The US Army War College Quarterly: Parameters

Volume 48
Number 1 *Parameters Spring 2018*

Article 7

Spring 3-1-2018

Countering Russian Disinformation

Timothy P. McGeehan

Countering Russian Disinformation

Timothy P. McGeehan

ABSTRACT: This article proposes three types of strategies for countering information operations campaigns. The author also presents considerations for the military role in these efforts.

Technology-based strategic advantages are perishable. In recent years, the accelerating pace of the diffusion of technology has shown many of these advantages to be downright fleeting. Secure worldwide communications, high-resolution satellite imagery, and unmanned aerial systems were once the purview of nations that had made massive governmental investments in long-term research and development, infrastructure, training, and personnel. Now they are all freely available, and affordable, for private civilians to purchase. Likewise, military hardware—such as precision-guided munitions, advanced sensor networks, electronic warfare systems, and cybercapabilities—have expanded beyond the inventories of a few select nations to become the backbone of adversarial antiaccess/area denial strategies to limit Western military action. In this strategic environment, the advantage lies not with the nation who overtly displays power but with the nation who covertly controls information.

Previous offset strategies rooted in industrial-age processes, relied on military technologies few nations could easily replicate. In contrast, a variety of actors now draw many advanced information technologies that may yield competitive advantage, such as big data algorithms and artificial intelligence capabilities, directly from today's industry. To some extent these technologies, and the operational concepts to employ them, have already proliferated. Furthermore, many companies working at the leading edge of emerging dual-use technologies are leery of partnering with Western governments, which frequently insist on owning the intellectual property (the lifeblood of information-age companies), impose export regulations (drastically limiting the market and opportunity for profit), and use cumbersome contracting processes (that tend to be much slower and less flexible than those of industry).[1] These limitations encourage technology companies to sell their wares to America's global power competitors as initiatives such as Defense Innovation Unit-Experimental (DIUx) flounder.[2]

Commander Timothy P. McGeehan, a member of the information warfare community, holds a bachelor's degree from the US Naval Academy, a master of arts degree from the Naval War College, as well as a master's degree and a doctorate degree from the Naval Postgraduate School. He was a Director Fellow with the Chief of Naval Operations (CNO) Strategic Studies Group and has served with the CNO Strategic Actions Group.

1 John Louth, Trevor Taylor, and Andrew Tyler, *Defence Innovation and the UK: Responding to the Risks Identified by the US Third Offset Strategy* (London: Royal United Services Institute, 2017); and Robert Hummel and Kathryn Schiller Wurster, "Department of Defense's Innovation Experiment," Science, Technology, Engineering, and Policy Studies, June 30, 2016, http://www.potomacinstitute.org/steps/featured-articles/83-department-of-defense-s-innovation-experiment.

2 Damon V. Coletta, "Navigating the Third Offset Strategy," *Parameters* 47, no. 4 (Winter 2017–18): 47–62; and Patrick Tucker, "As Pentagon Dawdles, Silicon Valley Sells Its Newest Tech Abroad," *Defense One*, April 22, 2016.

Influencing Perception

Modern strategists understand the well-established goal of influencing the perceptions of a population remain constant even as the technology of the Information Age evolves. Alexander the Great employed propaganda "to not just help him achieve victory but sustain his influence long after leaving."[3] Clausewitz wrote at length about moral as well as matériel factors, including the importance of the passions of the people in relation to the ability of a nation to wage war. More recently, General Douglas MacArthur stated, "One cannot wage war under present conditions without the support of public opinion, which is tremendously molded by the press and other forms of propaganda."[4] Today, capabilities that target and successfully manipulate the perceptions of another nation's public, particularly in a Western democracy, can seem to strengthen military power. As Valery Gerasimov, Chief of the Russian General Staff, observed, "The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."[5]

War is fundamentally about securing strategic and political objectives. A nation that can achieve those objectives without resorting to physical force not only avoids the associated cost in blood and treasure but also may nullify its adversary's military capabilities, no matter how effective they may be. Military tacticians frequently discuss "breaking the kill chain" to refer to the series of steps a combat system must take from initially detecting a target to establishing a firing solution through actually delivering a weapon. While one can attempt to interrupt this series of events at any stage, it is preferable to attack the kill chain "as far to the left" as possible in order to buy time and employ multiple defenses to increase the chance of survival.[6] With this in mind, the overall kill chain can be extended much further, to include the decision to deploy military forces in the first place.

In a Western democracy, the people are the ultimate decision-makers. They determine who is elected to office and, by extension, their desires broadly shape foreign policy and guide military interventions. Russia is attempting to offset Western technological superiority by going straight to the population and shaping their opinions in favor of Russian objectives. In doing so, they could preempt the entire Western war machine and ensure it is not brought to bear. This strategy was explicitly described by Russian strategists Sergey G. Chekinov and Sergey A. Bogdanov, who advocated for actively engaging in an "information struggle" to achieve "information superiority" and "create conditions for the government to achieve its political objectives in peacetime, without using armed force."[7] Over 2000 years ago, Sun Tzu extolled indirect methods, deception, and

3 Haroro J. Ingram, *A Brief History of Propaganda during Conflict: Lessons for Counter-Terrorism Strategic Communications* (The Hague: International Centre for Counter-Terrorism, 2016), 7.

4 US Joint Chiefs of Staff (JCS), *Doctrine for Joint Psychological Operations*, Joint Publication (JP) 3-53 (Washington, DC: JCS, 2003), I-9.

5 Valery Gerasimov, "The Value of Science Is in the Foresight," *Military Review* 96, no. 1 (January-February 2016): 27.

6 Jonathan Greenert and Mark Welsh, "Breaking the Kill Chain," *Foreign Policy*, May 17, 2013.

7 Sergey G. Chekinov and Sergey A. Bogdanov, "Initial Periods of Wars and Their Impact on a Country's Preparations for a Future War," *Military Thought* 21, no. 4 (December 2012): 27, quoted in Michael Petersen and Richard Moss, "Use the Truth as a Weapon," *Proceedings* 144, no. 2 (February 2018): 71.

breaking the enemy's resistance without fighting. Now, Russia is using that advice to break the kill chain about as far left as possible.

Thucydides showed the population of a democracy could be manipulated by rhetoric to pursue actions not necessarily in its best interests, and J. Robert Oppenheimer underscored this point, warning responsible employment of psychology to influence people would become even more important to Western society than the responsible use of physics and nuclear weapons. He described how advances in psychology would present "the most terrifying prospects of controlling what people do and how they think and how they behave and how they feel."[8]

Today a clever adversary can leverage a modern understanding of human psychology to advance his own agenda by exploiting citizens through the dissemination of falsehoods that appear believable. Notably, this acceptance occurs because the disinformation appeals to the target audience's preexisting moral, ethical, cultural, religious, or racial beliefs. Likewise, an adversary can target the fault lines along the conflicting views of a democracy's subgroups with tailored messaging designed to polarize a debate further and drive a wedge between the groups. This tactic erodes the trust between citizens and their government, and makes the truth less about objective facts and more about subjective beliefs they hold.

While propaganda and disinformation have been employed against the populations of Western nations (most famously by the "active measures" of the Soviet Union during the Cold War), changing technology has enabled a much more potent capability.[9] By utilizing the internet as a direct conduit to individual Western citizens, Russia has created an extremely efficient asymmetric weapon. Russia did not have to spend lavishly, develop new technology, fund infrastructure, or procure new platforms to attack these targets: commercial industry, advertising firms, and people (the targets) provided it themselves.

For example, recent surveys have shown 77 percent of American adults reported having a smartphone, and 72 percent of Americans said that they get news on those devices.[10] The statistics are similar in Europe. Every time one of these citizens accesses the internet, particularly social media during a political campaign season, they essentially deploy to the front lines in an information war where they are bombarded with content. Moreover, in this war, civilians are not collateral damage; they are the target. Facebook testified to Congress that on their platform alone approximately 126 million Americans (about 40 percent of the US population) may have viewed Russian-sponsored posts and content during the last presidential election. That figure was later revised upward

8 J. Robert Oppenheimer, "Analogy in Science," *American Psychologist* 11, no. 3 (1956), 128.

9 Michael Dhunjishah, "Countering Propaganda and Disinformation: Bring Back the Active Measures Working Group?," War Room, July 7, 2017, https://warroom.armywarcollege.edu/articles/countering-propaganda-disinformation-bring-back-active-measures-working-group/.

10 Lee Rainie and Andrew Perrin, "10 Facts about Smartphones as the iPhone Turns 10," Pew Research Center, June 28, 2017, http://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/; and Amy Mitchell et al., "Pathways to News," Pew Research Center, July 7, 2016, http://www.journalism.org/2016/07/07/pathways-to-news/.

to 150 million.[11] Russia has deployed similar information operations (IO) campaigns against elections in France, Germany, and the Ukraine, as well as the Brexit referendum and Catalan independence vote.[12] Other nations have taken note, and similar activity was reported in 18 elections worldwide over the last year.[13]

Dissecting the IO Campaign

Interestingly, the current Russian IO campaign contains some elements of the previous American offset strategies. The First Offset Strategy, also known as the New Look, relied on the nuclear weapons capability to offset the numerical superiority of conventional Soviet forces.[14] Akin to employing nuclear weapons and the consequences of lingering radiation, the current Russian IO campaign not only overwhelms the information space but also pollutes it with falsehoods to the point that all truth becomes relative, rendering the information space unusable by any party. Likewise, marketing techniques developed for the "attention economy," enable remote operatives to conduct reconnaissance and targeting from afar and to deliver tailored disinformation directly to specific audiences. This technique is reminiscent of the Second Offset's "reconnaissance strike complexes" and the development of weapons with "near-zero miss" accuracy required after the Soviets achieved nuclear parity.[15] Humans can also team with botnets to ensure maximum online delivery of content during a messaging campaign, which is essentially an expression of the Third Offset's "human machine teaming" vision. In fact, a recent study found between 9 percent and 15 percent of Twitter posts are already created by bots, which underscores this point and hints at the potential for growth.[16]

Moreover, the current Russian IO campaign most closely resembles Giulio Douhet's original airpower theory. Instead of attacking though an enemy's army to reach their population, Douhet advocated flying over the army for direct contact. With severe enough punishment through aerial bombing, to include poison gas, the population would force their government to sue for peace. Douhet believed the difficulty of searching the extended airspace favored the attacker, as the defender would have to spread his assets thin, reducing the mass he could bring to bear should he find and close with the attacking bomber.[17] Douhet likened

11 David Ingram, "Facebook Says 126 Million Americans May Have Seen Russia-Linked Political Posts," Reuters, October 30, 2017; Sarah Frier, "Facebook, Twitter Testimony Shows Widespread Russian Meddling," Bloomberg, October 30, 2017; and Spencer Ackerman, "Facebook Now Says Russian Disinfo Reached 150 Million Americans," *Daily Beast*, November 1, 2017.

12 "How the World Was Trolled: Once Considered a Boon to Democracy, Social Media Have Started To Look Like Its Nemesis," *Economist*, November 4, 2017; "Londongrad: Russian Twitter Trolls Meddled in the Brexit Vote. Did They Swing It?," *Economist*, November 23, 2017; and Vasco Cotovio and Emanuella Grinberg, "Spain: 'Misinformation' on Catalonia Referendum Came from Russia," CNN, November 13, 2017.

13 "Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," Freedom House, accessed May 9, 2018, https://freedomhouse.org/report/freedom-net/freedom-net-2017.

14 Shawn Brimley, "Offset Strategies & Warfighting Regimes," War on the Rocks, October 15, 2014, https://warontherocks.com/2014/10/offset-strategies-warfighting-regimes/.

15 Katie Lange, "3rd Offset Strategy 101: What It Is, What the Tech Focuses Are," DoDLive, March 30, 2016; and Anthony D. McIvor, ed., *Rethinking the Principles of War* (Annapolis: Naval Institute Press, 2005), 85.

16 Onur Varol et al., "Online Human-Bot Interactions: Detection, Estimation, and Characterization," Cornell University Library, March 27, 2017, https://arxiv.org/pdf/1703.03107v2.

17 Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (Washington, DC: Air Force History and Museums Program, 1998).

this defense to "a man trying to catch a homing pigeon by following him on a bicycle."[18] Defending the Western public against internet-enabled campaigns to shape perception is likewise challenging. The proposition that a nation can equally counter every adversarial post, story, tweet, or advertisement is not reasonable.

Countering the IO Campaign

If Douhet's airpower theory provides insight into the attack, it is also worth examining for a method of defense. He advocated an active defense by attacking an adversary's airfields to destroy their air force before it could even take off.[19] That would be analogous to targeting the blogging "troll farms" that the Russians use to create and spread their disinformation.[20] However, this solution could be fleeting, as the users could just shift locations, change IP addresses, and establish new accounts if they were located and blocked.

There are significant differences that make the airpower analogy incomplete—for example, there is a finite number of aircraft but an endless supply of disinformation. Aircraft require a sophisticated industrial base, long-term maintenance programs, and logistical support to deploy them and to keep them operational, whereas disinformation does not. If an aircraft is shot down or crashes, it is out of the fight. Disinformation can be reused with multiple audiences, or it can linger unattended until someone comes across it, much like unexploded ordnance or mines. These dissimilarities highlight the need for a different solution.

Artificial Intelligence

Douhet's airpower theory failed to account for the impacts of advancing technology. Airpower did not crush the United Kingdom during the Blitz in World War II, despite the bombing campaign's deliberate targeting of the civilian population and its will. Newly deployed radar technology enabled the Royal Air Force to husband its fighter resources and vector them efficiently to intercept German bombers. The advantage of the attackers to maneuver throughout the three-dimensional airspace, complicating the defender's search via aircraft, was "offset" by the defenders having technology that searched the entire airspace, allowing them to mass forces as desired.[21]

Artificial intelligence (AI) could play a role analogous to radar. Emerging AI capabilities may act as an early warning system to detect and vector limited resources, intercepting adversarial information threats and protecting Western citizens from disinformation. With advances in machine learning, AI may reach the point where it can instantaneously discern and flag fake news and other disinformation on a massive scale. Executing "command by negation," AI could alert human analysts to the incoming disinformation, determine its origin and delivery route, and suggest additional counters, to include posting or redirecting users to information that debunks erroneous claims.

---

18 Douhet, *Command of the Air*.

19 Douhet, *Command of the Air*.

20 David Filipov, "The Notorious Kremlin-Linked 'Troll Farm' and the Russians Trying To Take It Down," *Washington Post*, October 8, 2017.

21 Timothy McGeehan, "Emerging Threats to Future Sea Based Strategic Deterrence," *Submarine Review* (December 2017): 103.

Containment and Resilience

The disinformation and "fake news" phenomenon also has analogies to epidemiology. During a public health crisis, identifying and containing disease outbreaks is critical. Timely responses save lives. Likewise, quickly disseminating the truth to debunk fake news is critical as the longer a story goes without comment the more truthful it appears. During the Ebola outbreak of 2014–15, for example, people in the United States unwittingly propagated incorrect information on social media regarding transmission mechanisms and reporting local outbreaks.[22] These rumors led the Centers for Disease Control and Prevention public affairs team to focus proactively by providing accurate information via posts on its website and social media accounts, pushing information and updates, issuing timely corrections, and holding public question-and-answer sessions. Similar strategies could be employed to counter disinformation.

Another comparison to epidemiology is the idea of inoculation. Just as public health authorities give particular focus to vulnerable subsets of a population, there is a need to identify and preemptively message groups that may be susceptible to disinformation in a "mass vaccination" messaging campaign. This leads to the concept of "herd immunity," where enough people in the population have been inoculated to prevent the spread of disease (or disinformation). Similar "self-regulating" of inaccurate information has been observed in social media during emergency management, but more as a counter to inaccurate information (misinformation), not as a counter to sophisticated large-scale campaigns of intentionally spread disinformation.[23] Countermessaging campaigns also will have to be synchronized and coordinated internationally with allies and partners, because disinformation, like disease, does not recognize borders.

Education

The prevention campaigns described above cannot be effective if the population does not understand them, believe them, or have an awareness of their implications. Education is paramount. It is a national security imperative that Western governments produce citizens capable of critical thought and discerning the truth. In 1958, President Dwight D. Eisenhower complemented the First Offset Strategy with the National Defense Education Act "to strengthen our American system of education so that it can meet the broad and increasing demands imposed upon it by considerations of basic national security."[24] The act focused on improving the state of American education, especially in science and engineering, to create the workforce that could sustain the offset's technical advantage. Today an analogous education effort is needed to counter disinformation.

---

22 Victor Luckerson, "Fear, Misinformation, and Social Media Complicate Ebola Fight," *Time*, October 8, 2014.

23 Tomer Simon, Avishay Goldberg, and Bruria Adini, "Socializing in Emergencies—A Review of the Use of Social Media in Emergency Situations," *International Journal of Information Management*, October 2015): 609–19, doi:10.1016/j.ijinfomgt.2015.07.001.

24 Dwight D. Eisenhower, "Statement by the President upon Signing the National Defense Education Act," The American Presidency Project, September 2, 1958, http://www.presidency.ucsb.edu/ws/?pid=11211.

Western citizens must have a grasp of the functions and the mechanisms of democracy. A lack of basic understanding of the associated institutions and their complex interplay leads to a decline in trust, which can be exploited by adversaries.[25] While this education should be prioritized, federal funding for civics education was completely cut in 2011 and only partially restored in 2015.[26] This ignorance is compounded by the widespread adoption of new information technologies that have the potential to increase human performance; however, they also bring risks. Students and teachers alike deemphasize the "memorization of facts" because they can be accessed immediately using the omnipresent internet-enabled device (computer, tablet, or smartphone). This practice essentially outsources traditional memory functions.[27] Unfortunately, in looking up facts online one can quite easily be directed to false information.

In the "attention economy," where content is tailored for quick consumption due to short attention spans instead of complete information for comprehensive analysis, many people outsource their responsibility for critical thought altogether by, again, deferring to a search engine. This reliance assumes the facts and analysis found online are reliable. This issue is magnified by "citizen reporting," blogs, and the "death of expertise" (where the increased access to information, reliable or not, makes amateurs believe they are just as well informed as any of the world's leading experts who have lifelong experience in a particular field).[28]

In the attention economy, the population disseminates suspect content that competes for attention with traditional authoritative vetted content. Network effects take over, and these ideas propagate through social networks based not upon authority but on popularity. Some of the internet's most highly trafficked websites, such as Reddit, promote content based upon users' ratings and have been used intentionally by Russian trolls to insert disinformation that was amplified and spread unwittingly by legitimate users.[29]

Many people's capacity for deep thought and analysis has become atrophied through disuse, and they are unable to consider objectively the reliability of sources.[30] To help people vet content, technology providers have provided feedback and reliability ratings that give sources the appearance of authority via quantifiable measures such as the number of times a post has been "liked" or a website has been visited. However, these measures are easily manipulated, not just by state-sponsored campaigns but by marketing and public affairs firms armed with phony user accounts and automated bots, selling "retweets," followers,

25 John Gould, ed., *Guardian of Democracy: The Civic Mission of Schools* (Philadelphia: Leonore Annenberg Institute for Civics of the Annenberg Public Policy Center at the University of Pennsylvania / Campaign for the Civic Mission of Schools, 2011).

26 Max Boot, "America is Turning Into a Confederacy of Dunces," *Foreign Policy*, October 6, 2016; and Anna Saavedra, "Strengthening Our Democracy Starts in School," *US News*, December 17, 2015.

27 Saavedra, "Strengthening Our Democracy"; Boot, "Confederacy of Dunces"; and Nicholas G. Carr, *The Shallows: What the Internet is Doing to Our Brains* (New York: W. W. Norton, 2011), 6.

28 Thomas M. Nichols, *The Death of Expertise: The Campaign against Established Knowledge and Why It Matters* (Oxford: Oxford University Press, 2017).

29 April Glaser, "Reddit Is Finally Reckoning with How It Helped Spread Russian Propaganda in 2016," *Slate*, March 5, 2018.

30 Carr, *Shallows*.

subscribers, "likes," and reviews. Costs are minimal: 10,000 site visitors for $17.00, 100 Twitter followers for $0.34, or 100 YouTube subscribers for $0.66.[31]

While education systems are adapting to target the breadth of skills required to excel in the new environment, international surveys reveal communication and creativity rank above critical thinking in education policies.[32] Critical thinking must receive more focus to create citizens who can objectively evaluate information and its sources, determine plausibility of content, and look for hidden agendas. Researchers at Stanford University recently published a study revealing 80–90 percent of students "had trouble judging the credibility of the news they read."[33] Likewise, citizens need to understand the pitfalls of social media and be wary of the "echo chamber" effects that isolate them from the outside world and limit the information they receive to only what they already think. While there is a renewed focus on STEM education to create a capable and competitive twenty-first century workforce, Western nations need to reinvigorate their civics and social studies programs as well as focus on "digital literacy" to build citizens into "hard targets" for disinformation. The curriculum should include a continuing education component to ensure positive impacts are individually sustainable.

Role of the Military

Returning to the air defense analogy, Western citizens expect their militaries to intercept inbound attacks; military defense from disinformation could follow a similar model. As one of the most trusted institutions in many nations, the military could have unique authority to set the record straight.[34] Furthermore, it appears that some of the incoming disinformation is actually coming from adversary military units.[35]

However, this chain of reasoning raises several red flags regarding civil-military relations. Western militaries are not "thought police," and although they may play a supporting role in interagency processes, they should not lead a whole-of-government effort. There are attribution challenges that arise from the many stories and rumors that are not necessarily articles from state-run news outlets but instead originate on social media or websites. These situations lead to additional issues like separating legitimate free speech from disinformation, particularly if a Western democracy's own citizens post the content. These matters should be reserved for legal authorities, not the military. Furthermore, regardless of who determines disinformation, there must be transparency in the processes and algorithms to avoid abuse by authorities.

---

31 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public* (n.p.: Trend Micro, 2017), 27–28.

32 Esther Care, Kate Anderson, and Helyn Kim, "Visualizing the Breadth of Skills Movement across Education Systems," Brookings Institution, September 16, 2016.

33 Kelly McEvers, "Stanford Study Finds Most Students Vulnerable to Fake News," NPR, November 22, 2016; and Brooke Donald, "Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online," Stanford Graduate School of Education, November 22, 2016.

34 Brian Kennedy, "Most Americans Trust the Military and Scientists To Act in the Public's Interest," Pew Research Center, October 18, 2016.

35 Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016; and Tony Barber, "Russia's Dark Art of Disinformation," *Financial Times*, September 16, 2016.

Examples of successful interagency groups who counter propaganda and disinformation, such as the Active Measures Working Group of the 1980s, can provide a template for military participation in these efforts.[36] In late 2016, President Barack Obama signed the Countering Disinformation and Propaganda Act into law as part of the National Defense Authorization Act, which correctly cast the Department of Defense in a supporting vice leading role.[37]

The Way Ahead

History has shown military offset strategies do not confer an enduring advantage. That said, they can allow one nation to nullify temporarily some aspect of another's superiority. With its current IO campaign, Russia seeks to exert a certain level of control over the perceptions of Western citizens. The true effectiveness of Russian efforts is difficult to quantify; they may even prove counterproductive in the long term.[38] However, the intent alone is alarming. Russia has attempted to influence Western democracies via their most fundamental command and control system, their elections, and may further attempt to undermine the mutual commitment that underpins the North Atlantic Treaty Organization.[39] Focusing on artificial intelligence, public health approaches, and above all education will enable Western governments to ensure any impacts of the current Russian IO campaign are short-lived.

36 Dhunjishah, "Countering Propaganda."

37 "President Signs Portman-Murphy Counter-Propaganda Bill into Law," Senator Rob Portman, December 23, 2016.

38 Bill Bray, "Where Russian Information Warfare Is Failing," *Proceedings* 144, no. 1 (January 2018): 1379.

39 Scott Shane, "The Fake Americans Russia Created to Influence the Election," *New York Times*, September 7, 2017.