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

Heather S. Gregg, *Connections QJ* 23, no. 2 (2024): 159-171
https://doi.org/10.11610/Connections.23.2.01

Research Article

Hybrid Threats and Strategic Competition

Heather S. Gregg

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

Abstract: Strategic competition is not new, nor is the use of activities short of warfare by governments to shape the international system in their favor. However, the ability of state and non-state actors to directly influence populations through a range of rapid and non-attributable actions is different from previous iterations of strategic competition. These activities, referred to in this article as hybrid threats, directly challenge state sovereignty and represent the key distinguishing feature of contemporary strategic competition. To clarify this argument, the article aims to provide working definitions of strategic competition and its distinction from great power competition; to explain what hybrid threats and hybrid warfare are and their roles in the broader strategic objectives of state and non-state actors; to describe how strategic competitors and adversaries perceive these activities; and to emphasize the importance of building resilience within populations to counter hybrid threats.

Keywords: hybrid threats, hybrid warfare, irregular warfare, strategic competition, great power competition, unrestricted warfare, political warfare, grey zone activities.

Introduction

Strategic competition is not new, nor is the use of activities short of warfare by governments to shape the international system in their favor. In the nineteenth century, for example, the British and Russian empires employed a range of economic, political, diplomatic, and espionage activities in Central Asia to compete for influence and control in what became known as "the Great Game." During the Cold War, the United States and its allies similarly competed with the Soviet Union through a complex mix of foreign policy measures short of full-scale war to shape the international system in their favor and avoid escalation to

Creative Commons BY-NC-SA 4.0

conventional and nuclear war. These activities are, in fact, the very foundation of international relations.

The return to "great power competition" following Russia's illegal annexation of Crimea in 2014 and China's challenges to sea lines of communication in the South China Sea has renewed focus on activities short of open warfare to shape the international system. While this phase of strategic competition shares some similarities with its historical antecedents, several factors make it unique, including new technologies and the rise of non-state actors with global reach and influence. Perhaps most critically, the ability of actors to directly influence another state's population through a range of actions—affecting that state's capacity to project power both domestically and internationally—distinguishes this phase of strategic competition from earlier ones. These activities, referred to in this article as "hybrid threats" (HT), directly challenge state sovereignty and are the defining feature of contemporary strategic competition.

Western states face several challenges in countering the use of HT by adversaries seeking to influence their populations. The most significant of these challenges is a lack of consensus on terminology, which hampers a unified effort to counter HT activities in this new phase of strategic competition. To address this issue, this article aims to provide clear definitions for the terms used to describe the actors, their objectives, and the tactics they employ to influence and shape the current international system. Specifically, it distinguishes between great power competition and strategic competition, defines and categorizes the types of HT used in strategic competition and their objectives, differentiates HT from hybrid warfare (HW), and concludes by proposing that effective countermeasures should focus on states building resilience within their populations.

Great Power Competition vs. Strategic Competition

Perhaps one of the greatest challenges to understanding hybrid threats as part of strategic competition is the lack of consensus on what constitutes strategic competition and how it differs, if at all, from great power competition. Although the terms are often used interchangeably, they are not synonymous. The United States began using the term "great power competition" to shift its security priorities from the "Global War on Terror" to addressing threats posed by "near-peer competitor states" following Russia's illegal annexation of Crimea in 2014.[1] The 2015 National Defense Strategy, under the Obama administration, highlighted great power competition as a key concern, a focus that continued in

[1] Jim Garamone, "Dempsey: U.S. Forces Must Adapt to Deal with Near-Peer Competitors," *Joint Chiefs of Staff*, August 17, 2015, accessed January 22, 2024, www.jcs.mil/Media/News/News-Display/Article/613868/dempsey-us-forces-must-adapt-to-deal-with-near-peer-competitors/.

national security documents under both the Trump and Biden administrations.[2] These documents, and others, emphasize threats posed by Russia and China.

Great power competition involves near-peer adversaries using a range of statecraft instruments to challenge the international status quo. Critical to great power competition is a state's capacity and capability to create and project power through its military, nuclear arsenal, economic strength, diplomatic influence, and ability to attract and sway other actors in the international system. Additionally, it requires the wisdom to effectively combine these elements for strategic success. These capabilities align with what Joseph Nye famously categorized as hard, soft, and smart power, respectively.[3]

Strategic competition differs from great power competition in several key respects. Most notably, strategic competition involves more than just "near-peer competitors" like China and Russia. In the current international system, a variety of state and non-state actors are challenging the global political, economic, and military status quo—commonly referred to as the "rules-based order"—with the aim of reshaping the system to their advantage. The creation of BRICS in 2010 (comprising Brazil, Russia, India, China, and South Africa) and its expansion to five additional countries in 2024 (Egypt, Ethiopia, Iran, UAE, and Saudi Arabia) represents a significant challenge to the Western-led global economic and financial institutions established after World War II.[4] The emergence of new security partnerships, particularly through arms sales, also poses a challenge to the current international order. For instance, Türkiye, a NATO ally, maintains ties with several countries that challenge Western-based rules and norms, including Russia. In 2023, Türkiye became one of the leading producers of weapons systems, such as the AKINCI unmanned aerial vehicle, which it now exports to various countries, including Saudi Arabia and Pakistan.[5]

States with regional ambitions also exert influence in ways that reshape the strategic landscape. Qatar, for instance, has taken on an increased diplomatic role throughout the Middle East, acting as an intermediary for U.S. negotiations with the Taliban in Afghanistan and attempting to broker a truce between Hamas

---

[2] Ronald O'Rourke, "Great Power Competition: Implications for Defense – Issues for Congress," *Congressional Research Services*, October 3, 2023, Report, R43838, accessed January 22, 2024, https://sgp.fas.org/crs/natsec/R43838.pdf; See also: Michael J. Mazarr, Bryan Frederick, and Yvonne K. Crane, *Understanding a New Era of Strategic Competition* (Santa Monica: RAND Corporation, November 2022), https://www.rand.org/pubs/research_reports/RRA290-4.html.

[3] Joseph S. Nye, Jr., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs Books, 2005).

[4] Alyssa Ayres, "How the BRICS Got Here," *Council on Foreign Relations*, August 31, 2017, accessed January 22, 2024, https://www.cfr.org/expert-brief/how-brics-got-here.

[5] Ali Bakir, "Turkey's Defense Industry Is on the Rise: The GCC Is One of Its Top Buyers," *Atlantic Council*, August 4, 2023, accessed January 16, 2024, https://www.atlanticcouncil.org/blogs/menasource/turkey-defense-baykar-gcc-gulf/.

and Israel following the October 7, 2023, attacks.[6] India's central role in shaping BRICS, along with its continued rise as a major consumer market and growing exporter, positions it as a major contender in regional dynamics and the global economy.[7] Similarly, as previously mentioned, Türkiye is expanding its regional and even global influence through its arms exports.

Amid these challenges to the current international status quo, non-state actors continue to play a role in strategic competition, both as independent agents and as "proxies" for states seeking to challenge the global order. Hamas, for example, has prompted a shift in U.S. military posture and aid priorities following the October 7, 2023, attacks on Israel. The extent to which Hamas operates as an independent non-state actor or in collaboration with Iran and other states remains a topic of debate.[8] Equally important, despite the defeat of the Islamic State in Syria and Iraq, ISIS continues to shape security priorities in various regions, particularly in sub-Saharan Africa, where both ISIS and Al-Qaeda threaten stability, prompting involvement from Western powers as well as Russia and China.[9]

In sum, strategic competition involves an array of state and non-state actors seeking to challenge Western-established economic, security, legal, and political norms and institutions.[10] While Russia and China may be the primary threats, they are not the only actors capable of challenging the global system.

Hybrid Threats, Hybrid Warfare, and Strategic Competition

This era of strategic competition encompasses both the capabilities and intentions of state and non-state actors to shape regional dynamics and the international system in their favor. What distinguishes strategic competition today, however, is the ability of these actors to directly target a country's population, aiming to hinder governments from projecting power both

---

6 Stephen Kalin, "Gaza Diplomacy Cements Qatar's Global Mediator Role," *The Wall Street Journal,* November 25, 2023, accessed January 27, 2024, https://www.wsj.com/world/middle-east/gaza-diplomacy-cements-qatars-global-mediator-role-29e0ffb7.

7 Bhaskar Chakravorti and Gaurav Dalmia, "Is India the World's Next Great Economic Power?" *Harvard Business Review*, September 6, 2023, accessed February 2, 2024, https://hbr.org/2023/09/is-india-the-worlds-next-great-economic-power.

8 Fatima Al-Kassab, "What Is the 'Axis of Resistance' of Iran-Backed Groups in the Middle East?" *NPR*, October 26, 2023, accessed January 22, 2024, https://www.npr.org/2023/10/26/1208456496/iran-hamas-axis-of-resistance-hezbollah-israel.

9 Jason Warner et al., *The Islamic State in Africa: The Emergence, Evolution, and Future of the Next Jihadist Battlefront* (New York: Oxford University Press, 2021), https://doi.org/10.1093/oso/9780197639320.001.0001.

10 Here institutions refer to Douglas North's definition: "Institutions are the humanly devised constraints that structure political, economic, and social interaction. They consist of both informal constraints (sanctions, taboos, customs, traditions, and codes of conduct), and formal rules (constitutions, laws, property rights)…[to] reduce uncertainty in exchange." Douglas C. North, "Institutions," *Journal of Economic Perspectives* 5, no. 1 (Winter 1991): 97-112, https://doi.org/10.1257/jep.5.1.97.

domestically and internationally. These activities—often difficult to detect and even harder to attribute to a specific actor—are known as hybrid threats. In fact, hybrid threats may be the principal means of strategic competition today.

Countering hybrid threats is complicated by a lack of consensus on terminology and the broader objectives of these activities within strategic competition. In Europe, one of the most frequently cited definitions of HT comes from the Hybrid Center of Excellence (Hybrid CoE), established in 2017 as a collaborative initiative between NATO, the European Union, and partner nations. The center was created in response to Russia's illegal annexation of Crimea and parts of eastern Ukraine. The Hybrid CoE defines HT as a "concept" that,

> … refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.[11]

This definition highlights several key points for understanding hybrid threats in the context of strategic competition. First, the Hybrid CoE's "concept" identifies both state and non-state actors as perpetrators of HT, indicating that it is not exclusively a state-driven activity. For instance, at their peak, ISIS and Al-Qaeda employed a range of HT tactics to undermine political legitimacy and challenge state security in regions like the Middle East, Africa, Southeast Asia, and the West. The September 11th attacks, as terrorism scholar Bruce Hoffman notes, compelled the United States and its allies to completely redirect their foreign policy, altering the course of history.[12]

Critically, ISIS and Al-Qaeda maintained a robust information warfare capability designed to propagate their grand strategic narratives of providing an alternative worldview and political system to Western, secular liberalism.[13] Before the demise of the Islamic State in 2017, ISIS also possessed the capability to attract an estimated 40,000 "foreign fighters" and supporters to its so-called caliphate in Syria and Iraq.[14] These groups still have the ability to carry out acts

---

[11] Hybrid CoE, "Hybrid Threat as a Concept," accessed January 22, 2024, www.hybrid coe.fi/hybrid-threats-as-a-phenomenon/.

[12] Bruce Hoffman, "Rethinking Terrorism and Counterterrorism Since 9/11," *Studies in Conflict & Terrorism* 25, no. 5 (2002): 303-316, https://doi.org/10.1080/105761002 901223.

[13] Samantha Mahood and Halim Rane, "Islamist Narratives in ISIS Recruitment Propaganda," *The Journal of International Communication* 23, no. 1 (2017): 15-35, https://doi.org/10.1080/13216597.2016.1263231.

[14] Richard Barrett, "Beyond the Caliphate: Foreign Fighters and the Threat of Returnees" (New York, NY: The Soufan Center, October 2017), https://thesoufancenter.org/wp-

of terrorism globally, utilizing this crude and unlawful form of force to exert influence and shape state behavior. One could argue, therefore, that ISIS and Al-Qaeda were engaging in a form of strategic competition with the West. The 2018 U.S. National Defense Strategy, in fact, listed "violent extremist organizations" alongside four countries—China, Russia, Iran, and North Korea—as significant threats to the U.S. homeland.[15]

Despite the pivot away from the Global War on Terror, non-state actors continue to play a significant role in strategic competition, both as independent actors and as so-called "proxy forces" receiving varying levels of support or funding from states. As described earlier, Hamas's actions have compelled the United States and other Western powers to recalibrate their security priorities following the October 7, 2023, attack in Israel. Non-state actors, therefore, can participate in strategic competition by disrupting the international order and influencing countries' foreign policy priorities.

Second, the Hybrid CoE's definition is valuable for its emphasis on the effects of hybrid threats. Their concept highlights that HT aim to "deliberately target democratic states' and institutions' vulnerabilities." In other words, HT seek to exploit various vulnerabilities within a state with the overall goal of undermining a country's democratic system. These vulnerabilities may include ethnic and/or religious fissures within the population, migration issues, economic disparities, and disagreements over a country's values and norms, to name a few. Ultimately, state and non-state actors "weaponize" these vulnerabilities to further divide and weaken nations.

In the United States, for instance, scholars and law enforcement have identified Russian efforts to exploit racial tensions prior to the 2016 and 2020 presidential elections, including the amplification of social media posts on all sides of the racial debate.[16] Importantly, Niklas Nilsen and colleagues note that state and non-state actors can also target non-democracies, broadening the definition of HT's goals to encompass any political system. They argue that actors utilize HT to "achieve outcomes without a war, to disrupt, undermine or damage the target's political system and cohesion…" [17] This broader perspective helps expand the discussion on how HT operates in strategic competition, as it includes

---

content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf.

[15] U.S. Department of Defense, " Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge," https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[16] Jason Parham, "Targeting Black Americans, Russia's IRA Exploited Racial Wounds," *Wired*, December 17, 2018, accessed January 19, 2024, www.wired.com/story/russia-ira-target-black-americans/.

[17] Niklas Nilsson et al., "Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021), 2, https://doi.org/10.5040/9781788317795.0005.

both state and non-state actors engaging in HT activities to destabilize non-democracies as well as democracies.

However, the Hybrid CoE's definition falls short of capturing the broader goal of actors using hybrid threats as part of strategic competition: weakening the current global system and reshaping it to their advantage. As will be elaborated, actors employing HT often aim to exploit existing vulnerabilities within a country to weaken and divide it, thereby hindering its ability to project power regionally and globally. In this context, the objective of HT is not merely to undermine democratic institutions (or any political system) but to erode these institutions in a way that diminishes a country's capacity to project power, thus creating a window of opportunity for the acting state to operate unobstructed and ultimately alter the regional or international system in its favor.

Third, the Hybrid COE's definition highlights that HT include "a wide range of means … designed to remain below the threshold of detection and attribution." Typically, definitions of HT focus on a limited set of activities, including disinformation, mal-information, and cyber operations such as Distributed Denial of Service (DDoS) attacks or ransomware.[18] However, the Hybrid COE's definition is valuable because it allows for the possibility that HT could include virtually anything. Mark Galeotti explores in depth the notion that nearly anything can be weaponized—information, resources, criminal networks, and even imagination—to target populations and weaken states' abilities to project power, particularly in an era of heightened interdependence.[19]

Similarly, Mikael Weissmann identifies categories of hybrid threats rather than discrete events. His seven categories include diplomatic,[20] economic, technological, information, "unconventional methods" (a catch-all category encompassing activities like terrorism and organized crime), civil (activities targeting civil society), and non-kinetic attacks against the military, including activities like information warfare designed to undermine the morale of opposing

[18] Disinformation is incorrect information deliberately spread to cause harm. Mal-information is true information deliberately spread to cause harm, and misinformation is false information spread without the intention to cause harm. Information as HT involves intention and, therefore, disinformation and mal-information are the better terms. See: Claire Wardle, "Understanding Information Disorder," *First Draft News*, September 22, 2020, accessed January 22, 2024, https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

[19] Mark Galeotti, *The Weaponization of Everything: A Field Guide to the New Way of War* (New Haven: Yale University Press, 2022).

[20] Although Weissmann does not specify this, "public diplomacy" is the act of heads of state speaking directly to populations with the aim of influencing them, conforming to this article's definition of HT as directly targeting populations. See: Mikael Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare: The Role of the Military in the Grey Zone," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, 65-66, https://doi.org/10.5040/9781788317795.0011.

troops.[21] This list of categories is valuable because it provides a range of specific activities to observe and future activities to consider. For instance, significant attention has been paid to how state and non-state actors utilize cyber activities, often masking attribution and detection, for strategic goals.[22] These activities could be classified within Weissmann's "technological" category. However, in addition to cyber activities, the technological category could also encompass the rapidly expanding use of AI as a hybrid threat or the potential exploitation of big data for strategic purposes. Therefore, Weissmann's categories facilitate the organization and cataloging of current activities while also considering future possibilities.

Additionally, two more categories could enhance Weissmann's HT list. The first focuses on "resources" as a hybrid threat, including energy, food, and water, highlighting how state and non-state actors exploit these vulnerabilities for strategic purposes. Following Russia's full-scale invasion of Ukraine in 2022, Europe's reliance on Russian oil and natural gas became a major concern, prompting several European countries to reduce their dependence on Russian energy.[23] Russian and Ukrainian grain exports also emerged as critical vulnerabilities, subject to weaponization.[24] The second category involves the use of culture, values, and history as hybrid threats. In a September 2022 speech, Vladimir Putin claimed that "the dictatorship of the Western elites is directed against all societies, including the peoples of the Western countries themselves. This is a challenge to all. This is a complete denial of humanity, the overthrow of faith and traditional values." He has also framed his operations in Ukraine and beyond as a defense of Russians' historic rights. [25] Thus, culture, values, and history represent another significant type of HT.

Finally, Hybrid CoE's emphasis on the challenges of detecting HT and, when detected, attributing them accurately is critical for understanding these activities within the context of strategic competition. Mikael Weissmann's insightful edited volume on hybrid warfare notes that "deception and denial are inherent in hybrid methods, and it is sometimes difficult to know for sure that warfare is

---

[21] Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare," 65-66.

[22] Christian Payne and Lorraine Finlay, "Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack," *The George Washington International Law Review* 49, no. 3 (2017): 535-568, https://149801758.v2.pressablecdn.com/wp-content/uploads/_pda/ILR-Vol-49.3_Panye-Finlay.pdf.

[23] Mark Finley and Anna B. Mikulska, "Wielding the Energy Weapon: Differences Between Oil and Natural Gas" (Houston: Rice University's Baker Institute for Public Policy, June 26, 2023), https://doi.org/10.25613/G9P2-3F78.

[24] Josep Borrell, "Russia Must Stop Using Food as a Weapon," *European Union External Action*, August 2, 2023, accessed January 27, 2024, https://www.eeas.europa.eu/eeas/russia-must-stop-using-food-weapon_en.

[25] Reuters, "Extracts from Putin's Speech at Annexation Ceremony," *Reuters*, September 30, 2022, accessed January 19, 2024, https://www.reuters.com/world/extracts-putins-speech-annexation-ceremony-2022-09-30/.

ongoing, and in the same way, it is inherently difficult to identify if, and when, a perceived threat of future action becomes reality." [26] Similarly, David Kilcullen's concept of "liminal warfare" identifies several levels of attack based on attribution: ranging from clandestine (undetected action) to covert (detected but unattributable action) to ambiguous (detected action with a suspected but unprovable actor) to overt (both action and actor are visible). The gaps between these attack types complicate the challenge of formulating a timely and proportional response without inadvertently or accidentally escalating the conflict. Kilcullen refers to this as the "liminal zone," a concept closely related to the grey zone.[27]

Beyond Hybrid CoE's definition of HT, there are a few additional points to consider. First, it is important to recognize that strategic competition does not always involve state and non-state actors using HT to target populations. Economic competition, treaties, and alliances are all legal activities and part of "normal" international relations. For example, the emergence of BRICS as a challenge to Western economic and financial institutions illustrates strategic competition through lawful and transparent means. In contrast, HT relies on illegal or legally ambiguous ("grey") activities that are difficult to trace, aiming to target a country's population and ultimately weaken and limit that state's ability to project power.

Second, there is disagreement over the use of the term "hybrid threat" to describe these activities. George Kennan, the U.S. diplomat who helped formulate the United States' post-World War II containment strategy against the Soviet Union, referred to such actions as "political warfare," a term that remains in use today.[28] The U.S. Department of Defense, on the other hand, has adopted the term "irregular warfare" (IW) for activities similar to HT. U.S. Joint Doctrine Publication 1, Volume 1 "Joint Warfighting," along with the 2020 IW annex to the National Defense Strategy, defines IW as "a struggle among state and non-state actors to influence populations and affect legitimacy." The definition further explains that "Irregular warfare favors indirect warfare and asymmetric warfare approaches, though it may employ the full range of military and other capabilities in order to erode the adversary's power, influence, and will." In essence, IW shares similar activities and objectives with HT.[29]

---

[26] Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare," 63.

[27] David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, March 2020).

[28] For Kennan, see: "269. Policy Planning Staff Memorandum," *Office of the Historian*, May 4, 1948, accessed January 21, 2024, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269. For an example of the use of "political warfare" today, see Linda Robinson et al., "The Growing Need to Focus on Modern Political Warfare," Research Brief RB-10071-A (Santa Monica: RAND Corporation, 2019), www.rand.org/pubs/research_briefs/RB10071.html.

[29] Currently, the U.S. Department of Defense is working on a new definition of IW.

In addition to the definitional disagreements in the West, China and Russia have developed their own terminology for HT. In 1999, two Chinese theorists, Qiao Liang and Wang Xiangsui, introduced the concept of "unrestricted warfare." They described the "future battlefield as an 'extended domain,' not a battlefield where lethality took precedence, but one in which the goal of any nation-state (or sub-state actors) is to 'paralyze and to undermine the enemy' by degrading the will of its people and the state to wage an armed conflict in the first place." [30] Similarly, Russian theorist and Chief of the Armed Forces' General Staff, General Valery Gerasimov, has referred to "unrestrictive warfare" to describe Russia's use of a full spectrum of operations aimed at shaping regions and the international system to Russia's advantage.[31]

Finally, several scholars advocate for a clear distinction between hybrid threats and hybrid warfare. Weissmann, for instance, references the International Institute for Strategic Studies' definition of HW to differentiate it from HT:

> The use of military and nonmilitary 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.[32]

Distinguishing between hybrid threats and hybrid warfare is important in the context of strategic competition. The use of military "tools"—ranging from "non-kinetic" activities like troop positioning to the actual use of force—is generally visible and signals one state's intentions to another. In contrast, HT is less apparent, complicating detection and making a timely and appropriate response more challenging. Additionally, HW involves directly targeting the population as well as engaging another nation's military. It is the combination of hybrid threats and kinetic activities, both of which strategically target populations, that makes HW especially difficult to counter and distinct from conventional—what the United States refers to as "traditional"—warfare.

The NATO definition of hybrid warfare captures this complexity, often using the terms hybrid warfare (HW), hybrid threats (HT), and hybrid activities interchangeably:

---

[30] As described by Mark Thomas. See Mark Thomas, "The Chinese Roots of Hybrid Warfare," *CEPA*, August 10, 2022, accessed January 20, 2024, https://cepa.org/article/the-chinese-roots-of-hybrid-warfare/.

[31] Thomas, "The Chinese Roots of Hybrid Warfare." See also: ARIS, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: The United States Army Special Operations Command, 2018), www.soc.mil/ARIS/books/pdf/14-02984_LittleGreenMen-UNCLASS-hi-res.pdf.

[32] Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare," 64.

> 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 used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies.[33]

Despite the overlapping terminology, NATO's definition of hybrid warfare encapsulates the key elements of both hybrid threats and hybrid warfare as discussed here – namely, the combination of non-kinetic and kinetic activities, the primary purpose "to sow doubt in the minds of target populations," and the overarching objective to "destabilise and undermine societies," with the ultimate goal of reshaping the regional and global order in favor of the adversary.

From these various definitions, several commonalities emerge that can inform a working definition of HT and HW as they pertain to strategic competition:

- *Perpetrators*: Both state and non-state actors can engage in HT and HW. Non-state actors may operate independently or collaborate loosely with states.
- *Targets*: The primary target of HT and HW is a state's population. Actors exploit key vulnerabilities within these populations through HT and HW activities.
- *Nature of activities*: HT activities typically fall short of open warfare. They are often concealed, and when they are visible, they can be difficult to attribute to a specific actor, complicating responses. HW includes a combination of open warfare and HT activities. The principal target of HW is still populations, which differentiates it from conventional war. While attribution may be known, formulating an effective response that counters both HW and HT activities without escalating the conflict is challenging.
- *Objectives*: The goals of HT and HW are to undermine national unity, sow division within populations, and challenge the legitimacy of governments. Ultimately, these activities aim to compel governments to focus inward on domestic issues, thereby weakening their capacity to project power externally.
- *Impact on strategic competition*: In the context of strategic competition, both HW and HT seek to weaken and divide cooperation among states, including alliances, and to limit collective security efforts in projecting power within the international system. This creates opportunities for actors to reshape the global order in their favor.

[33] "Countering Hybrid Threats," *NATO*, August 18, 2023, accessed January 23, 2024, https://www.nato.int/cps/en/natohq/topics_156338.htm.

Conclusion

This article posits that, while strategic competition is not a new phenomenon, the ability of state and non-state actors to challenge the international order by directly targeting populations through various hybrid threats and hybrid warfare activities represents a novel development. If the primary target of HT and HW is indeed a state's population, then effectively countering these threats necessitates preparing and strengthening populations against such attacks – this is what "societal resilience" means.

While the topic of building societal resilience warrants a comprehensive manuscript of its own, this article concludes by identifying three key measures that states can adopt to enhance societal resilience. First, governments should prioritize building awareness and resilience against disinformation and mal-information campaigns, which may represent one of the most significant HT challenges countries face today. This enormous undertaking encompasses a wide range of efforts, from addressing the cognitive effects of social media and developing critical thinking skills among populations to countering the erosion of trust in traditional sources of information, including the press and government institutions.

Second, governments should focus on enhancing resilience within their critical infrastructure and key services. NATO's baseline requirements for national resilience identify seven key areas:

- Assured continuity of government and critical government services
- Resilient energy supplies
- Effective management of uncontrolled movement of people
- Resilient food and water resources
- Capacity to address mass casualties
- Robust civil communications systems
- Resilient civil transportation systems.[34]

To this list, it is essential to add the ability of governments to provide credible information, as this capability is crucial for strengthening resilience against disinformation and mal-information.

Third, governments should take proactive steps to prepare their populations for the possibility of war, including the grim reality of nuclear conflict. On January 7, 2024, Sweden's Civil Defense Minister, Carl-Oskar Bohlin, and Chief of Defense, Micael Bydén, publicly urged Swedish citizens to mentally prepare for the possibility of war as the country finalized its NATO membership. This

[34] Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defence," *NATO Review*, February 27, 2019, accessed January 28, 2024, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

announcement caused a stir in Sweden.[35] However, preparing one's population for a range of hybrid threats, along with the potential for warfare that intentionally targets civilians, is essential for building resilience against both hybrid threats and hybrid warfare.

These are just three areas where all states should focus on building societal resilience to defend against hybrid threats and the potential for hybrid warfare. Given that populations are the primary targets of these threats, governments must actively engage with their citizens to mitigate the impact of HT and prepare for the realities of HW.

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.

About the Author

Heather S. Gregg, PhD, is a Professor of Irregular Warfare/ Hybrid Threats at the George C. Marshall European Center for Security Studies in Garmisch, Germany. She is also a senior fellow at the Foreign Policy Research Institute. Her academic focus includes irregular warfare, hybrid threats, terrorism and counterterrorism, the causes of extremism, and leveraging culture in population-centric conflicts. This encompasses building resilience and repairing communities and national unity in the wake of war and political instability.
E-mail: heather.gregg@marshallcenter.org

[35] Hope O'Dell, "Why Is Sweden Telling Its Citizens to Prepare for War?" *Chicago Council on Global Affairs*, January 24, 2024, accessed January 28, 2024, https://globalaffairs.org/bluemarble/sweden-tells-citizens-prepare-war-russian-aggression-nato-membership.

Bibligraphy

"269. Policy Planning Staff Memorandum," Office of the Historian, May 4, 1948, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269.

"Countering Hybrid Threats," NATO, August 18, 2023, https://www.nato.int/cps/en/natohq/topics_156338.htm.

"Extracts from Putin's Speech at Annexation Ceremony," *Reuters*, September 30, 2022, https://www.reuters.com/world/extracts-putins-speech-annexation-ceremony-2022-09-30/.

Al-Kassab, Fatima, "What Is the 'Axis of Resistance' of Iran-Backed Groups in the Middle East?" *NPR*, October 26, 2023, https://www.npr.org/2023/10/26/1208456496/iran-hamas-axis-of-resistance-hezbollah-israel.

ARIS, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: The United States Army Special Operations Command, 2018), https://www.soc.mil/ARIS/books/pdf/14-02984_LittleGreenMen-UNCLASS-hi-res.pdf.

Ayres, Alyssa, "How the BRICS Got Here," Council on Foreign Relations, August 31, 2017, https://www.cfr.org/expert-brief/how-brics-got-here.

Bakir, Ali, "Turkey's Defense Industry Is on the Rise: The GCC Is One of Its Top Buyers," Atlantic Council, August 4, 2023, https://www.atlanticcouncil.org/blogs/menasource/turkey-defense-baykar-gcc-gulf/.

Barrett, Richard, Beyond the Caliphate: Foreign Fighters and the Threat of Returnees (New York, NY: The Soufan Center, October 2017), https://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf.

Borrell, Josep, "Russia Must Stop Using Food as a Weapon," European Union External Action, August 2, 2023, https://www.eeas.europa.eu/eeas/russia-must-stop-using-food-weapon_en.

Chakravorti, Bhaskar, and Gaurav Dalmia, "Is India the World's Next Great Economic Power?" *Harvard Business Review*, September 6, 2023, https://hbr.org/2023/09/is-india-the-worlds-next-great-economic-power.

Finley, Mark, and Anna B. Mikulska, "Wielding the Energy Weapon: Differences Between Oil and Natural Gas" (Houston: Rice University's Baker Institute for Public Policy, June 26, 2023), https://doi.org/10.25613/G9P2-3F78.

Galeotti, Mark, The Weaponization of Everything: A Field Guide to the New Way of War (New Haven: Yale University Press, 2022).

Garamone, Jim, "Dempsey: U.S. Forces Must Adapt to Deal with Near-Peer Competitors," Joint Chiefs of Staff, August 17, 2015, https://www.jcs.mil/Media/News/News-Display/Article/613868/dempsey-us-forces-must-adapt-to-deal-with-near-peer-competitors/.

Hoffman, Bruce, "Rethinking Terrorism and Counterterrorism Since 9/11," *Studies in Conflict & Terrorism* 25, no. 5 (2002): 303-316, https://doi.org/10.1080/105761002901223.

Hybrid CoE, "Hybrid Threat as a Concept," https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

Kalin, Stephen, "Gaza Diplomacy Cements Qatar's Global Mediator Role," *The Wall Street Journal*, November 25, 2023, https://www.wsj.com/world/middle-east/gaza-diplomacy-cements-qatars-global-mediator-role-29e0ffb7.

Kilcullen, David, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, March 2020).

Mahood, Samantha, and Halim Rane, "Islamist Narratives in ISIS Recruitment Propaganda," *The Journal of International Communication* 23, no. 1 (2017): 15-35, https://doi.org/10.1080/13216597.2016.1263231.

Michael J. Mazarr, Bryan Frederick, and Yvonne K. Crane, Understanding a New Era of Strategic Competition (Santa Monica: RAND Corporation, November 2022), https://www.rand.org/pubs/research_reports/RRA290-4.html.

Nilsson, Niklas, et al., "Security Challenges in the Grey Zone: Hybrid Threats and Hybrid Warfare," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, ed. Mikael Weissmann et al. (London: I.B. Tauris, 2021), 2, https://doi.org/10.5040/9781788317795.0005.

North, Douglas C., "Institutions," *Journal of Economic Perspectives* 5, no. 1 (Winter 1991): 97-112, https://doi.org/10.1257/jep.5.1.97.

Nye, Joseph S., *Soft Power: The Means to Success in World Politics* (New York: Public Affairs Books, 2005).

O'Dell, Hope, "Why Is Sweden Telling Its Citizens to Prepare for War?" Chicago Council on Global Affairs, January 24, 2024, https://globalaffairs.org/bluemarble/sweden-tells-citizens-prepare-war-russian-aggression-nato-membership.

O'Rourke, Ronald, "Great Power Competition: Implications for Defense – Issues for Congress," Congressional Research Services, October 3, 2023, Report, R43838, https://sgp.fas.org/crs/natsec/R43838.pdf.

Parham, Jason, "Targeting Black Americans, Russia's IRA Exploited Racial Wounds," Wired, December 17, 2018, https://www.wired.com/story/russia-ira-target-black-americans/.

Payne, Christian, and Lorraine Finlay, "Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack," *The George Washington International Law Review* 49, no. 3 (2017): 535-568, https://149801758.v2.pressablecdn.com/wp-content/uploads/_pda/ILR-Vol-49.3_Panye-Finlay.pdf.

Robinson, Linda, et al., "The Growing Need to Focus on Modern Political Warfare," Research Brief RB-10071-A (Santa Monica: RAND Corporation, 2019), https://www.rand.org/pubs/research_briefs/RB10071.html.

Roepke, Wolf-Diether, and Hasit Thankey, "Resilience: The First Line of Defence," NATO Review, February 27, 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Thomas, Mark, "The Chinese Roots of Hybrid War-fare," CEPA, August 10, 2022, https://cepa.org/article/the-chinese-roots-of-hybrid-warfare/.

U.S. Department of Defense, "Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge," https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Wardle, Claire, "Understanding Information Disorder," *First Draft News*, September 22, 2020, https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

Warner, Jason, et al., *The Islamic State in Africa: The Emergence, Evolution, and Future of the Next Jihadist Battlefront* (New York: Oxford University Press, 2021), https://doi.org/10.1093/oso/9780197639320.001.0001.

Weissmann, Mikael, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare: The Role of the Military in the Grey Zone," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, edited by Mikael Weissmann et al. (London: I.B. Tauris, 2021), 65-66, https://doi.org/10.5040/9781788317795.0011.