Defining HYBRID WARFARE

By **JAMES K. WITHER**

Following the Russian Federation's invasion of Crimea in March 2014, hybrid warfare ceased to be a subject studied only by military strategists and entered the wider policy domain as a significant security challenge for the West. The term hybrid warfare attempts to capture the complexity of 21st-century warfare, which involves a multiplicity of actors, blurs the traditional distinctions between types of armed conflict, and even between war and peace. Although hybrid warfare is a Western term, not Russian, all sorts of hostile Russian activities — from the covert use of special forces to election manipulation and economic coercion — have been labeled hybrid and caused growing alarm in Western security establishments. There are many definitions of hybrid warfare and these definitions continue to evolve. Defining hybrid warfare is not just an academic exercise because these definitions may determine how states perceive and respond to hybrid threats and which government agencies are involved in countering them.

Russian President Vladimir Putin speaks at a concert in Crimea's regional capital of Simferopol in March 2019. Putin has used a full arsenal of hybrid warfare tools to advance Russia's interests in the region. GETTY IMAGES

Historians have used the term hybrid warfare simply to describe the concurrent use of conventional and irregular forces in the same military campaign. Peter R. Mansoor, for example, defined hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents and terrorists), which could include both state and nonstate actors, aimed at achieving a common political purpose." These characteristics have been typical of wars since ancient times. From a historical perspective, hybrid warfare is certainly not a new phenomenon. In the 2000s, the use of the term hybrid became a common way to describe the changing character of contemporary warfare, not least because of the increasing sophistication and lethality of violent nonstate actors and the growing potential of cyber warfare. Definitions of hybrid warfare emphasized the blending of conventional and irregular approaches across the full spectrum of conflict. Writing in 2007, Frank Hoffman defined hybrid warfare as "different modes of warfare

including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of nonstate actors." The integration of conventional and irregular methods of warfare arguably distinguished such hybrid wars from their historical forms. Traditionally, conventional and irregular operations tended to take place concurrently, but separately, and operations by irregular fighters were normally secondary to campaigns by conventional military forces. Before 2014, military analysts considered the brief war between Israel and Hezbollah in 2006 as the conflict that most fitted contemporary definitions of hybrid war. Hezbollah surprised the Israel Defense Forces with its sophisticated combination of guerrilla and conventional military tactics and weaponry as well as its effective strategic communication campaign.

Police in Ukraine stand guard near a "green men" symbol drawn by anti-Russia activists on the wall of a bank in Kyiv in 2014. Prosecutors suspect the bank was used to fund pro-Moscow activities. Green men refers to the camouflaged gunmen sent to Crimea as part of Russia's hybrid assault. AFP/GETTY IMAGES

Hybrid warfare is by its very nature asymmetrical. U.S. military analysts use the term asymmetrical warfare to describe the strategies and tactics of state and nonstate opponents of the United States seeking to advance their strategic objectives despite its superior conventional military power. Asymmetrical methods of warfare, essentially pitting one's strengths against another's weaknesses, have always been a feature of successful strategy. Asymmetry naturally includes nonkinetic approaches that exploit the gray area between war and peace. However, the impact of emerging information technology allows state and nonstate actors to target decision-makers and the public through the globalized, networked media and the internet. This potentially widens the concept of war to include cultural, social, legal, psychological and moral dimensions where military power is less relevant.

Russia's actions in Ukraine in 2014 created the current preoccupation with hybrid warfare. Western commentators used hybrid as the most appropriate term to describe the variety of methods employed by Russia during its annexation of Crimea and support to rebel militant groups in eastern Ukraine. Russian techniques included the traditional combination of conventional and irregular combat operations, but also the sponsorship of political protests, economic coercion, cyber operations and, in particular, an intense disinformation campaign. The 2015 edition of *The Military Balance* provided arguably the most comprehensive definition of the latest manifestation of hybrid warfare: "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." This definition of hybrid warfare differs from those discussed earlier because it emphasizes nonmilitary methods of conflict and, in particular, information warfare that targets public perception, a key center of gravity in contemporary conflict.

Use of weaponized information is the most distinguishing feature of Russia's campaign in 2014 and its more recent efforts to divide and destabilize Western states. The Russian approach to information warfare combines psychological and cyber operations, which are critical components of what Russian analysts, most notably Chief of the General Staff Gen. Valery Gerasimov, have called new generation or nonlinear warfare. Russian information warfare seeks to blur the lines between truth and falsehood and create an alternative reality. It exploits existing societal vulnerabilities in target states, attempts to weaken state institutions and undermine the perceived legitimacy of governments. New generation warfare emphasizes the use of nonkinetic techniques that promote social upheaval and create a climate of collapse, so that little or no military force is necessary. The armed forces have a supplementary role in this strategy. Special forces may conduct reconnaissance, subversion and espionage while, if necessary, large-scale conventional military exercises close to a target state's borders seek to coerce and intimidate. Ideally, the use of armed force remains below the threshold that might trigger a conventional military response. Latvian analyst Jānis Bērziņš summarizes the Russian approach to modern warfare: "The main battlespace is in the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare. ... The main objective is to reduce the necessity for deploying hard military power to the minimum necessary."

In many respects, Russian methods date back to the Soviet era and the application of *maskirovka* — military deception. Advances in information technology

and processing have greatly increased the scope of maskirovka, allowing the Russian government to employ multimedia propaganda and misinformation on a massive scale. The concept of "reflexive control" (perception management) is a key element of maskirovka. This concept, which originated with the work of Soviet psychologist Vladimir Lefebvre, employs specially prepared information that inclines an opponent to make decisions that have been predetermined as desirable by the initiator of the information. Reflexive control methods include blackmail, camouflage, deception and disinformation, all intended to interfere with an opponent's decision-making cycle in a way favorable to Russian policy.

Russia is not the only state to exploit hybrid forms of warfare. China has studied so-called unrestricted warfare methods since the late 1990s. Unrestricted warfare techniques include computer hacking and viruses, subversion of the banking system, market and currency manipulation, urban terrorism and media disinformation. The extent to which unrestricted warfare has become official Chinese doctrine is not clear, although elements of the concept are evident in China's "Three Warfares" policy regarding its territorial claims in the East and South China seas. China has avoided the overt use of military force, but has exploited psychological operations, media manipulation and legal claims (lawfare) to advance its objectives.

Like the planners of unrestricted warfare, Russian analysts make no secret that their objective is to counter perceived overweening U.S. power. Russian commentators and analysts claim that Russia has remained under sustained and effective information attack by the U.S. since the end of the Cold War. From a Russian perspective, events such as perestroika and the "color revolutions," as well as multilateral organizations such as the International Monetary Fund and World Bank, are instruments of hybrid warfare intended to destabilize Russia. Russian President Vladimir Putin has even accused the U.S. of seeking to undermine the Russian state's core identity and values. Certainly, the U.S. and its close allies engaged in political warfare against the Soviet Union in the Cold War, using propaganda and psychological operations akin to those of contemporary hybrid warfare, but these operations were discontinued after the Soviet Union collapsed.

It has been long-standing Russian policy to seek ways to weaken, divide and ultimately neutralize NATO. The security of the Baltic states, with their significant Russian-speaking minorities, is of particular concern because the countries border Russia, and these minorities potentially provide Putin with leverage to create problems for the Alliance. Other countries on NATO's periphery are also vulnerable to Russian influence. There are fears that Bulgaria, for example, may be susceptible to state capture by criminal organizations linked to Russian intelligence agencies. NATO has recognized its vulnerability to Russian hybrid warfare techniques and has stationed forces in the most vulnerable countries to reassure member governments and bolster military deterrence. Alliancewide efforts have been made to identify and counter Russian cyber and information operations through new initiatives such as the Counter Hybrid Support Teams, established in 2018. Nordic states have embraced or revived whole-of-society or total-defense concepts. For example, Estonia's National Defence Concept of 2017 addresses psychological, civil and economic defensive measures as well as military preparedness. Since its Warsaw summit in 2016, NATO has put renewed emphasis on civil preparedness to boost member-state population and institutional resilience through collaboration between government ministries, civic organizations, the private sector and the public. Awareness of Russian information warfare has made governments, publics and, critically, social media companies less susceptible to disinformation and deception. This mindfulness should prevent Russian intelligence services from effective influence operations, such as their interference in the U.S. election in 2016.

Gen. Valery Gerasimov, Russia's first deputy defense minister and chief of the general staff of the Russian Armed Forces, arrives for a Victory Day parade in Moscow in May 2019. REUTERS

Hybrid warfare does not change the nature of war. Coercion remains at the core of hybrid warfare as it does any form of war. The aim remains the same, namely to gain physical or psychological advantage over an opponent. It is undoubtedly a challenge for national security establishments to address the wide range of threats that can be labeled hybrid warfare. Cast the definitional net too wide and hybrid warfare becomes too broad a term to be of any practical use to policymakers. Define warfare too narrowly and officials may fail to appreciate the significance of nontraditional techniques of warfare employed by an adversary as a prelude to the use of direct military force. □