TO: US and allied national security communities
FROM: Atlantic Council's Gray Zone Task Force
DATE: December 22, 2022
SUBJECT: Scoping the gray zone: Defining terms and policy priorities for engaging competitors below the threshold of conflict

---

In October, the Scowcroft Center for Strategy and Security's Forward Defense practice convened current and former practitioners and other experts for a private workshop under its Adding Color to the Gray Zone project, which seeks to advance a US and allied strategic framework for hybrid conflict. Participants discussed what actions should and should not be encompassed by the term "gray zone," the value in defining the gray zone and hybrid conflict, and the most pressing issues for the United States to address in this realm.

Strategic context

Through hybrid conflict or warfare, US adversaries are blurring the lines between peace and war, in a space often referred to as the gray zone. Without firing a single bullet, US adversaries are striking at the fibers of US and allied societies, economies, and governments to test confidence in systems that underwrite both the US constitutional republic and the US-led, rules-based international order. Gray zone competition is a critical and practical element of twenty-first-century security. The ability of the United States to defend against gray zone threats and leverage its advantages for national imperatives will affect its competitive edge in the coming years. There is much debate, however, around what the gray zone and hybrid conflict or warfare signify. While reaching agreement on this terminology is a critical first step for any strategy, it serves only as the early pages of any strategy, and US adversaries are chapters ahead in their respective playbooks.

The value of defining key terms

While definitions for the *gray zone* and *hybrid conflict or warfare* are critical for stakeholder synchronization and coordination, reaching consensus on such terminology is neither practical nor worth the effort beyond a common critical mass accomplished through working definitions versus absolute ones. This analysis adopts the following working definitions:

- The **gray zone** is the space in which defensive and offensive activity occurs above the level of cooperation and below the threshold of armed conflict. Gray zone operations, activities, and actions (OAA) are often, but not always, clandestine, covert, unofficial, or outside accepted norms of behavior. Gray zone OAA are aimed at undermining the security of the target entity or projecting the national or organizational interest of the initiator but without triggering active armed conflict. While the gray zone can be thought of chronologically (i.e., after peace, before active hostilities), it is referred to spatially to reflect that this is not necessarily the case. In fact, gray zone activity can occur during active armed conflict between actors.

- **Hybrid conflict** (also referred to as **hybrid warfare**) is a subset of statecraft that uses the diplomatic, informational, military, and economic (DIME) levers[1] of national power across the competition continuum, including cooperation, competition (including gray zone OAA), deterrence, and armed conflict for the purposes of achieving national security objective(s) against a state or non-state actor(s).

[1] DIME has expanded to include financial, intelligence, law, and development levers, with acronyms such as MIDFIELD and DIMEFIL created to account for this. The continued use of DIME bridges the gap between past and present generations of practitioners and remains consistent with the security community's default verbiage.

These working definitions are meant to offer a meeting point for further discussion, as the task force recognizes and welcomes debate about what is and is not considered gray zone OAA or hybrid conflict. Providing an 80 percent solution allows us to go beyond definitions and begin tackling the tougher and more substantive question of *how* the United States and its allies and partners act and respond in the gray zone.

According to these definitions, one might argue that few methods do *not* fall under the gray zone; everything from political speeches and economic policies to legal agreements and information operations, all the way up to arms sales and active armed conflict, may fall under the umbrella of hybrid conflict. This broad lens, however, deliberately offers a strategic shift in the way in which security threats are viewed. Given that security today is shaped by conventional military threats as well as unconventional military and nonmilitary threats, it compels us to redefine what is meant by conflict and consider it as a spectrum persisting well beyond the physical battlefield, threatening not just the lives of American warfighters but also the American way of life. In a sense, the gray zone can be viewed as a distinct (and limitless) domain, with hybrid conflict the activity that falls within this realm. This does not indicate a novelty in the nature of warfare so much as how war is characterized.

This characterization is another area where a strategic competitor like China is ahead of the United States. Chinese doctrinal literature like *Unrestricted Warfare* and concepts such as the "Three Warfares" have characterized conflict with the United States in this way for nearly thirty years. It is also consistent with theater campaign plans, which provide guidance to US geographic combatant commanders for coordinating Phase Zero activities shaping the battlespace, and ironically, with Sun Tzu's quote that "every battle is won before it is ever fought."

Putting definitions into context

What falls within the gray zone? Put simply, it depends. Gray zone activity persists in a delta of norms, wherein the United States, its allies, and its adversaries are all playing by distinct sets of rules and thus work under different thresholds for conflict.

Beyond lexicon, policymakers need to consider the real-world applications of the gray zone terminology, recognizing that **target** (*who or what* is being targeted) and **intent** (*what* end state the actor is aiming to accomplish) are two key variables in the gray zone equation, and they affect whether actions are characterized as gray zone activity or ordinary statecraft. Identical policy actions might be classified differently depending on whether they intentionally coerce or deter a specific target. For example, when is policy categorized as purely economic versus coercive? While US government investment requires promise of at least breaking even, China subsidizes its private sector even when a deal is projected to lose money—the former policy satisfies economic interests, whereas the latter points to an ulterior motive.

Furthermore, whether an act is classified as hybrid often depends on where one sits: The US government commonly views its own actions as statecraft while cataloging the same or similar actions conducted by adversaries as hybrid conflict. For example, the 2022 National Defense Strategy characterizes only competitor approaches as falling within the gray zone, even while referencing comparable US and allied methods. Similarly, the enemy always gets a vote, and while the United States may consider certain actions as operational preparation of the environment, competitors may view them as acts of aggression, hostility, or even war. In parallel, the way in which the United States defines and acts in the gray zone affects whether allies and partners follow suit. Definitional and values-driven consensus can ensure like-minded nations and organizations are on the same page when it comes to hybrid conflict.

Key priorities in the gray zone

While the hybrid problem set is expansive, three key focus areas emerged from the workshop discussion:

- *Countering Chinese and Russian malign activities and deterring aggression.* Specific priorities in the gray zone should be framed around the broader strategic goal of preventing and responding to Chinese and Russian hybrid threats. China and Russia are the United States' key strategic competitors, and nowhere is this more evident than in the gray zone. China leverages hybrid activity to protect its brand of authoritarianism (for example, power projection through its Belt and Road Initiative infrastructure projects), whereas Russia aims to weaken NATO and command its near abroad (e.g., the use of unmarked "Little Green Men" to seize Crimea in 2014). Both China and Russia have long leveraged gray zone activity to inflict significant information, influence, intelligence, and technical losses on the United States and allies. How they manifest hybrid conflict, however, differs: Russia fuses military and nonmilitary methods to sow chaos, while China's approach is far more pervasive and employs continuous nonmilitary operations to offset US military superiority. The United States' recognition of a broadening paradigm from legacy traditional deterrence of its adversaries to increased focus on information and influence is central to the integrated deterrence mandated by the US National Security Strategy and National Defense Strategy.

- *Adapting to the information age.* Emerging technologies continue to revolutionize how people and nations receive and consume information, necessarily changing the way in which information activity is conducted in the gray zone. Technological advancements are transforming both the hybrid threats facing the United States and the tools at its disposal. For example, for all its good, technological innovation has also caused supply chain sensitivities vulnerable to adversarial exploitation including through industrial espionage, intellectual property theft, and cyberattacks. US entities need to become more creative in anticipating such threats and solving for them, such as through obfuscating data and reducing an adversary's confidence. Another example is found in open-source intelligence (OSINT). With the proliferation of social media, OSINT can be just as critical as classified sources and methods of intelligence—yet the US government's traditional bias toward classified intelligence is hindering its ability to stay ahead in the information domain. This space is ripe for public-private partnership, as vulnerabilities are not necessarily housed in US government entities but rather in assets and infrastructure not traditionally or organically protected by the government or military (e.g., social media platforms).

- *Involving economic policies and institutions.* Any discussion of the gray zone is incomplete without adequate consideration of economic policies and their key stakeholders. Economic strategy is a key component of strategic competition, with industrial policy, debt financing, and sovereign debt policy being among the policies leveraged by China and Russia to meet their own strategic ends. Furthermore, US adversaries are targeting the commercial sector, shifting much of the impetus for action on economic and private sector actors that should play a leading role in the gray zone. Civil and commercial partnerships will be a cornerstone of a US response in the gray zone, and the private sector must be strengthened against economic coercion and intellectual property theft or risk weakening the US strategic approach.

The way forward

Gray zone threats are a whole-of-nation problem and should prompt a whole-of-nation response. While the United States currently views the gray zone largely through a military or intelligence framework, and a defensive one at that, other US departments and agencies, commercial stakeholders, and international entities have a major—in some cases leading—role to play.[2] A cohesive US strategy, perhaps coordinated by an entity independent of practitioner equities, is necessary to synchronize and optimize US government and commercial actors and their efforts in this space.

Such a strategy must be well resourced and well articulated. The United States should look past traditional military personnel to build out its hybrid response, creating new paradigms that do not necessarily adhere to the legacy system(s) but involve relevant stakeholders who can view the adversary without political and/or military bias. Moreover, the United States should update the training of its diplomatic corps to ensure its cadre understands the inner workings of key institutions central to their job description. Additionally, communicating with and educating a public audience will be a foundational requirement for gray zone efforts, as society at large must recognize that the United States is routinely fighting in the gray zone and citizens must understand the ways in which they play a role. This approach has precedence in World Wars I and II, and even the Cold War. Consistent and synchronized messaging across the government will help maintain the effectiveness and credibility of the messaging needed to deter adversaries from using hybrid methods.

*The Atlantic Council's **Gray Zone Task Force** consists of technical and policy experts, former government officials, and private sector executives. These individuals leverage their deep knowledge and extensive experience in impacted and impactful industries to examine adversarial acts in the gray zone and determine how the United States and its allies and partners can leverage hybrid tactics to meet their own strategic ends.*

[2] The 2022 National Defense Strategy recognizes that many of the tools for campaigning in the gray zone fall outside its arsenal, acknowledging the need to rely on its interagency counterparts.