Russian Actions and Methods against the United States and NATO

Maj. Collins Devon Cockrell, U.S. Army

Russia has worked to upend the post-Cold War European order through an aggressive campaign of information warfare in recent years—so much so that the 2017 European Command Posture Statement identifies Russia as the primary threat, stating that "Russia seeks to undermine this international system and discredit those in the West who have created it."[1] In January 2017, retired Gen. James Mattis, then the nominee for U.S. secretary of defense, stated that Russia was the number one threat to the United States and was engaging in a continuing effort to "break the North Atlantic alliance."[2] President Vladimir Putin's speech at Munich in 2007 declared that Russia would execute a foreign policy that no longer recognized a U.S.-led, unipolar system.[3] Putin stated publically that the West, specifically the United States, was attempting to make Russia a weak "vassal" state and was preventing Russia from reclaiming its role as the inheritor of the Soviet Union's counterbalance role in the world.[4] The hyperbolic and confrontational worldview of the Russian ruling elite can be summarized in reported comments by Andrey Krutskikh, a senior advisor to President Putin, at a February 2017 Moscow conference:

> You think we are living in 2016. No, we are living in 1948. And do you know why? Because in 1949, the Soviet Union had its first atomic bomb test. And if until that moment, the Soviet Union was trying to reach agreement with [President Harry] Truman to ban nuclear weapons, and the Americans were not taking us seriously, in 1949 everything changed and they started talking to us on an equal footing.[5]

As a direct reflection of this, Russia is intervening in political systems across Europe in order to destabilize established and newer democratic states. Putin's stated goal is the restoration of "Great Russia."[6] This paper briefly overviews United States and NATO information operations (IO) doctrine and contrasts those with current analysis of Russian concepts of information warfare.[7] This overview is intended to orient readers to important distinctions in doctrine, capacity, and purpose so that Western actors have a firm understanding from which to make decisions.

U.S. doctrine defines information operations as "the integrated employment, during military operations, of IRCs [information-related capabilities] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."[8] These IRCs include military information support operations (MISO),

Maj. Collins Devon Cockrell, U.S. Army, serves as the S-3, 7th Psychological Operations Group, Mountain View, California. He holds an MA in political science from the University of Arkansas and an MMAS from the Command and General Staff College, Fort Leavenworth, Kansas. His previous assignments include course manager and instructor of the Psychological Operations Officer Qualification Course at the John F. Kennedy Special Warfare Center and School, Fort Bragg, North Carolina, as well as tours in Korea and deployments to Iraq in 2004 as an engineer and in 2009 as a psychological operations detachment commander.

cyberspace operations, electronic warfare, military deception, civil military operations, and public affairs.[9] As a coordinating function within the realm of disseminating and shaping information, IO is a critical part of all offensive, defensive, and stability operations. In U.S. doctrine, the main effort of influencing foreign target audiences is by psychological operations (PSYOP) forces performing MISO. PSYOP forces are doctrinally tasked to

> develop and convey messages and devise actions to influence select foreign groups and promote themes to change those groups' attitudes and behaviors. MISO can also degrade the enemy's combat power, reduce civilian interference, minimize collateral damage, and increase the population's support for operations.[10]

U.S. and Western IO actions and programs to respond to Russian actions have increased since the annexation of the Crimea from Ukraine. NATO member states have recognized the increasing threat of Russian efforts to influence their internal politics and exacerbate divisions. However, these Western programs are an order less than Russian activity because of the power of Russian corruptive influence. A core part of U.S. and NATO strategy is the support and development of organizations that analyze threats in the

The cover photo of the NATO Strategic Communications Centre of Excellence's first journal issue of *Robotrolling* 2017 visually depicts the rise of automation in social media. The NATO Strategic Communications Centre of Excellence is one of dozens of institutions dedicated to information gathering and analysis to assist NATO members with its complex decision-making process. (Graphic from *Robotrolling* 1 [2017], accessed 8 September 2017, http://www.stratcomcoe.org/robotrolling-20171.)

information domain and make recommendations to Western governments, militaries, and coalitions. For example, in 2014, NATO approved the establishment of the NATO Strategic Communications Centre of Excellence (StratCoE) in Riga, Latvia.[11] This organization is tasked with countering violent extremism and hostile influence, especially in the area of the Baltic States. It has produced an extensive amount of analysis of Russian activities across the continent. Not a formal part of the NATO command structure, NATO StratCoE serves as a type of influence think tank for NATO, tasked "to contribute to the Alliance's communication process by providing comprehensive analyses, timely advice and practical support to the Alliance."[12] The focus is understanding extremism and hostile influences, as well as supporting the NATO Military Committee's strategic communications plan and Alliance doctrine. One of the most prominent researchers working for NATO organizations, Keir Giles, has also written official NATO analysis, including the 2016 NATO "Handbook of Russian Information Warfare."[13] NATO StratCoE is an effective support to NATO members on issues of extremism, as well as Russian actions targeting Europe.

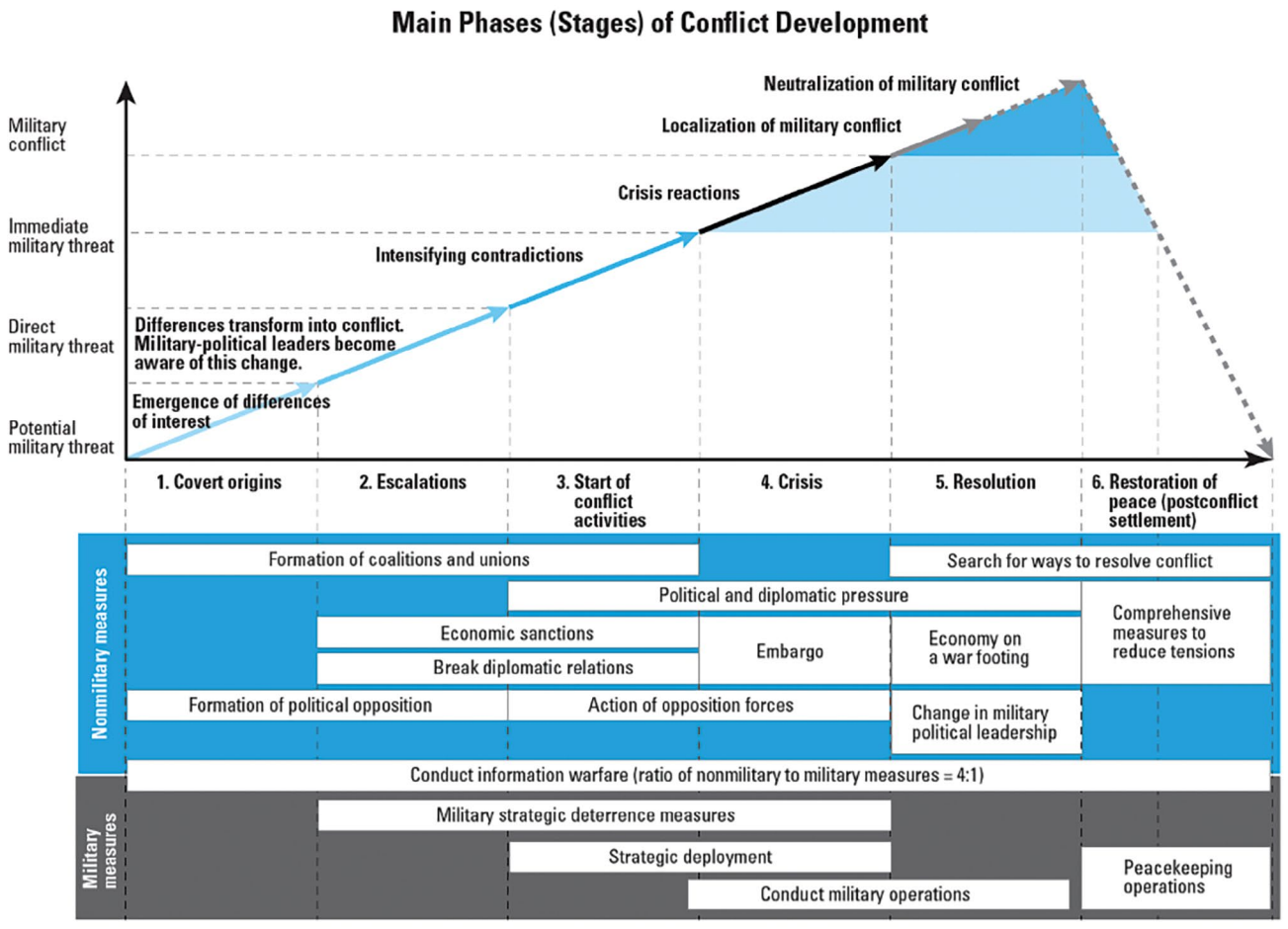
NATO doctrine on PSYOP nests within the U.S. MISO doctrine. It uses similar terms for key concepts, like target audience analysis, the analytical process by which the most useful population or group is identified for achieving a behavioral change in support of mission requirements and supporting the commander's goals.[14] The limitations on NATO's ability to respond to Russian actions is not a doctrinal insufficiency, but rather the problem of twenty-nine member states coordinating a timely and unified response within a rapidly changing information environment. Outside of declaration of hostilities against NATO members, the processes for action by member states through the military committees that coordinate activities cannot match the unified action of the Russian dictatorship. NATO member states have recognized the increasing threat of Russian efforts to influence their internal politics and also exacerbate division. As Constance Steltenmuller of the Brookings Institution testified before the Senate Intelligence Committee in June 2017, the goal of Russian information warfare is to succeed in "destabilizing the European project from the inside out: dismantling decades of progress toward building a democratic Europe that is whole, free, and at peace."[15] In April 2017, nine European Union and NATO member states agreed to create a combined organization for active cooperation in "countering hybrid warfare" to be located in Helsinki.[16] The current National Defense Authorization Act authorizes a $80 million dollar "Countering Russian Influence Fund," to support "civil society organizations and other entities."[17] Controversy has followed this action by Congress to require a specific action by the US Government, as the U.S. Department of State refused until August 2017 to provide a plan to spend the funds through the State Department's Global Engagement Center.[18]

In these and other ways, NATO and allied European states are coordinating their responses to this onging conflict with Russia in the information domain. But the strategies of coalitions are much more complicated to execute than those of a unified, authoritarian actor like Russia. Further, the essential element of both U.S. and NATO PSYOP and influence doctrine centers on the persuasive messages being disseminated being based upon truthful information to influence the target audience. As the NATO manual states, "PSYOPS must be based on true information. Using false information is counter-productive to the long-term credibility and success of PSYOPS."[19] This is both a strength and a limitation. The strength is that credibility and the power it conveys, but the limitation is that Russia has no such constraints to its influence campaigns.

Russia's view of this kind of warfare is that is can begin before hostilities have begun. As cited by Keir Giles in his NATO Defense College monograph "Handbook of Russian Information Warfare":

> The Russians use information from a covert stage through six phases of warfare to the re-establishment of victory. Information confrontation is conducted in every phase, including covertly, in peace and in war. Our doctrines do not allow us to do a lot of this stuff till the fighting basically starts.[20]

President Putin and his military strategists have based their actions upon what in Russia is called "new generation warfare." In the *Military Doctrine of the Russian Federation,* first published in 2000, the "Russians recognized the need/necessity for their armed forces to operate in the 'information space' and the existence of 'information threats' faced by the Russian army."[21] For

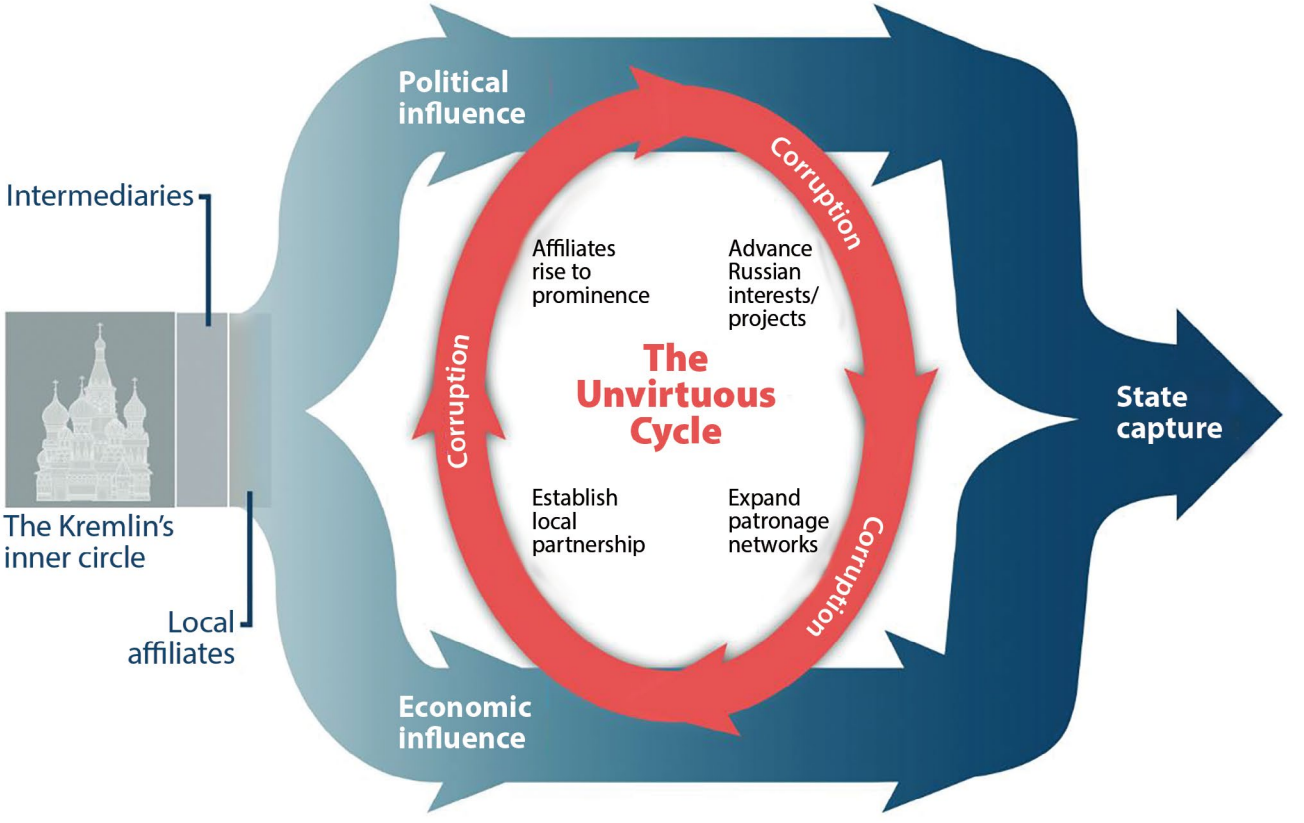


(Graphic from National Security Analysis Department, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014,* Assessing Revolutionary and Insurgent Strategies Study [unclassified working draft, Fort Bragg, NC: U.S. Army Special Operations Command], 18.)

Figure 1. The Role of Nonmilitary Methods in Interstate Conflict Resolution

the United States and NATO, hybrid warfare, along with information warfare, is the term most often used by military and civilian analysts to describe Russian activities. U.S. doctrine states that "a *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects."[22] This definition is in line with Russian conception of new generation warfare. Importantly, the Russian view of this kind of warfare differs from asymmetric warfare as the tool of an inherently weak opponent against a stronger one. Russia turns this on its head in regards to former Soviet states. Russia uses these hybrid methods against weaker or peer states to achieve foreign policy or military goals. Russia aims to achieve decisive political outcomes with little or no military power, but it is ready to use overwhelming military force if necessary.[23] In this way, an alliance like NATO is at a disadvantage, not just because it is a coalition structure, but because these hybrid or asymmetric methods are more difficult to categorize as having crossed the threshold of an actual "attack" against a member state.

Since 2012, Russia's military strategy has been centered around the "Gerasimov Doctrine," derived from a series of speeches and statements from the Russian Army's Chief of Staff, General Valery Gerasimov. General Gerasimov's ideas are his synthesis of a kind of unconventional warfare or asymmetric warfare. This method aims to create a viable "internal opposition" within a state.[24] This phased process of Russian irregular warfare, described in figure 1, is cogently articulated by Charles K. Bartle in the 2016 article



(Graphic from Heather Conley, James Mina, Rusland Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* [Washington, DC: Center for Strategic & International Studies, 2016], 3, accessed 18 July 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf.)

Figure 2. Channels of Russian Influence

"Getting Gerasimov Right."[25] It was also cited in the 2016 U.S. Special Operations Command document *"Little Green Men": A Primer on Modern Russian Unconventional Warfare.*[26]

As Gerasimov stated:

> The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.[27]

Gerasimov's discussion of the coordination of economic, diplomatic, political, combined with military force, is akin to the older term "political warfare" to define these actions. It is a term that originated in World War Two but is again in use in the U.S. special operations community.[28] Russian military strategy envisions targeting otherwise stable countries which can then be rapidly destabilized using nonmilitary actions.[29] Russian methods are centered on locating the weaknesses and internal divisions of the targeted state and exploiting those to undermine their society. These actions can include "involvement of the population's protest potential, special operations forces, and covert military and information warfare measures."[30]

As vividly described in *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Russian influence, coordinated through Russian ethnic criminal networks, can be used to increase societal corruption and has an effect like a debilitating disease, where "malign Russian influence can be likened to a virus that attacks democracies."[31] Russia uses economic power, specifically channeled through paths of corruption, to influence decision makers and political and economic institutions across Europe. The goal of this covert influence directed at elected officials, businessmen, media organizations, political parties, and political movements is to "sway, through coercion and corruption, the region's

policies away from European integration and toward Russia."[32] Figure 2 (on page 5) from *The Kremlin Playbook* illustrates this process.

The activities that Russia has pursued across Europe over the last five years are not new, though innovative application of technological means to disseminate their messages has made these activities far more effective than previous attempts. Russian influence methods and doctrine dates to before and during World War II:

> Modern Russian information warfare theory directly derives from *spetspropaganda,* first taught as a subject at the Russian Military Institute of Foreign Languages in 1942, but with origins lying deep in Marxist-Leninist ideology.[33]

Current Russian information warfare is a well-executed update of these older methods. These older tactics center on two main elements: *active measures* and *reflexive control.* Active measures include efforts to influence, undermine, disrupt, and discredit targeted countries, their institutions and nongovernmental organizations.[34] Reflexive control is similar both to U.S. Department of Defense descriptions of military deception and psychological operations. But this activity operates without the requirement of using truthful information. As Russian analyst Timothy Thomas describes in his 2013 article *Russian Military Thought,* reflexive control attempts to manipulate and confuse the decision maker of the targeted organization to paralyze "the adversary's (decision makers) intelligent (creative) activity."[35] The NATO "Handbook of Information Warfare" defines reflexive control as intending to "manipulate the decision making of the targeted organization "by altering key factors in the adversary's perception of the world … by causing him to choose the actions most advantageous to Russian objectives."[36] Russian doctrine, as expressed through the Russian general staff, asserts the following:

> Wars will be resolved by a skillful combination of military, nonmilitary, and special nonviolent measures that will be put through by a variety of forms and methods and a blend of political, economic, informational, technological, and environmental measures, primarily by taking advantage of information superiority.[37]

Jolanta Darczewksa, writing from the Polish perspective, also argues that Russian information warfare is a return to Soviet practices:

> The doctrinal assumptions about information warfare demonstrate not so much a change in the theory of its conduct (the changes mainly relate to the form of its description, and not the content), but rather a clinging to old methods (sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population).[38]

Russian methods today are far advanced of those used against Georgia in 2008, especially involving the targeted use of use of social media. In *Social Media as a Tool of Hybrid Warfare,* the NATO Strategic Communications Centre identified "hybrid trolls" that operate "in the context of a particular political or military agenda."[39] The Russian government uses fake websites that appear to be independent sources of information. These "sock puppet" sites acting as news aggregators have been especially effective in influencing audiences outside Russia during operations like those in Crimea. Igor Panarin is an influential theorist of Russian information warfare and extreme Russian nationalism. Speaking in 2014, as noted by Darczewska, Professor Panarin, then on faculty at the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, described actions aimed at Ukraine during the Crimean annexation as "defensive information warfare" executed as a planned and coordinated campaign, approved by and directed personally by Putin.[40]

As an important part of the Russian nationalist movement and a useful resource for Russian influence, Russians living outside of Russia proper have been identified and recruited into the role of agents of influence, as "compatriots living abroad." Viewed by Russia to be legally connected to the mother state, compatriot status provides rights outside of national citizenship to the self-identified Russian.[41] Russia uses this network of ethnic Russians and Russia supporters as a way to exert pressure and influence in targeted states. Both criminal and noncriminal ompatriots are often used as "proxy groups" on behalf of Russian interests. These individuals can be used to give the impression that there was local support for Russian actions. They can serve as on the

ground witnesses to events and support the narrative of an existential threat to ethnic Russians in the Baltic States, Ukraine, and Georgia. These proxy groups include criminal networks, Russian language fraternal organizations, Russian Orthodox Church associations, and paramilitaries like the Gray Wolves motorcycle club.[42]

In October 2016, Russia organized a violent coup in Montenegro to prevent it voting to request NATO membership status.[43] In the Baltics, Russian forces carefully employed intimidation and staged actions of violence aimed at the Russian population, while simultaneously portraying through the media deployed NATO troops as rapists and rioters. Additionally, NATO forward-deployed troops have had their social media targeted with Russian operatives threatening their families back home.[44]

Recently, Russia used attacks against individual Ukrainian soldiers with targeted cell phone messages during battles against the Russian-supported insurgency in the eastern Ukrainian provinces.[45] The May 2017 French presidential election saw a massive effort by Russia to support the far-right candidate, Marine Le Pen, including direct financial support in the form of multi-million euro loans to her National Front Party.[46] The social media effort used Russian "Twitter bots," or "active amplifiers," which were extremely dynamic, spreading anti-Macron and pro-Le Pen messages. These Russian controlled bots have shifted their efforts towards the September 2017 elections to attack Chancellor Angela Merkel and support far-right German candidates as detailed in the online research done by the Atlantic Council's Digital Forensic Research Lab.[47] As also noted by Steltenmuller, the German equivalent of the FBI has stated that "Russian intelligence services are also 'attempting to influence Germany's decisionmakers and public opinion.'"[48] Russian methods include Russian-influenced right wing political parties, the use of ethnic Russians in Germany as proxies and the support of automated message amplifiers across media platforms. As can be seen with these and other events, Russian information warfare techniques are sophisticated and multifaceted.[49]

This article is only a brief discussion of Russian and Western information doctrine and methods. It attempts to introduce the reader to a rapidly growing body of open source research analyzing the significant threat of Russian actions against U.S. allies and treaty partners. It is clear that Russian actions and aggression toward the United States and our allies will not decrease. Russian actions have now shifted to influence the upcoming German elections and central European NATO members. Russia continues its synchronized actions across Europe. Stronger institutions, more aggressive campaigns of response and better unified action on behalf of U.S. interests will be essential to counter this Russian aggression. ■

Notes

1. "U.S. European Command Posture 2017: Posture Statement of General Curtis M. Scaparroti, Commander, U.S. European Command February 25, 2017," U.S. European Command website, 23 March 2017, accessed 18 August 2017, http://www.eucom.mil/mission/eucom-2017-posture-statement.

2. Missy Ryan and Dan Lamothe, "Placing Russia First among Threats, Defense Nominee Warns of Kremlin Attempts to 'Break' NATO," *Washington Post* online, 12 January 2017, accessed 14 July 2017, https://www.washingtonpost.com/world/national-security/senate-set-to-question-trumps-pentagon-pick-veteran-marine-gen-james-mattis/2017/01/11/b3c6946a-d816-11e6-9a36-1d296534b31e_story.html?utm_term=.824924803d00.

3. 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), 9.

4. Katri Pynnöniemi, "The Metanarratives of Russian Strategic Deception," in *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, FIIA [Finnish Institute of International Affairs] Report 45, eds. Katri Pynnöniemi and András Rácz (Helsinki: FIIA, 2016), 97.

5. David Ignatius, "Russia's Radical New Strategy for Information Warfare," *Washington Post* online, 18 January 2017, accessed 13 September 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.492f34e18be9.

6. NATO Strategic Communications (StratCom) Centre of Excellence, *Analysis of Russia's Information Campaign against Ukraine: Examining Non-Military Aspects of the Crisis in Ukraine from a Strategic Communications Perspectives* (Riga, Latvia: NATO StratCom Centre of Excellence, 2015), 15, accessed 20 July 2017, http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.

7. This article is adapted from a part of the author's thesis completed for award of a Masters in Military Arts and Sciences at the Command and General Staff College. Collins D. Cockrell, "Gray Zone Warfare: German and Russian Political Warfare 1935-1939 and 2014" (thesis, Fort Leavenworth, KS: Command and General Staff College, 2017).

8. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2014), ix.

9. Ibid., II-4. Information related capabilities "are the tools, techniques, or activities that affect any of the three dimensions of the information environment. They affect the ability of the target audience (TA) to collect, process, or disseminate information before and after decisions are made. The TA is the individual or group selected for influence."

10. JP 3-13.2, *Military Information Support Operations* (Washington, DC: U.S. GPO, 21 November 2014), vii. As of the publication of this article, JP 3-13.2 is under revision.

11. For more information on the NATO StratCom Centre of Excellence, visit http://www.stratcomcoe.org/about-us.

12. Ibid.

13. Keir Giles, "Handbook of Russian Information Warfare" (NATO Defense College Fellowship Monograph Series 9, Rome, Italy: NATO Defense College, November 2016).

14. Allied Joint Publication 3.10.1, *Allied Joint Doctrine for Psychological Operations* (Brussels: NATO Standardization Office, September 2014), 1-3.

15. Constance Steltenmuller, "The Impact of Russian Interference on Germany's 2017 Elections," 28 June 2017, accessed 5 September 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

16. "NATO Welcomes Opening of European Centre for Countering Hybrid Threats," NATO website, 11 April 2017, accessed 14 July 2017, http://www.nato.int/cps/en/natohq/news_143143.htm?utm_source=twitter&utm_medium=press&utm_campaign=20170411-hybrid.

17 "In Massive Spending Bill, U.S. Lawmakers Back Several Measures Targeting Russia" Radio Free Europe/Radio Liberty, 4 May 2017, accessed 16 August, 2017, https://www.rferl.org/a/us-spending-bill-government-running-senate-trump/28468643.html.

18. Nahal Toosi, "Tillerson Moves toward Accepting Funding for Fighting Russian Propaganda," *Politico* online, 31 August 2017, accessed 5 September 2017, http://www.politico.com/story/2017/08/31/rex-tillerson-funding-russian-propaganda-242224.

19. Allied Joint Publication 3.10.1, *Allied Joint Doctrine for Psychological Operations*, 1-6.

20. Giles, "Handbook of Russian Information Warfare," 11.

21. Jolanta Darczewska, "Russia's Armed Forces on the Information War Front: Strategic Documents," OSW [Centre for Eastern Studies] Studies no. 57 (Warsaw, Poland: OSW, June 2016), 8. For an English translation of current Russian doctrine, see "The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5 February 2010," School of Russian and Asian Studies website, 20 February 2010, accessed 17 July 2017, http://www.sras.org/military_doctrine_russian_federation_2010.

22. Training Circular 7-100, *Hybrid Threat* (Washington, DC: U.S. GPO, November 2010), V.

23. Diego A. Ruiz Palmer, "Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons," (Research Paper No. 120, Rome, Italy: NATO Defense College, October 2015), 2.

24. National Security Analysis Department, "Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014, Assessing Revolutionary and Insurgent Strategies Study (unclassified working draft, Fort Bragg, NC: U.S. Army Special Operations Command), 27. See also "SOF Support to Political Warfare White Paper" (Fort Bragg, NC: U.S. Army Special Operations Command, 10 March 2015), 201, accessed 18 July 2017, http://www.soc.mil/swcs/ProjectGray/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20(10MAR2015)%20%20%20.pdf.

25. Charles K. Bartle, "Getting Gerasimov Right," *Military Review* 96, no. 1 (January-February 2016), 35.

26. National Security Analysis Department, "*Little Green Men*," 27.

27. Valery Gerasimov, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* 96, no. 1 (January-February 2016): 24. Gerasimov's article was originally published in *Military-Industrial Kurier*, 27 February 2013.

28. "SOF Support to Political Warfare White Paper."

29. Jolanta Darczewska, "The Devil is in The Details: Information Warfare in the Light of Russia's Military Doctrine," OSW Point of View no. 50 (Warsaw, Poland: OSW, May 2015), 12.

30. Timothy L. Thomas, *Russian Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, KS: Foreign Military Studies Office, 2015), 238–39.

31. Heather Conley James Mina, Rusland Stefanov, and Martin Vladimov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Center for Strategic and International Studies, 2016), 26.

32. Alina Polyakova, Marlene Laruelle, Stefan Meister, and Neil Barnett, *The Kremlin's Trojan Horses*, 3rd ed. (Washington, DC: Dinu Patriciu Eurasia Center, Atlantic Council, November 2016), 4, accessed 17 July 2017, http://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf.

33. Edward Lucas and Peter Pomeranzev, *Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe* (Washington, DC: Center for European Policy Analysis, August 2016), 6.

34. Katri Pynnöniemi, "The Conceptual and Historical Roots of Deception," in *Fog of Falsehood*, 38.

35. Alexey A. Prokhozhev and Nikolay I. Turko, "The Basics of Information Warfare" (report, Systems Analysis on the Threshold of the 21st Century: Theory and Practice Conference, Moscow, 27–29 February 1996), quoted in Thomas, *Russian Military Strategy*, 118.

36. Giles, "Handbook of Russian Information Warfare," 19.

37. Sergey Checkinov and Sergei Bogdanov, "Forecasting the Nature and Content of Wars of the Future: Problems and Assessments," *Voennaya Mysl'* (Military Thought), no. 10 (2015): 44–45, quoted in Giles, "Handbook of Russian Information Warfare," 6.

38. Darczewska, "The Devil is in the Details," 12.

39. NATO StratCom Centre of Excellence, *Social Media as a Tool of Hybrid Warfare* (Riga, Latvia: NATO StratCom Centre of Excellence, May 2016), 27, accessed 20 July 2017, http://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

40. Jolanta Darczewska, "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study," OSW Point of View no. 42 (Warsaw, Poland: OSW, May 2014), 24.

41. Vera Zakem, Paul Sanders, and Daniel Antoun, *Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union*, CNA [Center for Naval Analyses] Occasional Paper (Arlington, VA: CNA, November 2015), 14.

42. Orysia Lutsevych, "Agents of the Russian World: Proxy Groups in the Contested Neighbourhood" (research paper, London: Chatham House, The Royal Institute of International Affairs, April 2016), 19.

43. Milena Veselinovic and Darran Simon, "Montenegro: Russia Involved in Attempted Coup," CNN, 21 February 2017, accessed

17 July 2017, http://www.cnn.com/2017/02/21/europe/montenegro-attempted-coup-accusation/index.html.

44. Tom Porter, "British Soldiers' Latvia Brawl 'Was Set Up As Part Of Russian Propaganda Sting,'" *International Business Times*, 2 November 2016, accessed 14 July 2017, https://sg.news.yahoo.com/british-soldiers-latvia-brawl-set-104233445.html.

45. Raphael Satter and Dmytro Vlasov, "Ukraine Soldiers Bombarded By 'Pinpoint Propaganda' Texts," ABC News, 11 May 2017, accessed 14 July 2017, http://abcnews.go.com/Technology/wireStory/sinister-text-messages-reveal-high-tech-front-ukraine-47341695.

46. Gabriel Gatehouse, "Marine Le Pen: Who's Funding France's Far Right?," BBC News, 3 April 2017, accessed 14 July 2017, http://www.bbc.com/news/world-europe-39478066.

47. @DFRLab, "The Kremlin's Audience in France: Breaking Down the Amplifiers of Sputnik and RT in French," Atlantic Council's Digital Forensic Research Lab, medium.com, 14 April 2017, accessed 14 July 2017, https://medium.com/dfrlab/the-kremlins-audience-in-france-884a80515f8b.

48. Steltenmuller, "The Impact of Russian Influence on Germany's 2017 Elections."

49. Snegovaya, *Putin's Information Warfare in Ukraine*, 20.