
BOOK REVIEW

Hybrid Warfare: Security and Asymmetric Conflict in International Relations

Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per
Thunholm (Eds) (I.B. Tauris, 2021), 314



Hybrid Warfare: Security and Asymmetric Conflict in International Relations

Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm (Eds) (I.B. Tauris, 2021), 314

In recent years, hybrid threats and warfare have increased the grey zone of war and peace. The security challenges arising from such threats are high on the global security agenda. The book *“Hybrid Warfare: Security and Asymmetric Conflict in International Relations,”* edited by Weissmann et al., attempts to identify the existing tools for countering hybrid threats by providing the analysis of both practitioners and scholars. It comprises seventeen chapters. Apart from an introductory chapter, the book has four parts: (i) the view of practitioners, (ii) tools and means, (iii) cases, and (iv) conclusions. Moreover, it focuses on the challenges posed by hybrid threats and warfare to the Western world and highlights their ability to deal with them.

The authors argue in the introductory chapter that hybrid threats and warfare are overlapping concepts. Russia, China, Iran, North Korea, and non-state actors such as ISIS and Hezbollah are considered challengers to the global hegemony of the West. The West is countering the challenges of hybrid warfare and identifying and addressing its vulnerabilities.

The book’s first part consists of three chapters and broadly discusses NATO, the US, and the EU’s perspectives on hybrid warfare. In the context of NATO, Alexander Crowther has noted that NATO Wales Summit Declaration in 2014 highlighted the significance of necessary tools and procedures to respond to hybrid threats. That NATO faced hybrid challenges from Russia and took several actions to counter them, including collaboration with allies, use of media and other information tools to minimize support for Russia and maximize support for NATO, and preparing for the defense of allies under Article 5 of the North Atlantic Treaty.

In the context of the US, this part takes a closer look at the means available in the US to devise a robust response to hybrid warfare. It underscores that the new elements in hybrid threats, such as cyber

and social media, help disseminate propaganda relatively cheaply than other tactics. While discussing the EU's perspective on hybrid warfare in chapter four, "A Perspective on EU Hybrid Threat Early Warning Efforts," Patrick Cullen argues that the Ukraine crisis has influenced the EU's engagement with hybrid warfare. This part also focuses on developing the EU hybrid threat early warning and detection mechanisms proposed and implemented by the European External Action Service (EEAS) and its Hybrid Fusion Cell.

Part two of the book comprises six chapters and explores five main themes: (i) conceptualizing and countering hybrid warfare, (ii) the role of the military in the grey zone, (iii) Russia and China's perspectives on hybrid warfare, (iv) modern information environment, and (v) intelligence cooperation in the context of the role of the military against hybrid scenarios. In chapter five, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare: The Role of the Military in the Grey-zone," Mikael Weissmann stresses that the military's role in the grey zone must be recognized and employed efficiently, while also ensuring that democratic norms are maintained. While highlighting the viewpoint of Russian academics on hybrid warfare, he mentions that the West is engaged in non-military subversive campaigns against Russia for regime change or to reshape Russian national identity to advance Western interests.

While underlining the viewpoint of Chinese academics on hybrid warfare in chapter seven, "China and its Hybrid Warfare Spectrum," Dr Lora Saalman writes that most Chinese scholars cite the US as the origin point of hybrid warfare during the 1980s and 1990s. The US had orchestrated military operations, color revolutions, and regime changes, which impacted countries such as former Czechoslovakia, Iraq, Syria, Iran, Yemen, Libya, Kosovo, Venezuela, and Georgia. The author highlights that according to Chinese academics, "Washington coined the concept of hybrid warfare, and Moscow perfected it." This part also stresses that the modern information environment has brought new opportunities and vulnerabilities for states.

In the context of intelligence cooperation, Henrik Häggström explains in chapter nine, "Hybrid Threats and New Challenges for Multilateral Intelligence Cooperation," that since 9/11, multilateral intelligence cooperation has increased internationally. He notes that NATO, the EU, and the UN have launched several intelligence initiatives in the past years to improve their capacity to address hybrid threats effectively. This section underscores the combination of poorly designed systems and new technologies broadening global cyber threats' extent and severity.

Part three of the book contains six chapters based on case studies related to the US, China, the Baltic states, Ukraine, Iran, and Catalonia. In the context of the US, Jed Willard traces the history of US hybrid engagement from the Revolution (1775) to the end of the Cold War (1991). This part discusses the US's current and future hybrid challenges and potential capacity in the hybrid domain. While discussing the case study of China, Dr Gulizar Haciyakupoglu argues that some features of China's political warfare are unique to Taiwan, mainly in the historical, cultural, and asymmetric military context.

The third case study in this section deals with the Baltic states, in which Dr Dorthe Bach Nyemann has presented three components related to hypothetical Russian hybrid operations in the Baltic states: (i) Russia's capabilities to operate as a hybrid actor, (ii) Russia's chances of success in implementing a hybrid warfare strategy, and (iii) Russia's interests and goals in the Baltic states.

In the case study of Ukraine, Niklas Nilsson assesses key features of Ukraine's response to Russian hybrid strategy after the annexation of Crimea. The author notes that Ukraine launched a strategic information campaign to promote its narrative of the conflict. In the context of Iran, Rouzbeh Parsi explains Iran's understanding of hybrid warfare and its capability to carry out hybrid operations. The last case study deals with Catalonia, where Ruben Arcos explains that the Catalonian issue demonstrates how disinformation activities can exploit existing vulnerabilities in political and social cohesion.

Part four of the book is based on the concluding chapter, where Dr Mikael Weissmann, Dr Niklas Nilsson, and Björn Palmertz suggest the "Hybridity Blizzard Model" as a novel way to understand the dynamics of hybrid threats and their countermeasures. The authors have also emphasized collaboration among military, political, economic, civilian, and informational spheres and across the public and private sectors, from the local and regional to national and international levels.

The book is a timely contribution to security studies and hybrid warfare. The essays in the volume can help identify, analyze, and counter hybrid threats and warfare. However, the book mainly emphasizes the Western threat perception in the context of hybrid warfare but does not discuss hybrid challenges posed by Western countries for their rivals.

Reviewed by Farzana Wahid Buksh, MPhil scholar of International Relations at the University of Karachi.