The US Army War College Quarterly: Parameters

Volume 48
Number 1 *Parameters Spring 2018*

Article 8

Spring 3-1-2018

Victory without Casualties: Russia's Information Operations

T. S. Allen

A. J. Moore

Victory without Casualties: Russia's Information Operations

T. S. Allen and A. J. Moore

ABSTRACT: This article argues Russian information operations are a decisive tool of state power rather than a supporting element. Uniquely, Russian leaders are significantly more likely to employ diplomatic, military, and economic tools in pursuit of informational objectives than other states' leaders.

Russia is a resurgent geopolitical actor that the United States identified as a major competitor in the 2017 National Security Strategy.[1] Russia has maintained its position as a great power, despite its relative material weakness, through its superior use of information as a tool of asymmetric statecraft. Russian leaders consider information operations (IO) a decisive tool of state power and engage in continuous international competition in the information domain executed by both state and nonstate actors. These coordinated efforts to project influence using information and disinformation make Russian foreign policy unique. The logic of information operations often guides Russia's coordinated military, diplomatic, and economic efforts. Whereas other states' information operations are generally guided by facts, Russia's foreign policymakers create "facts" to be broadcast to targeted audiences in order to achieve strategic objectives.

Although Russia has long employed information as a tool of state power, since 2013 its military thinkers have increasingly adopted a novel approach to information that places such considerations at the forefront of their strategy. Scholars and policymakers have used many phrases—including new generation warfare, new-type warfare, hybrid warfare, and nonlinear warfare—to describe this contemporary military doctrine.[2] But these phrases often obscure Russian thinking. Just as previous Soviet leaders did, today's Russian military leaders attempt to obfuscate their intentions and to malign their competitors by accusing their opponents of employing Russia's desired military capabilities.[3]

In a widely quoted article on modern warfare, Russian Armed Forces Chief of Staff General Valery Gerasimov noted the effectiveness with which Western powers were using information to subvert states. Some commentators, including many in Russia, exaggerated the importance of Gerasimov's article, claiming it was the foundation of a new doctrine. Russian-controlled propaganda outlets used a prominent repudiation of these reports as evidence that Russia had a fundamentally benign foreign

1 Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: White House, 2017).

2 Timothy L. Thomas, "The Evolving Nature of Russia's Way of War," *Military Review* 97, no. 4 (July/ August 2017).

3 Timothy L. Thomas, *Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), 5.

policy, was not subverting its neighbors, and was under attack by enemy propagandists.[4] Moreover, the Kremlin asserted the Color revolutions in Georgia (2012), Ukraine (2004), and Kyrgyzstan (2005); the Arab Spring in the Middle East and North Africa (2010–11), and even the Moscow protests (2011–12) were the result of planned Western interventions using hybrid warfare.[5] Russia claims only foreign states conduct hybrid warfare (Гибридная война). But Russia clearly does as well. As Dmitri Peskov, Russian President Vladimir Putin's press secretary, said in 2017, "If you call what's going on now a hybrid war, let it be hybrid war. It doesn't matter: It's war."[6]

Information operations, a key component of Russia's contemporary way of war, encompasses all the uses of information and disinformation, by states or nonstate actors, as a tool of state power and includes military information support operations, cyberspace operations, electronic warfare, military deception, psychological operations, public affairs, and strategic communications. In 2011, the Russian Ministry of Defense concept for future information operations defined information warfare (информационная война) "as the ability to . . . undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a state to make decisions in the interest of their opponents."[7] Russian military doctrine also describes a broader concept of information confrontation (информационное противоборство) that incorporates military/technical battlefield effects and informational/psychosocial effects "designed to shape perceptions and manipulate the behavior of target audiences."[8] The distinction between information war and information confrontation is the "subject of detailed debate in official Russian sources" but is "of little practical impact for assessing Russian approaches."[9] Thus, this article expands on Russian definitions to encompass all aspects of Russian information operations as it is executed.

Many people outside Russia recognize Russian information operations and statecraft are unique, a "sharp power" influence that is "not principally about attraction or even persuasion; instead, it centers on distraction and manipulation."[10] Some Western military thinkers have also echoed Russia's emphasis on informational/psychosocial effects. According to the US Department of Defense, information operations "ultimately register an impact in the human cognitive dimension,"

4 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine'," *Foreign Policy*, March 5, 2018; and " 'Gerasimov Doctrine' Finally Put To Rest? Russia 'Expert' Apologizes for Coining Snappy Term," *RT*, March 6, 2018.

5 Nicolas Bouchet, "Russia's 'Militarization' of Colour Revolutions," *CSS Policy Perspectives* 4, no. 2 (January 2016).

6 Dmitri Peskov, quoted in Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *New York Times Magazine*, September 13, 2017.

7 *Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in Information Space* (Moscow: Russian Ministry of Defense, 2011) quoted in Timothy L. Thomas, "Russia's 21st Century Information War: Working To Undermine and Destabilize Populations," *Defence Strategic Communications* 1, no. 1 (Winter 2015): 12.

8 Defense Intelligence Agency (DIA), *Russia Military Power: Building a Military to Support Great Power Aspirations* (Arlington, VA: DIA, 2017), 38.

9 Kier Giles, *Handbook of Russian Information Warfare*, fellowship monograph 9 (Rome: NATO Defense College, 2016), 6.

10 Christopher Walter and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Snapshot* (blog), *Foreign Affairs*, November 16, 2017.

which is "composed of the attitudes, beliefs, and perceptions of those who transmit, receive, respond to, or act upon information."[11] Some strategists suggest military organizations conduct cognitive maneuver to affect the cognitive domain, in a manner similar to the Russia concept of information confrontation.[12] But unlike the Western understandings, Russians perceive information operations to be a decisive tool, rather than a supporting element, of state power.

Origins

Modern Russian information operations are shaped by many traditions. Russian leaders have long placed exceptional value on using information to manipulate their enemies. Russian scholars developed an elaborate theory of information operations called reflexive control (Рефлексивное управление) that "occurs when the controlling organ conveys (to the objective system) motives and reasons that cause it to reach the desired decision, the nature of which is maintained in strict secrecy."[13] This theory uses all means available to shape the information environment and manipulate what an opponent thinks to force him to make a desirable decision.[14]

At the tactical level, czarist and Soviet forces were masters of tactical military deception (маскировка). At the strategic level, Soviet intelligence and security services were primarily focused on subversion, known as active measures (активные мероприятия). Since forming the first Foreign Bureau of the czarist secret police, Okhrana, in 1883, Russia has pursued its foreign policy objectives through subversion. During the Cold War, the intelligence services were the Soviet Union's main tool for shaping the international environment.[15] These agencies used active measures and reflexive control to undermine Russia's enemies and were also paranoid regarding adversarial countermeasures. The Soviet Union's active measures during the Cold War sought to divide the North Atlantic Treaty Organization (NATO) alliance, subvert governments not aligned with the Union of Soviet Socialist Republics (USSR), and shape the class consciousness of targeted societies to make them more amenable to the Communist agenda.[16] The United States and its allies countered these efforts using both defensive means and countermeasures such as Voice of America and BBC broadcasts of pro-Western information into the Eastern Bloc. By the 1970s, about half of the Soviet population routinely listened to Western radio broadcasts.[17]

---

11 US Department of Defense (DoD), *Strategy for Operations in the Information Environment* (Washington, DC: DoD, 2016).

12 Allison Astorino-Courtois, ed., "A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap" (white paper, Strategic Multi-Layer Assessment Office, October 2017).

13 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 7 (2004): 241.

14 Can Kasapoglu, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," research paper 121 (Rome: North Atlantic Treaty Organization [NATO] Defense College, 2015).

15 Ben B. Fischer, "Okhrana: The Paris Operations of the Russian Imperial Police," Central Intelligence Agency, July 7, 2008.

16 Christopher M. Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 9–17.

17 Gregory Mitrovich, "Cold War Broadcasting Impact" (report, Hoover Institution and Cold War International History Project conference, Stanford University, October 13–16, 2004), 19.

Although Soviet active measures efforts were more extensive, aggressive, and better coordinated than similar Western efforts, they were not ultimately successful.[18] The transatlantic Alliance survived, while Western information exposed Soviet hypocrisy and contributed to the political collapse of the Soviet Union. Retrospectively, some Russian scholars claimed the United States employed reflexive control to undermine the Soviet Union by provoking it into a costly arms race it could not win in the 1980s.[19] As early as 1990, the KGB also began publicizing conspiracy theories about vast American efforts to subvert the USSR.[20] Other Russians blamed the destabilizing myth of capitalist plenty and the American Dream for causing mass discontent.[21] In sum, many Russians believe Western efforts to subvert the Soviet Union with information were far more extensive—and successful—than they in fact were, which helps explain their confidence in the effectiveness of information operations. Russians also believe the United States continues to wage a massive information campaign against Russia. Putin has even claimed the internet is a "CIA project" intended to undermine Russia.[22]

Today, Russia invests in information operations capabilities due to their cost effectiveness and strategic impact. Despite recent modernization, Russia is unlikely to defeat the United States or NATO in a conventional military conflict. But the Kremlin wishes to reassert its historic control over former Soviet states, including some NATO members, and to increase its influence in the Middle East relative to that exerted by the United States. To solidify control without provoking a war it cannot win, Russia competes with the West by using a key nonmilitary means, information operations, in the gray zone short of declared war.[23]

Decisiveness

Russian leaders think they can win wars with information operations partially due to their belief that America prevailed in the Cold War with Western reflexive control initiatives, intelligence-led subversion campaigns, and the promise of capitalism. Every senior Russian leader today "went to bed in one country and awoke in different ones" when the Soviet Union collapsed in 1991.[24] As Russia recovered from this catastrophe, intelligence and military officers faced near-state collapse and rampant cronyism, and in many cases, became enmeshed in organized crime.[25] Russian leaders also set out to rethink and to retool the art of subversion. In the 1998 book *If War Comes Tomorrow? The Contours of Future Armed Conflict*, Russian General Makhmut Akhmetovich

18 Andrew and Mitrokhin, *Sword and the Shield*, xxx.

19 Thomas, "Russia's Reflexive Control," 239.

20 Andrew and Mitrokhin, *Sword and the Shield*, 479.

21 Svetlana Aleksievich, *Secondhand Time: The Last of the Soviets*, trans. Bela Shayevich (New York: Random House, 2016), 166.

22 Ewen MacAskill, "Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup," *Guardian*, April 24, 2014. Some early Internet users also thought the internet could undermine Soviet information control. Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Public Affairs, 2015), 1–63.

23 Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016.

24 Putin repeated this phrase when he described the collapse of the Soviet Union during his 2014 speech on the annexation of Crimea. "Address by President of the Russian Federation," Kremlin, March 18, 2014, http://en.kremlin.ru/events/president/news/20603.

25 Edward Lucas, *Deception: Spies, Lies and How Russian Dupes the West* (London: Bloomsbury, 2012), 316.

Gareev argued information operations would be the decisive element in future wars.

> The systematic broadcasting of psychologically- and ideologically-biased materials of a provocative nature, mixing partially truthful and false items of information . . . can all result in a mass psychosis, despair and feelings of doom and undermine trust in the government and armed forces; and, in general, lead to the destabilization of the situation in those countries, which become objects of information warfare, creating a fruitful soil for actions of the enemy.[26]

As early as 2004, Russian military academic Vladimir Slipchenko stated, "Information has become a destructive weapon just like a bayonet, bullet or projectile."[27] More recent Russian military statements also suggest the decisive nature of information operations. In 2013, Gerasimov argued, "The role of nonmilitary means of achieving political goals has grown and, in many cases, they have succeeded the power of force of weapons in their effectiveness." He claimed contemporary states can be rapidly overpowered by "means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces."[28] Likewise, an article in the Russian journal *Military Thought* argued "information superiority and anticipatory operations will be the main ingredients of success in new-generation wars."[29]

After invading Georgia in 2008, Russia redoubled its efforts to improve its IO capabilities.[30] When Russia annexed Crimea in 2014, it employed these new capabilities in the culmination of a long-standing Russian IO campaign to influence the Russian diaspora in Crimea and convince the world that Ukraine, which was previously part of the Soviet Union, is not a state and has no independent culture. In 2014, about 27 percent of Ukrainians watched Russian television, which is Russia's main propaganda tool and the primary source of information in most post-Soviet states.[31] Russia also has employed extensive online propaganda against Ukraine since the early 2000s. [32] Additionally, since Russia resumed control of the Black Sea Fleet's leased port at Sevastopol, Crimea, in 1997, it established an air of Russian superiority over Ukrainian armed forces personnel stationed on adjacent bases, which undermined the morale of the Ukrainian forces there.[33]

---

26 Makhmut Akhmetovich Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, ed. Jacob W. Kipp (London: Frank Cass, 1998), 51–52.

27 Makhmut Akhmetovich Gareev and Vladimir Slipchenko, *Future War* (Fort Leavenworth: Foreign Military Studies Office, 2007), 33.

28 Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military-Industrial Kurier*, February 27, 2013, translated in Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *The Blog, Huffington Post*, September 2, 2014.

29 Sergei G. Chekinov and Sergei A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013), 23.

30 Timothy L. Thomas, "Russian Information Warfare Theory: The Consequences of August 2008," in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, ed. Stephen J. Blank and Richard Weitz (Carlisle, PA: Strategic Studies Institute, 2010).

31 Kateryna Kruk, *Analyzing the Ground Zero: What Western Countries Can Learn from Ukrainian Experience of Combating Russian Disinformation*, Kremlin Watch Report 11.12.2017 (Prague: European Values, 2017), 13.

32 Samuel C. Woolley and Philip N. Howard, *Computational Propaganda Worldwide: Executive Summary*, working paper 2017.11 (Oxford: University of Oxford, 2017), 4.

33 Ilan Berman, "How Russian Rule Has Changed Crimea," *Snapshot* (blog), *Foreign Affairs*, July 13, 2017.

The Russian invasion of Crimea, the culmination of Russia's decades-long cognitive attack on Ukraine, altered the identity of Crimeans and solidified their nascent Russian identity. Instead of waking up in a different country, Crimeans woke up in a country they had been conditioned to believe was theirs all along. Before the invasion began, cells of Russian agents travelled to Crimea to coordinate unrest. Then, in February 2014, Russian soldiers wearing no identifiable insignia invaded Crimea.[34] The Ukrainian security services were isolated by an "electronic knockdown." The massive cyberattack by Russia's state and nonstate actors amplified the effects of tactical electronic warfare and the coordinated seizure of key pieces of physical information technology by armed forces.[35] The Ukrainians were also uncertain of their legal chain of command due to the ongoing political upheaval in Ukraine. Military members were uncertain if their officers had been coopted and uncertain of the enemy's identity. The majority of the Ukraine's armed forces withdrew from Crimea without fighting.

The logic of information operations drove Russian tactical actions in Crimea. Russian forces rapidly seized physical control of key media infrastructure in the region.[36] At key military installations, Russia paralyzed Ukrainian forces by surrounding them with concentric cordons of military personnel, Cossacks, and pro-Russian pensioners. The inner cordon of Russian military personnel was thus concealed, while the outer cordon presented a sympathetic popular face that Ukrainian relief forces could not fight though. This formation posed an impossible tactical/informational dilemma to Ukrainian forces. Russian forces ensured there were television cameras ready to film powerful propaganda if the Ukrainian forces attacked the elderly "protestors" and effectively deterred a Ukrainian defense.[37]

By leading with information operations, Russia conquered Crimea without physically fighting for it. Only one soldier, a Ukrainian, was killed during the annexation, a figure which stands in stark contrast to the 90,000 Russians and Germans who died fighting over the same territory during World War II. Russia had effectively used information as a substitute for blood and treasure, and had achieved what some Ukrainians refer to as "victory without casualties." Putin later admitted that Russian soldiers had seized Crimea, although during the invasion, the Russian government claimed no Russian troops were involved.[38] The denials were part of an extensive global disinformation campaign incorporating several narratives tailored to convince international policymakers and populations that Russia was not attacking Ukraine, which disrupted any potential international response.[39]

---

34 Johns Hopkins University Applied Physics Laboratory, *"Little Green Men:" A Primer on Modern Russian Unconventional Warfare in Ukraine, 2013–2014* (Fort Bragg, NC: US Army Special Operations Command, 2015).

35 András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, report 13 (Helsinki: Finnish Institute of International Affairs [FIIA], 2015), 39.

36 Johns Hopkins, "*Little Green Men*," 47.

37 Interviews with Ukrainian witnesses to the 2014 Russian military intervention in Crimea, 2015.

38 "Putin Admits Russian Forces Were Deployed to Crimea," Reuters, April 17, 2014; and "Little Green Men: The Annexation of Crimea as an Emblem of pro-Kremlin Disinformation," EU vs Disinfo, March 16, 2018.

39 Katri Pynnöniemi and András Rácz, eds., *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, report 45 (Helsinki: FIIA, 2016).

Russian IO efforts have been most extensive and successful at home: "Russia is actively fortifying the mentality of its citizenry for war."[40] The majority of the Russian people support Russian foreign policy, especially towards the United States and NATO.[41] Even the Russian opposition's resistance to Russia's blatantly illegal intervention in Ukraine remains muted.[42] Russia achieved this apparent national unity by inundating its population with pro-Kremlin propaganda at an accelerated pace since 2013.[43] No Russian IO efforts abroad have been comparably extensive or successful.

Efforts in Russian-speaking Ukraine extend from this internal effort. Soviet propaganda once portrayed Donbas as a cornerstone of the Soviet industrial base. Joseph Stalin named Sevastopol and Kerch Hero Cities for withstanding Nazi sieges during the Second World War. And Russia weaponizes this heritage with constant references to the Great Patriotic War and use of the St. George ribbon and Soviet iconography, which promulgate identity-based narratives that mobilize Pan-Slavic and Russian nationalism.[44] Similarly, messages of post-Soviet identity delivered on Russian television, from digital sources, and in print publications in Ukraine provide purpose and motivation to separatists and Russian proxy forces.[45]

Characteristics

Russia's information operations maintain *continuous activity* as the nation is always in a declared or undeclared war.[46] A *hybrid force* of state and coerced or co-opted nonstate actors execute information confrontation. This force promotes the state's carefully crafted *emotional appeals* to manipulate a variety of audiences.[47] As a post-truth society, Russia promotes a *subverted reality* by inviting relativism through messages such as RT's motto: "Question more."[48] Through such actions as expelling foreign media and nongovernmental organizations, and maintaining state ownership of media platforms outside of Russia, Russia maintains *platform control*, which gives it the capability to reach key domestic and foreign audiences.[49] No less important than the previous characteristics is the *manipulation of the Russian diaspora*—individuals with actual or latent Russian identities—that Russia pursues to garner the

40 Lukas Milevski, "Prospective Strategy for Baltic Defense: The Russian Public and War Termination in the Baltic States," *Military Review* 98, no. 1 (January/February 2018): 68.

41 Margaret Vice, *Russians Remain Confident in Putin's Global Leadership* (Washington, DC: Pew Research Center Report, 2017).

42 Robert Mackey, "Navalny's Comments on Crimea Ignite Russian Twittersphere," *New York Times*, October 16, 2014.

43 Soldatov and Borogan, *Red Web*, 149–73.

44 Masha Gessen, *The Future Is History: How Totalitarianism Reclaimed Russia* (New York: Riverhead Books, 2017), 435; and Sergei Kurginyan, " 'Essence of Time' Manifesto," Europe Essense of Time, August 14, 2011, http://eot.su/sites/default/files/manifest_eot.pdf.

45 Kruk, "Analyzing the Ground Zero," 13.

46 Giles, *Handbook of Russian Information Warfare*, 16–32; and John Chambers, *Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the US Army* (West Point, NY: Modern War Institute, 2016), 26.

47 *Disinformation: A Primer in Russian Active Measures and Influence Campaigns, Before the Senate Intelligence Committee* 115th Cong. (March 30, 2017) (testimony, Clint Watts, Robert A. Fox Fellow, Foreign Policy Research Institute, and Senior Fellow, Center for Cyber and Homeland Security, George Washington University).

48 Gessen, *Future is History*, 22.

49 "Russia: Government vs. Rights Groups," Human Rights Watch, March 6, 2018.

support of those most likely to accept the Kremlin's scripted narratives as fundamentally correct.[50]

Hybrid Force

Hybrid actors receive instructions from the presidential administration and the Russian intelligence and security services. In some cases, such as Ukraine in 2014, the entities coordinate operations very effectively. But much of the time, they appear less well coordinated. The key to effective coordination is probably direct involvement and clear guidance from Putin, who is capable of taking total control of special operations when he considers it necessary despite his struggle to exercise command and control of the Russian government.[51] Since 2008, the Russian armed forces have also formed information operations troops and enhanced information capabilities.[52] Nongovernment entities such as the Internet Research Agency, an infamous troll farm that produces manipulative social media content, and groups of supportive or coerced hackers also conduct information operations in coordination with the Russian government.[53] The involvement of such nonstate actors has increased the flexibility and deniability of Russian information operations.

Emotional Appeal

Russian leadership develops narratives with an emotional appeal that can be transmitted through traditional media and online social networks. They rely on individuals they do not command to spread their narrative. Although Russian actors employ fake social media profiles to plant stories and about 45 percent of Twitter activity within Russia originates with bots, these profiles have limited direct reach outside Russia.[54] To reach the international audience, Russia manipulates individuals into propagating the state's narrative using novel, emotionally appealing stories, which are often completely false.

Russia does not lead with a fact-based narrative because novel stories spread more rapidly than more mundane stories on social media. When artfully written, Russia's stories easily make the jump from the bubble of trolls and bots to mainstream audiences around the world. "Lies," as one analysis of computational propaganda puts it, "spread faster than the truth."[55] In one remarkable example of disinformation in 2014, Russian media claimed Ukrainian soldiers had crucified a child whose family supported Russia's annexation of Crimea. The false story rapidly went viral and spread across social media in Russia, Ukraine, and the West.[56] Conversely, the more believable and truthful stories promulgated by Western information operations spread less rapidly and

---

50 Rhonda S. Zaharna, "Reassessing 'Whose Story Wins': The Trajectory of Identity Resilience in Narrative Contests," *International Journal of Communication* 10 (2016): 4407–38.

51 Gleb Pavlovsky, "Russia Politics under Putin: The System Will Outlast the Master," *Foreign Affairs* 95, no. 3 (May/June 2016).

52 DIA, *Russian Military Power*, 32.

53 DIA, *Russian Military Power*, 40.

54 Woolley and Howard, *Computational Propaganda*, 4.

55 Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 2018): 1146–51, doi:10.1126/science.aap9559.

56 Anna Nemtsova, "There's No Evidence the Ukrainian Army Crucified a Child in Slovyansk," *Daily Beast*, July 15, 2014.

are at a significant disadvantage in the competition to be novel, trending, and viral.[57]

Subverted Reality

Beyond spreading flagrant lies, Russian information operations seek to enhance relativism and subvert the very idea of an objective, impartial, or nonpartisan truth, which leads audiences to approach every truth-claim with the fundamental belief that nothing is certain. Relativism maximizes Russian influence because relativistic populations are more vulnerable to emotional manipulation and reflexive control. Relativism also undermines the credibility of Western institutions and leaders. Moreover, these disruptions to basic political and media functions delay international responses to the Kremlin's deniable gray-zone activity by drawing out the time it takes for other states to recognize and to develop political consensus about Russian actions.

Another strategy for subverting reality, disseminating multiple contradictory narratives, creates information fatigue in which populations are overwhelmed with information and unable to determine what information is accurate—or more dangerously, no longer care.[58]

Platform Control

The Russian government has the ability to influence or control many mass-media platforms. Within Russia, leaders have sought to eliminate sources of information that deviate from the official line. Russian officials suspect foreign entities because Russia's own media and many Russian nongovernmental organizations are tools of the state. Even in the West, many popular television channels and radio stations, such as Sputnik, RT, and Anna News, are agents of Russian influence. Numerous US media outlets, especially online, cite or copy Russian-generated stories. Online, platform control is less important, as social media can be influenced by bots and reflexive control of mainstream users.

Russia has recognized the emerging threat since at least 2000 when the Russian national security concept claimed "a serious danger arises from the desire of a number of countries to dominate the global information domain space."[59] In 2014 Russian law mandated all digital data on Russian citizens be stored inside its borders.[60] More recently, an advisor to Putin said Russia is prepared to be isolated from the global internet.[61] Russia has also banned most use of personal social media accounts by its military personnel.[62]

---

57 Mervyn Frost and Nicholas Michelsen, "Strategic Communications in International Relations: Practical Traps and Ethical Puzzles," *Defence Strategic Communications* 2 (2017): 9–34.

58 Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money* (New York: Institute of Modern Russia, 2014); and Christopher Paul and Miriam Matthews, *Russia's "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND Corporation, 2016).

59 "Russia's National Security Concept," Arms Control Association, January 1, 2000.

60 Sergei Blagov, "Russia Clarifies Looming Data Localization Law," Bloomberg Law, August 10, 2015.

61 "Putin Adviser Says Russia Ready To Deal With Internet Cutoff," Radio Free Europe/Radio Liberty, March 6, 2018.

62 "Russian Soldiers To Lose Smartphone Privileges over Leaks," *Moscow Times*, February 16, 2018.

In addition to controlling domestic access to information, Russia also seeks to isolate other states' populations from electronic information for limited periods of time similar to the Ukrainians' experience in 2014. Future electronic knockdowns may include physical attacks against information technology infrastructure that could create an immense shock in modern, information-centric societies.

Manipulation of the Russian Diaspora

The most successful Russian information operations outside of Russia target Russian speakers in former Soviet countries where their narratives resonate. Narrative battles are inherently identity battles.[63] Russian diaspora populations exist throughout Russia's near abroad as well as the United States and Western Europe. In 1992, President Boris Yeltsin established Russia's right to intervene in neighboring states to protect Russian people. Under Putin, in both Ukraine and Georgia, Russia has portrayed itself as protecting ethnically Russian separatists from non-Russophone governments to justify military intervention. Moreover, Russia's foreign policy seeks to influence all Russian *compatriots*, which include "Russian Federation citizens living abroad, former citizens of the USSR, Russian immigrants from the Soviet Union or the Russian Federation, descendants of compatriots, and foreign citizens who admire Russian culture and language."[64]

Although Russia crafts emotionally appealing nationalist narratives in which it is the protector of disaffected Russian compatriots abroad, it would be a mistake to assume that Russian information operations will only target, or even primarily target, the Russian diaspora. Russia fights on all narrative fronts and prioritizes to achieve the greatest gains. In the current conflict in Ukraine, for example, Russia crafts messages to several different layers of identity-defined audiences. Within Russia, it messages Russian citizens to ensure their support for the regime, primarily on television.[65] Near Russia, it messages would-be Russian citizens who are fighting to secede from Ukraine, on television, in print media, and through directed word-of-mouth.[66] Further abroad, it messages the Russian diaspora population in the West, in Russian on television and on social media; this population simultaneously receives messages targeted at the populations of their countries of residence, primarily on social media. Since these narratives have no guiding logic of facts, audiences often receive contradictory information. This conflict would undermine fact-based information but it advances Russia's objective to increase relativism.[67] Russia is not concerned about its own credibility because its core identity-defined audience will likely continue to believe its messaging.

---

63 Zaharna, "Reassessing 'Whose Story Wins.'"

64 Heather A. Conley et al., *Russian Soft Power in the 21st Century: An Examination of Russian Compatriot Policy in Estonia* (Washington, DC: Center for Strategic and International Studies, 2011), 12.

65 Vera Zakem et al., *Mapping Russian Media Network: Media's Role in Russian Foreign Policy and Decision-Making* (Arlington: CNA, 2018).

66 Kruk, "Analyzing the Ground Zero."

67 Alexey Kovalev, "Life after Facts: How Russian State Media Defines Itself through Negation," openDemocracy, June 13, 2016; and Paul and Matthews, *Russia's "Firehose of Falsehood."*

Unknown

While we have been able to observe several major Russian IO campaigns, there are still many outstanding questions about them. Most importantly, the West is uncertain if Russian information operations truly are decisive. The fact that Russia conducts information operations does not automatically mean it is successfully achieving its objectives with information operations.

As the West seeks to avert military conflict with Russia, understanding the conditions under which Russia will escalate from information operations to armed force is essential—but uncertain. Distinguishing the opening period of a hybrid campaign from routine Russian activity is challenging because "the preparatory phase of hybrid warfare does not differ that much from the conventional tools of Russian diplomacy."[68] Russia's decision to employ military forces is opportunistic and will likely be made only on the verge of actual operations, as it was in Crimea.[69]

Future Russian information operations will not inexorably escalate to kinetic action. Instead, Russia will consistently use information operations as an independent, decisive tool of statecraft. Russia launched an extensive cyberattack against Estonia in 2007 that was broadly comparable to its electronic knockdown of Georgia in 2008; but it did not attack Estonia.[70] In Estonia and Georgia, similar IO action in different geopolitical contexts, indicated disparate strategic intent. Given Russia's emphasis on the ability of information operations to paralyze military organizations and whole societies, the Kremlin may attempt to use the tool to prevent enemy military action as a nonkinetic preemptive or preventative option.

We must determine how Russia will use information as a future escalatory or de-escalatory action. We must also determine how Russia integrates information operations across other domains, which is of particular interest to the US Army as it develops multidomain battle doctrine. Russian maneuver in the physical domains of land, sea, air, and space may be intended to cause effects or to create advantages in the information domain. It is clear that the Russian armed forces are willing to use kinetic operations to seize control of key information technology. The more interesting question is the extent to which they are willing to use kinetic operations to align ground truth with propaganda themes or create new propaganda opportunities.

Conclusion

Russia, which claims the internet is a foreign plot, has mastered the use of the global network as a force-projection platform and a space for cognitive maneuver. By weaponizing information and employing information operations as a decisive tool of state power, Russia is now pressing its offensive advantages in the information domain to nullify its relative weaknesses in other domains. If Russia can divide any potential

68 Rácz, "Russia's Hybrid War," 73.

69 Daniel Triesman, "Why Putin Took Crimea: The Gambler in the Kremlin," *Foreign Affairs* 95, no. 3 (May/June 2016).

70 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

political base of support for military operations against it, its military limitations become irrelevant.

Paradoxically, Russia also is vulnerable in the information domain. Thus, Russian leaders are working to isolate Russian societies from supposed Western influence while expanding their own influence abroad. The Kremlin may be more susceptible to internal pressure than many have realized, which underscores its weakness. Putin's aggressive efforts to control the information domain are driven in part by an awareness that his aggressive foreign policy carries domestic political risks.

Russia has made a concerted effort to use their most advanced information capabilities against larger populations to alter recent elections in several Western countries. Whether this effort had an impact, however, is a matter of intense debate.[71] If it did not, the simplest explanation is that Russian operations were always intended for use in Russia's near abroad rather than distant states. Subversion, as a general rule, cannot create political divisions but merely exploit existing divisions within a population. Russia is intimately aware of—and often responsible for—the divisions in its near abroad but has a harder time understanding and manipulating them further afield. Some divisions, however, are obvious. The most dangerous for the United States is the inherent division between America and its allies since they are America's strategic center of gravity.[72]

In a society which values freedom of speech and, arguably, freedom of information, the United States cannot counter Russian information operations by imitation. Even at the height of the Cold War, the United States was never willing to engage in the sort of subversive influence operations employed by the Soviet Union. The United States, a democratic country with a strong rule of law, will always be at a disadvantage in playing a disinformation game. By leveraging its dominance in the information domain, fortifying itself and its allies against disinformation, and engaging in a whole-of-society approach to countering Russian information operations, however, America and its allies can defeat the Russian threat. Ukraine, which has significantly inhibited the impact of Russian information operations with private and public partnerships, is one model to consider. The challenge is to counter Russian disinformation without undermining Western values and subverting ourselves.

---

71 Robert M. Faris et al., *Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election*, version 1.3 (Cambridge, MA: Berkman Klein Center for Internet & Society, 2017).

72 General Joseph F. Dunford Jr., "Allies and Partners Are Our Strategic Center of Gravity," *Joint Force Quarterly* 87 (4th Quarter 2017).

T. S. Allen

Captain T. S. Allen, US Army, serves as the intelligence officer of Able Squadron, Asymmetric Warfare Group, which is aligned to EUCOM and AFRICOM. He is a graduate of the US Military Academy and holds a master of arts in war studies from King's College London, where he studied as a Rotary Scholar.

A. J. Moore

Master Sergeant A. J. Moore, a US Army senior infantry sergeant, serves as Troop Sergeant Major of 2 Troop, Able Squadron, Asymmetric Warfare Group. He has continuously deployed forward in support of global contingency operations in Afghanistan and Iraq with the 75th Ranger Regiment and 173rd Airborne Brigade since October 2001. He has also served as a senior operational advisor to US forces in Ukraine and Israel.