Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

James K. Wither, *Connections QJ* 22, no. 1 (2023): 7-27
https://doi.org/10.11610/Connections.22.1.02

Research Article

Hybrid Warfare Revisited: A Battle of 'Buzzwords'

James K. Wither

George C. Marshall European Center for Security Studies,
https://www.marshallcenter.org

Abstract: Hybrid warfare is the most common term used by commentators to describe the complexity and multifaceted character of contemporary warfare. Hybrid warfare refers to coercive methods of strategic competition that take place below the threshold of conventional military conflict and is usually applied to the blend of military and non-military methods of warfare employed by the West's principal adversaries, Russia and China. The term hybrid warfare has evolved from an essentially military concept to one that potentially embraces all the instruments of state power. Hybrid warfare remains an ill-defined and contested term, and there are many other buzzwords, such as irregular warfare, hybrid threats, and gray zone aggression, that are used to describe the same phenomenon. This article examines the evolution of thinking on hybrid warfare and these related concepts. It highlights the challenges that scholars and practitioners have faced in trying to define and apply these terms in the policy environment in a manner that promotes common understanding and strategic coherence.

Keywords: warfare, strategic competition, NATO, Russia, China, United States.

Introduction

Until the Russian Federation's seizure of Crimea in March 2014, the subject of hybrid warfare was largely of interest only to military analysts. Subsequently, the term entered the wider security policy domain in the West, and all manner of hostile Russian activities were characterized as hybrid warfare. Increasingly, "hybrid" has also been used to describe operations by China in the South China Sea, Iranian proxy warfare, and North Korea's machinations on the Korean peninsula. In the process, hybrid warfare evolved from an essentially military concept to

one that potentially embraced all the instruments of state power. The topic has also generated a significant quantity of academic literature and policy papers over the years. But hybrid warfare remains an ill-defined and contested term, being often used as a catch-all to characterize contemporary war. The status of the term hybrid warfare reflects the continuing challenge of capturing the complexity of conflict in the 21st century, a phenomenon that involves a multiplicity of actors and blurs the distinctions between different lethal and non-lethal forms of warfare and even between traditional notions of war and peace.

This article updates and develops the author's earlier *Connections* 2016 piece, "Making Sense of Hybrid Warfare." [1] It offers further analysis on the evolution of thinking on the subject, particularly in the context of strategic competition. It also examines related concepts that academics, practitioners, and commentators frequently use to describe the character of contemporary warfare. These notably include irregular warfare, hybrid threats, and gray zone aggression, although many other terms exist. To add non-Western perspectives, the article contains synopses of Russian and Chinese approaches to hybrid warfare. The final section offers preliminary observations on the character of the war in Ukraine. Like its predecessor, this article tries to "make sense" of the current terminology being used to describe the character of contemporary warfare and the extent to which the term hybrid warfare and related concepts assist our understanding.

There are multiple definitions of hybrid warfare. However, the author favors the one proposed by General Ben Hodges, former commander of the U.S. Army in Europe. It offers an appropriate blend of earlier and post-2014 uses of the term and retains the coercive foundation of the concept:

> Hybrid warfare is the blending of conventional warfare, irregular warfare, and the use of other capabilities such as cyber, disinformation, money, and corruption in order to achieve a political outcome that is always backed up by the threat or the use of conventional weapons.[2]

The Origins of the Hybrid Warfare Concept

In 1999, eminent strategist Colin Gray stated that "wars can be waged between conventional regular armies, between regulars and irregulars, and between irregular opponents." [3] Gray's thinking reflected the common, traditional Western approach that defined warfare as large-scale, organized violence and made a clear distinction between war and peace. Perspectives started to change in the

---

1 James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, http://dx.doi.org/10.11610/Connections.15.2.06.

2 Ben Hodges, "Lt-Gen Ben Hodges on the Future of Hybrid Warfare," *CEPA*, April 8, 2021, accessed October 24, 2022, https://cepa.org/article/lt-gen-ben-hodges-on-the-future-of-hybrid-warfare/.

3 Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 159.

2000s as a result of the armed conflicts that followed "9/11." By 2006, Gray conceded that the "The convenient binary distinction between regular and irregular warfare is much less clear in practice than it is conceptually … when regular forces adopt an irregular style of war, and when irregular warriors shift back and forth between open and guerrilla warfare, the distinction can disappear." [4] Along with terms such as asymmetrical, irregular, and non-conventional warfare, hybrid became a common way to describe the changing character, if not nature, of warfare. Before 2014, military specialists considered the brief war between Israel and Hezbollah in 2006 as the conflict that most fitted contemporary definitions of hybrid war. Hezbollah surprised the Israel Defence Forces with its sophisticated combination of guerrilla and conventional military tactics and an effective strategic communication campaign. Definitions of hybrid warfare at the time emphasized the blending of conventional and irregular approaches across the full spectrum of armed conflict. The most influential contemporary definition was produced by Frank Hoffman:

> … different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of non-state actors.[5]

A mix of state and non-state military forces and the use of propaganda had been a feature of wars since ancient times. Hybrid warfare, as defined in the 2000s, was hardly a new phenomenon.[6] A report by the U.S. Government Accountability Office in 2010 concluded that "hybrid warfare was not a new form of warfare." [7] However, the integration of conventional and irregular methods of warfare arguably distinguished contemporary hybrid wars from their historical forms. Traditionally, conventional and irregular operations, such as operations by partisans and regular forces on the Eastern Front in the Second World War, took place concurrently but separately. Operations by irregular fighters were also normally secondary to campaigns by conventional military forces.

Analysts also used the term asymmetrical warfare to reflect efforts by state and non-state opponents of the United States to find ways to advance their strategic objectives without confronting America's conventional military power.

---

4 Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Orion Books, 2006), 199.

5 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, December 2007), 8, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

6 For a detailed analysis, see Peter R. Mansoor, "Hybrid War in History," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012).

7 Loretta Sanchez, Jeff Miller, and Adam Smith, "Hybrid Warfare," GAO-10-1036R (Washington, DC: United States Government Accountability Office, September 2010), accessed October 24, 2022, https://www.gao.gov/products/gao-10-1036r.

"Unrestricted Warfare," published by two People's Liberation Army (PLA) colonels in 1999, offered a blueprint for asymmetrical warfare against the United States. Among the book's proposals were non-kinetic methods of warfare that later became part of the hybrid playbook, such as media disinformation, economic coercion, and computer hacking.[8] As targeting an opponent's vulnerabilities rather than playing to their strengths is simply a smart strategy, there was skepticism about the usefulness of the term. Strategist Hew Strachan, for example, complained that asymmetrical warfare was being applied too loosely to every form of armed conflict that was not a conventional interstate war.[9] The theory of Fourth Generation Warfare also featured in contemporary debate.[10] A prescient element of this concept was the role that emerging technology could play in the cognitive sphere of future wars, when networked media and the Internet could be used to shape policymakers and public opinion in a targeted state to undermine its will to fight. Mark Galeotti later described this form of non-kinetic warfare as "a war on governance" that manipulated public grievances and mistrust, societal faultlines, and disputed government legitimacy.[11] Like much else discussed in this article, there were Cold War historical precedents for such a strategy. And Chinese philosopher Sun Tzu had discussed the potential of subversion to shape the battlespace as long ago as the fifth century BC. His treatise "The Art of War" contained the famous aphorism "subjugating the enemy's army without fighting is the true pinnacle of excellence." [12] This remains a fundamental objective of hybrid warfare.

Hybrid Warfare in Ukraine 2014

Russia's campaign in Ukraine in 2014 was a major catalyst for change in Western thinking and triggered a surge of analysis on the implications for Western security.[13] Scholars and security analysts labeled Russian strategy and tactics "hybrid warfare," although some queried the novelty of the concept.[14]

---

8 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), accessed November 5, 2022, https://www.ooda loop.com/documents/unrestricted.pdf.

9 See for example Hew Strachan, *The Direction of War: Contemporary Strategy in Historical Perspective* (Cambridge: Cambridge University Press, December 2013), 82.

10 See for example Tim Benbow, "Talking 'Bout Our Generation? Assessing the Concept of Fourth Generation Warfare," *Comparative Strategy* 27, no. 2 (2008): 148-163, https://doi.org/10.1080/01495930801944685.

11 Interview by Octavian Manea with Dr. Mark Galeotti, "Hybrid War as a War on Governance," *Small Wars Journal*, August 19, 2015, accessed October 24, 2022, https://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance.

12 Sun Tzu, *The Art of War*, Translated by Samuel B. Griffith (Oxford: Oxford University Press, 1971), 41, 77.

13 For sources see Wither, "Making Sense of Hybrid Warfare."

14 See for example Geraint Hughes, "Little Green Men and Red Armies: Why Russian 'Hybrid War' Is Nothing New," Research Blog, *Defence in Depth*, King's College London, March 14, 2016, https://defenceindepth.co/2016/03/14/little-green-men-and-red-

In Crimea, Russia mounted a covert operation using locally stationed troops, special operations forces (SOF), and proxies. Concurrent military maneuvers masked the operation in Crimea, and Russian troops and proxies rapidly seized control in an essentially bloodless campaign.[15] Crimea was a successful military operation, but it was the use of supporting non-kinetic methods of warfare that attracted the most interest from observers and led to the operation being labeled "hybrid."[16] Russia's tactics included an aggressive disinformation campaign that portrayed the new government in Kyiv as a fascist junta, electronic warfare attacks on Ukrainian security services' communications, the sponsorship of civil unrest, economic coercion by Gazprom, and the use of proxy forces. Russia's strategic disinformation campaign also successfully manipulated Ukrainian and Western perceptions, fostered confusion and distrust, and crippled effective crisis decision-making. However, given Ukraine's particular vulnerabilities in 2014, the wider applicability of Russia's tactics was exaggerated. In the case of later operations in Eastern Ukraine, it soon became apparent that Russia's overall campaign was characterized by a series of largely improvised approaches rather than a coherent overarching strategy.[17]

Discussion of hybrid warfare stretched the concept further than earlier definitions, explicitly emphasizing non-military approaches that focused on psychological, informational, and cyber operations conducted below the threshold of what traditionally constituted warfare. The 2015 Military Balance, for example, defined hybrid warfare as:

> the use of military and non-military tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure.[18]

---

armies-why-russian-hybrid-war-is-not-new/; and Bettina Renz, "Russia and 'Hybrid Warfare'," *Comparative Politics* 22, no. 3 (2016): 283-300, https://doi.org/10.1080/13569775.2016.1201316.

[15] Michael Kofman et al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine," Research Report RR-1498-A (Santa Monica, CA: RAND Corporation, 2017), xi, accessed October 20, 2022, https://doi.org/10.7249/RR1498.

[16] See for example: Ralph D. Thiele, "Crisis in Ukraine – The Emergence of Hybrid Warfare," ISPSW Strategy Series, May 2015, accessed October 20, 2022, www.files.ethz.ch/isn/190792/347_Thiele_RINSA.pdf; and Stephen Blank, "Russia, Hybrid War and the Evolution of Europe," *Second Line of Defense*, February 14, 2015, https://sldinfo.com/2015/02/russia-hybrid-war-and-the-evolution-of-europe/.

[17] Michael Kofman and Matthew Rojansky, "A Closer Look at Russia's 'Hybrid War'," *Kennan Cable*, no. 7 (Wilson Center, April 2015), 5, https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.

[18] "Editor's Introduction: Complex Crises Call for Adaptable and Durable Capabilities," *The Military Balance* 115, no. 1 (2015), 5, https://doi.org/10.1080/04597222.2015.996334.

Such descriptions of hybrid warfare went beyond Hoffman's military-focused definition to one that embraced the wider strategic threat environment to include many elements of typical inter-state strategic competition. Hoffman himself was critical of these broader uses of the term and reaffirmed his opinion that hybrid warfare should be distinguished from non-violent forms of conflict.[19]

Russian Hybrid Warfare

Russian operations in Ukraine significantly influenced the emerging Western concept of hybrid warfare. However, much initial thinking was based on a misinterpretation of the work of Russian military analysts, as the Russian concept of hybridity in warfare differs significantly from that in the West.

Western misconception began with an article by the Russian Chief of the General Staff, General Valery Gerasimov, in 2013. His analysis of modern warfare appeared to offer a blueprint for the subsequent Russian operations in Ukraine. Gerasimov described contemporary warfare as "blurring the lines between the states of war and peace" and involving:

> the broad use of political, economic, informational, humanitarian and other non-military means, supplemented by civil disorder among the local population and concealed armed forces.[20]

He claimed that non-lethal approaches might prove more effective than military force because they could create social upheaval and promote a climate of collapse. Gerasimov was not the only Russian military analyst to put an operational emphasis on information and psychological warfare,[21] but it was primarily his thinking that led to speculation that Russia had embarked on a new strategy characterized by a shift from military force towards non-lethal methods of warfare. However, from Gerasimov's perspective, contemporary hybrid warfare (*gibridnaya voyna*) was not invented in Russia but rather represented a Western stratagem employed to destabilize states like Russia that stood in the way of U.S. dominance.[22] Even events such as the "Color Revolutions" and the "Arab Spring"

---

[19] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (2018), 40, https://cco.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf.

[20] Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Kurier*, February 27, 2013, available in English in Mark Galeotti, "The Gerasimov Doctrine and Russian Non-Linear War," *In Moscow's Shadows Blog*, July 6, 2014, accessed October 24, 2022, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

[21] See, for example, Col. S.G. Chekinov and Lt. Gen. S.A. Bogdanov, "The Nature and Content of a New-Generation War," *Voyennaya Mysl'* (*Military Thought*), no. 10 (2013), 13, https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf.

[22] See, for example, Ofer Fridman, "Hybrid Warfare or Gibridnaya Voyna? Similar, But Different," *The RUSI Journal* 162, no. 1 (2017): 42-49, https://doi.org/10.1080/03071847.2016.1253370; and Mason Clark, "Russian Hybrid Warfare," *Military Learning*

were viewed as hybrid forms of warfare employed to advance American interests.

In 2020, a report from the U.S. Institute for the Study of War criticized the tendency to view Russian approaches to hybridity as conducted below the level of conventional war. The report described this viewpoint as "dangerously wrong" as Russia included a considerable conventional component in its theory and practice of hybrid war.[23] In later statements, Gerasimov himself appeared to clarify his thinking, emphasizing that the effective application of non-military measures in operations ultimately relied on military force.[24] A recent article on Russia's "special military operation" in Ukraine provides further insight into Russian doctrine. The authors argue that Russian military analysts viewed this action, at least as initially conceived, as the use of conventional military force to achieve specific military-political objectives below the threshold of war.[25]

Mark Galeotti maintains that there are two distinct forms of Russian non-linear or hybrid war. One strand employs non-kinetic tools such as information operations and subversion intended to demoralize and divide Western states and their partners, in effect, a modernized version of the Soviet Union's Cold War concept of "Active Measures." The other involves tactics to undermine an opponent's legitimacy, will, and capacity to resist prior to violent intervention, including the use of military force, a concept more akin to the hybrid military-political war against Ukraine.[26]

Hybrid Threats

Academic misgivings about terminology did not prevent NATO and the European Union (EU) from embracing the term hybrid warfare, or more particularly, hybrid threats, to classify what was viewed as an emerging, systemic security challenge to democratic states after 2014. Although the terms hybrid warfare and hybrid

and the Future of War Series (Washington, DC: Institute for the Study of War, September 2020), 16-17, https://www.understandingwar.org/report/russian-hybrid-warfare.

[23] Clark, "Russian Hybrid Warfare," 8. See also Keir Giles, "'Hybrid Warfare' and Russia's Ground Forces," NIDS International Symposium "A New Strategic Environment and Roles of Ground Forces," January 30, 2019, pp. 79-92, http://www.nids.mod.go.jp/english/event/international_symposium/pdf/2018/e-05.pdf.

[24] Michael Kofman et al., "Russian Military Strategy: Core Tenets and Operational Concepts," *Center for Naval Analyses*, October 2021, 27, accessed November 21, 2022, www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts.

[25] Roger N. McDermott and Charles K. Bartles, "Defining the 'Special Military Operation'," Article Review, Russian Studies Series, 5/22, NATO Defense College, accessed October 25, 2022, https://www.ndc.nato.int/research/research.php?icode=777.

[26] Mark Galeotti, "(Mis)Understanding Russia's 'Two Hybrid Wars'," *Eurozine*, November 29, 2018, accessed October 25, 2022, https://www.eurozine.com/misunderstanding-russias-two-hybrid-wars/.

threats are frequently used synonymously by European analysts,[27] policy documents normally refer to hybrid "threats" rather than hybrid "warfare." Overall, there has been insufficient effort to differentiate between the two terms, although Sean Monaghan has made perhaps the most definitive and useful distinction:

> Hybrid threats combine a wide range of non-violent means to target vulnerabilities across the whole of society to undermine the functioning, unity, or will of their targets, while degrading and subverting the status quo. This kind of strategy is used by revisionist actors to gradually achieve their aims without triggering decisive responses, including armed responses.
>
> Hybrid warfare is the challenge presented by the increasing complexity of armed conflict, where adversaries may combine types of warfare plus non-military means to neutralise conventional military power.[28]

Elisabeth Braw has made a similar distinction. She suggests that the term hybrid warfare applies when conventional military force is employed alongside non-military tools, while broader campaigns to weaken a country's resilience through a range of largely non-kinetic means are better described as hybrid threats.[29]

NATO's strategic thinking has evolved from an earlier focus on hybrid as a mix of regular and irregular forms of warfare to a more comprehensive approach that includes non-military challenges. These threats were discussed prominently in NATO's "Reflection Process" report in 2020, [30] and their significance is evident from the Alliance's most recent definition of hybrid threats:

> Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are

---

[27] See, for example, Mikael Weissmann, "Hybrid Warfare and Hybrid Threats Today and Tomorrow: Towards an Analytical Framework," *Journal on Baltic Security* 5, no. 1 (2019): 17-26, https://journalonbalticsecurity.com/journal/JOBS/article/40/info; and Niklas Nilsson et al., "Security Challenges in the Gray Zone: Hybrid Threats and Hybrid Warfare," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, Bloomsbury Collections, ed. Mikael Weissmann, Niklas Nilsson, Björn Palmertz, and Per Thunholm (London: Bloomsbury Publishing, 2021).

[28] Sean Monaghan, "Countering Hybrid Warfare Project," Information Note, MCDC Countering Hybrid Warfare Project, March 2019, 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf.

[29] Elisabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression* (Washington, DC: American Enterprise Institute, March 2022), 9. Frank Hoffman makes a similar distinction – see Hoffman, "Examining Complex Forms of Conflict," 39.

[30] NATO, "NATO 2030: United for a New Era," Analysis and Recommedations of the Reflection Group Appointed by the NATO Secretary General, November 25, 2020, 45-46, accessed November 8, 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations.[31]

Both NATO and the EU recognize that hybrid threats involve the full range of tools of national power. However, institutional approaches differ on the range of threats and the emphasis to be placed on non-kinetic challenges. A Hybrid COE report, for example, treats hybrid threats as a political concept, defined as: "… unacceptable foreign interference in sovereign states' internal affairs and space." [32] The EU External Action Service and the EU's Joint Framework for Hybrid Threats use similar definitions. These perspectives illustrate that the EU's hybridity threat focus is on coercive statecraft rather than on violent conflict.[33] Arguably, this suggests an understandable reluctance to militarize activities that are a normal feature of strategic competition in international politics. Some commentators have expressed concern that the liberal use of the term "warfare" may broaden the range of activities considered belligerent and potentially lower the threshold for escalation.[34]

Differences in perspective are inevitable, given the nature of bureaucratic politics and the complexity of the issues involved. However, they complicate the development of a common understanding by policymakers of contemporary security challenges and efforts to build the necessary resilience to address them. To date, there remains no unambiguous definition of hybrid warfare/threats and the meaning of the terms continues to evolve.[35] NATO's latest strategic concept does not mention the term hybrid warfare, nor does it offer a definition of hybrid threats, though the description of these threats suggests that the Alliance now leans towards the use of hybrid to denote primarily non-kinetic challenges.[36]

---

[31] Quoted in "NATO's Response to Hybrid Threats," *NATO*, accessed November 4, 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm.

[32] European Commission / Hybrid COE, *Landscape of Hybrid Threats: A Conceptual Model* (Luxembourg: Publications Office of the EU, 2021), 10, accessed November 6, 2022, https://op.europa.eu/en/publication-detail/-/publication/b534e5b3-7268-11eb-9ac9-01aa75ed71a1.

[33] Dick Zandee, Sico van der Meer, and Adája Stoetman, "Hybrid Threats: Searching for a Definition," in *Counterig Hybrid Threats: Steps for Improving EU-NATO Cooperation*, Clingendael Report (The Hague, The Netherlands: The Clingendael Institute, October 2021), pp. 6-29, https://www.clingendael.org/pub/2021/countering-hybrid-threats/2-hybrid-threats-searching-for-a-definition/.

[34] See, for example, John Raine, "War or Peace? Understanding the Grey Zone," *IISS*, April 3, 2019, accessed November 9, 2022, https://www.iiss.org/blogs/analysis/2019/04/understanding-the-grey-zone.

[35] Zandee, van der Meer, and Stoetman, "Hybrid Threats: Searching for a Definition," 9; and Ewan Lawson, "We Need to Talk About Hybrid," *The RUSI Journal* 166, no. 3 (2021): 58-66, 59-61, https://doi.org/10.1080/03071847.2021.1950330.

[36] "NATO 2022 Strategic Concept" (NATO, June 2022), 3, accessed November 4, 2022, https://www.nato.int/strategic-concept/index.html.

Irregular Warfare

American scholars have supplied much of the literature on hybrid warfare, and officials have frequently used the term. However, irregular warfare is the term often used in the U.S. to indicate what is described above as hybrid threats and warfare, as well as conflict in the gray zone.[37] Analysts recognize that the range of different terms used to explain essentially similar phenomena does not help the overall quest for definitional clarity and understanding. Writing in 2016, Antulio Echeverria expressed concern that the mix of terminology created "a wealth of confusion that has clouded the thinking of policymakers and impaired the development of sound counter-strategies."[38] Recently, David Ucko and Thomas Marks claimed that the range of "jargon" illustrated the U.S.'s continuing difficulty in comprehending irregular warfare, arguing that: "The terminology belies a struggle to overcome entrenched assumptions about war – a confusion that generates cognitive friction with implications for strategy.[39] The U.S. Joint Staff's curriculum guide for irregular warfare also acknowledges that a mix of similar concepts and confusion over terminology can act as an obstacle to clarity when teaching the concept to military students.[40]

Prior to the 2018 U.S. National Defense Strategy (NDS), irregular warfare focused primarily on the challenge posed by violent non-state adversaries. The term was defined in the Irregular Warfare Joint Operating Concept of 2010 as "…a violent struggle among state and non-state actors for legitimacy over the relevant populations."[41] The 2018 NDS officially downgraded terrorism and insurgency as national security priorities in favor of inter-state strategic competition. The Irregular Warfare Annex, released in 2020, announced a shift in priorities from fighting global extremist organizations to countering nation-state peer competitors. Irregular Warfare was redefined in this document as "a struggle

---

[37] See, for example, David H. Ucko and Thomas A. Marks, *Crafting Strategy for Irregular Warfare: A Framework for Analysis and Action*, Strategic Monograph, 2nd edition (Washington, D.C.: National Defense University Press, September 2022) https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3163915/crafting-strategy-for-irregular-warfare-a-framework-for-analysis-and-action-2nd/; and Seth G. Jones, "The Future of Competition: U.S. Adversaries and the Growth of Irregular Warfare," *CSIS*, February 4, 2021, accessed November 7, 2022, https://www.csis.org/analysis/future-competition-us-adversaries-and-growth-irregular-warfare.

[38] Antulio J. Echevarria, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy* (Carlisle, PA: US Army War College Press, April 2016), 1, https://press.armywarcollege.edu/monographs/425/.

[39] Ucko and Marks, *Crafting Strategy for Irregular Warfare*, 3.

[40] U.S. Joint Staff, "Curriculum Development Guide for Irregular Warfare," Office of Irregular Warfare and Competition, Directorate for Joint Force Development (J-7), June 3, 2022, 7.

[41] U.S. Department of Defense, "Irregular Warfare: Countering Irregular Threats," Joint Operating Concept, Version 2, May 17, 2010, 9, accessed November 7, 2021, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.

among state and non-state actors to influence populations and affect legitimacy." [42] The crucial focus on the competition for legitimacy remained, but the word "violent" was notably absent. Ucko and Marks have suggested that the new definition may indicate "a subtle but meaningful shift that looks likely to shape future doctrine." [43] But they also warn against demilitarizing the concept and losing sight of the essential character of irregular warfare regardless of how it is defined – the element of covert or overt coercion.[44] The term irregular competition has already been mooted as an alternative to irregular warfare,[45] which might assist cooperation with civilian agencies that view a concept described as "warfare" beyond their remit. Nevertheless, given America's traditional reliance on militarized responses to foreign policy challenges, such a change would likely prove challenging in practice.[46]

The 2022 U.S. NDS is dominated by a discussion of Integrated Deterrence, a full spectrum strategy to address the range of military and non-military threats confronting American security. But in terms of characterizing the threat, the strategy document makes the most frequent reference to hostile gray zone activities, defined in the NDS as "coercive approaches that may fall below perceived thresholds for U.S. military action." [47] In view of the discussion above, it is not clear whether "gray zone" or "irregular" warfare will provide the frame of reference to address strategic competition in the future, but definitional confusion seems set to continue.

Gray Zone Aggression

The Center for Strategic and International Studies (CSIS) defines gray zone challenges as follows:

---

[42] U.S. Department of Defense, "Summary of the Irregular Warfare Annex to the National Defense Strategy," 2020, 2, https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.

[43] Ucko and Marks, *Crafting Strategy for Irregular Warfare*, 10.

[44] Ucko and Marks, *Crafting Strategy for Irregular Warfare*, 10. See also David H. Ucko and Thomas A. Marks, "Redefining Irregular Warfare: Legitimacy, Coercion, and Power," *Modern War Institute*, October 18, 2022, accessed November 8, 2022, https://mwi.usma.edu/redefining-irregular-warfare-legitimacy-coercion-and-power/.

[45] See, for example, Jeremiah C. Lumbaca, "Irregular Competition: Conceptualizing a Whole-of-Government Approach for the United States to Indirectly Confront and Deter State and Nonstate Adversaries," *Military Review* (July-August 2022), accessed November 15, 2022, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2022/Lumbaca/.

[46] See, for example, Robert M. Gates, "The Overmilitarization of American Foreign Policy: The United States Must Recover the Full Range of Its Power," *Foreign Affairs* (July/August 2020), https://www.foreignaffairs.com/articles/united-states/2020-06-02/robert-gates-overmilitarization-american-foreign-policy.

[47] U.S. Department of Defense, "National Defense Strategy of the United States of America," 2022, 6, https://www.defense.gov/National-Defense-Strategy/.

> An effort or series of efforts intended to advance one's security objectives at the expense of a rival using means beyond those associated with routine statecraft and below means associated with direct military conflict between rivals. In engaging in a gray zone approach, an actor seeks to avoid crossing a threshold that results in open war.[48]

Like other terms identified in this article, "gray zone" is a loose and ill-defined concept. Gray zone has been used to represent a phase of a conflict, an operating environment, and a tactic. However, it is generally accepted that ambiguity is a defining characteristic of gray zone activities as they can be hard to recognize and attribute and are almost always denied by perpetrators. A primary challenge for policymakers is to decide what constitutes "routine statecraft" and "direct military conflict," as the boundaries of the gray zone are hard to delineate in practice.

After 2014, hybrid warfare was widely used to describe hostile activities that blurred the distinction between peace and war. However, Michael Mazarr was among the first to distinguish "gray zone strategies" from hybrid forms of warfare. Mazarr argued that hybrid warfare, as usually defined, referred to the use of violence to achieve political objectives and was therefore "closer to a variety of conventional warfare than a true alternative to it." [49] Contemporary gray zone strategies, on the other hand, employed traditional, non-lethal tools of rivalry and statecraft made more effective by new technologies. Mazarr likened gray zone activities to George Kennan's concept of Political Warfare, which envisaged measures short of war being employed in strategic competition with the Soviet Union.[50] Like Mazarr, Elisabeth Braw distinguishes between hybrid warfare, which involves "the persistent use of military force," and what she terms gray zone aggression, defined as "… hostile acts outside the realm of armed conflict to weaken a rival country, entity or alliance." [51]

Braw's examples of gray zone aggression include a range of activities, such as Chinese investment in cutting-edge technology companies, which she acknowledges is "far from traditional national security thinking." [52] Seth Jones also lists a range of Chinese activities, such as influence operations on university campuses and even attempts to censor Hollywood, that questionably qualify as national

---

[48] Melissa Dalton et al., "By Other Means – Part 2: U.S. Priorities in the Gray Zone," A Report of the CSIS International Security Program (Center for Strategic and International Studies/ Rowman & Littlefield, August 2019), 2, https://defense360.csis.org/by-other-means-part-ii-u-s-priorities-in-the-gray-zone/.

[49] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: USAWC Press, 2015), 44-46, accessed November 10, 2021, https://press.armywarcollege.edu/monographs/428/.

[50] Mazarr, *Mastering the Gray Zone*, 48-51.

[51] Braw, *The Defender's Dilemma*, 10-11.

[52] Braw, *The Defender's Dilemma*, 12.

security threats.[53] Malign business activities and coercive attempts to gain influence by foreign powers should certainly be an area of concern for targeted states. But there is a danger that including too broad a range of measures as examples of gray zone aggression strips the term of practical utility and makes it difficult for governments to prioritize the most urgent non-kinetic security challenges. A complicating factor is that malign gray zone activities are often legal, which means they do not necessarily trigger an appropriate response from security officials. China uses its official social media presence to assert its influence around the world and push specific narratives on sensitive issues such as human rights and COVID-19.[54] Whether this activity constitutes normal strategic communication, hostile gray zone aggression, or both is a matter of judgment.

Authoritarian adversaries of the West have capitalized on liberal democracies' media freedoms, open civil societies, and private sector economies, which make them particularly vulnerable to gray zone tactics. Russia employs a mixture of cyber operations, espionage, covert action, and disinformation against Western countries. Russian attempts to weaken its rivals have not changed since Soviet times, but advances in computing, information technology, and processing have greatly increased their reach and effectiveness. Mark Warner, Chair of the U.S. Senate's Intelligence Committee, observed that "social media has allowed Russia to supercharge its disinformation efforts ... where propaganda and fake news can spread like wildfire." [55] Russia's interference in the 2016 U.S. presidential election represents the highlight of its disinformation campaign against the West. Fabricated stories on social media, hacks of Democratic Party information systems, and the release of stolen files and emails created doubt and confusion and exacerbated societal divisions.

Russia's cyber operations have also become increasingly sophisticated, being tailored to specific objectives in targeted states. The NotPetya virus unleashed in 2017 was intended to cause maximum disruption as part of Russia's ongoing hybrid war against Ukraine. This attack injected malicious code into automated Ukrainian tax preparation software, which impacted operations by banks, hospitals, energy companies, airports, and government agencies. By contrast, the SolarWinds supply chain intrusion in the U.S. in 2020 was more typical of cyber operations against Western states. The purpose of the attack was espionage. The SolarWinds company was not the primary target. It was simply the means to gain access to U.S. government systems. A RAND study examining Russian gray zone

[53] Jones, "The Future of Competition."

[54] BBC Monitoring, "China's Public Diplomacy on Twitter and Facebook," 2021, 8, https://www.academia.edu/80483985/Chinas_public_diplomacy_on_Twitter_and_Facebook.

[55] "Return of Global Russia," Speech by Senator Mark Warner to the Carnegie Endowment for International Peace, March 1, 2018, accessed November 11, 2022, https://www.warner.senate.gov/public/index.cfm/blog?ID=F2851C9D-3E4A-4F85-A54E-92F1B747360C.

competition in Europe distinguished between "everyday" actions, namely propaganda, disinformation, and influence operations, and the direct threat or use of violence, such as the attempted coup in Montenegro in 2016.[56] This distinction is broadly similar to Galeotti's arguments above regarding the twin-track approaches of Russian hybrid warfare.

China's approach to gray zone aggression is less militarized than Russia's. As the world's leading trading nation, China has a more extensive range of non-kinetic tools to wield. The gray zone provides China with multiple opportunities to expand its power and influence through activities as varied as the construction and militarization of islets in the South China Sea, cyber hacks to steal scientific research from Western institutions, and predatory business practices.

Since 2003, China has adopted the "Three Warfares" (*san zhong* zhanfa) doctrine, which incorporates elements of *Unrestricted Warfare*, the Communist Party's revolutionary traditions, and Sun Tzu's *The Art of War*.[57] The first element of *psychological warfare* seeks to disrupt an opponent's leadership decision-making capacity by deception or intimidation. The frequent intrusions into Taiwan's Air Defense Identification Zone, for example, are intended to weaken the Taiwan government and people's resolve to resist China's demands. The second element, *legal warfare*, uses domestic law as the basis for China's claims in international law. China rejected the UN Convention on the Law of the Sea's ruling on its claims in the South China Sea, asserting its historical legal rights instead. The final element, *media warfare,* is employed to shape domestic and international public opinion in support of psychological and legal warfare. Consequently, China conducts a massive digital media operation to manipulate public opinion throughout South-East Asia. Like the Russian military, the People's Liberation Army regards information dominance as crucial to its military strategy. Three Warfares doctrine serves this larger strategic concept while avoiding escalation to conventional warfare.[58] It is perhaps the perfect example of a gray zone stratagem.

China is by no means the only state to employ economic coercion. For instance, the recent decision by the United States to impose export controls on

---

[56] Stacie L. Pettyjohn and Becca Wasser, "Competing in the Gray Zone: Russian Tactics and Western Responses," Research Report RR-2791-A (RAND Corporation, 2019), Chapter 4, https://doi.org/10.7249/RR2791.

[57] Doug Livermore, "China's Three Warfares in Theory and Practice in the South China Sea," *Georgetown Security Studies Review*, March 25, 2018, https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

[58] Livermore, "China's Three Warfares;" and David Knoll, Kevin Pollpeter, and Sam Plapinger, "China's Irregular Approach to Warfare: The Myth of a Purely Conventional Fight," *Modern War Institute*, April 27, 2021, accessed November 15, 2022, https://mwi.usma.edu/chinas-irregular-approach-to-war-the-myth-of-a-purely-conventional-future-fight/.

semiconductors and related manufacturing equipment to China has been described as an "economic war."[59] But economic coercion has become a particularly prominent instrument of Chinese foreign policy,[60] being used to punish states, such as Australia, that challenge its policies.[61] China's Belt and Road Initiative is more ambiguous. It offers positive inducements to governments that lack access to international funding while, at the same time, providing China with potential influence over their domestic politics and access to natural resources and strategic facilities. More than other areas of Chinese foreign policy, its economic activities blur the threshold between robust statecraft and gray zone aggression.

Gray Zone Warfare

Defining the threshold between gray zone aggression and direct military conflict presents both analytical and practical challenges, especially as coercive military activities are a regular feature of gray zone tactics. Prior to the invasion of Ukraine, Russia used military deployments and provocative exercises to coerce Ukraine and intimidate European states. China's Maritime Militias frequently employ forceful methods against foreign fishing boats to back Chinese territorial claims in the South China Sea. Military operations classified as "gray zone" are sometimes hard to distinguish from outright warfare. Some scholars have described Russian military operations in Eastern Ukraine and violent campaigns by jihadist groups in the Middle East and Africa as gray zone conflicts.[62] Although Iran's conventional forces are relatively weak, it has nevertheless successfully employed proxy forces in violent conflicts throughout the Middle East to advance its strategic interests. Iran has even been described as the "quintessential

[59] Eric Levitz, "Biden's New Cold War Against China Could Backfire," *Intelligencer*, November 14, 2022, https://nymag.com/intelligencer/2022/11/biden-economic-war-china-chips-semiconductors-export-controls.html.

[60] Bonnie Glaser, "How China Uses Economic Coercion to Silence Critics and Achieve Its Political Aims Globally," Testimony before the Congressional Executive Commission on China, December 7, 2021, accessed November 14, 2022, https://www.cecc.gov/events/hearings/how-china-uses-economic-coercion-to-silence-critics-and-achieve-its-political-aims.

[61] Ashley Townshend and Thomas Lonergan, "Australia Must Adopt Unorthodox Options to Disrupt China's Grey-Zone Threats," *The Guardian*, September 28, 2021, accessed November 13, 2022, https://www.theguardian.com/australia-news/commentisfree/2021/sep/28/australia-must-adopt-unorthodox-options-to-disrupt-chinas-grey-zone-threats.

[62] See for example Hoffman, "Examining Complex Forms of Conflict," 36; and David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone'," *War on the Rocks*, May 19, 2015, accessed November 10, 2022, https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/.

gray zone actor whose entire modus operandi is influenced by this particular way of war." [63]

During the Cold War, the superpowers sought to pursue their rivalry while avoiding a direct armed conflict that could have raised the risk of nuclear war. But plenty of wars occurred around the world during this period; many were exploited as proxy wars by the superpowers as they juggled to achieve strategic advantage. Proxy warfare has returned in the new era of strategic competition, although it is no longer just a binary-state activity. Proxy warfare has been defined as: "(armed conflicts) …in which belligerents use third parties as either a supplementary means of waging war, or as a substitute for the direct employment of their own armies." [64] The secretive and indirect use of state military and irregular forces, which nowadays can include private military companies, "hacktivists," and criminals, is a feature of the violent edge of the gray zone and belies attempts to define the "zone" only in terms of non-kinetic coercive measures.

The words "war" and "warfare" are routinely applied beyond their original, primary association with politically motivated, organized violence. Governments often use the word "war" when describing internal or external threats to their power. Terms such as economic warfare, cyber warfare, or lawfare complicate efforts to distinguish between war, conflict, and competition in international politics. The lack of consensus among Western analysts that coercive actions in the gray zone constitute warfare is not surprising, but the West's adversaries appear to have no such doubts. President Putin has declared on several occasions that Russia is in a civilizational war with the West, and Russia's political and military leadership regards non-kinetic tactics as an important element of warfare. China's "Three Warfares" strategy is intrinsically a form of warfare, and the PLA conducts gray zone operations that can be fully integrated into conventional military strategy and tactics. Iran wages a persistent asymmetrical war against its principal enemies, Israel and the United States. Several analysts subscribe to the view that gray zone aggression is a form of warfare, although none would suggest that a military response is always appropriate or necessary.[65] George Kennan arguably accepted this principle back in the 1940s when he referred to the

[63] Michael Eisenstadt, "Iran's Gray Zone Strategy: Cornerstone of Its Asymmetrical Way of War," *PRISM* 9, no. 2 (2021): 77-97, 78, accessed November 10, 2022, https://ndupress.ndu.edu/Journals/PRISM/PRISM-9-2/.

[64] Geraint Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics* (Eastbourne: Sussex Academic Press, 2012), 2.

[65] See, for example, Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2022), 18; Ucko and Marks, "Redefining Irregular Warfare;" Arsalan Bilal, "Hybrid Warfare – New Threats, Complexities and 'Trust' as the Antidote," *NATO Review*, November 30, 2021, accessed October 24, 2022, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html; and Raphael S. Cohen et al., "The Future of Warfare in 2030: Project Overview and Conclusions," Research Report RR-2849/1-AF (Santa Monica, CA: RAND Corporation, 2020),

containment strategy of Political Warfare as "the logical application of Clausewitz's doctrine in time of peace." [66] Some contemporary scholars have also invoked Clausewitz when discussing hybrid threats. Sean Monaghan, for instance, argues that hybrid aggression targets the government, the people, and the military – all three elements of Clausewitz's famous "trinity" on which governments depend to retain and wield power.[67]

A Hybrid Perspective on Russia's War in Ukraine

Many commentators assumed that the gray zone would remain the main arena for strategic competition.[68] Russia's attack on Ukraine in February 2022 has challenged this paradigm. Richard Hass, President of the Council of Foreign Relations, has described Russia's war in Ukraine in game-changing terms:

> Russia's aggression has upended many assumptions that influenced thinking about international relations in the post-Cold War era. It has ended the holiday from history in which wars between countries were rare. It has hollowed out the norm against countries' acquiring territory by force.[69]

It is too soon to tell whether Hass' assumptions are correct. But the war is likely to provide scholars and policymakers with plenty of material to analyze for years to come. Naturally, much discussion has focused on conventional warfighting and the possible use of nuclear weapons, but the conflict also continues to be viewed through the lens of hybrid warfare.[70] Russia has combined its conventional military operations with cyber, disinformation, and economic warfare campaigns intended to undermine the ability and will of the Ukrainian govern-

13-14, accessed November 15, 2022, https://www.rand.org/pubs/research_reports/RR2849z1.html.

66 George Kennan, "Policy Planning Staff Memorandum," May 1948, accessed November 15, 2022, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

67 Monaghan, "Countering Hybrid War Project," 3.

68 See, for example, Kevin Bilms, "Gray Is Here to Stay: Principles from the Interim National Security Strategic Guidance on Competing in the Gray Zone," *Modern War Institute*, March 25, 2021, accessed November 9, 2022, https://mwi.usma.edu/gray-is-here-to-stay-principles-from-the-interim-national-security-strategic-guidance-on-competing-in-the-gray-zone/.

69 Richard Haass, "The Dangerous Decade: A Foreign Policy for a World in Crisis," *Foreign Affairs* (September/October 2022), https://www.foreignaffairs.com/united-states/dangerous-decade-foreign-policy-world-crisis-richard-haass.

70 See, for example, Scott Jasper, "Can Russian Hybrid Warfare Win the Day in Ukraine?" *The National Interest*, October 7, 2022, accessed November 19, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/can-russian-hybrid-warfare-win-day; Manoj Joshi, "The Russia-Ukraine War: Ukraine's Resistance in the Face of Hybrid Warfare," *Observer Research Foundation*, June 6, 2022, accessed November 2, 2022, https://www.orfonline.org/expert-speak/ukraines-resistance-in-the-face-of-hybrid-warfare/.

ment and people to resist. Beyond Ukraine, Russia has intensified its disinformation and propaganda efforts in Africa, the Middle East, and Latin America, achieving some success in deflecting blame for the war. Cyberattacks have continued, notably against Lithuania and Estonia during the summer of 2022, and Putin has used the threat of nuclear escalation as psychological warfare to pressure the West into restricting the weaponry it sends to Ukraine. The degradation of Russian military forces in combat has already prompted speculation that Russia's leaders will put even greater emphasis on hybrid forms of warfare in the future.[71]

There is no shooting war between Russia and NATO, but both are actively engaged in hostile operations below this threshold. Economic sanctions are the West's principal gray zone weapon, and the U.S. and its allies imposed unprecedentedly severe sanctions against Russia after the start of the war. These were described by *The Economist* as "high risk economic warfare"[72] and by Russian Foreign Minister, Sergey Lavrov, as a "total hybrid war" against his country.[73] Russia has responded to sanctions by exploiting its energy leverage over Europe. Gas supplies have been dramatically reduced with the apparent aim of creating painful energy rationing during winter that will persuade European states to pressure Ukraine to negotiate.[74] Acts of sabotage, widely attributed to Russia but not proven, on the Nord Stream pipelines in September have demonstrated the vulnerability of critical infrastructure and raised the stakes for the West.[75] Russia has mounted surveillance of oil and gas installations and transatlantic, undersea communications cables; cables close to Svalbard and the Shetland Islands were recently severed in suspicious circumstances. U.S. cyber-security officials also claim that Russia has pre-positioned cyber assets ready for major attacks against Western critical infrastructure targets.[76] Transatlantic cables and

---

[71] Andrea Kendall-Taylor and Michael Kofman, "Russia's Dangerous Decline: The Kremlin Won't Go Down Without a Fight," *Foreign Affairs* (November/December 2022), https://www.foreignaffairs.com/ukraine/russia-dangerous-decline; Ucko and Marks, "Redefining Irregular Warfare."

[72] "A New Age of Economic Conflict," *The Economist*, March 2, 2022, https://www.economist.com/leaders/a-new-age-of-economic-conflict/21807968.

[73] Cameron Jenkins, "Kremlin Official Says West Has Declared 'Total War' on Russia," *The Hill*, March 25, 2022, accessed November 16, 2022, https://thehill.com/policy/international/russia/599722-lavrov-says-west-has-declared-total-war-on-russia/.

[74] Peter Clement, "Putin's Risk Spiral: The Logic of Escalation in an Unraveling War," *Foreign Affairs*, October 26, 2022, https://www.foreignaffairs.com/ukraine/putin-risk-spiral-logic-of-escalation-in-war.

[75] Melissa Eddy, "Pipeline Breaks Look Deliberate, Europeans Say, Exposing Vulnerability," *The New York Times*, September 28, 2022, https://www.nytimes.com/2022/09/27/world/europe/pipeline-leak-russia-nord-stream.html; Richard Milne, "Damaged Baltic Sea Pipelines Put Western Powers on Alert for Sabotage," *Financial Times*, September 29, 2022.

[76] Marcus Willett, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no. 5 (October-November 2022): 7-26, quote on p. 21, https://doi.org/10.1080/00396338.2022.2126193.

other vital infrastructure represent strategic vulnerabilities should Putin choose to escalate, although a deliberate strike against them would risk crossing the threshold to open war with NATO. Writing in *The Observer*, Simon Tisdall describes Russia's activities as "non-military hybrid warfare" with the intention "…to harm, confuse, frighten, enfeeble and divide target states while maintaining plausible deniability." [77]

Many analysts have categorized the conflict as a proxy war.[78] As discussed above, proxy warfare has characterized many recent armed conflicts where states seek to influence the outcome of a war in another country without direct military involvement. America and its allies have supplied billions of dollars worth of military and economic aid, including weapons, training, intelligence, and cybersecurity expertise in support of Ukraine's war effort. The United States has officially denied it is involved in a proxy war, but as Secretary of Defense, Lloyd Austin, acknowledged in April 2022, the U.S. has broader goals than simply assisting Ukraine to defend itself. According to Austin, "we do want to make it harder for Russia to threaten its neighbors, and leave them less able to do that." [79] As during Cold War proxy wars, both Biden and Putin have so far abided by the often tacit "invisible rules" intended to prevent dangerous escalation to a direct military conflict.[80]

---

[77] Simon Tisdall, "Unseen and Underhand: Putin's Hidden Hybrid War Is Trying to Break Europe's Heart," *The Observer*, October 23, 2022, https://www.theguardian.com/commentisfree/2022/oct/23/unseen-and-underhand-putins-hidden-hybrid-war-is-trying-to-break-europes-heart.

[78] Eliot A. Cohen, "America's Hesitation Is Heartbreaking," *The Atlantic*, March 14, 2022, www.theatlantic.com/ideas/archive/2022/03/ukraine-united-states-nato/627052/; Sam Winter-Levy, "A Proxy War in Ukraine Is the Worst Possible Outcome – Except for All the Others," *War on the Rocks*, March 28, 2022, accessed November 21, 2022, https://warontherocks.com/2022/03/a-proxy-war-in-ukraine-is-the-worst-possible-outcome-except-for-all-the-others/; Hals Brand, "Russia Is Right: The U.S. Is Waging a Proxy War in Ukraine," *The Washington Post*, May 10, 2022, www.washingtonpost.com/business/russia-is-right-the-us-is-waging-aproxy-war-in-ukraine/2022/05/10/2c8058a4-d051-11ec-886b-df76183d233f_story.html; Dov S. Zakheim, "Russia's Invasion of Ukraine Has Sparked a Proxy World War," *The Hill*, November 18, 2022, accessed November 21, 2022, https://thehill.com/opinion/national-security/3739744-russias-invasion-of-ukraine-has-sparked-a-proxy-world-war/.

[79] U.S. Department of Defense, "Secretary of Defense Lloyd J. Austin III Holds a News Conference Following Ukraine Defense Consultative Group Meeting, Ramstein Air Base, Germany," Transcript, April 26, 2022, accessed November 21, 2022, https://www.defense.gov/News/Transcripts/Transcript/Article/3011263/secretary-of-defense-lloyd-j-austin-iii-holds-a-news-conference-following-ukrai/.

[80] Liana Fix and Michael Kimmage, "What If the War in Ukraine Spins Out of Control? How to Prepare for Unintended Escalation," *Foreign Affairs*, July 19, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-07-18/what-if-war-in-ukraine-spins-out-control.

Conclusion

The discussion above illustrates that policymakers and scholars of warfare are confronted by a variety of different, but overlapping terms, often used synonymously to describe similar phenomena. The term hybrid warfare has been rightly criticized for being ill-defined, ahistorical, and applied to elements of inter-state strategic competition that can questionably be described as warfare as traditionally understood. Alternative terms discussed here, such as irregular warfare, hybrid threats, and gray zone aggression, have been subject to similar criticism but, like hybrid warfare, are also commonly employed by analysts and practitioners. The plethora of buzzwords can create confusion and misunderstanding, which may negatively impact the development of coordinated, focused, and effective responses to the range of threats posed by the West's authoritarian adversaries. While establishing common terminology and definition to characterize contemporary warfare would be helpful, it should be obvious from the discussion above that this would probably prove impossible in practice.

Although it remains a disputed term in academic discourse, hybrid warfare continues to be employed by practitioners and commentators as an established term to describe the blended character of contemporary warfare. Despite valid arguments about overly broad and ambiguous terminology, the debate on hybrid warfare and other related concepts has provided a useful framework to challenge the traditional, Western binary distinctions between peace and war and conventional and irregular warfare. Analysis of these terms has provided crucial insights into how modern state and non-state actors exploit and integrate kinetic and non-kinetic methods of warfare to pursue their strategic objectives. The discussion has helped develop greater awareness of the coercive behaviors employed by adversaries that exploit the West's vulnerabilities in the competitive space between statecraft and open warfare. The effectiveness of these tactics has been amplified by developments in cyber, informational, and economic methods of warfare that have arguably permanently altered the notion of what constitutes force in international politics. Most significantly, the concept of hybrid warfare has awakened Western states to the need for comprehensive approaches to national security that go beyond traditional defense institutions to embrace both military and civilian governmental agencies, civil society, and private sector organizations.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 22, 2023, is supported by the United States government.

About the Author

James K. Wither is a retired British Army Officer and former researcher in contemporary warfare at the Imperial War Museum in London. He also served as a Professor of National Security Studies at the George C. Marshall European Center for Security Studies, where he specialized in irregular warfare and counterterrorism research and teaching.
E-mail: jkw53a@gmail.com