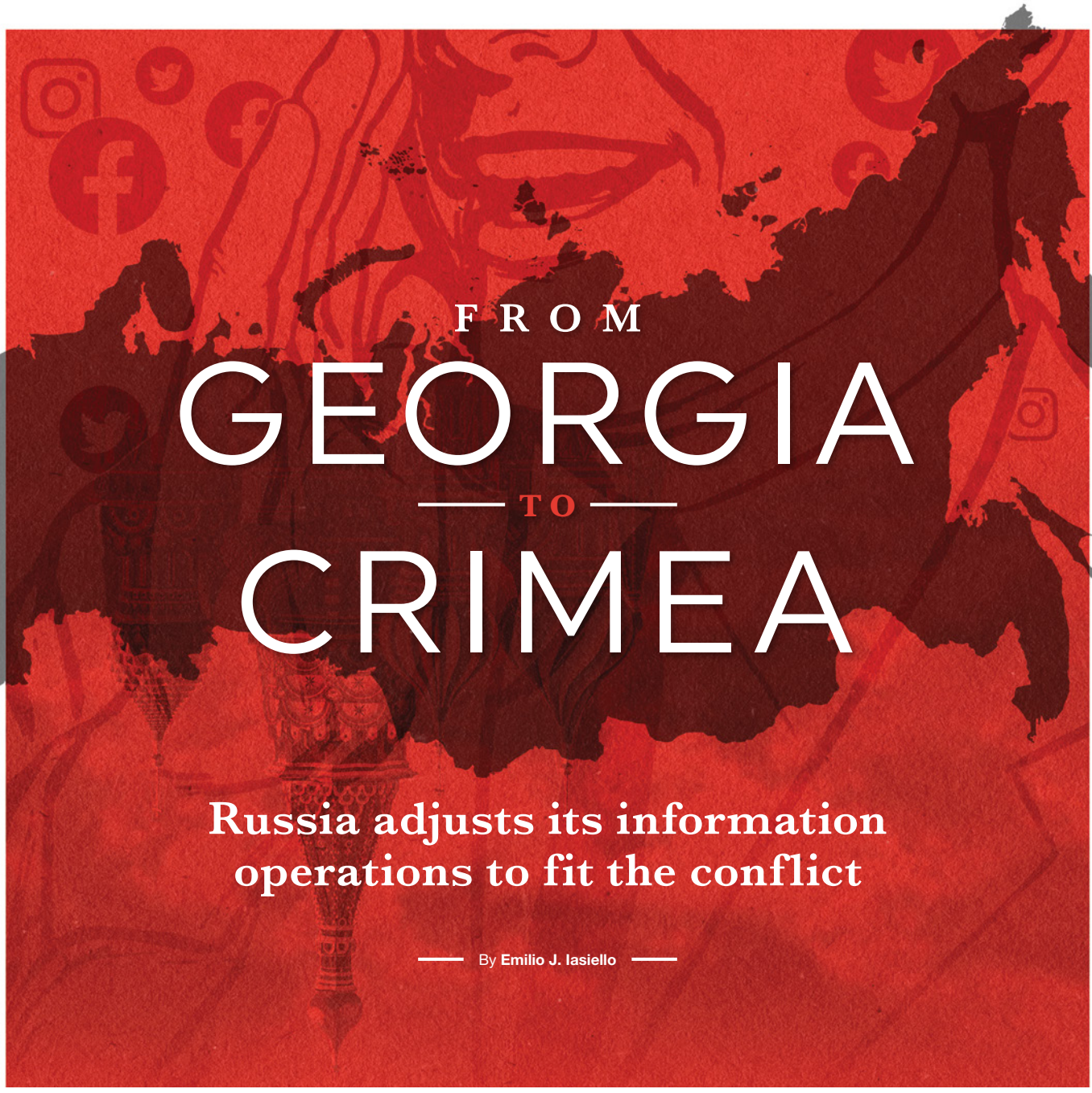

FROM GEORGIA TO CRIMEA

Russia adjusts its information operations to fit the conflict

By **Emilio J. Iasiello**

PER CONCORDIAM ILLUSTRATION

Russia has a long history of propaganda and disinformation operations — techniques it now adapts to the online environment. As the information space expands beyond the technologies facilitating its use, Russia uses broad information-based efforts classified by their effects: information-technical and information-psychological. A major milestone for these efforts surfaced in 2008 when pro-Russian cyber attacks occurred concurrently with Russian military operations in Georgia. During that brief conflict, a resilient Georgia overtook Russia in the larger information war, forcing Russia to rethink how it conducted information-based operations. Six years later, Russia adjusted its information confrontation strategy against Ukraine to quickly and bloodlessly reclaim Crimea and keep potentially intervening countries at bay. Clearly, Russia finds value in manipulating the information space, particularly in an age when news can be easily accessed through official and nonofficial outlets. Building on its success in Crimea, Russia is outpacing its adversaries by leveraging the information space to bolster its propaganda, messaging and disinformation capabilities in support of geopolitical objectives.

INFORMATION CONFRONTATION

Russia views offensive information campaigns more as influencing agents than as destructive actions, though the two are not mutually exclusive. Simply put, the information space allows information resources, including "weapons" or other informational means, to affect internal and external

audiences through tailored messaging, disinformation and propaganda campaigns. Igor Panarin, an influential scholar and well-regarded Russian information warfare expert, outlined the basic instruments involved in the larger information struggle: propaganda (black, gray and white); intelligence (specifically, information collection); analysis (media monitoring and situation analysis); and organization (shaping the opinion of politicians and mass media). In terms of influence operations, Panarin identified information warfare vehicles such as social control, social maneuvering, information manipulation, disinformation, purposeful fabrication of information, lobbying, blackmail and extortion.

Therefore, the essence of information confrontation focuses on this constant information struggle between adversaries. Reviewing the application of these principles in Georgia and Crimea, two well-known instances of Russian geopolitical involvement, help illustrate how Russia's understanding of information confrontation has evolved. It also provides insight into the outcomes of such practices in the context of on-demand media coverage.

GEORGIA, 2008

Russia and Georgia competed to control the flow of information to the global community during their brief conflict in 2008. Both sides employed kinetic (conventional military strikes and troop movements) and nonkinetic (cyber attacks, propaganda, and denial and deception) offensives. Russia's analysis and criticism of its efforts in the conflict led to some serious military reforms in its larger defense apparatus, wrote Athena Bryce-Rogers in an article in *Demokratizatsiya: The Journal of Post-Soviet Democratization*. Although experts observed alternating mission successes, the general consensus is that the Georgian government used the information and media space to its advantage to influence public opinion more successfully than Russia did.

Information-technical warfare

Russia's perception of technical and psychological information confrontation, working in concert with military attacks, became evident during the conflict in Georgia. Despite the lack of a substantive connection between the orchestrators of the cyber attacks and the Russian government, policy analyst David Hollis in a Small Wars Journal article, claimed that this nonattributable action was the first time cyber attacks and conventional military operations had been used together. Such attacks included webpage defacements, denial-of-service and distributed-denial-of-service attacks against Georgian government, media, and financial institutions, as well as other public and private targets. The attacks successfully denied citizen access to websites related to communications, finance and government, leaving some to speculate about Russian complicity, though no hard connection was made.

Information-psychological warfare

Russia also engaged in concurrent information-psychological operations, including propaganda, information control and

Russian troops atop an armored vehicle pass by a poster of then-Russian Prime Minister Vladimir Putin as they leave Tskhinvali, the capital of Georgia's separatist-controlled territory of South Ossetia, in August 2008. THE ASSOCIATED PRESS

disinformation campaigns, with varying results, especially in contrast to Georgia's efforts in the same areas. According to Ariel Cohen and Robert E. Hamilton in their 2011 book, *The Russian Military and the Georgia War: Lessons and Implications*, Russia focused on delivering key themes to the international community: Georgia and Mikheil Saakashvili, its president, were the aggressors; Russia was compelled to defend its citizens; neither the United States nor its Western allies had any basis for criticizing Russia because of similar actions these nations had taken in other areas of the world. By using television footage and daily interviews with a military spokesman, Russia attempted to control the flow of international information and sought to influence local populations by dictating news, sharing the progress of Russian troops protecting Russian citizens, and propagandizing Georgian "atrocities." A review of Georgian, Russian and Western media coverage during this period revealed then-Russian President Dmitry Medvedev was perceived as less aggressive than his Georgian counterpart. Indeed, a CNN poll conducted at the time found 92% of respondents believed Russia's intervention was justified.

Georgia wins the information war

But instead of acquiescing to Russia's information confrontation over the course of the crisis, Georgia launched an aggressive counterinformation campaign by employing its own disinformation and media manipulation. Georgia requested assistance from professional public relations firms and private consultancies to help promote its message, limited the availability of Russian news coverage, and reported Russian air raids on civilian targets, thereby becoming the victim of a Russian military invasion. Ultimately, Georgia gained the upper hand in the information conflict, a fact corroborated by Russia's review of its military's performance, which noted deficiencies in both the information-technical and information-psychological domains. Georgia won the hearts and minds of the global community even though Russia won the physical battlespace.

A Ukrainian soldier guards a road not far from the Russian border in April 2014 as a reported 40,000 Russian troops gathered along the border just weeks after annexing Crimea. AFP/GETTY IMAGES

UKRAINE, 2014

Six years after the Georgian conflict, Russia applied the lessons learned from its information activities in Georgia to its efforts in Ukraine. It learned to employ dedicated "information troops" and to strategically time cyber attacks, long considered a first-strike option for maximum effectiveness, particularly against important targets such as critical infrastructures. Unlike the concurrent digital attacks and military invasion in Georgia, cyber attacks against Crimea shut down the telecommunications infrastructure, disabled major Ukrainian websites and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula on March 2, 2014. Cyber espionage before, during and after Crimea's annexation also leveraged information that could support short-term and long-term objectives.

Information-technical means

Cyber espionage operations employed simultaneously with other methods of information collection appeared to accelerate battlefield tactics. Unlike in Georgia, cyber espionage targeted the computers and networks of journalists in Ukraine in addition to Ukrainian officials and those with NATO and the European Union. Exploiting such targets can provide insight into opposing journalistic narratives as well as advanced knowledge of important diplomatic initiatives. Operation Armageddon, for example, began targeting Ukrainian government, law enforcement and military officials in mid-2013 — just as active negotiations began for an EU-Ukraine Association Agreement, which Russia publicly deemed a national security threat.

As in Georgia, nationalistic hackers, such as the Ukraine-based CyberBerkut, also engaged in a variety of cyber attacks against Ukraine. This group executed distributed denial-of-service attacks and defacements against Ukrainian and NATO webpages, intercepted U.S.-Ukrainian military cooperation documents, and attempted to influence the Ukrainian parliamentary elections by disrupting Ukraine's Central Election Commission network. There was no evidence of collusion or direction by the Russian government, but the attacks did lend to the overall confusion during the crisis, particularly for Ukraine. Such attacks indicated that the Russian military had embraced Russian Gen. Valery Gerasimov's strategy on future warfare, that conflicts will retain an information aspect that is part of larger "asymmetrical possibilities for reducing the fighting potential of the enemy."

Information-psychological means

Unlike Russia's forceful invasion of Georgia, the contest over Crimean territory was more of an infiltration. In the absence of a direct threat, Russia relied on nonkinetic

options such as propaganda, disinformation, and denial and deception to influence internal, regional and global audiences. This reflexive control strategy — implementing initiatives to convey specially prepared information to an ally or an opponent to persuade them to make a voluntary decision predetermined by the initiator of the initiative — explains Russia's reliance on the approach as an extension of information-psychological activities in Ukraine during and after the Crimean crisis, as well as the method's prominence in Russia's information confrontation philosophy. According to British academic Keir Giles, in an article for NATO's Strategic Communications Centre of Excellence, the Russian approach to information confrontation was evolving, developing, adapting and, just like other Russian operational approaches, identifying and reinforcing success while abandoning failed attempts and moving on.

In a noticeable improvement from its efforts in Georgia, Russia used television broadcasts to generate support for actions in Crimea and to bolster Moscow's claim that its intervention was necessary to protect native Russian speakers. Additionally, pro-Russian online media mimicked anti-Russian news sources to influence opinion. For example, the website Ukrayinska Pravda was a pro-Russian version of the popular and generally pro-Ukrainian news site Ukrains'ka Pravda. The pro-Russian sources communicated false narratives about actual events, such as denying the Russian military's presence in Ukraine or blaming the West for conducting extensive informational warfare against Russia.

One significant lesson Russia learned from the Georgian conflict was how pervasively the internet could disseminate news from legitimate and semi-official organizations as well as personal blogs. Russian President Vladimir Putin acknowledged the role the internet played in influencing the outcome of regional conflicts and recognized Russia was behind other governments in this space, saying, "We surrendered this terrain some time ago, but now we are entering the game again." Russia began to support journalists, bloggers and individuals within social media networks who broadcast pro-Russian narratives. In one case, Russia paid a single person to hold different web identities, another person to pose as three different bloggers with 10 blogs, and a third to continually comment on news and social media. Such Russian trolls may be crass and unconvincing, but they do gain visibility by occupying a lot of space on the web. Arguably, "Russia's new propaganda is not … about selling a particular worldview, it is about trying to distort information flows and fueling nervousness among European audiences," wrote Alexey Levinson on the fact-checking website Stopfake.org. By adapting denial-and-deception strategies applied during the Georgian conflict, outside interlopers remained confused during the Crimean crisis. By denying involvement in the attacks until the later stages of the conflict, Russia could continue messaging its desire to de-escalate the crisis while increasing chaos. Since the U.S., NATO and the EU could not predict Russia's objectives, Russia could leverage reflexive control to operate within Western decision-making loops, reducing the costs of its actions against Ukraine and keeping the U.S. and its allies out of the conflict. Once Putin admitted the presence of Russian troops in Ukraine, he had already annexed Crimea. Ultimately, the U.S. conceded Russian control of Crimea and sent then-Secretary of State John Kerry to mitigate the threat of further expansion into Ukraine.

Russia's victory

Noticeably improved, Russia's strategic communications proactively targeted pro-Russian rebels, the domestic population and the international community to alienate Ukraine from its allies and sympathizers. Two key themes promoted the Ukrainian government as being anti-Russian and fascist and declared that the Russian administration would improve the population's quality of life. Messages directed at the pro-Russian rebels kept them engaged in the fight whereas messages to the domestic population in Russia created moral justification for supporting the rebels in eastern Ukraine and conveyed the extant intermittent prospect of widespread combat operations there. Six years after the U.S., NATO and several European governments sided with Georgia, Moscow sought to mitigate Crimea's external support via information activities aimed at influencing foreign government actions.

Moscow used pro-Russian media sources to spread photos of Ukrainian tanks, flags and soldiers altered to bear Nazi symbols in an effort to associate the Ukrainian government with resurgent Nazism, and thereby influence some European countries, such as Germany, to distance themselves from Kyiv. Another example involved disseminating images depicting columns of "refugees" fleeing Ukraine to Russia, when in reality these were people who commuted between Ukraine and Poland daily.

While the larger struggle with Ukraine continues, Russia's successful and bloodless usurpation of Crimea testifies to the lessons learned in Georgia's South Ossetia region. Russia's information confrontation strategy was more centralized and controlled in Crimea. Perhaps the most telling aspect of its success is that Russia kept its biggest adversaries, the U.S. and NATO, from intervening, thereby enabling a referendum in which the Crimean Parliament voted to join Russia. While the West refuses to acknowledge Crimea's secession, Russia claims full compliance with democratic procedures, a fact difficult to argue against on the international stage.

UKRAINE NOW

While some believe Ukraine is winning the information war because of the EU sanctions against Russia, discontent with the sanctions is growing among the EU citizenry, particularly in Greece, Hungary, Italy and, perhaps most importantly, in Germany. Furthermore, the sanctions are not the result of Ukrainian information warfare efforts as much as the international perception of Russia as the aggressor state, a view influenced by Russia's annexation of the region and suspected involvement in the downing of a Malaysia Airlines flight in 2014.

What's more, the longer Russia engages in eastern Ukraine, the more its objectives evolve. Russia is no longer entirely focused on inspiring pro-Russia militants in the region to rejoin Russia. It also seems to be combating U.S. influence while trying to keep Ukraine out of NATO. According to a 2015 report by the Institute for the Study of War, Russia has demonstrated that obfuscating its true intent preserves its options while confusing its adversaries. Hypothesizing by adversaries over Russia's true intent gives it the advantage, where it can leverage its flexibility to reach resolutions that benefit its interests. For example, while the U.S. and Russia were at odds over how to handle Syria, Russia's aid to embattled Syrian President Bashar al-Assad's forces successfully stopped U.S.-backed oppositionists to the extent that it compelled the U.S. into a quid-pro-quo relationship in which U.S. operational coordination against terrorist groups was given in exchange for Russia's commitment to stop Assad from attacking civilians and the U.S.-backed moderate opposition.

THE COLOR REVOLUTIONS, WHICH RESULTED IN SUCCESSFUL REGIME CHANGES, REINFORCED THE BELIEF THAT CONSTRUCTING, CONTROLLING AND DISSEMINATING INFORMATION EFFECTIVELY AND SUBSTANTIALLY INFLUENCES THE OUTCOME OF GEOPOLITICAL EVENTS.

This involvement made Russia an equal partner in the region, regardless of al-Assad's return to power. Similarly, Russia may surrender its short-term goals for eastern Ukraine to have autonomous rights in favor of the strategic gain of Ukraine not joining NATO. Some believe the economic burdens of eastern Ukraine may be too much for Russia to take on. If true, using the region as a bargaining chip for the greater prize serves Russia's long-term objectives.

EVOLUTIONARY THINKING

Information warfare has been referred to as an asymmetric weapon, and the incidents with Georgia and Crimea certainly support this categorization. The color revolutions, which resulted in successful regime changes, reinforced the belief that constructing, controlling and disseminating information effectively and substantially influences the outcome of geopolitical events. Russia, generally perceived as one of the leading powers in information warfare, lost its information struggle against Georgia in the early stages of the conflict. Conversely, by applying an adaptive approach, Russia adjusted its information confrontation strategy, successfully facilitating its appropriation of Crimea from Ukraine. Simply put, Russia learned from its mistakes in Georgia and thereby influenced the outcome in Crimea. As one Russia expert remarked during a Radio Free Europe/Radio Liberty report, "When you look at how Russia is attempting to copy Western style press briefings by the military ... it speaks volumes to their understanding of how better to structure public opinion around a military operation."

After its distributed denial-of-service attacks in Estonia in 2007, Russia's information-confrontation activities evolved from a tool used primarily for disruption to a tool of influence. The managing director for the Center for Security and Strategic Research at the National Defense Academy of Latvia echoes this sentiment by asserting influence operations are "at the very center of Russia's operational planning." Indeed, the more nonmilitary means are employed in areas of geopolitical tension, the more essential the leveraging of information confrontation becomes. As information is generally regarded as soft power, it may be most effectively implemented when there is no force-on-force military conflict, when information can be used to inform, persuade, threaten or confuse audiences, such as Russia's efforts to influence the 2016 elections in the U.S.

Unsurprisingly, Russian writing on information confrontation continues to evolve, a testament to the strategy being dynamic, much like the domain in which it is applied. While Gerasimov may have helped redirect Russian military thinking about the role of nonmilitary methods in the resolution of conflicts, other military experts built on that foundation. In 2013, retired Russian Col. S.G. Chekinov and retired Russian Lt. Gen. S.A. Bogdanov wrote that "a new-generation war will be dominated by information and psychological warfare that will seek to achieve superior control of troops and weapons and to depress opponents' armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory."

The use of the term "new-generation war" is a nod to the criticality of information dominance at a time when both the content of information and the technologies it traverses are heavily relied upon for civilian and military matters. Though new-generation war does not appear to have been used in military writings since 2013, a lack of official refutation by military officers suggests it may still be a relevant professional approach toward warfare.

Many Western scholars have categorized Russian tactics in Ukraine as hybrid warfare, the use of hard and soft tactics that rely on proxies and surrogates to prevent attribution, to conceal intent, and to maximize confusion and uncertainty. A 2015 article in *Military Thought* suggests this interpretation of the events in Ukraine may be incorrect and more accurately describes Western actions. In fact, by the end of 2015, Russian officers altogether refuted the use of "hybrid" to describe their activities. Nevertheless, the complementary and supportive role of information confrontation in Ukraine suggests it is best implemented in concert with other conventional and unconventional activities to achieve maximum effectiveness in larger campaigns

and not as a stand-alone tactic.

In 2015, the director of the Russian General Staff's Main Operational Directorate explained a "new-type warfare," similar yet distinct from hybrid and new-generation warfare, that associates indirect actions with hybrid ones. Other authors of new-generation warfare accepted the new terminology, particularly for activities focused on military, nonmilitary and special nonviolent measures to achieve information dominance, which logically includes actions in Ukraine. According to analyst Timothy L. Thomas, one author stressed that "information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, the global computer networks (blogs, various social networks, and other resources)."

Unsuccessful attempts to place information confrontation under the rubric of any specific modern warfare strategy, such as new-generation war, hybrid warfare, or new-type warfare, may further testify to the reciprocally dynamic and malleable nature of the strategy and conflict activities. The one aspect consistently carried through official Russian documents concerning information security doctrine and military strategy, and carried out in these regional conflicts, is the belief that information superiority is instrumental to future victories.

As the world moves toward conflicts in which, as Gerasimov describes, "Wars are not declared but have already begun," it is evident that — whether referred to as information warfare, information confrontation, information operations or information struggle — no state is guaranteed victory based solely on an abundance of resources or capabilities. The art of information confrontation must be practiced continuously, refined over time and tailored to specific audiences.

Russia actively refines its methods in real-time conflicts as it leverages and incorporates its information struggle into nonmilitary means to achieve political objectives. In this way, Russia is not learning from others as much as it is learning from itself. And therein may lie information confrontation's greatest strength: There is no cookie-cutter playbook from which it originates or to which it applies. Information campaigns can be tailored to suit each unique environment. The information campaign that worked in Crimea may produce different outcomes elsewhere, which reinforces Russia's lessons-learned approach — do not fight the next battle in the same way as the last one. The greatest asset of this capability is its flexibility to assume greater or lesser responsibilities dependent on requirements. This is paramount as the role of nonmilitary means to achieve political and strategic goals in conflicts has significantly increased.

CONCLUSION

Applying information warfare theories in today's geopolitical climate remains a work in progress. An around-the-clock news cycle and the various ways of disseminating and consuming information worldwide make it challenging to compete in information-based operations. But as observed in Georgia, smaller nations can competitively control information and influence target audiences to at least mitigate the efforts of, if not defeat, larger nations. Even after learning from its missteps in Georgia, Russia did not gain many Ukrainian regions. It lost opportunities in Luhansk and Donetsk when Russian troops were unable to penetrate the regions promptly. Russia, however, appears to be guided by Gerasimov's principle of refining information confrontation strategies by continuing to engage in various forms of official and unofficial messaging, as well as perfecting the art.

Ukrainian border guards patrol the Ukrainian side of the Ukraine-Russia border in Milove in eastern Ukraine in 2018. THE ASSOCIATED PRESS

One scholar of Russian propaganda refers to it as a war on information rather than an information war. Given the value Russia places on manipulating information, perceptions of the information space as potentially dangerous, and a successful agent for ousting governments and influencing public opinion and behavior, are understandable. A former KGB general stated the overall goal of Soviet propaganda was not far from the "subversion" pursued by Russia's modern internet disinformation campaign: "active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs."

While the media has focused on offensive cyber attacks and disruptive efforts to cripple critical infrastructures and to impede public access to financial institutions and emergency services, Russia understands the potential power associated with influencing via cyberspace. As such, Russia continues to refine its online information operations against regional and international targets, outpacing opponents in its nonoffensive cyber capabilities and demonstrating that not all threats in cyberspace are written in binary. □

This article first appeared in the journal *Parameters*.