Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

James K. Wither, *Connections QJ* 15, no. 2 (2016): 73-87
http://dx.doi.org/10.11610/Connections.15.2.06

Research Article

Making Sense of Hybrid Warfare

James K. Wither

George C. Marshall European Center for Security Studies, http://www.marshallcenter.org

Abstract: The term hybrid warfare has been widely analyzed by scholars, policymakers and commentators since Russia occupied Crimea in March 2014. The topic has ceased to be a subject only studied by military strategists, but has entered the wider policy domain as a significant security challenge for the West. This article seeks to place the debate about hybrid warfare in a broader analytical and historical context and summarizes discussion to date on this and related strategic concepts. The Russian approach to hybrid warfare as demonstrated by operations in Ukraine is a particular focus for discussion.

Keywords: Warfare, Strategy, Russian Federation, NATO, European Security.

Introduction

Since the Russian Federation invaded Crimea in March 2014, analysis and commentary on the concept of hybrid warfare have increased exponentially.[1] An Internet search will identify hundreds of entries covering the phenomenon.

[1] Recent analyses include: Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks* (blog), 28 July 2014, http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats (accessed 8 December 2015); Max Boot, "Countering Hybrid Warfare," in *Armed Conflict Survey 2015*, ed. Nigel Inkster (London: IISS, 2015); Ralph D. Thiele, "Crisis in Ukraine – The Emergence of Hybrid Warfare," *ISPSW Strategy Series*, May 2015; Rod Thornton, "The Changing Nature of Modern Warfare," *RUSI Journal* 160:4 (2015): 40–48; Lawrence Freedman, "Ukraine and the Art of Limited War," *Survival* 56:6 (2014): 7–38; Michael Kofman and Matthew Rojansky, "Kennan Cable No. 7: A Closer Look at Russia's Hybrid War," *Wilson Center*, 14 April 2015, https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war (accessed 8 December 2015).

Hybrid warfare has become the most common term used to try and capture the complexity of twenty-first-century warfare, which involves a multiplicity of actors and blurs the traditional distinctions between different types of armed conflict and even between war and peace. Hybrid warfare has ceased to be a topic only for military strategists, as it has now entered the broader public domain and become a major security concern for Western governments. Both NATO and the European Union (EU) are working on strategies to strengthen defensive capabilities and prevent hybrid attacks.

This article seeks to clarify the different ways in which the term hybrid warfare and related terms have been used by scholars and policy analysts and summarize discussion on the topic to date. The paper will examine, in particular, the Russian approach to hybrid warfare as demonstrated by operations in Ukraine and will briefly assess the significance of these developments for Western security policy.

Defining Hybrid Warfare

Not surprisingly, there are many definitions of hybrid warfare. The concept has been delineated in different, if related, ways and these definitions have evolved in a relatively short period of time. Defining hybrid warfare is not just an academic exercise. The way the term is defined may determine how states perceive and respond to hybrid threats and which government agencies are involved in countering them.

One approach to hybrid warfare takes an historical perspective. This defines the term simply as the concurrent use of both conventional and irregular forces in the same military campaign. Military historian Peter R. Mansoor, for example, defines hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents, and terrorists), which could include both state and non-state actors, aimed at achieving a common political purpose."[2] Viewed from this perspective, hybrid warfare is clearly nothing new. There are numerous examples of hybrid techniques and approaches at the tactical, operational and strategic levels stretching back at least as far as the Peloponnesian War and the writings of the Chinese philosopher, Sun Tzu, in the fifth century BC. Irregular fighters have proved to be the bane of numerous conventional militaries. Formidable armies such as Napoleon's Grand Armée and Hitler's Wehrmacht struggled to combat irregular fighters who understood and exploited the local human and geographical terrain and targeted vulnerable logistic bases and lines of communication. Over time, guerrilla operations had a significant and lasting impact on the broader conventional military campaigns of which they were part. Recent counter insurgency (COIN) campaigns in Iraq and Afghanistan have once again highlighted the difficulty of defeating de-

[2] Peter R. Mansoor, "Hybrid War in History," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present,* ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012), 2.

termined irregular fighters without committing human rights abuses against the local population and consequently undermining domestic and international public support for the campaign.

During the 2000s, the use of the term "hybrid" became a common way to describe contemporary warfare, particularly because of the increasing sophistication and lethality of violent non-state actors and the growing potential of cyber warfare. Although there was no agreement that this necessarily constituted a new form of warfare,[3] definitions of hybrid warfare emphasized the blending of conventional and irregular approaches across the full spectrum of conflict. For example, in 2007 Frank G. Hoffman, a leading analyst of the concept, defined hybrid warfare as "Threats that incorporate a full range of 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 non-state actors."[4] During its war with Georgia in 2008, Russia, for example, made use of a combination of regular armed forces, South Ossetian and Abkhazian militias and Russian special operations forces (SOF) operating covertly as "local defense" troops. The mixing of conventional and irregular methods of warfare arguably distinguished such hybrid wars from their historical forms. In the past, conventional and irregular operations tended to take place concurrently but separately, rather than being integrated. In addition, operations by irregular fighters were normally secondary to campaigns by conventional military forces.

Prior to 2014, the conflict between Israel and Hezbollah in 2006 was the most frequently used example of a war that fitted contemporary definitions of hybrid warfare. Hezbollah, which had been trained and equipped by Iran, surprised Israel with its sophisticated combination of guerrilla and conventional military tactics and employed weaponry and communication systems normally associated with the armed forces of developed states. At the strategic level, Hezbollah made effective use of the Internet and other media for information and propaganda. Its information management proved much more successful than Israel's in influencing global opinion from the start of the conflict. As the discussion above illustrates, a hybrid combination of conventional and irregular methods of warfare has been used throughout history. Yet what is apparent from Hezbollah's example and others, including the guerrilla fighters in Chechnya and more recently Islamic State (IS), is that modern weapon systems have greatly increased the lethality of non-state actors. Developments in information technology have also provided these groups with an unprecedented ability to engage in information warfare and compete effectively with states to shape public opinion. The US Quadrennial Defense Review Report in 2010

[3] U.S. Government Accountability Office (GAO), *Hybrid Warfare*, GAO-10-136R (Washington, DC: GAO, 2010), available at http://www.gao.gov/products/GAO-10-1036R (accessed 4 December 2015).

[4] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 8.

acknowledged these changes when it defined hybrid warfare in the following manner: "today's hybrid approaches may involve state adversaries that employ protracted forms of warfare, possibly using proxy forces to coerce or intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states."[5]

Hybrid Warfare Post 2014

As noted above, Russia's actions in Ukraine in 2014 intensified interest in the concept of hybrid warfare. For many Western commentators, "hybrid" appeared to be the best way to describe the variety and blending of tools and methods employed by the Russian Federation during its annexation of Crimea and support to separatist groups in eastern Ukraine. Russian techniques included the traditional combination of conventional and irregular combat operations, but also the support and sponsorship of political protests, economic coercion, cyber operations and, in particular, an intense disinformation campaign. In an interview in July 2014, former NATO Secretary General Anders Fogh Rasmussen described Russian tactics as "hybrid warfare," which he defined as "a combination of military action, covert operations and an aggressive program of disinformation."[6] The 2015 edition of *Military Balance* provides a very comprehensive definition of the latest manifestation of hybrid warfare, highlighting the methods employed, namely "the use of military and non-military 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."[7]

What distinguishes this definition of hybrid warfare from those discussed earlier is the emphasis on non-military methods of conflict and, in particular, information warfare. The employment of coercive information operations is the most distinguishing feature of the recent descriptions of hybrid warfare and allows some comparisons to be drawn between IS's campaigns in the Middle East and the very different war and theater of operations in Ukraine. IS has effectively blended conventional and guerrilla tactics and gross acts of terrorism, but it has also exploited propaganda and information warfare to an unprecedented extent for a non-state actor. Sophisticated social media campaigns have glorified its cause and high-quality visual propaganda has contributed to the

---

5 Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, 2010), 8, http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf (accessed 4 December 2015).

6 Mark Landler and Michael R. Gordon, "NATO Chief Warns of Duplicity by Putin on Ukraine," *The New York Times*, 8 July 2014, www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html (accessed 7 December 2015).

7 "Complex Crises Call for Adaptable and Durable Capabilities," *The Military Balance* 115:1 (2015): 5.

group's ability to recruit thousands of foreign fighters to its ranks. Information warfare was also central to Russia's successful campaign in Crimea in 2014. At the tactical level, electronic warfare (EW) and cyber attacks neutralized the ability of the Ukrainian authorities to respond, while broader media exploitation techniques blurred the lines between truth and falsehood, creating an alternative reality for those observers who accepted the Russian media's view of events. Russia's strategic information campaign in Ukraine sought to exploit existing societal vulnerabilities, weaken government and state institutions and undermine the perceived legitimacy of the Ukrainian state. Like IS, Russia used information operations to influence and shape public perception, a recognition that the latter has become the strategic center of gravity in contemporary armed conflicts.

It is hardly surprising that Russian analysts have argued that information and psychological warfare are the foundations for victory in what they refer to as "new-generation war."[8] A recent NATO Strategic Communications (STRATCOM) Center of Excellence (COE) report on Russian information warfare in Ukraine drew similar conclusions regarding the significance of "information superiority" to Russia's success,[9] while NATO's Supreme Allied Commander Europe (SACEUR), General Philip Breedlove, reflected the consternation felt by many Western officials when he described the Russian campaign as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[10] According to former Russian TV producer Peter Pomerantsev, this "Blitzkrieg" goes much further than historical information warfare operations. He argues that "The new Russia doesn't just deal with the petty disinformation, forgeries, lies, leaks, and cyber-sabotage usually associated with information warfare. It reinvents reality."[11]

Related Theories of Contemporary Warfare

Arguably, the concept of hybrid warfare adds little to the notion of asymmetrical warfare. This term, popularized after the Cold War, sought to characterize

[8] For example, see Sergei G. Chekinov and Sergei A. Bogdanov, "The Nature and Content of New Generation War," *Voyenna Mysl (Military Thought)* 4 (2013): 12-23, http://www.eastviewpress.com/Files/MT_from%20the%20current%20issue_No.4_2013.pdf (accessed 9 December 2015).

[9] NATO Strategic Communications Center of Excellence (StratCom COE), *Analysis of Russia's Information Campaign Against Ukraine* (Riga: NATO StratCom COE, 2014), 4, http://issuu.com/natostratcomcoe/docs/ukraine_research_natostratcomcoe_02 (accessed 15 December 2015).

[10] John Vandiver, "SACEUR: Allies Must Prepare for 'Hybrid Warfare,'" *Stars and Stripes*, 4 September 2015, www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464 (accessed 7 December 2015).

[11] Peter Pomerantsev, "How Russia Is Revolutionizing Information Warfare," *Defense One*, 9 September 2014, http://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635 (accessed 10 December 2015).

the kinds of strategies and tactics employed by state and non-state opponents of the US and its allies to counter the West's overwhelming technological advantages and firepower. These asymmetrical methods could naturally shift into non-military fields expanding the grey area between war and peace that Russia has exploited in Ukraine. However, so-called asymmetrical methods of warfare, essentially pitting one's strengths against another's weaknesses, have always been a feature of successful military strategies. Many of the elements identified as hybrid warfare also appear in discussion of "fourth-generation warfare," a contested theory originating in 1990s.[12] A key concept in fourth-generation warfare is the exploitation of emerging information technology, which allows non-state military actors to erode the will of states to fight by targeting decision-makers and the public through the globalized, networked media and the Internet. Thus, widening a "war" to include cultural, social, legal, psychological and moral dimensions where military power is less relevant.

Recent definitions of hybrid warfare are also similar to the Chinese theory of unrestricted warfare. This concept is discussed at length in the book, *Unrestricted Warfare*, which was published in 1999 by two colonels from the People's Liberation Army (PLA).[13] It proposes methods of warfare to enable countries like China to confront an opponent with superior military technology such as the US. Similar to the concept of hybrid warfare, unrestricted warfare involves the use of a multitude of means, both military and non-military, to strike back at an enemy during a conflict. One of the authors stated in an interview that "the first rule of unrestricted warfare is that there are no rules, with nothing forbidden."[14] Consequently, unrestricted warfare methods include: computer hacking, subversion of the banking system, markets and currency manipulation (financial war), terrorism, media disinformation and urban warfare. The authors, Qiao Liang and Wang Xiangsui, argue that developments in information technology and globalization have conclusively changed the conduct of war, which has consequently moved beyond the military realm to a "new concept of weapons," such as the use of computer viruses during combat operations.[15] These "new" techniques of warfare are curiously referred to as "kinder weapons," but the aim of their use remains Clausewitzian, that is to compel an opponent to bend to China's will. As a quotation from "Unrestricted Warfare" explains: "a kinder war in which bloodshed may be avoided is still

[12] Tim Benbow, "Talking 'Bout Our Generation? Assessing the Concept of Fourth-Generation Warfare," *Comparative Strategy* 27:2 (2008): 148–163. Even more contested is the notion of "Fifth Generation Warfare," on which readers can see for example Donald J. Reed, "Beyond the War on Terror: Into the Fifth Generation of War and Conflict," *Studies in Conflict and Terrorism* 31:8 (2008): 684–722.

[13] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 2, https://www.oodaloop.com/documents/unrestricted.pdf (accessed 15 December 2015).

[14] Ibid., 2.

[15] Ibid., 25.

war. It may alter the cruel process of war, but there is no way to change the essence of war, which is one of compulsion, and therefore it cannot alter its cruel outcome, either."[16] The extent to which unrestricted warfare has become official Chinese doctrine is not clear. However, recent reports suggest that these techniques may be evident in China's "three warfares" approach to its territorial claims in the East and South China seas.[17]

Are Non-Military Hybrid Methods Really Warfare?

Hybrid warfare tends to be used to describe all wars that are not strictly conventional, namely waged between the legally constituted armed forces of nation-states. Arguably, therefore, the term hybrid warfare is too vague to be of practical use to analysts and policymakers. As Latvian analyst, Jānis Bērziņš, notes "The word hybrid is catchy, since it may represent a mix of anything."[18]

The inclusion of a range of non-military means in a definition of hybrid warfare runs the risk of describing normal inter-state competition and conflict as war even in the absence of the threat or use of violence. A realist concept of international politics already posits inter-state relations as naturally competitive and conflictual. An environment in which sovereign states, primarily concerned with their security, act in pursuit of their national interests and struggle for power, cooperating and competing with other states as necessary to best achieve their objectives. The usual economic, diplomatic and informational measures used in inter-state competition are not normally classified as warfare in the absence of the threat or actual use of force. However, many of the statements emanating from Russia's government and media suggest that Russia perceives itself as at "war" with Western democracy, culture and values.[19] This development suggests that, at least for the foreseeable future, Russia has returned to a Soviet-era style battle of ideas with the West where, to reverse Clausewitz, peace is essentially a continuation of war by other means. Rod Thornton has suggested that the West must adjust to a situation where it is in a "permanent" state of hybrid war with Russia.[20] However, war in this context is

---

16 Ibid., 30.

17 See for example: John Garnaut, "US Unsettled by China's Three Warfares Strategy: Pentagon Report," *The Sydney Morning Herald*, 11 April 2014, www.smh.com.au/federal-politics/political-news/us-unsettled-by-chinas-three-warfares-strategy-pentagon-report-20140410-36g45.html (accessed 16 December 2015); and James R. Holmes, "Exposing China's Provocations," *The Diplomat*, 28 August 2014, http://thediplomat.com/2014/08/exposing-chinas-provocations (accessed 16 December 2015).

18 Jānis Bērziņš, "A New Generation of Warfare," *Per Concordiam* 6:3 (2015): 24, http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V6N3_en.pdf (accessed 9 December 2015).

19 "Russia's War on the West," *The Economist*, 14 February 2015, www.economist.com/news/leaders/21643189-ukraine-suffers-it-time-recognise-gravity-russian-threatand-counter (accessed 17 December 2015).

20 Thornton, "The Changing Nature of Modern Warfare," 45.

arguably the status quo of international politics and it is misleading and potentially dangerous to describe Russia's broader aims and methods simply as a form of warfare. Analyst Ralph Thiele, for example, includes Russian investments in key sectors of European economies and Russian organized crime links with local criminal elements in the Russian model of hybrid war.[21] In this author's opinion, only when non-military methods are coordinated or integrated with the actual threat or use of armed force should policymakers describe international political rivalry as a form of hybrid warfare. Naturally, a response to a real threat of hybrid warfare would require a comprehensive or "whole of government" effort, as non-conventional methods of warfare cannot be addressed by military means alone. It is probably a stretch to classify efforts to target corrupt Russian officials as a form of "warfare," although it might certainly be an element of soft power employed by Western states in their competition with Vladimir Putin's Russia. Overall, it is worth remembering that even at the height of the Cold War, the Soviet Union and the US were able to temper their rivalry to pursue mutually beneficial nuclear arms control agreements and limit proxy wars.

New Generation Warfare: Russia's Hybrid Warfare

Like the authors of *Unrestricted Warfare*, Russian analysts make no secret that their objective is to advocate approaches to warfare that will counter perceived overweening and threatening US power. Many Russian commentators and analysts claim that Russia has been under sustained and effective information attack by the US since the 1980s. Events such as perestroika and the "color revolutions" and multilateral organizations such as the IMF and World Bank are all considered instruments of irregular warfare intended to destabilize Russia.[22] From a Russian perspective, the seizure of Crimea and operations in eastern Ukraine are strategic defensive campaigns to counter US hybrid warfare against its national interests and values.

Hybrid warfare is a Western term, not a Russian one. When Russian analysts write on the subject, they use the terms "new generation warfare" or "non-linear war." The former was introduced to Western audiences through a paper published by General Valery Gerasimov, the Chief of the Russian General Staff, in February 2013. Consequently, the Russian approach to hybrid war is sometimes referred to inaccurately as the "Gerasimov Doctrine." Gerasimov describes new generation warfare as: "the broad use of political, economic, informational, humanitarian and other non-military means … supplemented by

[21] Thiele, "The Crisis in Ukraine," 6.

[22] Bērziņš, "A New Generation of Warfare," 23; and Bret Perry, "Non-Linear Warfare in the Ukraine: The Critical Role of Information Operations and Special Operations," *Small Wars Journal*, 14 August 2015, http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera (accessed 9 December 2015).

civil disorder among the local population and concealed armed forces."[23] Gerasimov recognizes that many of the methods he identifies were not traditionally part of what would be considered wartime activities. However, he believes that they are typical of twenty-first-century warfare and actually more significant for the achievement of strategic goals than military means because they can reduce the fighting potential of an enemy by creating social upheaval and promoting a climate of collapse without the overt use of violence.[24] Nevertheless, it is evident from Gerasimov's paper that the armed forces have an essential supplementary role in new generation warfare. This is particularly the case with special operations forces (SOF) that can be used under the guise of "peacekeeping and crisis regulation" to link up with opposition groups inside a targeted state.[25] In their discussion of new generation warfare, analysts Sergei G. Checkinov and Sergei A. Bogdanov also envisage the employment of SOF in "large-scale reconnaissance and subversive missions under the cover of the information operation."[26]

The use of SOF under cover of information operations was clearly evident in Ukraine in 2014. Covert *spetsnaz* units (the "little green men") were employed to seize government buildings and key infrastructure targets and arm separatist militia, while the Russian government spread doubt and confusion through repeated denials of Russian involvement. Other techniques of hybrid or new generation warfare were used to demoralize and intimidate opponents. These included exercises by Russian conventional forces close to the Ukrainian border, cyber attacks on Ukrainian government systems and a wider diplomatic and media offensive to undermine the legitimacy of the new government of Ukraine. The ultimate aim of this sort of "warfare" is to apply psychological pressure to cause the collapse of the target state from within so that the political objectives of the conflict can be achieved without fighting – the acme of strategic skill according to Sun Tzu. Bērziņš accurately sums up the Russian approach to modern warfare as follows:

> … 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, making the opponent's military and civil population support the attacker to the detriment of their government and country.[27]

---

[23] General Gerasimov's article is available in English from Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (blog), 6 July 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war (accessed 11 December 2015).

[24] Ibid., 2–3.

[25] Ibid., 3–4.

[26] Chekinov and Bogdanov, "The Nature and Content of New Generation War," 20.

[27] Jānis Bērziņš, *Russian New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga: National Defence Academy of Latvia, 2014), www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx (accessed 14 December 2015).

Many of the methods Russia has used in Ukraine date back to the Soviet era and the application of *maskirovka*, or military deception. This was effectively applied by Soviet forces during World War II and in Cold War proxy conflicts. For example, *maskirovka* was used on a grand scale in Operation Bagration in 1944 when an entire German Army Group was destroyed. At the other end of the conflict spectrum, *maskirovka* techniques were employed in Eastern Europe after 1945 when Soviet interior ministry troops (NKVD) used covert means to take over state institutions, undermine civil society and crush all opposition to the imposition of Communist rule.[28] In the twenty-first century, 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. These have been used to build support for the government's foreign policy within Russia and to wage a wider "information war" against Ukraine and the West. In the current NATO context, Julian Lindley-French defines *maskirovka* as "war that is short of war, a purposeful strategy of deception that combines use of force with disinformation and destabilisation to create ambiguity in the minds of Alliance leaders about how best to respond."[29]

The concept of "reflexive control" (perception management) is a key element of *maskirovka.*[30] This originated with the work of former Soviet psychologist Vladimir Lefebvre who developed the theory while researching ways to influence and control an enemy's decision-making processes. The theory can be described as the use of specially-prepared information that inclines an opponent to voluntarily make a decision that has been predetermined as desirable by the initiator of the information. 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. The continued post-Soviet interest in reflexive control techniques was demonstrated by the launch of a new security studies journal entitled *Reflexive Processes and Control* as recently as 2001.[31]

In practice, the execution of new generation warfare poses significant challenges. A wide range of parties—civil and military, regular and irregular, as well

---

[28] For a detailed account of this process see: Anne Applebaum, *Iron Curtain: The Crushing of Eastern Europe 1944–1956* (London: Allen Lane, 2012).

[29] Julian Lindley-French, *NATO: Countering Strategic Maskirovka* (Calgary: Canadian Defence and Foreign Affairs Institute, 2015), 4, http://www.cgai.ca/nato_countering_strategic_maskirovka (accessed 8 December 2015).

[30] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17 (2004): 237–256; and Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, 2015), http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf (accessed 11 December 2015).

[31] Thomas, "Russia's Reflexive Control Theory and the Military," 237.

as their activities—must be coordinated, integrated and controlled to achieve the overall military and political objectives. Unified political control is especially difficult, as irregular and state actors often have differing political interests. Even for an authoritarian state such as Russia, control and coordination proved difficult during operations in Ukraine, which appear to have been less well-orchestrated than many Western commentators believed at the time.[32] For example, analysis by the Wilson Center concludes that Russian actions in Ukraine were not part of a well-coordinated master strategy, but rather reflected "the unplanned succession of different tools to fit different—often unexpected—operational realities."[33]

Russian Hybrid Warfare as a Threat to NATO

Much concern has been expressed about NATO's vulnerability to Russian hybrid warfare techniques. Naturally, the security of the Baltic States, with their significant Russian-speaking minorities, is of particular concern. It has been longstanding Russian policy to weaken, divide and ultimately neutralize NATO. The Baltic States provide Putin with the potential leverage to achieve this aim. Just as Russian meddling in Ukraine started long before the annexation of Crimea, political and social pressure has been ratcheted up in the Baltic States.[34] Some European intelligence agencies have also expressed fears about Bulgaria, where the entire political system is believed to be compromised by criminal organizations linked to the Russian state by Russian intelligence agencies.[35] NATO strategy to combat Russian hybrid warfare needs to combine diplomatic, military, informational, economic and law enforcement efforts. Yet such a comprehensive approach must be properly integrated, rather than simply involving civilian agencies in support of military forces or replacing armed forces with civilian measures due to a reluctance to deploy the former.

In a crisis involving the Baltic States, Russia would likely seek to divide NATO members by staying below an obvious Article 5 threshold, at least initially. As during the Ukraine crisis in 2014, disinformation, intimidation and propaganda would be used to try to encourage the less robust members of NATO to accept the Russian version of events, which would, of course, conveniently reinforce their existing inclination to avoid a military response. Disinformation would be used against NATO governments and wider public opinion to keep the Alliance politically and militarily off-balance. Intimidation would likely highlight Russia's

[32] Freedman, "Ukraine and the Art of Limited War," 11; Kofman and Rojansky, "A Closer Look at Russia's Hybrid War," 5.

[33] Kofman and Rojansky, "A Closer Look at Russia's Hybrid War," 5.

[34] See for example Andrew Osborn, "Putin a Threat to Baltic States, Western Officials Say," *Reuters*, 19 February 2015, http://uk.reuters.com/article/uk-britain-russia-baltics-idUKKBN0LN0FT20150219 (accessed 18 December 2015).

[35] Sam Jones, "Ukraine: Russia's New Art of War," *Financial Times*, 28 August 2014, http://www.ft.com/intl/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html (accessed 10 December 2015).

apparent willingness to employ nuclear weapons to de-escalate NATO "aggression." Effective strategic communication could counter Russian narratives, but it would need to be responsive, coherent and consistent. Although the EU adopted a strategic communication action plan in 2015, there is no evidence that EU planning includes coordination with the NATO'S STRATCOM COE, which was founded in 2014.[36] Such coordination would be vital to respond effectively to a Russian disinformation and propaganda campaign. Unfortunately, authoritarian societies have an advantage, as they can more easily mobilize all of the resources of the state for political purposes without the restrictions imposed by a decentralized distribution of power and a democratic consensus-building process. In contrast, liberal democracies have a distaste for propaganda and psychological warfare and the NATO alliance would find it difficult to agree on the content and presentation of a strategic communication campaign. As the STRATCOM COE acknowledges, Russia has a potential asymmetrical advantage over the West, as the latter's free media cannot compete with centrally-controlled and synchronized Russian information warfare operations.[37]

However, NATO may not be as vulnerable to information warfare as many believe. Propaganda can have a particularly strong effect when a population, as in Russia, is denied alternative sources of information, but elsewhere propaganda must be plausible enough to shape beliefs and emotions and exploit general uncertainty, mistrust and paranoia. Russian government pronouncements and media sources have become increasingly discredited in the West, especially since their responses to the shooting down of flight MH 17 over Ukraine in July 2014. Increased control of the national media and the Internet as well as harassment of dissenters made it possible to shape Russian public opinion. However, despite the efforts of Russia Today (RT) and a veritable army of Internet trolls to contradict and abuse news outlets and social media that take anti-Russian positions, Russian information operations have largely failed to influence non-Russian-speaking audiences.[38] Ukrainian government sources claim that there is now a very low level of public confidence in any official Russian media,[39] and despite Russia's intense information campaign, support for pro-Russian separatists even amongst Russian-speaking Ukrainians was lower

[36] Bastian Giegerich, "Hybrid Attacks Demand Comprehensive Defence," *Ethics and Armed Forces* 2 (2015): 15, http://www.ethikundmilitaer.de/fileadmin/Journale/2015-12_English/Hybrid_Warfare-Enemies_at_a_Loss_2015-2.pdf (accessed 9 December 2015).

[37] StratCom COE, *Analysis of Russia's Information Campaign Against Ukraine*, 3.

[38] Freedman, "Ukraine and the Art of Limited War," 23; and Snegovaya, "Putin's Information Warfare in Ukraine," 18–20.

[39] "Sociology of Information Warfare in Ukraine," *Europe Insight*, 11 October 2015, http://en.europeinsight.net/sociology-of-information-warfare-in-ukraine (accessed 10 December 2015).

than anticipated. This partly explains Russia's need for more overt military involvement in the conflict in the summer of 2014.[40]

During crisis, Russian tactics will likely involve covert support to local pro-Russian activists. As in Ukraine, ambiguity and deniability will make it difficult to confirm that an attack is under way. The following quotation from Mark Galeotti starkly illustrates the potential difficulties of responding to these methods, especially forcefully:

> The first little green man, after all, might instead be a 15-year-old Russian-Estonian girl waving a "Russian-speakers have rights, too" placard in the border city of Narva. Shoot her? Of course not. The second might be her older brother, throwing rocks at the police coming to arrest her. Shoot him? Hopefully not, especially as you can guarantee that footage of the incident would promptly be blasted across Russian TV channels.[41]

Paramilitary police would probably be better equipped and trained than soldiers to handle such situations, which is another example of where closer cooperation between the EU and NATO would undoubtedly be beneficial.

If a crisis were to escalate, Russia might be tempted to seize territory in vulnerable frontline states by overt military means before the Alliance could mount an effective collective response.[42] The nightmare scenario for NATO would be the occupation of part of a member state, even if temporarily. Such action would force the Alliance to invoke Article 5 of the Washington Treaty and risk a direct armed confrontation with a nuclear-armed Russia or fail to respond to the aggression and risk the collapse of NATO as a viable military alliance. Despite the misgivings of states such as Germany, effective deterrence will require the permanent stationing of significant multinational forces on the territory of states that might be at risk in order to deny Russia the option of a military fait accompli. Although NATO's new 5,000-strong Very High Readiness Joint Task Force (VJTF) should be able to deploy rapidly, it may still arrive too late to deter Russian adventurism. The Russian approach to hybrid warfare does not exclude the direct use of military force when necessary. In summer 2014, when Russia had exhausted its use of non-military hybrid methods, military operations in Ukraine took on the character of limited conventional war. Russian battalion tactical groups (BTG) intervened directly in combat against the Ukrainian army. Fighting involved clashes between armored forces, intense urban infantry battles, heavy artillery barrages and, at least on the Russian side, the employment of "drones" for surveillance and target acquisition, electronic

[40] Kofman and Rojansky, "A Closer Look at Russia's Hybrid War," 5.

[41] Mark Galeotti, "Time to Think About Hybrid Defense," *War on the Rocks*, 30 July 2015, http://warontherocks.com/2015/07/time-to-think-about-hybrid-defense (accessed 8 December 2015).

[42] See Elbridge Colby and Jonathan Solomon, "Facing Russia: Conventional Defence and Deterrence in Europe," *Survival* 57:6 (2015): 23–24.

warfare and air defense assets.[43] NATO troops have already started to learn from the experiences of Ukrainian soldiers about Russian tactics and technologies, in particular the use of drones to direct artillery fire and Russian electronic jamming capabilities.[44] However, such tactical improvements alone are unlikely to be enough to provide credible conventional deterrence against armed attack.

Conclusion

Hybrid warfare does not change the nature of war. Violence remains at the core of hybrid warfare as it does any other form of war, and its aim is the same as any other act of war, namely, to exploit the threat or use of organized violence to gain physical or psychological advantages over an opponent. However, the plethora of terminology—hybrid, asymmetrical, unconventional, non-linear, new generation, fourth and fifth generation, grey wars etc.—reflects the difficulties that strategists and scholars continue to have in categorizing the complex armed conflicts of the twenty-first century. Although the term "hybrid" is currently the most popular, it is by no means the only one to describe these wars. The fact that many armed conflicts blur the lines between war and peace and involve the use of instruments that were not traditionally part of warfighting further complicates the problem. It is undoubtedly a challenge for traditional security establishments to address the wide range of threats identified by the analysts and scholars of hybrid warfare. Cast the definitional net too wide, and a term like hybrid warfare becomes too all-encompassing to be of any practical use to policymakers. Define warfare too narrowly, and policymakers may fail to appreciate the significance of many non-traditional techniques of warfare that are being employed by an adversary as a prelude or adjunct to the use of military force.

Regardless of how the threat is labelled, strategists must decide how best to address the methods employed by their adversaries, whether state or non-state actors. Sometimes the most appropriate responses may involve the application of specific political, informational, economic, diplomatic or, in the case of a physical threat, military tools of statecraft. More complex threats require a whole of government or comprehensive approach. Usually, the best strategies involve the coordination and direction of all of the effective instruments of state power, no matter how the threat is defined. Undoubtedly, NATO needs to enhance its military deterrence capability, but in the case of the West's adversarial relationship with Putin's Russia, the temptation to describe this rivalry as

[43] Philip A. Karber, *Lessons Learned from the Russo-Ukrainian War* (Vienna, VA: The Potomac Foundation, 2015).

[44] "Situation Report," *Foreign Policy*, 10 December 2015, http://foreignpolicy.com/2015/12/10/situation-report-carter-gets-through-another-hill-appearance-new-book-by-former-intel-chief-nato-training-against-russian-tactics-india-comes-to-the-pentagon-house-wants-to-supply-kurds-new-nort (accessed 14 December 2015).

hybrid warfare may inflame an already challenging security situation and blind governments to potentially productive traditional diplomatic policy initiatives.

About the author

Professor Wither is a retired British Army officer and former researcher in 20th century warfare at the Imperial War Museum in London. He has taught terrorism, warfare and related security studies subjects at a wide variety of institutions, including the FBI Academy, the UK Defence Academy, the NATO School, the NATO Centre of Excellence – Defence Against Terrorism (COE-DAT), the Geneva Centre for Security Policy and various staff colleges and military universities in Europe and Eurasia. *E-mail*: witherj@marshallcenter.org.