ARTICLES

Hybrid Warfare in the Grey Zone: Strategy, Systems, and Statecraft in Contemporary Conflict

Author: Violina Sarmah • **Published:** February 02, 2026 • **Source:** Centre for New Age Warfare Studies



Understanding Hybrid Warfare in the Grey Zone

Hybrid Warfare (HW) has been conceptualized as a fluid and evolving form of conflict that transcends traditional dichotomies between peace and war, or conventional and irregular warfare.[i] Emerging from analyses of both non-state and state actors, HW describes the integration of military and non-military instruments, political, economic, informational, and civilian to exploit the vulnerabilities of a target system. While the concept lacks definitional clarity, it remains valuable for understanding twenty-first-century security challenges, particularly the blurred boundaries between kinetic and cognitive domains of war. Initially applied to non-state actors like Hezbollah, HW has evolved to describe state behavior, notably Russia's operations in Ukraine and China's "Three Warfares" doctrine, where ambiguity, plausible deniability, and synchronization of instruments of power become strategic tools. HW as a multi-dimensional system operating across vertical (intensity) and horizontal (domain) axes, enabling actors to escalate or de-escalate conflict while staying below the threshold of open war. This approach shifts the tactics by targeting perception, legitimacy, and decision-making rather than physical destruction, making hybrid warfare a contest over influence rather than territory. HW not as a substitute for traditional warfare but as a conceptual lens that compels states to rethink strategy, deterrence, and resilience in an era of permanent, multidomain competition[ii]

While the term gained prominence after Russia's 2014 annexation of Crimea, its strategic logic is neither novel nor confined to modern conflicts.[iii] Hybrid warfare is best understood as the coordinated use of conventional and irregular forces, combined with non-military instruments such as cyber operations, disinformation, and economic coercion, to achieve political objectives below the threshold of declared war. Drawing from Russia's "new generation warfare," Wither emphasizes the centrality of *information superiority* and *psychological warfare* tools that shape perception and will rather than battlefield outcomes. This mode of warfare, built upon Soviet-era doctrines like *maskirovka* (deception) and *reflexive control* (perception management), allowed Russia to manipulate adversaries' decision-making processes and create ambiguity that paralyzes NATO's response. He also highlights parallels between Russia's model and China's "Unrestricted Warfare" and "Three Warfares" doctrines, both of which blend economic, legal, and informational tactics to circumvent Western military strength. For policymakers, the challenge lies in distinguishing between normal geopolitical competition and hybrid aggression coordinated with the threat or use of force, as overextension of the term risks turning all conflict into "war."[iv]

Hybrid Warfare as a Multidomain System

Hybrid warfare confounds Western binary thinking by operating in the "grey zone," where deterrence and diplomacy overlap.[v] To counter such threats, there is a need of paradigm shift from traditional military superiority to societal *resilience*, the capacity to absorb, adapt, and recover from hybrid attacks through integrated civil-military coordination. For Giegerich, hybrid warfare is the "evil twin" of NATO's comprehensive approach; both require the synchronization of political, informational, economic, and military instruments, but where hybrid actors exploit seams between these domains, NATO must learn to close them. He concludes that hybridity is now a structural feature of conflict, one that demands flexible, networked defense strategies rather than rigid military doctrines.[vi]

Information Warfare and Influence Operations

The theoretical understanding of hybrid warfare is expanded by placing technology and cyber operations at its core. The rapid evolution of information and communication technologies has transformed not only the tools but also the *philosophy* of conflict, blurring the line between kinetic and cognitive domains.[vii] Unlike earlier Western conceptions that emphasize "gray zone" ambiguity or the Gerasimov doctrine,[viii] hybrid war is now a high-tech, system-based strategy aimed at achieving strategic stand-off through the coordinated use of cyber aggression, information operations, and social manipulation. Hybrid warfare seeks not territorial occupation but the destabilization of a state's internal systems its economy, governance, public trust, and digital infrastructure through cascading effects on critical nodes.[ix] Though conflicts represent a paradigm shift; wars are increasingly fought through *technological ecosystems* rather than battlefields. The response must include not only military modernization but the creation of national cyber-defense and information-resilience architectures. Their analysis thus situates hybrid warfare as both an outcome of technological acceleration and a warning that future conflicts will be waged through 'code, cognition, and connectivity' as much as through force.[x]

Hybrid Warfare and Cyber Operations

China's strategic behavior operates in the *gray zone* which is a continuum of competition below the threshold of open conflict. Hybrid operations cannot be cleanly separated from China's broader civil and economic statecraft because infrastructure projects, trade coercion, cyber intrusions, and disinformation campaigns often function as coordinated instruments of influence.[xi] This hybridity is traced from early efforts like Confucius Institutes and the Belt and Road Initiative to more aggressive measures in the South China Sea, cyber espionage, and pandemic-related propaganda.[xii] By juxtaposing these with U.S. and Russian doctrines from Hoffman's "hybrid war"[xiii] and Gerasimov's "non-linear

warfare"[xiv] to the U.S. Army's "multi-domain operations," China's version of hybrid warfare merges ideological legitimacy with technological and informational dominance.[xv] There are no fixed rules defining gray zone competition; rather, it is a fluid strategy of continuous statecraft. For policymakers, the report serves as a caution that China's hybrid operations function as a grand strategic enterprise blending persuasion, coercion, and denial to reshape the international order without firing a shot.

Cyber Escalation and Narrative Warfare: Taiwan and US–China

Recent developments underscore how China's hybrid and gray-zone strategies continue to evolve in the digital domain. According to Taiwan's National Security Bureau, Chinese cyberattacks on Taiwanese government departments have risen by 17 percent in 2025, averaging 2.8 million attacks per day. These intrusions target medical, defence, telecommunications, and energy systems, combining data theft with disinformation operations that use dark-web networks, online forums, and coordinated "troll armies" to undermine public confidence in state institutions. The report highlights how Beijing's cyber operations no longer serve only intelligence or espionage functions; they form part of a larger strategy of *psychological destabilization* a hallmark of hybrid warfare. By blending cyber aggression with propaganda and economic coercion, China sustains constant pressure on Taipei while remaining below the threshold of conventional conflict.[xvi] The intensifying cycle of mutual cyber accusations between Beijing and Washington further illustrates how hybrid warfare has become embedded in great power relations. In October 2025, China's Ministry of State Security accused the U.S. National Security Agency of infiltrating the National Time Service Center, a critical infrastructure unit responsible for maintaining China's standard time network. According to Beijing, the alleged U.S. operation exploited software vulnerabilities in mobile devices and internal messaging systems to conduct prolonged espionage, potentially disrupting financial, communication, and energy grids. The U.S. embassy in Beijing responded by counter-accusing China of orchestrating extensive cyber intrusions into American and global telecommunication networks. This exchange reveals the *reciprocal narrative warfare* that now defines Sino-American cyber competition each state weaponizes the language of sovereignty, security, and technological dependence to justify its digital operations. Such cyber confrontations operate firmly within the hybrid warfare paradigm; they target systems and perceptions rather than territory, blur the distinction between espionage and aggression, and escalate competition while avoiding open conflict. The dispute also demonstrates how cyber domains intersect with economic and geopolitical tensions, particularly amid ongoing trade frictions and resource-security rivalries such as rare-earth export controls.[xvii]

Economic and Regulatory Instruments of Hybrid Warfare

The United States' recent decision to expand restrictions on Chinese telecommunications equipment highlights how hybrid warfare now unfolds through economic regulation and technology governance. In October 2025, the Federal Communications Commission (FCC) unanimously voted to block new approvals for devices incorporating components from firms on its "Covered List," including Huawei, ZTE, China Mobile, and China Telecom. The agency also moved to revoke authorizations for previously approved equipment, citing risks of espionage and systemic vulnerability. The measure follows a broader campaign to remove millions of prohibited Chinese electronics from security cameras to smart watches from U.S. online marketplaces. This regulatory escalation reflects Washington's shift toward defensive hybrid deterrence, wherein the boundary between national security and market oversight blurs. By treating technology supply chains as potential instruments of coercion, the FCC's actions effectively transform administrative policy into a form of strategic containment. Chinese companies such as Hikvision and Dahua denounced the decision as politically motivated and economically harmful, revealing the contested narratives that surround hybrid economic warfare.[xviii]

Conclusion: Hybrid Warfare as a Permanent Feature of International Relations

Recognizing hybrid warfare as something that fits in the grey area between war and peace is important to properly understanding hybrid warfare. Hybrid warfare encompasses the use of armed and unarmed state actors, cyber, intelligence, finance, diplomacy, and economics through multiple domains of warfare including asymmetrical warfare or lawfare. The examples presented in this research support the idea that the use of hybrid warfare is an effective means of fulfilling a nation's political agenda without crossing the threshold of war as defined by international law.

The three most significant variables of hybrid warfare are the use of influence over land, the importance of power and influence with major nations and the increased use of information technologies. In the case of Russia, the use of information as a means of exercising influence was demonstrated through the media and through cyber operations to steal sensitive information from state and military officials, manipulate the perceptions of citizens within a country and disrupt any efforts to challenge the use of hybrid warfare by Russia. The integration of economic, technological and informational tools used by China clearly illustrates how hybrid warfare can be used to create an international competitive environment. The growing cyber and regulatory confrontations between the various major powers illustrate how much of hybrid warfare relies on exploiting the systemic weaknesses of other major nations through a combination of both technology and the digital infrastructure of cyber warfare.

For policy makers it is of importance that military power alone cannot effectively combat hybrid threats. In order to cope with these threats, it will be necessary to employ a combination of military and civilian actions and to have viable political institutions and economic institutions supported by both military and civilian authorities. Acknowledging that hybrid warfare is now a standard part of international relations, instead of only occurring occasionally will allow for a more rational analysis of the security concerns currently facing the world today.

End Notes:

[i] Reichborn-Kjennerud, Erik, and Patrick Cullen. *What is Hybrid Warfare?* Norwegian Institute for International Affairs (NUPI), Policy Brief No. 1/2016. Oslo: NUPI, 2016.

[ii] Reichborn-Kjennerud, Erik, and Patrick Cullen. *What is Hybrid Warfare?* Norwegian Institute for International Affairs (NUPI), Policy Brief No. 1/2016. Oslo: NUPI, 2016.

[iii] Wither, James K. *Making Sense of Hybrid Warfare. Connections: The Quarterly Journal*, Vol. 15, No. 2 (Spring 2016): 73–87. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2016.

[iv] Wither, James K. *Making Sense of Hybrid Warfare. Connections: The Quarterly Journal*, Vol. 15, No. 2 (Spring 2016): 73–87. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2016.

[v] Giegerich, Bastian. *Hybrid Warfare and the Changing Character of Conflict. Connections: The Quarterly Journal*, Vol. 15, No. 2 (Spring 2016): 65–72. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2016.

[vi] Giegerich, Bastian. *Hybrid Warfare and the Changing Character of Conflict. Connections: The Quarterly Journal*, Vol. 15, No. 2 (Spring 2016): 65–72. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2016.

[vii] Danyk, Yuriy, Tamara Maliarchuk, and Chad Briggs. *Hybrid War: High-tech, Information and Cyber Conflicts. Connections: The Quarterly Journal*, Vol. 16, No. 2 (Spring 2017): 5–24. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2017.

[viii] General Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," Voyenno-Promysh-lennyy Kurier online, 26 February 2013, http://vpk-news.ru/articles/14632

[ix] Danyk, Yuriy, Tamara Maliarchuk, and Chad Briggs. *Hybrid War: High-tech, Information and Cyber Conflicts. Connections: The Quarterly Journal*, Vol. 16, No. 2 (Spring 2017): 5–24. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2017.

[x] Danyk, Yuriy, Tamara Maliarchuk, and Chad Briggs. *Hybrid War: High-tech, Information and Cyber Conflicts. Connections: The Quarterly Journal*, Vol. 16, No. 2 (Spring 2017): 5–24. Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, 2017.

[xi] Cordesman, Anthony H., and Grace Hwang. *Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations.* Center for Strategic and International Studies (CSIS), Working Draft, June 15, 2020.

[xii] Cordesman, Anthony H., and Grace Hwang. *Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations.* Center for Strategic and International Studies (CSIS), Working Draft, June 15, 2020.

[xiii] 1 Frank G. Hoffman, "Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict," *Armed Forces Journal*, October 1, 2009, http://armedforcesjournal.com/hybrid-vs-compound-war/.

[xiv] General Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," Voyenno-Promysh-lennyy Kurier online, 26 February 2013, http://vpk-news.ru/articles/14632

[xv] Cordesman, Anthony H., and Grace Hwang. *Chronology of Possible Chinese Gray Area and Hybrid Warfare Operations.* Center for Strategic and International Studies (CSIS), Working Draft, June 15, 2020.

[xvi] Reuters. *"Taiwan Flags Rise in Chinese Cyberattacks, Warns of 'Online Troll Army'."* October 14, 2025.

[xvii] Reuters. *"China Accuses U.S. of Cyber Breaches at National Time Centre."* October 19, 2025.

[xviii] Reuters. *"U.S. Agency Votes to Tighten Restrictions on Chinese Tech Companies Deemed Threats."* October 28, 2025.

The views expressed are those of the authors and do not represent the views of CNAWS.