PERCEPTIONS ARE REALITY

Historical Case Studies of Information Operations in Large-Scale Combat Operations

Edited by Col. Mark D. Vertuli and Lt. Col. Bradley S. Loudon

LARGE-SCALE COMBAT OPERATIONS SERIES

Army University Press

This book is part of *The US Army Large-Scale Combat Operations Series*, which includes:

Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations

Bringing Order to Chaos: Historical Case Studies of Combined Arms Maneuver in Large-Scale Combat Operations

Lethal and Non-Lethal Fires: Historical Case Studies of Converging Cross-Domain Fires in Large-Scale Combat Operations

The Long Haul: Historical Case Studies of Sustainment in Large-Scale Combat Operations

Deep Maneuver: Historical Case Studies of Maneuver in Large-Scale Combat Operations

Into the Breach: Historical Case Studies of Mobility Operations in Large-Scale Combat Operations

Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations

Perceptions Are Reality

Historical Case Studies of Information Operations in Large-Scale Combat Operations

Edited by
Colonel Mark D. Vertuli and
Lieutenant Colonel Bradley S. Loudon

Army University Press
Fort Leavenworth, Kansas

Library of Congress Cataloging-in-Publication Data

Names: Vertuli, Mark D., 1973- editor. | Loudon, Bradley S., 1974- editor. | Army University Press (U.S.), issuing body.
Title: Perceptions are reality : historical case studies of information operations in large-scale combat operations / edited by Mark D. Vertuli and Bradley S. Loudon.
Description: Fort Leavenworth, Kansas : Army University Press, 2018. | Series: US Army large-scale combat operations series | Includes bibliographical references.
Identifiers: LCCN 2018036198 (print) | LCCN 2018039418 (ebook) | ISBN 9781940804521 (ebook) | ISBN 9781940804521
Subjects: LCSH: Information warfare--History. | Information warfare--Case studies. | Operational art (Military science)
Classification: LCC U163 (ebook) | LCC U163 .P47 2018 (print) | DDC 355.3/43--dc23 | SUDOC D 110.20:7
LC record available at https://lccn.loc.gov/2018036198

2018

Editor
Lynne M. Chandler Garcia

Chapter 3
The Fog of Russian Information Warfare

Lionel M. Beehner, Colonel Liam S. Collins, and Robert T. Person

"This is an arms race," Facebook Chief Executive Officer Mark Zuckerberg told a recent congressional panel in reference to the Russian Federation's use of social media to conduct information warfare. "They're going to keep getting better."[1] The tools and tactics of Russian information warfare may have changed over the decades, but as many analysts have noted, the ends remain largely unchanged since Soviet times: to complicate, contain, and constrain the projection of US strategic power and those of its allies, predominantly in Eurasia but also in the Middle East. It is an entirely rational way of shaping the strategic environment to gain advantage, given the quantitative and qualitative asymmetries between Russia and the West in conventional capabilities.

With the US Army shifting its doctrinal focus from counterinsurgency to large-scale combat operations, peer and near-peer competitors such as China, Iran, and Russia are taking on renewed importance.[2] But that does not necessarily imply a complete doctrinal shift toward large-scale conventional operations, given all the types of warfare these states prefer to wage. After all, so-called "contactless war," as the Russians define it, is meant to negate their military disadvantage by avoiding any direct contact with Western forces, whether by demonstrating fire discipline or deploying "little green men" in places like Crimea.[3] Russia has shown a remarkable ability and willingness, with fairly straightforward means, to disrupt democratic institutions, undermine social cohesion, and sow confusion, doubt, and distrust among Western allies and their publics. Social media has only accelerated the pace of information warfare (IW) advancement.

We should be clear by what is meant by Russian information warfare, or *informatsionnaya voyna*. Information warfare is not simply a tool to achieve some kind of limited tactical objective or advantage during wartime, typically in the initial phase of hostilities. Rather, information warfare should be considered more broadly. Calculated and systematic, it consists of operations aimed at degrading the enemy's ability to control the information space, deny it the technical capability to retaliate via cyberspace means, and defend a narrative of Russian nationalism to glorify its role on the world stage—a manipulative form of Russian "soft power." Russian information warfare comprises a bounty of tactical innovations, from traditional psychological operations (psy-ops) and strategic com-

munications aimed at controlling the narrative, to the sophisticated deployment of decentralized trolls and bots across social media and other online platforms.[4]

Russian information warfare—*informatsionnaya voyna*—consists of three pillars. First, and most benignly, it aims to put the best spin it can on ordinary news. It does this through state-controlled outlets like RT (formerly "Russia Today"), Russian-language radio ("Sputnik"), as well as through television outlets that cater to the Russian-speaking population of the former Soviet states. This spin generally paints Russia as a viable and preferred alternative and counter to US greed and aggression."[5] Second, it uses disinformation to create enough ambiguity to confuse people, both at home and abroad, about its current operations, whether in Ukraine, Syria, or elsewhere, all with the aim of providing a decoy and contributing to the proverbial "fog of war." Third, it outright lies when given true information and claims it is falsified. This last strategy has several objectives: to degrade trust in institutions across the world; push populations currently undergoing conflict to simply accept the status quo of the conflict and not push for resolution; and finally, it prevents countries in its desired sphere of "privileged interest" from Western alliances like NATO by keeping these areas in perpetual conflict.

Interestingly, while Western technology firms point to an arms race with peer competitors like the Russian Federation and the People's Republic of China, the US government does not consider itself at war. This naivety is a strategic mistake, we argue. In this chapter, we examine how Russian information warfare operates and how it should be conceptualized at the strategic level. How does information operations (IO) fit into Russia's larger strategic aims? What are its primary methods? And finally, and perhaps most importantly, how can the US military effectively combat Russian information warfare, while staying true to its values and simultaneously preventing conflict escalation? In this chapter, we advance three central arguments:

- First, Russia's leadership does not apply information warfare solely to support its military objectives—as a way to soften up the enemy or prep the battlefield, as it were—but rather vice versa. Its military operations in places like Ukraine or Syria are often ancillary to Russia's more immediate strategic objective: to challenge US interests wherever possible and undermine America's ability to advance unhindered its own strategic objectives. As such, it can be considered a form of post-Cold War strategic balancing by Moscow that involves political, economic, cyberspace, and—most formidably—information means to contain and constrain US

activities globally. In this sense, IW should not be seen as simply a tool in Russia's *military* toolkit. While Russian IW has certainly been used as part of military operations, it is often applied in pursuit of Russian political objectives where military objectives may be absent. Thus, when observers see evidence of Russian IW, they should not immediately jump to the conclusion that they are part of a military strategy to formally seize more land in Ukraine's east or send a column of tanks into the Baltics. Regarding Russia's IW efforts, the ends are to challenge American interests and undermine the foundations of Western democratic institutions; by sowing uncertainty, discord, and division in the United States and its allies, IW tactics are a particularly cheap, ambiguous, and effective means of achieving those strategic ends. To the degree that information warfare goes hand in hand with Russian conventional military operations, recent experience demonstrates that the latter are in some respect sideshows to the former, not the other way around.

• Second, while information warfare is frequently applied for non-military political ends, Russia nonetheless considers itself at war with the West and brings such a mentality to its operations. Moscow thus conducts information warfare primarily preemptively to weaken its enemy—the United States and Europe. Information warfare was formally incorporated into Russian military doctrine in 2010, and dates further back to the height of the Cold War, but it was been exponentially expanded on since. To date, Russia has seen itself as able to achieve "information dominance" —that is, the ability to penetrate the American information environment, from planting stories in the media to hacking the emails of politicians and their operatives, and influence political outcomes.[6]

• Third, when it comes to Russian aggression in the information realm, we are at war. Though it may be "political warfare," to borrow George Kennan's term from a 1948 Policy Planning Staff memo, it is warfare nonetheless.[7] To counteract Russian malicious activity, one must "fight fire with fire." US conventional deterrence in the region has primarily consisted of stationing several battalions in NATO partners like Poland and the Baltics. Yet, a recent RAND report found that Russia would overrun NATO forces in a matter of hours.[8] The imbalance is even more severe in the informational realm: there is neither a sufficient deterrent to prevent Russian IW attacks, nor a punitive mechanism to enact retaliatory measures beyond issuing statements condemning such acts. We recognize that attribution is an issue in this space, as is the risk of conflict escalation. However, the current defensive position of the United States is not working. To quote one congressman, "[W]hy not go on the offense to release information expos-

ing corruption at the Kremlin?"[9] Without looser rules of engagement and a more offensive strategy, we can expect Russia and its agents to continue its concerted information operations unabated as the United States continues to cede the strategic initiative in the information environment.

This chapter proceeds as follows: First we provide some background of Russian IW, define several key concepts, and identify the main methods Russia uses and the challenges they pose. Next, we lay out the larger strategic aims of Russian IW, both against the West and against Ukraine and other former Soviet states. Then we detail its IW methods by examining the case study of Ukraine. We conclude by outlining a list of recommendations for the US military to effectively combat Russia's IW efforts.

Information Operations 101

Clausewitz correctly noted that the nature of warfare never changes, only its character. He would have recognized the character of information warfare as a distinct and effective form of warfare to accomplish one's political ends, given that an enemy's center of gravity is shifting. The United States' greatest strength is paradoxically also its greatest weakness: that is, our freedom of speech and press. Here the Russians are practicing a playbook straight out of Clausewitz: attack the enemy where they are *most* vulnerable. The US military defines information operations as "the integrated employment, during military operations, of 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."[10] Further, it defines information warfare as "a threat's orchestrated use of information activities (such as cyberspace operations, electronic warfare, and psychological operations) to gain an advantage in the information environment." In other words, IO refers to friendly actions in the information environment, while IW is used to describe threat-based activities.

In keeping with our argument about Russian IW as a form of political warfare, it is important to note that the definition above is overly restrictive in defining information warfare as residing strictly within the confines of military operations. Thus, we find it useful to employ a "holistic concept [of information warfare] that includes computer network operations, electronic warfare, psychological operations, and information operations."[11] Information warfare—sometimes called "influence operations"—refer broadly to the practice of collecting information about an enemy as well as the dissemination of disinformation and propaganda to seek an advantage over one's adversary, whether in peacetime or wartime.

Russian information warfare is carried out through five main methods, ranging from psychological to technical: the manipulation of information (fake news), espionage (intelligence), political interference, military deception (plausible deniability), and cyberspace-based capabilities (social media). The latter is the only item that is really new and innovative, as it allows for increased speed and allows for further distance. We outline these methods below.

First, Russia has mastered the use of fake news and other disinformation to confuse or persuade media consumers, both in Russia and the West. The purpose of this effort is to erode public support and confidence in Western democratic institutions, to create and amplify public and a political discord, to create confusion in order to delay Western decision-makers at the highest levels, and to intensify the security competition in areas of strategic importance to both the West and to Russia. This is especially true in Eastern Europe and the South Caucasus along the fault line between NATO and the countries that once orbited within the Soviet Union's sphere of influence: the Baltic states, Georgia, and Ukraine. Intensifying the competition serves to rattle Russia's adversaries, provoke them, and influence their risk-averse publics to disapprove of taking any kind of serious retaliatory measures. Another byproduct of this use of IW is to support both directly and indirectly anti-establishment groups, parties, and politicians in the West—many of them right-wing or hyper-nationalist—as a way to provide them with a veneer of legitimacy and disrupt the democratic process. "Russia's new propaganda is not now about selling a particular worldview," as Alexei Levinson argues. "It is about trying to distort information flows and fuel nervousness among European audiences."[12]

Second, Russian IW includes the work of traditional Cold War-style espionage, like stealing compromising materials and information on one's enemy, known in Russian as *kompromat*.[13] During the Soviet era, this kind of information warfare was referred to as "reflexive control," a theory with deep roots in the Soviet Ministry of Defense's research into psychology and cybernetics that mapped how enemies formed decisions and framed problems.[14] "In the context of warfare," as Maria Snegovaya notes, "the actor that is most capable of predicting and mimicking the reasoning and actions of its opponent has the highest probability of success."[15]

During the Cold War, the primary foot soldiers on this front were KGB intelligence officers, including a young KGB officer in Dresden by the name of Vladimir Putin. Today Russia relies on "information troops," who act as guns for hire in the propaganda realm—contractors, former criminals, and other cyberwarfare actors and middlemen.[16] They are kept at

arm's length from Moscow, to provide the Kremlin with plausible deniability if caught. The aim of these mercenaries is manifold: to disrupt the enemy's telecommunications or data-storage systems; to interfere in and undermine democratic elections in the West, whether by releasing sensitive information, trolling, posting fake news, or other tactics it deems will undermine democracy.

Meddling in foreign elections is not a new tactic. Nor is it a technique unique to Russia or its Soviet predecessor. According to Dov Levin, "Between 1946 and 2000, the United States and the USSR/Russia intervened [to manipulate foreign elections] 117 times, or, put another way, in about *one of every nine* competitive national-level executive elections during this period."[17] What has changed, however, is the technological sophistication, the use of proxies operating on the behalf of nation states, and the ability to leverage the speed of social media. In February 2017, for example, the special prosecutor Robert Mueller charged thirteen Russians and three Russian companies for interfering in the 2016 US presidential election. Among the companies charged was Internet Research Agency, a "Russian troll farm," with the "strategic goal to sow discord in the US political system."[18] In his book, *War in 140 Characters*, David Patrikarakos profiles entire office buildings in Siberia devoted to creating fake news stories to influence voter behavior in Western elections.[19]

The fourth component of Russia's IW is to add to the fog of war and deny the presence of Russian military forces—specifically its use of *spetsnaz* forces in places like Ukraine. This is to distract and obfuscate the existence of an extensive military campaign—what the Soviets used to call *maskirovka*—that might trigger a more robust Western response or worse a backlash at home were the full facts of the operations, including death tolls, to be made public.[20] The Russian government always denies any use of this kind of warfare and instead attributes these attacks to Russian "patriots" operating on their own behalf, with no guidance from Moscow. This kind of disinformation campaign is hardly the work of a decentralized network of pro-Russia grassroots activists improvising on their own but rather is a heavily-structured, national-level effort to facilitate the accomplishment of Russia's strategic objectives. According to former KGB defector, Ion Mihai, this kind of campaign has three prongs: deny involvement, minimize damage, and if truth comes out, blame it on one's enemies.[21]

Finally, in addition to information brigades, election meddling, and deception, Russia employs digital technologies to influence social media and add greater speed and sophistication to its IW campaigns. This in-

cludes, as Keir Giles notes, "a complex blend of hacking, public disclosures of private emails, and use of bots, trolls, and targeted advertising on social media designed to interfere in political processes and heighten societal tensions."[22] Malicious actors can harvest the personal data of unsuspecting users of social media such as browsing history and consumer spending data, which allows them to target groups and individuals by their political views, their income bracket, and their location. They can then plant contradictory messages in news stories that already expose ideological fault lines. A case in point was Russia-linked bots and trolls pushing divisive stories and hashtags on social media that fueled the National Football League national anthem controversy. Russian hackers also plant false reports in mainstream media outlets. In May 2017, Qatari state media published false remarks made by the emir of Qatar praising Iran, creating an uproar among its Gulf neighbors.[23]

Russian Objectives

This section examines Russian objectives and how IW fits into Moscow's larger strategic aims. Russia is often said to be determined to undermine democracy as an end, and to rewrite the rules of the international order. On this point, Russia is actually quite agnostic to the normative value placed on democracy or liberalism. If the United States were a totalitarian dictatorship marching its forces across the globe, Russia might surmise that playing to people's liberal side might benefit its ability to resist American domination. Russia, in this role, is playing the foil to the United States. In this respect, Russia's grand strategy is non-ideological in its motivation: its target is not democratic institutions per se, rather the target is the political institutions of an adversarial state. That those institutions happen to be democratic is—from an ideological standpoint—immaterial. But from a practical standpoint, the openness of liberal democratic institutions makes them more vulnerable to attack.

What many Western audiences fail to appreciate is the fact that Russia believes itself to be fighting IO fire with IW fire. Moscow's narrative of the 2003 Rose Revolution in Georgia, the 2005 Orange Revolution and 2014 Maidan Revolution in Ukraine, and the 2011-2012 mass protests in Russia is one of a West intent on interfering in its own elections those of countries where Moscow has strong interests. Thus, the Kremlin's view is that its own schemes are simply tit for tat, a game of cat and mouse played against the world's dominant superpower. In seeking to challenge, constrain, and contain American interests, Russia seeks a more multipolar world where it is accorded a seat among the great powers beyond that which it already enjoys with a permanent veto-wielding Security Council position. In Mos-

cow's vision of a multipolar world, great powers like Russia should have a right to spheres of privileged interest, and a free hand to pursue their interests within their sphere unimpeded. The only way to achieve such a world is to roll back American influence. It should also be said that Russia is also a declining economic power playing a weak hand—politically, economically, and militarily. To counter American interests, it relies on IW as a cost-effective, less risky means of warfare.

But this logic requires unpacking. First, Russian information warfare is often treated as just one part of its larger military strategy, which includes a number of other uses of force. However, this diminishes IW's significance, and treats it as just one of several non-kinetic means—a basket of options sometimes referred to as "new generation warfare"—Russia employs in conjunction with kinetic means in pursuit of military objectives.[24] But as argued previously, Russia's objectives are often political in nature rather than military. In fact, IW in pursuit of political ends is appealing for its low cost, low risk, and its relative simplicity. Russia fancies itself as the "great disrupter," to disrupt requires no further end goal than the mere process of destabilizing Western democracy—including its norms, procedures, institutions. Sowing the seeds of chaos is, often times, the primary objective. To be sure, one might argue this is part of a grand design to tilt the rules of the game in its favor by throwing out any rulebook. As Edward Lucas and Ben Nimmo write, "Russia's approach, unlike Nazi Germany's ethnic and ideological one, is deeply nihilistic."[25] Yet it should be emphasized that nihilism is not the ends but rather the means. The ends is to contain and constrain American influence across the globe. When it comes to the bounds of acceptable behavior to achieve this ends, Russia will not follow any rules. As noted in the *Tallinn Manual 2.0* on cyberwarfare, "The Russians are masters at playing the 'gray area' in the law, as they know that this will make it difficult to claim they are violating international law and justifying responses such as countermeasures."[26]

Conceptually speaking, Russia's IW campaign is seen by many Westerners as defensive and in line with what Russia did during the Cold War. But Russia's information warfare activities should be seen as offensive, given that a large part of the effectiveness of IW as a means is its element of surprise. To reiterate, Russia considers itself to be "at war" (or more precisely, "at political war") with the West, yet the West does not consider itself "at war" with Russia. A popular theory among neorealists known as "offense-defense theory" offers insights into the challenge at hand. The theory posits that in cases where the offensive measures enhance a state's security more efficiently than defensive measures, and where a state's

intentions—whether offensive or defensive—are indistinguishable, then the threat of war and instability is greater.[27] The logic is that this kind of setting favors a first-mover advantage and allows for preemptive attacks. This principle also applies to the use of information warfare. There is an element of surprise built in, as well as one of asymmetry. These operations are offensive—even if non-kinetic—by design. According to Maria Snegovaya, "On the tactical level, information warfare allows Russia to achieve surprise in the time or manner of an attack. Russia thereby gains time and efficiency against the enemy's ground forces . . . Informational cover provides more flexibility and efficiency to the military, as well as improves speed of maneuverability and the speed of battlefield responses."[28]

Nonetheless, part of the confusion (and thus the utility from the Russian perspective) of IW is that it can be applied to political ends simultaneously with military ends. In such contexts it can be difficult to determine a priori what the objectives of some information operations are. This is the situation that we find in Ukraine, where political and military objectives are both part of the conflict's logic. It should be stated that Russia's strategy in Ukraine is complicated yet also haphazard. The objective of Russia's military operations in Ukraine *is not* simply to acquire territory—if it wanted to, Russia could have easily annexed militarily the Donbas, the conflict zone in eastern Ukraine, by now—but rather to keep Ukraine down, sow confusion among its public, and prevent Ukraine from joining Western institutions. Russia seeks to undermine the foundational principles of the very institutions that Ukraine seeks to join. In this regard, IW does not serve its military goals of controlling or annexing territory, but rather the other way around: *its military strategy supports its IW*. Ukraine in this regard is just one piece of Russia's larger grand puzzle—an important piece, to be sure, given their close historical ties. Russian military operations in Ukraine are but one component to weaken the West and by extension make the world more multipolar.

IW at the Tactical Level in Ukraine

Russia's information warfare in Ukraine dates back decades, but during the most recent campaign it began in earnest around the time of the Maidan Revolution in November 2013. Russia employed IW against Ukrainian institutions with several objectives in mind: to undermine support for the protesters and pro-western factions in Ukraine, to elicit fear among Ukraine's Russian-speaking and pro-Russian populations in its east and south, and to deny facts on the ground during operations to seize Crimea and interfere in the war in Ukraine's east. To accomplish these

objectives, Russia has employed a number of IW tactics, often in combination with cyber warfare, to influence enemy combatants, local populations, and allies.

First and foremost, the Kremlin sought to control the narrative in Ukraine through a number of efforts targeted at fence-sitters in the region. These efforts include referring to Ukraine in its media or press releases as a "failed" or "fascist" state; releasing forged documents from RAND corporation or the Ukrainian military to paint the latter as corrupt and the former as conspiratorial; citing hoax experts to push fake narratives; manipulating the titles of articles it publishes; amplifying the threat of Europe's disintegration and warning of the West's declining support for Ukraine (so-called "Ukraine fatigue"), a consequence of a pending refugee crisis from Ukraine.

Second, Russia has consolidated its control over all Russian media covering the conflict in Ukraine. Ukrainian-language broadcast media in the east was effectively neutralized, leaving state-controlled *RT* as the sole source television-based information available to local Ukrainians.[29] Because Russian servers hosted the dominant Russian-language social media platforms—*Vkontakte* and *Odnoklassniki*—the authorities were able to effectively block any pages with a pro-Maidan bent. It also allowed the Russian government to monitor sympathizers of the post-Maidan Ukrainian government, as well as recruit foot soldiers for its pro-separatist proxies. Second, the Kremlin put considerable spin on its portrayal of events in Ukraine, from the 2013-2014 Maidan Revolution, to the takeover of Crimea, to the ongoing war in the East. It portrayed Crimea as being land that historically belonged to Russia. It exaggerated the influence played by Ukrainian nationalists and neo-Nazis among the Maidan protestors, and later those fighting in the Donbas region in order to stoke fear among ethnic Russians and Russian-speaking Ukrainians. By demonizing the enemy, this was tactically important for its proxies, enabling the use of greater violence against their fellow citizens. Finally, the Kremlin-controlled Russian media ignored the presence of Russian soldiers and *spetsnaz* forces in Ukraine, and downplayed the illegality of Russia's land grab of Crimea. Conversely, Russia vastly overstated the role played by the United States in controlling the protests on Maidan and influencing events in the east.

Furthermore, Russian operatives sought to shape the battlefield by directly targeting and manipulating the minds of Ukrainian troops through subversive forms of propaganda and disinformation. In 2017, the Russian authorities created so-called "information operation troops," whose remit, according to Russian Defense Minister Sergei Shoygu, was to spread

"clever and efficient propaganda."[30] The aim of these troops encompasses a mix of strategic communications, psychological operations, and influence activities. They should not be treated as a separate cyberspace-based command, as their means go beyond just conducting cyberwarfare to disrupt networks but also include manipulating the media and planting counterpropaganda in order to control and distort the enemy's cognitive understanding of what is real and what is false. They involve planting fake news stories to stoke irredentist violence. A case in point is the steady stream of disinformation among Russian-language news broadcasts in the south and east of Ukraine threatening locals that Kiev would rescind their right to speak the Russian language. On Kolika Square in 2014, the journalist David Patrikarakos documented how a group of masked men armed with bats and clubs were told that a group of Ukrainian nationalists called *Pravy Sektor* ("Right Sector") was coming "to burn down our tents at 4:00 a.m." Much of the disinformation plays on people's traditional moral values. In 2014, it was also falsely reported by Russian media that Ukrainian soldiers had crucified a small boy.[31] Another popular meme circulated on Russian social media was that of an LGBT (lesbian, gay, bisexual, transgender) activist on the Maidan who harassed a straight passerby to the point of him bludgeoning her to death. The aim of such efforts is to paint the protestors with a broad brush stroke as LGBT activists, a way to sow distrust among rural and more conservative segments of Ukrainian society.[32]

The target of these IW efforts were also the members of the Ukrainian military fighting on the frontline. Shortly after the fighting started in eastern Ukraine in 2014, for example, soldiers deployed to the combat region started receiving "fake texts." The texts were often meant to threaten and demoralize troops in a "grinding" conflict with some texts reading: "Ukrainian soldiers, they'll find your bodies when the snow melts;" "Leave and you will live;" "Nobody needs your kids to become orphans;" "Ukrainian soldier, it's better to retreat alive than to stay here and die;" and "You will not regain Donbas back. Further bloodshed is pointless."[33]

Other texts were aimed to undermine unit cohesion and morale. Texts, often appearing to come from follow soldiers, have claimed the commander had deserted or that Ukrainian forces were being decimated and that "We should run away." Nancy Snow, a professor of public diplomacy at the Kyoto University of Foreign Studies, described this as "pinpoint propaganda." In previous conflicts, leaflets dropped by air or radio messages could easily be ignored—by refusing to pick up and read the leaflet or by tuning to another radio station—but it is nearly impossible to avoid reading text messages sent to one's phone.[34]

Russia combines its IW with kinetic operations, starting with a text message to a soldier, telling him he is "surrounded and abandoned." Ten minutes later, the soldier's family receives (recent contacts) a text message stating, "You son is killed in action." The friends and family likely call the soldier to see if the news is true. Seventeen minutes after the initial text message, the soldier receives another message telling him to "retreat and live" with an artillery strike following shortly thereafter to the location where the large group of targeted cell phones are detected. Thus, in one coordinated action, they use IW to target the soldier and his family and friends and combine it with electronic warfare, cyber electronic warfare, and artillery to produce both kinetic and psychological effects.[35] This is a technique that the Russian operatives are likely to employ in large-scale combat operations as well—blurring the geographical boundaries between the front line and the home front in new and potentially frightening ways.

Likewise, the soldiers of potential allies are not immune to Russian IW. NATO troops deployed in the Baltics and Poland as part of the deterrence mission have also been targeted. Instead of "pinpoint propaganda," soldiers have had their Facebook accounts hacked, data erased, or received messages stating "Someone is trying to access your iPhone" with a map appearing in the text with Moscow at the center of the map. One commander believes the intent of the IW is to intimidate the soldiers and to let them know that Russian intelligence forces are tracking them and their data is at risk.[36]

Russia has also targeted the US military, employing IW in an attempt to decrease its military readiness and that of its NATO allies. Russian media outlets have been known to reach out to the mayors of towns outside of the Hohenfels training area in Germany, asking them if the noise from military training is disruptive to the local population. This is a clear attempt to sow discord between the populations and the US base, with the intent of influencing the German government to put restrictions on military training.[37]

Finally, Russian IW in Ukraine has included attempts of technological interference in political institutions via cyberspace means, with mixed degrees of success. Ukraine provided a laboratory of sorts for Russian hackers who would later interfere more boldly in elections in the United States and in Western Europe.[38] The concept of "weaponized information" was honed in Ukraine to undermine its fledgling institutions and erode public trust. In addition to targeting critical infrastructure—Ukraine's electric grid, government websites, and banks—Russian operatives were active in planting fake news stories. The effectiveness of such operations, however,

are questionable. Examining the effects of Russian propaganda vis-à-vis Russian state-controlled TV in Ukraine, the political scientists Leonid Peisakhin and Arturas Rozenas found the effects to be uneven:

> Ukrainians who were already predisposed in Russia's favor found its media message persuasive. Pro-Russian Ukrainians who watched Russian TV were more likely to vote for pro-Russian candidates in the 2014 presidential and parliamentary elections than were anti-Russian Ukrainians who watched the same programming. Those with anti-Russian views were dissuaded by the Russian media message and became more likely to vote for pro-Western politicians. Individuals with no strong political priors seem not to have been swayed in either direction.[39]

The authors argue that the current erosion of credibility as a result of Russian IW poses not only a threat to Western democracies but also to Russia. Should Russia find itself in a protracted war, not unlike the current proxy conflict it faces in the Donbas, it may face an inflection point where the effectiveness of its propaganda increasingly wanes. This may result in its targeted audiences doubting even the false narratives put out by Russia's bots, hackers, and other spin-masters. Building on previous research, the authors also posit that Russian propaganda does not change minds but rather pushes voters to adapt more extreme points of view and increases political polarization, itself a factor that undermines democracy and liberal norms. Whether this is intended or not, the tactical effect of Russian IW in Ukraine is not to change minds but rather to push people toward the extreme and crowd out the middle. The middle is where democracy thrives, the polar extremes are where it withers and dies.

Conclusion & Countermeasures

The following includes a list of recommended countermeasures the United States and its allies should implement to counteract or deter Russia's use of information warfare.

• *As it did during the Cold War, the United States must contest the IO Battlespace.* The US was heavily invested in IO during the Cold War and the battle of ideas—the idea that capitalism and liberal democracy was superior to communism as an economic and political system—contributed significantly to the victory. But with the end of the Cold War, the United States cashed in its peace dividend and divested itself of national-level institutions, such as the United States Information Agency, that were designed to effectively coordinate and integrate strategic efforts and responses to threats. As a result, the United States has largely ceded the strategic

initiative to peer and near-peer actors by default. The United States must reinvest in strategic institutions, and arm those institutions with the mandate and authorities needed, to enable the United States to regain the initiative in the information environment. As the world's superpower, other nations follow the lead of the United States and if the United States elevated the importance of IO, other nations will follow.

• *Relax Rules of Engagement to Counteract Russian IW with IO.* The United States has done little to actually retaliate against Russia. The 2012 Magnitsky Act demonstrates the effectiveness such measures can have to pressure Moscow and "shame" powerful Russian individuals.[40] Congress has incorporated counter-propaganda funding into its most recent National Defense Authorization Act, in addition to proposed reforms to the Foreign Agent Registration Act and the Committee on Foreign Investment in the United States. However, these acts of legislation do not go far enough. The National Security Council, in its 2017 strategy, calls it "information statecraft."[41] But the United States is limited in its ability to engage in this type of warfare. As one senior NSC staffer put it, "we are not going to have an *RT*. The Russians do. The Iranians do."[42] Still, more innovative, less overt countermeasures are needed to deter, prevent, and punish future Russian aggression in this space, including a more sophisticated and targeted version of Radio Free Europe/Radio Liberty and Voice of America for the Facebook era.

• *Establish credible deterrence against IW.* Deterrence is premised on the threat of inflicting pain on an adversary in order to prevent them from taking an undesirable action. Importantly, the threatened pain must be sufficient to alter the cost-benefit analysis of the target state such that they alter their preferences: a successfully coerced adversary must prefer to avoid pain by complying rather than ignoring the threat and accepting the consequences. Thus, a successful coercive—or deterrent—threat depends on the capabilities to inflict pain and the willingness to do so. It remains to be seen whether the United States has the means to inflict sufficient pain on Russia as retaliation for its IW against our political system. But there should be no doubt as to our willingness to do so. If we are to have any hope of deterring future Russian interference in our democratic processes and institutions, we must make full use of the political and economic tools at our disposal, including sanctions and other forms of financial warfare, to establish a credible threat of pain. Furthermore, it should be clear to all—Moscow especially—that punitive measures are punishment for specific actions against American institutions. This requires shining a bright and very public light on those actions when doing so does not threaten re-

vealing intelligence sources and very publicly declaring the consequences of such actions. Only by regularly and visibly demonstrating to Moscow the cause and effect relationship between IW and punitive measures can we hope to establish a credible deterrent.

• *Provide IO Assistance to Allies.* The United States provides $50 billion in foreign assistance, yet almost none of this goes to support IO efforts.[43] Despite four years of being targeted by Russian IW, Ukraine is on the defensive and seems to have no response to Russian IW efforts. Ukraine should improve its defensive measures to prevent "pinpoint propaganda" and better counter Russia's "fake news." But it cannot do so without significant assistance and outside expertise. While the United States must improve its own capabilities, the United States has the capacity, in terms of expertise and funds, to help Ukraine and other allies.

• *Gather & Analyze More Data on IW*. The United States should catalog all attacks and take an evidence-based approach to identify sources and quantify their effectiveness as a way to track their own progress in deterring attacks and measure variation over time and space. For example, current efforts by the Ukrainian military to broadcast Ukrainian-language radio (Army FM) to the Donbas do not even track the number of listeners, much less the effect such positive messaging has on public attitudes. In the United States, to our knowledge, there is no database yet that tracks this sort of thing.

• *"Protect against Fake News."* Emilio Iasiello, a cyber analyst, recommends "leveraging 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."[44] The United States must do more than simply correct the record. By nature, corrections to the record or fact checks are reactive and are not effective to counter the effects of proactive fake news and Russian propaganda. In the battle of perception, the race to shape the early narrative is often times the decisive fight. Readers rarely care or read corrections, much less disclaimers, especially in an era of social media. To be effective, as Giles recommends, "Countermeasures should focus not on fact-checking but on the deceit—emphasizing that people were conned—and, like the original disinformation, should appeal to readers' emotions rather than their rationality."[45] This is tricky, given that Western governments are supportive of free speech, and so they cannot blanketly restrict news, even if it is false, coming from one country or its citizens.

• *Create a Robust Task Force.* In March 2015, the EU created a StratCom Task Force, whose purpose is to correct disinformation coming from Russian media. This kind of task force should be strengthened, and perhaps be bolstered with the addition of economic sanctions. A similar task force should be created in the United States and properly resourced and given teeth.

• *Establish Stronger Normative Framework for IO much like the Tallinn Manual did for cyberspace.* The trouble with propaganda in the digital age is there are no agreed-upon rules or norms, as there were during the height of the Soviet Union. Also the actors and perpetrators have been decentralized, making attribution more difficult, but also the adherence to norms or rules more problematic. Even though Russia will not abide by covenants agreed to by other states and international bodies, this can at least assist the West to determine the rules for the road for a post-Putin Russia that may determine that IO and the undermining of American influence is not in its best interest.

• *Strengthen retention rates among our allies.* Ukraine is a country teeming with information technology (IT) expertise. Yet, the government and its military have a hard time retaining expertise in this realm, due to higher salaries provided in the private sector. US assistance should be targeted to not only train our partners but be sure they retain their fighters.

• *Strengthen civil society.* Many of the most innovative and effective efforts made to target Russian disinformation and propaganda are coming from civil society groups like InformNapalm, which relies on open-source intelligence and employs volunteer hackers to discredit Russian narratives, or StopFake, which puts out media content to counteract Russian propaganda. These groups have been effective, given recent polls that show that a majority of Ukrainians now say that Russian propaganda constitutes a real threat.

• *Educate service members and their families of Russian IW practices.* American service members and their families must be warned of Russian IW practices and efforts so they are not discovering it for the first time when they are receiving a threatening text message—this will greatly reduce or eliminate the desired effect.

It is worth reassessing the threat of Russian information warfare given the recent doctrinal shift toward large-scale combat operations against peer and near-peer adversaries, which includes a wide spectrum of the use of force. Though it may be tempting to lament the threat that Russian IW poses to American interests and institutions in the 21st century, not to

mention those of our friends and allies, it is important to remember that we have been here before. As noted earlier, the legendary diplomat and scholar George Kennan was entirely familiar with the threat we face today, even if the technologies have changed. But what is important to recognize in his 1948 memorandum on political warfare is not the assessment of such a threat posed by our adversaries. Rather, it is the recognition that the United States must be willing and able to fight political wars just as we were willing to fight conventional wars to secure our interests. Kennan writes:

> Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP [the Marshall Plan]), and "white' propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[46]

Kennan's prescription remains just as valid as it did 70 years ago. It is time to recognize the threat that Russian IW poses to America's core interests and respond accordingly.

Notes

1. “Zuckerberg: Facebook is in ‘arms race’ with Russia,” *BBC News*, 11 April 2018, accessed 2 May 2018, http://www.bbc.com/news/world-us-canada-43719784.

2. See Mike Lundy, Rich Creed, “The Return of US Army Field Manual 3-0, Operations,” *Military Review*, November–December 2017.

3. Morgan Chalfant, “Former CIA Director: Don’t call Russian Election Hacking ‘Act of War,’” *The Hill*, 11 April 2018, accessed 20 June 2018, http://thehill.com/policy/cybersecurity/328344-former-cia-director-dont-call-russian-election-hacking-act-of-war.

4. Keir Giles, “Handbook of Russian Information Warfare,” NATO Defense College, November 2016.

5. Edward Lucas and Ben Nimmo, “Information Warfare: What is it and How to Win It?” Center for European Policy Analysis (CEPA) Infowar Paper No. 1, November 2015, 3–4.

6. Andrew Blake, “Michael Hayden, former CIA head, of Russia: ‘We took our eye off the ball,’” *Washington Times*, 1 May 2018.

7. George Kennan, “George F. Kennan on Organizing Political Warfare,” Wilson Center Digital Archive, 30 April 1948, accessed 13 June 2018, https://digitalarchive.wilsoncenter.org/document/114320.pdf.

8. Gabriel Samuels, “NATO puts 300,000 Ground Troops on ‘High Alert’ as Tensions with Russia Mount,” *The Independent*, 7 November 2016.

9. Greg Keeley, “Combatting Russian information warfare—in the Baltics,” *The Hill*, 9 April 2018.

10. Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: 27 November 2012), GL-3.

11. Sophia Porotsky, “Cold War 2.0: Russian Information Warfare,” *Global Security Review*, 8 February 2018, accessed 20 June 2018, https://globalsecuritytyreview.com/cold-war-2-0-russian-information-warfare/.

12. Quoted by Anne Vandermey, “Gaining Followers: The Internet and Cold War-style Propaganda in the Former Soviet Republics, *Wilson Quarterly*, Fall 2016, accessed 20 June 2018, https://wilsonquarterly.com/quarterly/the-lasting-legacy-of-the-cold-war/gaining-followers-the-internet-and-cold-war-style-propaganda-in-the-former-soviet-republic/.

13. Bruce McClintock, “Russian Information Warfare: A Reality that Needs a Response,” RAND Blog, 21 July 2017, accessed 20 June 2018, https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html.

14. Peter Mattis, “Contrasting China’s and Russia’s Influence Operations,” War on the Rocks, 16 January 2018.

15. Maria Snegovaya, “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare,” *Institute for the Study of War*, September 2015, 10.

16. Vladimir Isachenkov, “Russia announces new branch of military to focus on information warfare amid hacking allegations,” *The Independent*, 22 February 2017.

17. Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* 60, no. 2, 2016, 189–202.

18. Dustin Volz, "US grand jury indicts 13 Russian nationals in election meddling probe," *Reuters*, 16 February 2018.

19. David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century* (New York: Basic Books, 2017), 131–151.

20. J.B. Vowell, "Maskirovka: From Russia, With Deception," *RealClearDefense*, 30 October 2016.

21. Snegovaya, "Putin's Information Warfare in Ukraine."

22. Keir Giles, "Countering Russian Information Operations in the Age of Social Media," *Council on Foreign Relations Report*, 21 November 2017.

23. Giles, "Countering Russian Information Operations."

24. Phillip Karber, Joshua Thibeault, "Russia New Generation Warfare," AUSA, 20 May 2016, accessed 14 June 2018, https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare.

25. Lucas, "Information Warfare."

26. McClintock, "Russian Information Warfare."

27. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2, 1978, 167–214.

28. Snegovaya, "Putin's Information Warfare in Ukraine."

29. Michael Kofman, et al., "Lessons from Russia's Operations in Crimea and Eastern Ukraine," *RAND*, 2017.

30. Damien Sharkov, "Russia Announces Information Operations Troops with Counter Propaganda Remit." *Newsweek*, 22 February 2017.

31. Timothy Snyder, *On Tyranny: Twenty Lessons from the Twentieth Century* (New York: Duggan Books, 2017), 97.

32. Patrikarakos, *War in 140 Characters*, 161.

33. Raphael Satter and Dmytro Vlasov, "Ukraine soldiers bombarded by 'pinpoint propaganda' texts," *Associated Press*, 11 May 2017, accessed 14 June 2018, https://apnews.com/9a564a5f64e847d1a50938035ea64b8f Oleksandar Golovko, "Ukrainian Frontline: Cyber + EW + Psyops" PowerPoint brief (Kyiv, Ukraine: General Staff of the Armed Forces, 2018).

34. Satter and Vlasov, "Ukraine soldiers bombarded by 'pinpoint propaganda' texts."

35. Golovko, "Ukrainian Frontline."

36. Thomas Grove, Julia E. Barnes and Drew Hinshaw, "Russia Targets NATO Soldier Smartphones, Western Officials Say," *The Wall Street Journal*, 4 October 2017, accessed 10 May 2018, accessed 14 June 2018, https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402.

37. Interview with military officials in Hohenfels, Germany, on 8 May 2018.

38. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 2017.

39. Leonid Peisakhin, Arturas Rozenas, "When Does Russian Propaganda Work—and When Does it Backfire? Here's What We Found," *Washington Post*, 3 April 2018.

40. The 2012 Magnitsky Act, named after Sergei Magnitsky, a Russian tax accountant who died in prison under mysterious circumstances, punishes Russian officials believed responsible for his death.

41. Peter Grier and Harry Bruinius, "With National Security Strategy, Trump ushers new era of Statecraft," *Christian Science Monitor*, 18 December 2017, accessed 20 June 2018, https://www.csmonitor.com/USA/Politics/2017/1218/With-National-Security-Strategy-Trump-ushers-new-era-of-statecraft.

42. Nadia Schadlow, "Building National Security Strategy," Speech given to Modern War Institute at the US Military Academy at West Point, 2 February 2018, accessed 20 June 2018, https://mwi.usma.edu/event/writing-president-trumps-national-security-strategy-dr-nadia-schadlow/.

43. The US spent $49 billion in 2015; see James McBride, "How Does the US Spend Its Foreign Aid," Council on Foreign Relations, 11 April 2017, accessed 14 June 2018, https://www.cfr.org/backgrounder/how-does-us-spend-its-foreign-aid.

44. Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters* 47, no. 2, 2017, 62–63.

45. Giles, "Handbook of Russian Information Warfare."

46. George Kennan, "George F. Kennan on Organizing Political Warfare," Wilson Center Digital Archive, 30 April 1948, accessed 10 May 2018, https://digitalarchive.wilsoncenter.org/document/114320.pdf.