be as impactful as winning the battle.

9.2 China: Strategic Patience in the Grey Zone and the Use of Narrative for Legitimacy

China's global discourse strategy, known as (huàyǔquán), is rooted in controlling the terms of international debate. Through CGTN, Confucius Institutes, and global diplomatic messaging, China promotes itself as a responsible power. Simultaneously, it reframes history to validate its regional ambitions (Callahan, 2010).

China's approach to hybrid warfare and grey zone conflicts is rooted in its philosophy of strategic patience and long-term influence operations. Rather than sudden interventions, Beijing employs a slow, persistent, and multi-layered strategy to advance its interests, especially in the South China Sea, Taiwan Strait, and global information space (Mazarr et al., 2019).

Beijing utilizes a range of tools economic coercion, legal warfare (lawfare), cyber espionage, and maritime militia operations to assert control without triggering direct military confrontation. The concept of "Three War fares" psychological, media, and legal warfare codified by the People's Liberation Army (PLA), encapsulates China's belief that modern conflict includes shaping perceptions as much as deploying forces (Kania, 2016).

In the South China Sea, China constructs artificial islands and militarizes them while issuing historical and legal claims that lack broad international recognition. Simultaneously, it deploys civilian fishing vessels and coast guard ships to challenge the presence of other claimants (Poling, 2020).

Narrative control is central to China's grand strategy. Domestically, the Communist Party of China (CPC) uses narrative to maintain legitimacy, promoting themes of national rejuvenation, historical victimization by foreign powers, and the inevitability of China's rise. Internationally, Beijing positions itself as a responsible power offering an alternative to Western hegemony (Callahan, 2015).

During the COVID-19 pandemic, Beijing worked aggressively to reshape the global narrative, emphasizing its success in controlling the virus and casting doubt on Western responses (Thornton, 2020).

In the Taiwan conflict, China uses hybrid tactics to pressure the island militarily, economically, and psychologically. Frequent incursions by PLA aircraft, cyber attacks, and disinformation campaigns are designed to erode Taiwanese morale and international support (Sacks, 2022).

China's hybrid and grey zone strategy reflects a nuanced understanding of modern conflict. Rather than direct confrontation, Beijing aims to win without fighting reshaping norms, borders, and perceptions through persistent, layered influence.

9.3 Iran: Asymmetric Hybrid Warfare and the Weaponization of Ideological Narratives

Iran's revolutionary rhetoric blends anti-colonialism with religious identity. It frames the U.S. and Israel as existential threats, while presenting its regional influence as a moral obligation to protect oppressed Muslims. This narrative resonates deeply across Shia communities in Iraq, Lebanon, and Yemen (Alfoneh, 2012).

Iran's approach to hybrid warfare is shaped by its geopolitical constraints and revolutionary ideology. As a mid-level power facing superior conventional militaries particularly the United States and Israel—Iran has developed a highly asymmetrical and ideologically driven strategy centered on proxy warfare, cyber operations, and narrative influence (Byman, 2005).

At the core of Iran's strategy is the use of proxy militias. The Islamic Revolutionary Guard Corps (IRGC), especially its Quds Force, has cultivated networks across Iraq, Syria, Lebanon, and Yemen. Groups like Hezbollah, the Popular Mobilization Forces, and the Houthis act as force multipliers, allowing Iran to exert influence while maintaining plausible deniability (Levitt, 2013).

Cyber warfare has become a critical domain for Iran. Iranian hackers have conducted attacks on U.S. infrastructure, Saudi oil facilities, and Israeli targets. These operations, often attributed to state-sponsored groups like APT33 and APT35, exemplify Iran's capacity to project power through non-traditional means (Zetter, 2019).

Narrative is a vital element of Iran's hybrid warfare toolkit. Domestically, the regime frames its struggle as a resistance against Western imperialism and Zionism, rooted in Shi'a Islamic ideology. This narrative justifies internal repression and external aggression, rallying both domestic and regional audiences (Alfoneh, 2010).

During regional crises, Iran excels at controlling the story. After the assassination of Qassem Soleimani, Tehran portrayed him as a martyr and symbol of resistance, generating a surge of nationalism and sympathy across the region (Fulton et al., 2019).

Iran also targets Diasporas and online communities with tailored disinformation, particularly around contentious events like the Gaza conflict or U.S.-Iran negotiations. These campaigns blur facts, sow doubt, and erode the credibility of Western media.

In conclusion, Iran's hybrid warfare strategy integrates irregular forces, cyber tools, and ideological discourse to compete effectively despite conventional inferiority. Its success lies not just in battlefield outcomes but in shaping the narratives that define legitimacy, resistance, and sovereignty in a contested region.

10. Discussion

The study of hybrid warfare and grey zone conflicts through the prism of strategic narratives evidences a fundamental change in the nature of modern contemporary warfare in which language functions not only as a weapon but also as a battleground. Examples in the form of

Russia's disinformation campaigns in Ukraine (Pomerantsev, 2014), China's "Three Warfares" doctrine (Mattis & Brazil, 2019), and ISIS digital propaganda (Berger, 2018) illustrate that dominance comes in narrative form before it comes in the form of steel and stone. The combination of hybrid warfare theory (Hoffman 2007), constructivism (Wendt 1999), and soft power (Nye 2004) theoreticises the notion that actors are able to make use of the structurally uncertain space that transitions the binary model (of war and peace) in confusing what people think they know, in the sense that war-fighting manipulates perceptions, destroys institutional trust, and re-fabricates norms (Mazarr 2015). For example, Russian historical warfare (use of narrative and memory; e.g., portraying NATO expansion as an existential threat) and Chinese lawfare in the So uth Chinese Seademonstrates the manner in which discourse makes the very reality that it purports to describe (Shambaugh, 2020; Freier, 2015). This corresponds to Fairclough's (1995) critical discourse analysis, which argues that language does not just represent power relations but acts in it. The cases illustrate a paradox: democracies are prone to narrative warfare as a function of designer information ecosystems (Benkler et al., 2018) — yet, in a paradox, centralized control of discourse by authoritarian regimes undermines its credibility, thereby hindering their long-term soft power (Nye, 2011). Emerging threats are underscored in this review too, such as how AI-mediated deepfakes are deepening disinformation (Chesney & Citron, 2019) and social media algorithms are being weaponized to divide and rule societies (Woolley & Howard, 2019). Counterstrategies need to combine material deterrence with cognitive resilience—pairing NATO's Enhanced Forward Presence with narrative monitoring of the EUvsDisinfo kind (Pamment, 2020), even while nurturing civic media literacy (Wardle & Derakhshan, 2017). In the final analysis, this book demonstrates that 21st-century conflict is fought as much in the human mind as in physical space, and requires integrated solutions that overlap in security politics, communications, and democracy institution building.

The combination of constructivist, frame theory and hybrid warfare models posit that discourse is not only reflective, but trans-formative-in shaping conflict.

11. Conclusion

This article shows that modern warfare has changed substantially and hybrid warfare and grey zone operations are now deploying strategic narratives as powerful weapons to influence and manipulate perceptions, identities and institutional trust without engaging in the traditional methods of war making. We argue that in synthesising case studies of Russian disinformation, China's legal warfare and ISIS propaganda with theoretical insights from constructivism and critical discourse analysis, we can illustrate that controlling the narrative space is now as strategically important as dominating physical geography. To meet these emergent threats, democracies will need to pursue comprehensive defense strategies that at once incorporate technological countermeasures, institutional reforms, and journalistic media literacy, and which understand the character of 21st-century warfare as one that is waged not only on the battlefield but in the cognitive domain where narratives shape political realities. The results require immediate interdisciplinary response among security professionals, communication researchers, and policy-makers in curbing the use of democratized platforms for promoting discord and limiting the effects of weaponized communication.

9. References

1. Alfoneh, A. (2012). *Iran Unveiled: How the Revolutionary Guards Is Transforming Iran from Theocracy into Military Dictatorship*. AEI Press.
2. Awan, I. (2017). Cyber-extremism: ISIS and the power of social media. *Social Science and Public Policy, 54*(2), 138–149.
3. Batongbacal, J. (2016). After the arbitral tribunal ruling: The Philippines and China in the South China Sea. *Asia Maritime Transparency Initiative*. https://amti.csis.org/
4. Callahan, W. A. (2010). *China: The Pessoptimist Nation*. Oxford University Press.
5. DiResta, R. (2023). The future of synthetic media and trust. *Journal of Democracy, 34*(1), 45–58.
6. Edele, M. (2022). *Debating the Great Patriotic War: Stalinist Memory and the Politics of History in Russia*. Bloomsbury Academic.
7. Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51–58.
8. Galeotti, M. (2014). The 'Gerasimov Doctrine' and Russian non-linear war. *In Moscow's Shadows*. https://inmoscowsshadows.wordpress.com/
9. Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. *Potomac Institute for Policy Studies*.
10. Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & Francois, C. (2018). The IRA, social media and political polarization in the United States. *Computational Propaganda Project*. Oxford University.
11. Meta. (2022). *Adversarial Threat Report*. https://about.fb.com/news/
12. Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic Narratives: Communication Power and the New World Order*. Routledge.
13. NATO. (2022). *Strategic Concept 2022*. https://www.nato.int/strategic-concept/
14. Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation.
15. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber.
16. Shambaugh, D. (2020). *China and the World*. Oxford University Press.
17. Suoninen, A. (2020). *Media literacy education in Finland*. Finnish National Agency for Education.
18. Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework*. Council of Europe.
19. Zhao, S. (2020). Rhetoric of "Wolf Warrior Diplomacy": China's changing narrative. *Journal of Chinese Political Science, 25*(3), 497–518.
20. Galeotti, M. (2016). *Hybrid war or Gibridnaya Voina? Getting Russia's non-linear military challenge right.* Mayak Intelligence.
21. Mueller, R. S. (2019). *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. U.S. Department of Justice.
22. Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation.
23. Pomerantsev, P., & Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Institute of Modern Russia.
24. Callahan, W. A. (2015). *China dreams: 20 visions of the future*. Oxford University Press.

25. Kania, E. B. (2016). *The PLA's Three Warfares: Political and Psychological Warfare in Chinese Military Strategy*. Jamestown Foundation.
26. Mazarr, M. J., Casey, A., Demus, A., Frederick, B., & Matthews, L. (2019). *Hostile Social Manipulation: Present Realities and Emerging Trends*. RAND Corporation.
27. Poling, G. (2020). *Illuminating the South China Sea's Dark Fishing Fleets*. Center for Strategic and International Studies.
28. Sacks, D. (2022). *China's Gray Zone Tactics in the Taiwan Strait*. Council on Foreign Relations.
29. Thornton, P. M. (2020). *Crisis and Control: China's Response to the COVID-19 Pandemic*. The China Quarterly, 246, 342–362.
30. Alfoneh, A. (2010). *Iran Unveiled: How the Revolutionary Guards Is Transforming Iran from Theocracy into Military Dictatorship*. AEI Press.
31. Byman, D. (2005). *Deadly Connections: States That Sponsor Terrorism*. Cambridge University Press.
32. Fulton, W., Holliday, J., & Wyer, A. (2019). *Iranian Influence in the Levant, Iraq, and Afghanistan*. American Enterprise Institute.
33. Levitt, M. (2013). *Hezbollah: The Global Footprint of Lebanon's Party of God*. Georgetown University Press.
34. Zetter, K. (2019). *Iran's Hacker Army Is Getting More Aggressive*. Wired Magazine.

• Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics.* Oxford University Press.
• Fairclough, N. (1995). *Critical discourse analysis.* Longman.
• Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Potomac Institute.
• Mazarr, M. J. (2015). *Mastering the gray zone: Understanding a changing era of conflict.* US Army War College.
• Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic narratives: Communication power and the new world order.* Routledge.
• Nye, J. S. (2004). *Soft power: The means to success in world politics.* PublicAffairs.
• Pomerantsev, P. (2014). *The menace of unreality: How the Kremlin weaponizes information.* The Interpreter.
• Wendt, A. (1999). *Social theory of international politics.* Cambridge University Press.

• Brands, H. (2016). *Paradoxes of the gray zone.* U.S. Army War College.
• Freier, N. (2015). *Outplayed: Regaining strategic initiative in the gray zone.* U.S. Army War College.
• Galeotti, M. (2019). *Russian political war: Moving beyond the hybrid.* Routledge.

• Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy.* RAND Corporation.
• Berger, J. M. (2018). *Extremism.* MIT Press.
• Felbab-Brown, V. (2020). *Narco-terrorism and hybrid warfare.* Brookings Institution.
• Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Potomac Institute.
• Kilcullen, D. (2010). *Counterinsurgency.* Oxford University Press.

- Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla.* Oxford University Press.
- Marten, K. (2019). *Russia's use of semi-state security forces.* International Security, 44(3), 117–144.
- Rid, T. (2013). *Cyber war will not take place.* Oxford University Press.
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar.* Oxford University Press.
- Williams, P. (2016). *Criminals, militias, and insurgents in hybrid warfare.* Strategic Studies Institute.

- Hoffman, F. G. (2009). *Hybrid warfare and challenges.* JFQ, 52(1), 34-39.
- Pamment, J. (2020). *Strategic narratives in hybrid warfare.* Routledge.
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics.* Oxford University Press.

- Miskimmon, A., et al. (2017). *Forging the world: Strategic narratives and international relations.* University of Michigan Press.
- Pomerantsev, P. (2014). *The menace of unreality: How the Kremlin weaponizes information.* The Interpreter.
- Wodak, R., & Meyer, M. (2016). *Methods of critical discourse studies* (3rd ed.). Sage.**)**

- Katzenstein, P. J. (1996). *The culture of national security: Norms and identity in world politics.* Columbia University Press.

- Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic narratives: Communication power and the new world order.* Routledge.

- Nye, J. S. (2004). *Soft power: The means to success in world politics.* PublicAffairs.

- Nye, J. S. (2011). *The future of power.* PublicAffairs.