Russia's Improved Information Operations: From Georgia to Crimea

Emilio J. Iasiello

ABSTRACT: After a series of military reforms resulting from the 2008 conflict with Georgia, Russia used information warfare operations more effectively in Crimea. Russia's continued refinement of its information operations may keep it ahead of the United States.

Russia has a long history of propaganda and disinformation operations—techniques it continues to adapt to the online environment. As the information space is broader than the technologies facilitating its use, Russia utilizes broad information-based efforts classified by effects: information-technical and information-psychological. A major milestone for these efforts surfaced in 2008 when pro-Russian cyberattacks 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 conducts information-based operations.

Russia adjusted its information confrontation strategy six years later against Ukraine, quickly and bloodlessly reclaiming Crimea and keeping potentially intervening countries at bay. Clearly, Russia finds value in manipulating the information space, particularly in an age where news can be easily accessed on demand through official and nonofficial outlets. Based on its successes in Crimea, Russia is outpacing its main adversary, the United States, by leveraging the information space to bolster its propaganda, messaging, and disinformation capabilities in support of geopolitical objectives.

Russian Information Confrontation

Russia has been long credited with having formidable information warfare capabilities.[1] Russian information confrontation theory covers a wide range of these actions and the conceptual understanding of Russian information operations stemming from cultural, ideological, historical, scientific, and philosophical viewpoints.[2] The broad nature of these activities views offensive information campaigns more as influencing agents than as destructive actions, though the two are not mutually exclusive. Simply put, the information space lends information resources, including "weapons" or other informational means, to affect both internal and external audiences through tailored messaging, disinformation, and propaganda campaigns.

Mr. Emilio J. Iasiello provides cyberintelligence to Fortune 100 clients and analyzes cyberthreats for domestic and international audiences based upon his 15 years' experience as a strategic cyberintelligence analyst.

1 Paul M. Joyal, "Cyber Threats and Russian Information Warfare," Jewish Policy Center, Winter 2016, http://www.jewishpolicycenter.org/2015/12/31/russia-information-warfare/.

2 Timothy L. Thomas, "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," *Journal of Slavic Military Studies* 11, no. 1 (1998): 40–62, doi:10.1080/13518049808430328.

Igor Panarin, an influential scholar and a well-regarded Russian information warfare expert, outlined the basic instruments involved in the larger information struggle including propaganda (black, gray, and white); intelligence (specifically information collection); analysis (media monitoring and situation analysis); organization (coordinating and steering channels and influencing media to shape the opinion of politicians and mass media); and other combined channels.[3] In terms of influence operations, Panarin identified information warfare vehicles such as social control; social maneuvering; information manipulation; disinformation; purposeful fabrication of information; and lobbying, blackmail, and extortion.[4] Therefore, the essence of information confrontation focuses on this constant information struggle between adversaries.

Reviewing the application of these principles in two well-known instances of Russian geopolitical involvement helps illustrate if and how Russian understanding of information confrontation has evolved; it also provides insight into the outcomes of such practices in the context of on-demand media coverage.

2008 Georgia

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 (cyberattacks, propaganda, and denial and deception) offensives. As reported, Russia's postanalysis and criticism of its efforts in the conflict led to some serious military reforms in its larger defense apparatus.[5] Although experts observed alternating mission successes, Anatoliy Tsyganok, then deputy chief of the General Staff of the Russian Armed Forces believed Georgia won the information war at the preliminary stage of the conflict, but lost at the end of it.[6]

Information-Technical

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 cyberattacks and the Russian government, this nonattributable action was the first time cyberattacks and conventional military operations had worked together.[7] Such attacks included web page 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.[8] The attacks successfully denied citizen access to 54 websites related to communications, finance, and government, leaving some

3 Jolanta Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*, Point of View 42 (Warsaw: Centre for Eastern Studies, May 2014).

4 Ibid.

5 Athena Bryce-Rogers, "Russian Military Reform in the Aftermath of the 2008 Russia-Georgia War," *Demokratizatsiya: The Journal of Post-Soviet Democratization* 21, no. 3 (July 2013): 339–68.

6 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).

7 David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal* 7, no. 1 (January 2011).

8 Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010).

to speculate at least some Russian complicity even though no hard connection was made.[9]

Information-Psychological

Russia also engaged in concurrent information-psychological operations—including propaganda, information control, and disinformation campaigns—with varying results, especially in contrast to Georgia's efforts in the same areas. 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; and 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, most notably in Kosovo.[10]

By using television footage and daily interviews with a military spokesman, Russia controlled 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.[11] A review of Georgian, Russian, and Western media coverage during this period reveals Russian President Dmitry Medvedev was perceived as less aggressive than his Georgian counterpart and had little justification for Russian intervention in South Ossetia.[12] Indeed, a CNN poll conducted at the time found 92 percent of respondents believed Russia was justified for intervening.[13]

Why Did Georgia Win the Information War?

Instead of acquiescing to Russia's information confrontation over the course of the crisis, Georgians launched an aggressive counterinformation campaign by employing their own disinformation and media manipulation.[14] 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.[15]

Ultimately, Georgia gained the upper hand in the conflict—a fact corroborated by Russia's review of its military's performance, which noted deficiencies in both the information-technical and

---

9 Jon Oltsik, "Russian Cyber Attack on Georgia: Lessons Learned?," *Cybersecurity Snippets* (blog), *Network World*, August 17, 2009, http://www.networkworld.com/community/node/44448).

10 Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle, PA: SSI, 2011).

11 Katie Paine, "Reputation Redux: Russia Invades Georgia by Land and by Server," PR News, August 25, 2008, http://www.prnewsonline.com/reputation-redux-russia-invades-georgia-by-land-and-by-server/.

12 Hans-Georg Heinrich and Kirill Tanaev, "Georgia & Russia: Contradictory Media Coverage of the August War," *Caucasian Review of International Affairs* 3, no. 3 (Summer 2009).

13 Yasha Levine, "The CNN Effect: Georgia Schools Russia in Information Warfare," The eXiled Online, August 13, 2008, http://exiledonline.com/the-cnn-effect-georgia-schools-russia-in-information-warfare/.

14 Ibid.

15 Tanya Erofeeva, "Georgia-Russia War: An Information Control Story," Prezi, May 6, 2014, https://prezi.com/i4fk4qprev0s/georgia-russia-war-an-information-control-story/; Matthew Mosk and Jeffrey H. Birnbaum, "While Aide Advised McCain, His Firm Lobbied for Georgia," *Washington Post*, August 13, 2008; Mark Ames, "Georgia Gets Its War On . . . McCain Gets His Brain Plaque . . . ," The eXiled Online, August 9, 2008, http://exiledonline.com/georgia-gets-its-war-onmccain-gets-his-brain-plaque/; and Levine, "CNN Effect."

information-psychological domains.[16] Georgia won the hearts and minds of the global community even though Russia won the physical battlespace. The disinformation campaign was so successful that the European Union's final report on the crisis focused on US support and military assistance to Georgia.[17]

2014 Crimea

In 2014, Russia created a similar situation with the region of Crimea. Like South Ossetia, Crimea had a substantial Russian-speaking population (approximately 58 percent at the time) and was generally considered pro-Russian.[18] Unlike South Ossetia, Crimea served as Russia's only year-round warmwater port, hosting a large portion of the Russian military—the navy's Black Sea Fleet.[19]

Information-Technical

Six years after the Georgian conflict, Russia applied the lessons learned from the informational activities in Georgia to its efforts in Ukraine. Although there is no evidence of dedicated "information troops" in the Russian military who could directly engage in local and regional areas yet, the innuendo reveals Russia is intent on learning from its failures and fixing its problems.[20] Russia also learned about timing cyberattacks, which have long been considered a first-strike option for maximum effectiveness, particularly against important targets such as critical infrastructures.[21]

Unlike the concurrent digital attacks and military border crossing in Georgia, cyberattacks 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.[22] Cyberespionage before, during, and after Crimea's annexation also leveraged information that could support short-term and long-term objectives, a tactic that had not transpired, was not reported, or went unnoticed against Georgia.

According to one security company, cyberespionage operations employed simultaneously with other methods of information collection appeared to accelerate battlefield tactics.[23] Unlike in Georgia, cyberespionage targeted the computers and networks of journalists

16 Thomas, "Russian Information Warfare Theory."

17 Peter Wilby, "Georgia Has Won the PR War," Guardian, August 17, 2008; and Independent International Fact-Finding Mission on the Conflict in Georgia, *Report,* vol. 1, (Brussels: Council of the European Union, September 2009).

18 Associated Press and Reuters, "Everything You Need to Know about Crimea," Haaretz, March 11, 2014, http://www.haaretz.com/world-news/1.577286.

19 For more on Russia adding frigates to the fleet in early 2016, which further demonstrates the strategic importance of Crimea, see Alexander Mercouris, "Russia Strengthens Its Black Sea Fleet," *Duran* (Cyprus), June 12, 2016.

20 Keir Giles, "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power" Chatham House, March 21, 2016, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-03-21-russias-new-tools-giles.pdf.

21 Cynthia Ayers, "Cyber Triggers and the First Strike Dilemma," Mackenzie Institute, October 19, 2015, http://mackenzieinstitute.com/cyber-triggers-first-stike-dilemma/.

22 Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, no. 1. (2015): doi:10.5038/2378-0789.1.1.1001.

23 Brian Prince, "'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: LookingGlass," Security Week, April 28, 2015, http://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass.

in Ukraine as well as Ukrainian, North Atlantic Treaty Organization (NATO), and European Union (EU) officials. Exploiting such targets could have provided Russia with insight into opposing journalistic narratives as well as advanced knowledge of important of key diplomatic initiatives. Operation Armageddon, for example, began targeting Ukrainian government, law enforcement, and military officials in mid-2013—just as active negotiations commenced for an EU-Ukraine Association Agreement, which Russia publicly deemed a national security threat.[24]

As in Georgia, nationalistic hackers, such as the Ukraine-based CyberBerkut, also engaged in a variety of cyberattacks against Ukraine. This group executed distributed denial of service attacks and defacements against Ukrainian and NATO webpages, intercepted US-Ukrainian military cooperation documents, and attempted to influence the Ukrainian parliamentary elections by disrupting Ukraine's Central Election Commission network.[25] While there is no evidence of collusion or direction on behalf of the Russian government, the attacks did lend to the overall confusion of the crisis, particularly for Ukraine, and might be reflective of the Russian military embracing Russian General Staff General Valery Gerasimov's strategy on the future of warfare—conflicts will retain an information aspect part of larger "asymmetrical possibilities for reducing the fighting potential of the enemy."[26]

Information-Psychological

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 incline him to make a voluntarily 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.[27]

More robust in Crimea than in Georgia, one scholar characterizes the Russian approach to information confrontation as evolving, developing, adapting, and just like other Russian operational approaches, identifying and reinforcing success while abandoning failed attempts and moving

---

24 Jason Lewis, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," *LookingGlass* (blog), April 28, 2015, https://lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_FINAL.pdf.

25 Petro Zamakis, "Cyber Wars: The Invisible Front," Ukraine Investigation, April 24, 2014, http://ukraineinvestigation.com/cyber-wars-invisible-front/; Unwala and Ghori, "Cybered Bear;" and Agence France-Presse (AFP), "Hackers Target Ukraine's Election Website," Security Week, October 25, 2014, http://www.securityweek.com/hackers-target-ukraines-election-website.

26 Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," trans. Robert Coalson, *Military Review* 96, no. 1 (January–February 2016): 23–29; and Mercouris, "Russia Black Sea Fleet."

27 The Soviet Union first used the term reflexive control, but the systematic methods of shaping an adversary's perceptions, and thereby his decisions, to force actions favorable to Russia's interests is used today. See Can Kasapoglu, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," Research Paper 121 (Rome, Italy: NATO Defense College, 2015); and Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (June 2004): doi:10.1080/13518040490450529.

on.[28] A noticeable improvement from its efforts in Georgia, Russia used television broadcasts to generate support for actions in Crimea and to bolster the theme of Moscow's necessary intervention to protect native Russian speakers.[29] 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 would communicate false narratives about actual events, such as denying the presence of the Russian military in Ukraine or blaming the West for conducting extensive informational warfare against Russia.[30]

One significant lesson Russia learned from the Georgian conflict was how pervasively the Internet could disseminate news from legitimate and semiofficial organizations as well as personal blogs. Valdimir Putin, the Russian president, acknowledged the role of the Internet 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."[31] Russia now supports journalists, bloggers, and individuals within social media networks who broadcast pro-Russian narratives.[32]

In one case, Russia paid a single person to hold different web identities, another to pose as three different bloggers with ten blogs, and a third to comment on news and social media 126 times every 12 hours.[33] 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 now about selling a particular worldview, it is about trying to distort information flows and fueling nervousness among European audiences."[34]

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 continued messaging its desire to de-escalate the crisis while increasing chaos.[35] Since the United States, NATO, and

---

28 Keir Giles, *The Next Phase of Russian Information Warfare* (Latvia: NATO Strategic Communications Centre of Excellence, 2016).

29 Colin Daileda, "Could Russia Use Cyberwarfare to Further Destabilize Ukraine?," Mashable, April 14, 2014, http://mashable.com/2014/04/14/russia-ukraine-cyber-warfare/.

30 Sascha Dov Bachmann and Håkan Gunneriusson, "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere," in "International Engagement on Cyber V: Securing Critical Infrastructure," special issue, *Georgetown Journal of International Affairs* (Summer 2015): 198–211; and " 'Ukraine, West Wage Information War against Us'—Russians," RT, November 12, 2014, http://www.rt.com/politics/204827-ukraine-west-information-warfare.

31 Paul Goble, "Russia: Analysis from Washington—A Real Battle on the Virtual Front," Radio Free Europe/Radio Liberty, October 9, 1999, http://www.rferl.org/content/article/1092360.html.

32 Jill Dougherty, *Everyone Lies: The Ukraine Conflict and Russia's Media Transformation*, Shorenstein Center on Media, Politics and Public Policy Discussion Paper, #D-88 (Cambridge, MA: Harvard Kennedy School, 2014).

33 Bachmann and Gunneriusson, "Russia's Hybrid Warfare."

34 Alexey Levinson, "Public Opinion and Propaganda in Russia," Stop Fake, July 29, 2015, http://www.stopfake.org/en/public-opinion-and-propaganda-in-russia/.

35 Robert C. Rasmussen, "Cutting Through the Fog: Reflexive Control and Russian STRATCOM in Ukraine," Center for International Maritime Security, November 26, 2015, http://cimsec.org/cutting-fog-reflexive-control-russian-stratcom-ukraine/20156; and Yuras Karmanau and Vladimir Isachenkov, "Vladimir Putin Admits for First Time Russian Troops Took Over Crimea, Refuses to Rule Out Intervention in Donetsk," *National Post* (Toronto, Ontario), April 17, 2014, http://news.nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russian-troops-took-over-crimea-refuses-to-rule-out-intervention-in-donetsk.

the European Union could not predict Russia's objectives, Russia could leverage reflexive control to operate within Western decision-making loops, to reduce the costs of its actions against Ukraine, and to keep the United States and its allies out of the conflict. Once Putin admitted the presence of Russian troops in Ukraine, he had already annexed Crimea.[36] Ultimately, the United States conceded Russian control of Crimea and sent Secretary of State John Kerry to mitigate the threat of further expansion into Ukraine.[37]

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 being anti-Russian Fascist and declared the Russian administration would improve the population's quality of life. Messages directed at the rebels kept them engaged in the fight whereas messages to the domestic population created moral justification for supporting the rebels and conveyed the extant intermittent prospect of widespread combat operations in eastern Ukraine.

Six years after the United States, NATO, and several European governments sided with Georgia despite the attack on South Ossetia, Moscow sought to mitigate Crimea's external support via information activities aimed at influencing foreign government actions. [38] 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 Kiev.[39]

Another example involved disseminating images depicting columns of refugees fleeing Ukraine to Russia, when in reality the people commuted between Ukraine and Poland daily.[40] Even cyberoperations effectively leaked stolen information such as the phone conversation between US Assistant Secretary of State Victoria J. Nuland and US Ambassador to Ukraine Geoffrey R. Pyatt, which may have embarrassed the United States.[41]

Russia's Victory

While the larger struggle with Ukraine continues, Russia's successful and bloodless usurpation of Crimea testifies to the lessons learned in South Ossetia. Russia's information confrontation strategy was more

---

36 Bachmann and Gunneriusson, "Russia's Hybrid Warfare"; and Karmanau and Isachenkov, "Vladimir Putin."

37 Paul Lewis, Spencer Ackerman, and Jon Swaine, "US Concedes Russia Has Control of Crimea and Seeks to Contain Putin," *Guardian*, March 3, 2014.

38 "Putin Slams U.S., Georgia's Western Allies," Truthdig, August 11, 2008, http://www.truthdig.com/eartotheground/item/20080811_putin_slams_us_georgias_western_allies#below.

39 Unwala and Ghori, "Cybered Bear."

40 Peter Pomerantsev, "Can Ukraine Win Its Information War with Russia?," *Atlantic*, June 11, 2014, http://www.theatlantic.com/international/archive/2014/06/can-ukraine-win-its-information-war-with-russia/372564.

41 Daisy Sindelar, "Brussels, Kyiv, Moscow React to Leaked Nuland Phone Call," Radio Free Europe/Radio Liberty, February 7, 2014, http://www.rferl.org/content/nuland-russia-eu-ukraine-reaction/25256828.html.

centralized and controlled in Crimea.[42] Perhaps the most telling aspect of success, Russia kept its biggest adversaries—the United States and NATO—from intervening thereby enabling a referendum in which the Crimean parliament voted to join Russia.[43] While the West refuses to acknowledge Crimea's secession, Russia attests full compliance with democratic procedures, a fact difficult to argue against on an international stage.[44]

Despite marked improvements, Russia does not deserve all the credit. Ukraine did not learn from Russia's missteps and was ill-prepared to handle Russia's cyber, media, and kinetic onslaught. With a lack of funding and information outlets, there is also little evidence of an aggressive Ukrainian counterinformation campaign. Historically, Ukraine has maintained passive propaganda, public relations, and lobbying practices and does not seem interested in changing.[45] Even since the Crimean independence referendum, Ukraine has not proficiently mitigated Russian information confrontation. According to one commentator, Ukraine "has no international voice or image" even though the entire course of events—from the takeover of parliament in Simferopol and dismantling of the Ukrainian military presence on the peninsula to the disputed referendum and the de facto annexation of the area to the Russian Federation—was accompanied by intense activity aimed to control the flow of information.[46]

Ukraine Now

While one Ukrainian diplomat believes Ukraine is currently winning the information war, possibly due to the European Union maintaining sanctions against Russia, discontent with the sanctions is growing among European Union citizenry, particularly in Greece, Hungary, Italy, and perhaps most importantly, Germany.[47] Furthermore, the sanctions are not the result of Ukrainian information warfare efforts as much as international perception of Russia as the aggressor state—a view influenced by Russia's annexation of the region and suspected involvement in downing Malaysia Airlines flight MH17 (2014).[48]

What's more, the longer Russia engages eastern Ukraine, the more its objectives evolve. No longer entirely focused on inspiring separatists in the region to rejoin Russia in a manner similar to Crimea, Russia also seems to be combatting US influence in similar affairs

---

42 US Army Special Operations Command (SOC), *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014* (Fort Bragg, NC: SOC, June 2015).

43 Luke Harding and Shaun Walker, "Crimea Applies To Be Part of Russian Federation after Vote To Leave Ukraine," *Guardian*, March 17, 2014, https://www.theguardian.com/world/2014/mar/17/ukraine-crimea-russia-referendum-complain-result.

44 Sputnik, "US Policy toward Crimea Defies Reality," Russia Insider, March 16, 2015, http://russia-insider.com/en/2015/03/16/4534.

45 Taras Kuzio, "Is Ukraine Really Winning the 'Information War' with Russia?," *Kyiv Post*, July 18, 2016.

46 Pomerantsev, "Can Ukraine Win?"

47 RIA, "Parubiy: Ukraine Is Winning the Information War against Russia," Fort Russ, July 2, 2016, http://www.fort-russ.com/2016/07/parubiy-ukraine-is-winning-information.html; and Finian Cunningham, "Europe Revolts against Russian Sanctions," Strategic Culture Foundation, May 26, 2016, http://www.strategic-culture.org/news/2016/05/26/europe-revolts-against-russian-sanctions.html.

48 Ibid.

while trying to keep Ukraine out of NATO.[49] Moreover, Russia has demonstrated that obfuscating its true intent preserves its options while confusing its adversaries.[50]

Hypothesizing over Russia's true intent puts the advantage in its hands. Leveraging flexibility brings beneficial resolutions—for example, while assessing Syria in 2016, Russia's aid to Assad's forces successfully stopped US-backed opposition. The United States adopted a quid pro quo giving operational coordination against terrorist groups in exchange for a Russian commitment to stop Syrian President Bashar al-Assad from attacking Syrian civilians and the moderate opposition.[51]

This involvement made Russia equal partners in the region, regardless of 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.[52] If true, using the region as a bargaining chip for the greater prize serves Russia's long-term objectives.

Information Confrontation—Evolutionary Thinking

Information warfare has been referred to as an asymmetric weapon, and the incidents with Georgia and Crimea certainly support this categorization.[53] Following the Color revolutions, which resulted in successful regime changes, both the Georgian and Crimean incidents reinforce the belief that constructing, controlling, and disseminating information effectively and substantially influences the outcome of geopolitical events.[54]

Russia, generally perceived as one of the leading powers in information warfare, lost its information struggle against Georgia, the smaller country with less military capability and military history.[55] Conversely, by applying an adaptive approach, Russia adjusted its information confrontation strategy, successfully enabling Crimea's secession from Ukraine. Simply, Russia learned from its mistakes in Georgia, centralized generation and dissemination of its information and propaganda, and thereby subtly influenced Crimea's final outcome. As one Russian expert remarked, "When you look at how Russia is attempting to copy Western style press briefings by the military . . . it

49 Matthew Chance, "What Does Russia's President Putin Really Want?," CNN News, February 11, 2015, http://www.cnn.com/2015/02/11/world/chance-putin-analysis/.

50 Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Institute for the Study of War, September 2015).

51 Daniel R. DePetris, "America Has No Choice But To Cooperate with Russia in Syria," *The Skeptics* (blog), *National Interest*, July 18, 2016, http://nationalinterest.org/blog/the-skeptics/america-has-no-choice-cooperate-russia-syria-17027.

52 "Does Russia Really Want Eastern Ukraine?," *World Policy* (blog), http://www.worldpolicy.org/world-views/does-russia-really-want-eastern-ukraine.

53 James R. McGrath, "Twenty-First Century Information Warfare and the Third Offset Strategy," *Joint Forces Quarterly* 82, no. 3 (July 2016).

54 For more on the Rose Revolution (Georgia, 2012), the Orange Revolution (Ukraine, 2004), and the Tulip Revolution (Kyrgyzstan, 2005), see Anthony H. Cordesman, *Russia and the "Color Revolution": A Russian Military View of a World Destabilized by the US and the West* (Washington, DC: Center for Strategic and International Studies, 2014).

55 Andrew Lisa, "Information Warfare: Major Cyber War Powers," Strategy Page, March 13, 2014, https://www.strategypage.com/htmw/htiw/articles/20140313.aspx.

speaks volumes to their understanding of how better to structure public opinion around a military operation."[56]

Reviewing Russia's information-related activities since the 2007 Estonia distributed denial of service incident, information confrontation has evolved from a tool used primarily for disruption to a tool of influence. The managing director for the Center of Security and Strategic Research at the National Defense Academy of Latvia echoes the sentiment by asserting influence operations are "at the very center of Russia's operational planning."[57] Indeed, the more nonmilitary means are employed in areas of geopolitical tension, the more essential leveraging information confrontation becomes. As information is generally regarded as a soft power, it may be most effectively implemented in times other than force-on-force military conflict where, depending on its intent and objectives, information can be used to inform, persuade, threaten, or confuse audiences.

Unsurprisingly, Russian writing on information confrontation continues to evolve, a testament to the strategy being dynamic and fluid 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 thought leadership builds on the foundation. In 2013, two Russian authors acknowledged "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."[58]

The use of "new-generation war" nods to the criticality of information dominance in a time where the content of information is as heavily relied upon for civilian-military matters as well as the technologies it traverses. 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.[59]

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.[60] A 2015 article from *Military Thought* suggests this interpretation of the events in Ukraine may be incorrect,

---

56 Mike Eckel, "Russia's Shock and Awe: Moscow Ups Its Information Warfare in Syria Operation," Radio Free Europe/Radio Free Liberty, October 7, 2015, http://www.rferl.org/content/russia-syria-shock-awe-military-air-strikes-information-warfare/27293854.html.

57 Tony Balasevicius, "Russia's 'New Generation War' and Its Implications for the Arctic," Mackenzie Institute, November 10, 2015, http://mackenzieinstitute.com/russias-new-generation-war-implications-arctic/.

58 Colonel S. G. Chekinov (Res.) and Lieutenant General S. A. Bogdanov (Ret.), "The Nature and Content of a New-Generation War," *Military Thought* 4 (2013).

59 Timothy L. Thomas, *Russia Military Strategy: Impacting 21st-Century Reform and Geopolitics* (Fort Leavenworth, KS: Foreign Military Studies Office, 2015); and Timothy L. Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4. (October 2016): 554–575, doi:10.1080/13518046.2016.1232541.

60 Andrew Monaghan, "The 'War' in Russia's 'Hybrid Warfare'," *Parameters* 45, no. 4 (Winter 2015–16): 65–74.

more accurately describing Western actions.[61] In fact, by the end of 2015, Russian officers altogether refuted the use of "hybrid" to describe their activities.[62] 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 Operation's Directorate explained a "new-type warfare," similar yet distinct from hybrid and new-generation warfare, that associates indirect actions with hybrid ones.[63] 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. One author stressed "information warfare in the new conditions will be the starting point of every action now called the new-type of warfare (a 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)."[64]

Unsuccessful attempts to place information confrontation under the rubric of any specific modern war 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 the 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, in the process, leads states' conduct of such operations in the future. 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 suite 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

61 Thomas, *Russia Military Strategy*.

62 Ibid.

63 Thomas, "Russian Military Thought"; and 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, April 2016).

64 Thomas, "Russian Military Thought."

last one. The greatest asset of this capability is the flexibility to assume greater or lesser responsibilities given the nature of requirements, which is paramount as the role of nonmilitary means to achieve political and strategic goals in conflicts has significantly increased.

Recommendations

The United States needs to address hostile information activities from its adversaries more efectively. As observed in the recent hacking scandals surrounding the US presidential election in which Russia targeted and, according to the US intelligence community, used information to disrupt and ultimately help its candidate of choice to win, the soft power most effective in confounding the United States is information itself, and not necessarily any production or dissemination technology.[65] Given the fact that Russia spends approximately $400–$500 million per year on foreign information efforts, while the US spends $20 million USD on Russian language services, it is easy to see that the United States is far behind.[66] Some recommendations to address this shortcoming include:

National counterinformation strategy and center. The United States' offensive cybercapability is generally considered among the most sophisticated and powerful on the planet; however, as observed in efforts against the Islamic State, America has been less adept in countering online messaging despite substantial resources.[67]

In late December 2016, President Barack Obama authorized $611 billion for the military in 2017 and to establish a Global Engagement Center to track foreign propaganda and disinformation efforts undermining US national security interests.[68] Little information on the development of this entity is available to date, although a similarly named center focusing on Islamic State messaging is headquartered in the State Department. Such a center should serve as a central, coordinating entity as well as model the operations of the National Counterterrorism Center, which maintains cross-government civilian and military representation and directly advises the Director of National Intelligence. Furthermore, this center needs to collaborate with national security stakeholders to develop unique strategies for each state and nonstate actor.

Protect against fake news. The rampant proliferation of fake news, such as observed during the US elections and annexation of Crimea, undoubtedly plays a pivotal role in Russian information operations.[69] One initiative to help reduce fake news involves leveraging

---

65 US National Intelligence Council (NIC), Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution (Washington, DC: NIC, 2017).

66 Pavel Koshkin, "The Paradox of Kremlin Propaganda: How It Tries to Win Hearts and Minds," Russia Direct, April 2, 2015 http://www.russia-direct.org/analysis/paradox-kremlin-propaganda-how-it-tries-win-hearts-and-minds; and Warren Strobel, "U.S. Losing 'Information War' to Russia, Other Rivals: Study," Reuters, March 25, 2015.

67 Danny Vinik, "America's Secret Arsenal," Politico, December 9, 2015; Emilio Iasiello, "Rebooting the U.S.' New Counter Messaging Efforts against ISIS," Dead Drop, February 16, 2016, http://deaddrop.threatpool.com/rebooting-the-u-s-new-counter-messaging-efforts-against-isis/; Eric Geller, "Why ISIS Is Winning the Online Propaganda War," *Daily Dot* (Austin, TX), March 29, 2016; and Arturo Muñoz and Erin Dick, *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness* (Santa Monica, CA: RAND Corporation, 2015).

68 National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 (2016).

69 Andrew E. Kramer, "To Battle Fake News, Ukrainian Show Features Nothing but Lies," *New York Times*, February 26, 2017.

cutting-edge technology to help identify the fabrications as soon as they emerge. Artificial intelligence and data analytics can be used to detect words or word patterns that might indicate deceitful stories. In addition, the US government via the Department of Homeland Security should implement a strategy for educating the public as well as identifying and reporting fake news outlets in much the same way cyberscams are reported to the Federal Bureau of Investigation.

International engagement. The global nature of the Internet provides many outlets for disseminating legitimate and illegitimate information. A myriad of social media platforms can also be used to promote slanted news stories and propaganda via Internet trolls. Increasing international collaboration among law enforcement and intelligence professionals who specifically focus on these outlets will help agencies identify and disable these sources.

Conclusions

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 implementing information-based operations and tailoring messaging against competing narratives challenges. 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. Russia 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.

One scholar of Russian propaganda refers to it as less of an information war as much as a war on information. 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 Union 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 cyberattacks 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 the United States in nonoffensive cybercapabilities and demonstrating not all threats in cyberspace are written in binary.