Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare Power Balances

Description

Editorâ??s Note: this article is being republished with the permission of Small Wars Journal as part of a republishing arrangement between IWI and SWJ. The original article was published on 06.17.2025 and is available here.

SWJ Logo Tall

The contemporary security environment defies traditional categorizations of war and peace. We exist in what some analysts increasingly term a â??hybrid Cold War,â?• that is, a persistent state of competition that blends conventional capabilities with irregular tactics, cyber operations, and information warfare. This reality demands that defense professionals move beyond conceptual hand-waving to develop quantifiable frameworks for assessing power balances in these gray zones of conflict.

Recent dialogue among intelligence, military, and defense industry professionals has highlighted a critical gap: the absence of systematic approaches to measure hybrid warfare capabilities and effectiveness. NATOâ??s newly published Hybrid Threats and Hybrid Warfare Reference Curriculum represents a significant step forward, targeting over 800 defense and security academies worldwide. However, the curriculumâ??s focus on resilience-building, while necessary, reflects Western democraciesâ?? defensive posture in an arena where adversaries operate with fewer constraints.

Defining the Hybrid Battlefield

The mushy quality of hybrid warfare definitions has long frustrated practitioners. Unlike conventional warfareâ??s clear metricsâ??divisions, tanks, aircraftâ??hybrid capabilities resist easy quantification. The phenomenon encompasses everything from cyber-attacks on critical infrastructure to weaponized migration, cultural influence operations, and economic coercion.

Consider recent examples: Russian-backed interference in European elections, including direct support for political parties in Moldova; Chinese influence campaigns targeting Taiwanâ??s elections; and systematic attacks on undersea cables and telecommunications infrastructure across the Baltic

region. These activities exist in the gray zone between peace and war, and are designed to achieve political objectives without triggering conventional military responses.

This strategic ambiguity serves adversaries well. Russiaâ??s â??active measures,â?• refined during the Cold War and adapted for the digital age, exemplify hybrid warfareâ??s evolutionary nature. The *European Centre of Excellence for Countering Hybrid Threats* in Helsinki has documented how hybrid threats combine speed, scale, and intensity previously impossible before digital interconnectivity.

Measuring the Unmeasurable

To move beyond conceptual discussions, analysts need frameworks that quantify hybrid capabilities across multiple domains. Four critical areas emerge as measurable components of hybrid warfare power:

1. Disruptive Media and Social Influence

American soft power once dominated global narratives through initiatives like *Voice of America* and cultural programming. Today, the United States lacks coherent strategic objectives for information influence operations, creating opportunities for adversaries. The withdrawal of traditional mechanisms coincides with private sector narratives driven by commercial rather than strategic interests.

Russiaâ??s approach contrasts sharply. Russian cultural centers operate globally, ostensibly promoting language and culture while building influence networks. These centers, overseen by *Rossotrudnichestvo*â??Moscowâ??s official government agency responsible for civilian foreign aid and culture exchangeâ??maintain operations even in countries like Germany and the United States despite espionage allegations. Their directors often hold diplomatic immunity, complicating host nation responses.

Chinaâ??s â??three warfaresâ?• conceptâ??psychological, political, and lawfareâ??demonstrates systematic approaches to narrative warfare. The United Front department leverages Chinese diaspora communities and front organizations to maximize influence while maintaining plausible deniability.

2. Defense Industrial Base Agility

Traditional metrics measuring defense industrial base (DIB) strengthâ??dollar values, production capacity, employment figuresâ??miss critical factors in hybrid warfare. Agility becomes paramount when adversaries adapt tactics faster than acquisition cycles.

Ukrainian innovation during the current conflict illustrates this principle. Engineers integrated many different, non-interoperable unmanned aircraft systems into cohesive operations, demonstrating a force multiplier that formal defense establishments struggle to match. This adaptability challenges conventional assumptions about military procurement and development timelines.

American DIB strength remains globally dominant, but concerns about agility persist. The Pentagonâ??s requirements system operates on timelines that â??shoot behind the duck,â?• struggling to incorporate commercial innovation at operational speed. Current efforts to integrate artificial intelligence into wargaming represent attempts to accelerate requirements generation and validation processes.

3. Science and Technology Competition

Research enterprise competition reveals stark disparities in scale and focus. China now produces approximately 3.5 million STEM graduates annually compared to roughly 500,000 in the United States. More concerning, Chinese universities are projected to graduate over 77,000 STEM PhDs annually by 2025 compared to 40,000 in the United States.

These quantitative disparities matter less than qualitative applications. China currently cannot design cutting-edge computer chips, providing the United States approximately a decadeâ??s advantage in high-end semiconductors. However, this lead depends on maintaining technological barriers and preventing knowledge transfer.

American research advantages historically stemmed from attracting global talent and maintaining world-class universities. Politicization concerns and investment relationships with adversarial nations threaten these foundations. The challenge involves balancing openness with security without undermining innovation ecosystems.

4. Clandestine Capabilities

Traditional intelligence operationsâ??what some term â??nefarious deedsâ?•â??represent perhaps the most difficult hybrid warfare component to quantify. Democratic nations face constitutional, legal, and moral constraints that authoritarian adversaries exploit systematically.

Recent European incidents illustrate adversary capabilities: Bulgarian artillery plant fires and manager assassinations, Swedish telecommunications tower sabotage, and targeted recruitment operations against defense industry executives. These operations demonstrate sophisticated networks capable of sustained, coordinated activities across multiple nations.

American legal and political barriers limit comparable capabilities. The departure of experienced CISA leadership has affected state-level cybersecurity programs, while offensive cyber planning faces bureaucratic and constitutional constraints. Meanwhile, adversaries weaponize diaspora communities, requiring businesses to cooperate with intelligence services by lawâ??activities that would violate American civil liberties protections.

Developing Quantification Frameworks

Effective hybrid warfare assessment requires moving beyond traditional measures to incorporate â??discountâ?• and â??maximizationâ?• factors:

Discount Factors represent the constraints that reduce theoretical capabilities in practical application. Agility coefficients measure how rapidly organizations can adapt to evolving threats, with authoritarian systems often demonstrating superior responsiveness due to centralized decision-making structures. Constitutional constraints encompass the legal and moral limitations that democratic nations impose on power projection activities, creating operational boundaries that adversaries exploit systematically. Bureaucratic friction captures the coordination challenges inherent in democratic governance, where multiple agencies must align priorities and resources across complex institutional landscapes. Political will assessments evaluate the sustained commitment necessary for long-term hybrid operations, recognizing that democratic leadership changes can disrupt multi-year strategic initiatives.

Maximization Factors identify capabilities that amplify limited resources through strategic leverage. Alliance relationships enable nations to access partner capabilities that compensate for individual limitations, though coordination complexity can reduce effectiveness without proper integration frameworks. Private sector cooperation determines how effectively governments can mobilize commercial capabilities for national security objectives, with democratic market economies potentially offering advantages if properly coordinated. Technological integration measures the speed at which innovations translate into operational capabilities, highlighting the importance of agile acquisition processes and industry partnerships. Cultural resonance evaluates narrative effectiveness across target populations, recognizing that authentic cultural connections often prove more influential than sophisticated propaganda campaigns.

For example, NATO Europe spends three times Russiaâ??s defense budget but achieves disproportionately limited results due to traditional capability focus and coordination challenges. Conversely, adversaries maximize limited resources through unified command structures and fewer operational constraints.

Strategic Implications

Current hybrid warfare dynamics suggest adversaries already perceive themselves at war while democracies debate definitions. This asymmetry provides first-mover advantages in gray zone competition. The challenge involves developing response capabilities that maintain democratic values while effectively competing in hybrid domains.

Several priorities emerge:

Institutional coordination represents perhaps the most fundamental challenge facing American hybrid warfare responses. The United States government currently operates without master coordinators capable of aligning investments across agencies toward coherent strategic objectives. This fragmentation becomes particularly problematic in hybrid warfareâ??s cross-domain nature, where cyber operations, information campaigns, economic measures, and diplomatic initiatives must work synergistically rather than independently. NATO analysis emphasizes that effective countering of hybrid threats requires coordinated approaches involving all government sectors, while Atlantic Council experts warn that uncoordinated responses are ineffective ones. The challenge extends beyond traditional inter-agency cooperation to encompass coordination between federal, state, and local levels, as hybrid threats increasingly target sub-national vulnerabilities that federal agencies cannot address alone.

Private sector engagement offers significant untapped potential for hybrid warfare competition, but current frameworks inadequately balance commercial interests with national security priorities. Recent sanctions cooperation following Russiaâ??s invasion of Ukraine demonstrated remarkable private sector responsiveness, with major US corporations like Apple, Microsoft, McDonaldâ??s, and Starbucks voluntarily withdrawing from Russian markets despite significant financial costs. This unprecedented level of corporate cooperation occurred under exceptional circumstances that may not replicate for other adversaries or scenarios. Democratic nations must develop sustainable partnership models that leverage private sector capabilities without compromising market principles or creating government dependencies that undermine economic competitiveness.

Legal framework adaptation presents a fundamental tension for constitutional democracies competing in hybrid warfare domains. Current legal authorities often prove inadequate for addressing threats that exploit democratic openness while operating below traditional warfare thresholds. The challenge involves developing new authorities that enable effective responses while preserving civil liberties that define democratic governance. This balance ultimately determines whether democratic governance represents a strategic advantage through legitimacy and societal resilience, or a vulnerability through operational constraints that adversaries systematically exploit.

Measurement and assessment capabilities remain underdeveloped across hybrid warfare domains, limiting policymakersâ?? ability to evaluate progress or allocate resources effectively. Without quantifiable metrics, strategic decisions rely on intuition rather than evidence, potentially misallocating resources or missing critical vulnerabilities. Developing comprehensive hybrid warfare assessment frameworks requires accepting imperfect measures while building analytical capabilities for systematic evaluation. This challenge extends beyond measurement to encompass attribution difficulties, where adversary activities often involve multiple actors and plausible deniability that complicates response calculations. Recent CISA leadership departures illustrate how institutional disruption can undermine assessment capabilities, with over 1,000 staff departing the agency at a critical time when cyber threats from adversaries are escalating.

Conclusion

The hybrid Cold War is not theoreticalâ??it represents current reality. Adversaries systematically exploit democratic vulnerabilities while building capabilities across multiple domains simultaneously. American responses remain fragmented, lacking comprehensive frameworks for understanding, measuring, and competing in gray zone conflicts.

Moving forward requires abandoning comfortable binary distinctions between war and peace, conventional and irregular warfare. Instead, analysts must develop frameworks that quantify hybrid capabilities, measure competitive balances, and guide strategic responses. The alternative â?? continued reactive postures in an increasingly contested gray zone â?? risks strategic defeats without conventional battles.

The framework proposed here represents a starting point, not a destination. Effective hybrid warfare competition demands continuous adaptation, measurement refinement, and strategic innovation. Most importantly, it requires acknowledging that in hybrid warfare, as in conventional conflict, the enemy gets a voteâ??and they have already begun casting theirs.

About the Authors

Michael S. Groen

Lieutenant General Michaelâ?¯S.â?¯Groen is a retired U.S. Marine Corps officer with a 36-year career who culminated his service as Director of the Pentagonâ??s Joint Artificial Intelligence Center â?? after previously holding senior intelligence leadership roles in the Intelligence Community and the Joint Staff

â?? and is now a recognized technology and national security advisor.

Andrew Borene

Mr. Andrewâ?¯Borene is Executive Director at Flashpoint. A former senior intelligence professional at the Office of the Director of National Intelligence and the National Counterterrorism Center, he previously served as an associate deputy general counsel at the Pentagon and as a Marine Officer. A Certified Information Systems Security Professional and attorney, he is a regular broadcast media analyst and keynote speaker on geopolitical risk.

Doug Livermore

Doug Livermore is the Director of Engagements for the Irregular Warfare Initiative, a member of the Atlantic Councilâ??s Counterterrorism Group, the national vice president for the Special Operations Association of America, national director for external communications at the Special Forces Association, and the deputy commander for Special Operations Detachmentâ??Joint Special Operations Command in the North Carolina Army National Guard. A former senior government civilian, intelligence officer, and contractor in various roles at the Office of the Secretary of Defense, Department of the Navy, and Department of the Army.

This article was originally published by Small Wars Journal

Date Created
2025/07/09