Everything Flows: Russian Information Warfare Forms and Tactics

in Ukraine and the US Between 2014 and 2020

Samantha Mullaney

ABSTRACT

This case study builds on previous analyses of Russian information warfare and covers the forms and tactics in simultaneous campaigns in Ukraine and the US between 2014 and 2020, using Daniel P. Bagge's DOPES methodology to discern and analyze patterns within events data from the two campaigns. Use of DOPES illustrates that Russian information warfare possesses discernible forms and tactics across varying contextual situations and is highly flexible. The forms and tactics align with Russian information warfare (IW) doctrine and the goals of reflexive control. The case study concludes with a discussion of strategic and policy level recommendations to counter the effects of Russian IW.

INTRODUCTION

Russian IW includes the doctrine Russia uses to achieve specific aims, whether strategic, operational, or tactical, and Russia's methods; it encompasses both principles and procedures.[1] One of the main challenges for western scholars and practitioners in identifying Russia's IW abilities and effectiveness is finding evidence or data of outcomes. Some scholars conclude that the effects are minuscule.[2] However, looking at Russian IW by searching for evidence of outcomes paints a deceptive picture and can lead scholars to draw skewed conclusions.

This research builds on previous research and analysis of Russian strategic use of IW, especially regarding new-type warfare means and the forms and methods of fighting, as suggested by Timothy Thomas.[3] It also seeks to identify Russia's use of multiple elements

Samantha Mullaney, a graduate of Augusta University's Masters in Intelligence and Security Studies Program in Augusta, Georgia, focuses her research on information warfare forms, tactics, and implications. Her capstone included completing an information warfare internship at the Georgia Cyber Center, where she researched Russian information warfare forms and tactics in Ukraine and the US. Samantha has a BA in History from Fairfield University, an MA in Elementary Education from Boston University, and spent nearly a decade teaching in Djibouti, Yemen, Jordan, and the UAE. She speaks intermediate Arabic and basic German. samantha.mullaney@protonmail.com

of IW in simultaneous campaigns.[4] Finally, as Costello explains, the US must identify, understand, and evaluate Russia's tools in the Initial Phase of War (IPW) and IW campaigns.[5] Many scholars have chronicled Russia's IW in Ukraine and the US between 2014 and 2020 as separate studies, but few have attempted to categorize the known events in a manner that would identify common forms or tactics.

This paper's six sections cover first the doctrinal evolution of Russian IW and its use of reflexive control as the primary theoretical paradigm underpinning IW. Second, Bagge's methodology of events categorization is explained. Third, the paper lays out the events' categorization results by form, tactic, target and vulnerability. Fourth, the results are discussed. Fifth, the paper addresses how Bagge's methodology should be used in future research. Last, the paper identifies policy areas applicable to the results and how the US can combat the forms and tactics of Russian IW.

BACKGROUND

Information is a foundational weapon in the pursuit of geostrategic goals. Russia's primary goals include destabilizing the geopolitical balance and reasserting its sphere of influence through information superiority.[6] To do this, Russia views warfare more broadly than the US and sees a state's population as a means to attain its goals.[7] Moreover, as will become apparent through the discussion of reflexive control, Russia views knowing its adversary as the enabling mechanism for successful IW.

Russian IW Doctrine and Reflexive Control

IW is central to achieving Russia's strategic goals. The framing concept Russia uses to implement and achieve IW is reflexive control (RC), a theory that has evolved over a century. The concept of RC can be subdivided into two sections.[8] The first is the reflexive system, and the latter is the reflexive process.

The reflexive system includes the target and any other participant in the system, including the observer and target, and each of their mental constructs. Each person in the system has a mental construct of the system and how each other person views the system. When adversaries meet, Lefebvre posits that the outcome will be "determined by the way the adversaries represent each other's mental world."[9] Essentially, he who best understands the adversary's mental world can interpret decisions most correctly, thereby giving them the advantage. This is the reflexive process.

An often-overlooked element of reflexive control is that it is a means to accomplish other outcomes and is an end goal in and of itself. For example, an actor uses reflexive control to gather information about an adversary that can be used in other ways, but control over the decision-making process is also the goal.

New Russian use of reflexive control can debatably be identified as the creation of an operator of awareness. This is when the actor does not have a specific goal but where the influence projected onto the adversary narrows the possible decisions, enabling the actor to reasonably predict decisions.[10] Current RC utilizes psychological effects on decision-makers, communicates false or partially false information, coerces the enemy to envision defeat, and uses the enemy's resources against it.[11] In addition, the use of cyberspace has allowed the theory to implement methods of access to the masses.[12]

For example, a Russian Ministry of Defense document defines IW as conflict in the information space that seeks to force “a state to make decisions in the interests of their opponents” by undermining political, information, social, or economic systems, as well as implementing “mass psychological campaigns against the population of a State in order to destabilize society and the government.”[13] Other published doctrine similarly espouses utilizing psychological or ideological information to “undermine trust in the government...[and] lead to the destabilization of the situation.”[14]

For simplicity, in this case study reflexive control is defined as the ability to influence the adversary to make the decisions you want him to make by influencing, transforming, and ultimately undermining the decision-making system.[15] In essence, reflexive control is effective marketing on steroids and directed for statecraft instead of commerce and control rather than management. Most importantly, the practice of reflexive control creates small actions that seem trivial to the target but have massive and complex intentions.[16]

Modern Russian IW Doctrine

Modern Russian IW is distinguished from western definitions of the concept by multiple factors. First, there is no differentiation between peacetime and war or civilian and military spheres. This is a point of issue for democracies. Next, unlike recent doctrine in the US, Russia does not view IW through cyber-colored glasses.[17] Cyber elements are a tool used in Russian IW, and therefore there is no distinction between cyber and information spheres.[18] The only

distinction made in the Russian concept of IW is between code-based and content-based methods, or what some authors have termed information-psychological and information-technology methods.[19] Also, Russian IW is long-term. IW seeks to decay "the moral values, psychological state or even the decision maker's character" to alter the perception of information.[20]

Last, IW is not meant to be kinetic in the traditional, western conception of kinetic warfare. Russian General Valery Gerasimov, perhaps the easiest figurehead for Westerners to associate with Russian IW, explains that nonmilitary means could have higher success rates than kinetic means in achieving objectives, and psychological measures have become the norm.[21] The fact that some US scholars have attempted to view IW success through the lens of whether it impacts kinetic action is essentially a product of mirror-imaging and inhibits an accurate understanding of the purpose and methodology of Russian IW.

All forms of information become a legitimate target for Russia, regardless of the state of war. While individual Russian attempts at IW may seem ineffective, Giles explains that "credibility is not always a metric of success for Russian information warfare campaigns."[22] The goal is to eliminate objective truth, inhibit the ability to report on a situation, destabilize the society, weaken morals and confidence, and destroy empirical knowledge.[23] Destabilization can lead to pressure on government officials and citizens to accept a solution that they would not have under their own volition, closing the loop of the reflexive control process.[24]

Indirect actions taken under the umbrella of IW intend to influence the enemy across a broad range of sectors by distributing disinformation to destroy the enemy from within.[25] Included in the means of achieving this is the protest potential of a population and other measures that have the possibility of demoralizing the public.[26] The long-term nature of effective IW campaigns creates persistent narratives that end up causing members of the target society to question themselves.[27] Moreover, the IW methodology can achieve a wide range of strategic objectives through the use of reflexive control.[28] For Russia, IW is the starting point of the new type of warfare; it determines whether and which future actions should be taken.[29]

METHODOLOGY

This research uses Daniel P. Bagge's DOPES method to categorize events and correlate them with known patterns, which in turn relies on S.A. Komov's intellectual elements of IW.[30] It is important to note that Russia's IW is flexible depending upon the environment. The following categories are often used simultaneously, offensively, and in a long-term manner against an adversary to discredit, defame and divide the state through polemics.[31]

Events were collected through open-source information from government indictments and reports, think-tank publications, declassified military reports and publications, independent organizations' research and analysis, investigative journalism, and news reporting. The events were input to an Excel sheet and then categorized by form, tactic, target audience, vulnerability, and source citation. Following categorization of the events data, processes of IW were compared by stage of war.

The Ukraine events data is divided into three stages, a broad consolidation of Gerasimov's six stages of warfare: pre-Crimean invasion, post-Crimean invasion but pre-Eastern Ukraine invasion, and post-Eastern Ukraine invasion. These were three clear-cut transitions within the war and corresponded to the use of paramilitary forces. The US events data were divided into two phases, as three separate phases were unable to be identified and paramilitary forces were not used. The two stages are pre-and post-2016 election. The Russian IW campaign is ongoing in the US, as is clear from the findings below.

RESULTS

Ukraine

Table 1

Form Pre-Crimean Invasion	Form Post-Crimea, Pre-Eastern Ukraine	Form Post-Eastern Ukraine Invasion
Pressure	Pressure	Pressure
Distraction	Suggestion	Distraction
Division	Distraction	Deception

Table 1 shows that pressure is the constant form of IW Russians deployed in Ukraine, throughout all stages of war. Distraction made up nearly half of the forms implemented during the IPW, or pre-Crimean invasion, with division also highly utilized. The forms changed once Russia invaded Crimea, with suggestion being used in 65 percent of the events. Division increased, but far less than distraction and suggestion. Post-invasion of Eastern Ukraine, distraction regained its usefulness, and deception became more common. Figure 1 illustrates the growth of deception, distraction and pressure throughout the campaign while Table 2 highlights the percentage change of form over time.

Table 2

Form	Pre-Crimean Invasion Percentage	Post-Crimea, Pre-Eastern Ukraine Percentage	Post-Eastern Ukraine Percentage
Deception	25%	45%	61%
Deterrence	21%	42%	19%
Distraction	46%	52%	64%
Division	42%	45%	27%
Overload	4%	30%	25%
Pacification	21%	43%	20%
Paralysis	38%	41%	18%
Pressure	67%	71%	77%
Provocation	38%	25%	8%
Exhaustion	13%	47%	35%
Suggestion	38%	65%	54%

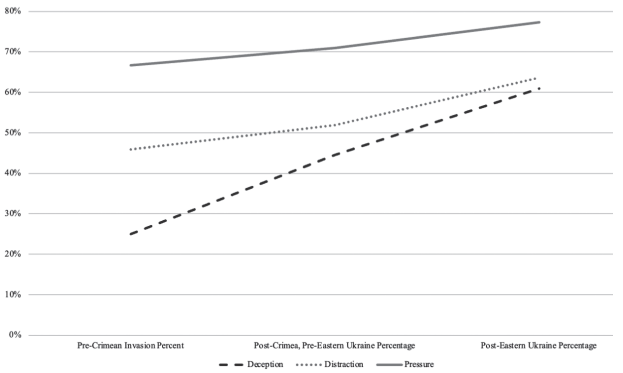

Figure 1. Forms in Information Warfare that Increase as War Progresses

Table 3

Tactic Pre-Crimean Invasion	Tactic Post-Crimea, Pre-Eastern Ukraine	Tactic Post-Eastern Ukraine Invasion
Political Action	Consolidation of control	Disinformation
Code-based	Code-based	Amplification
Disinformation	Cover	Code-based
Economic Manipulation	Electronic Warfare	Cross-legitimization

Table 3 shows that code-based tactics were used throughout the war, while people of influence were used more heavily at the beginning (13 percent) and middle phases (14 percent) rather than the end phase (10 percent). That said, disinformation through co-opted media and civil society outlets comprised the most common tactic in the final stage. Four out of the six tactics used in the IPW are not highly utilized in the middle phase, including political action, disinformation, and economic manipulation. Amplification and cross-legitimization became important toward the war's end. Figure 2 illustrates changes in use of tactics.

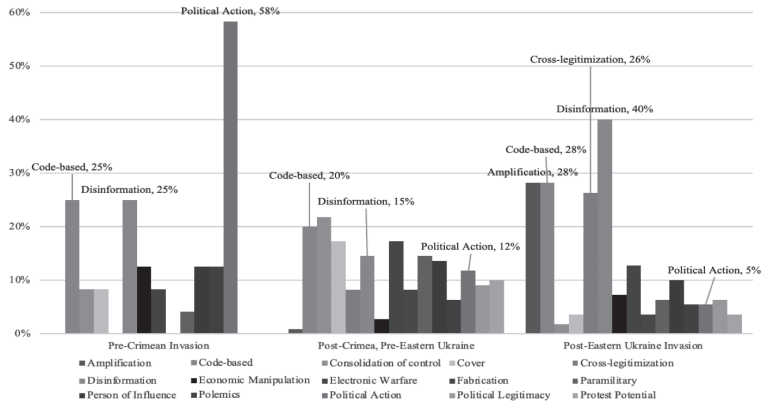

Figure 2. Tactic Used Over Time

Table 4

Target Pre-Invasion Crimea	Target Post-Crimea, Pre-Invasion of Eastern Ukraine	Target Post-Invasion of Eastern Ukraine
Russian domestic audience	Russian domestic audience	Russian domestic audience
Ukraine general population	Ukrainian government	Ukrainian general population
Ukrainian government	Ukrainian general population	Ukrainian government
NATO	NATO	NATO

Table 4 confirms that the Russian domestic audience remained the most important target throughout the war. Between the invasion of Crimea and the invasion of Eastern Ukraine, particular emphasis was placed on targeting the Ukrainian government (see Figure 3). NATO was a top target, but still significantly less targeted than the Russian or Ukrainian population.

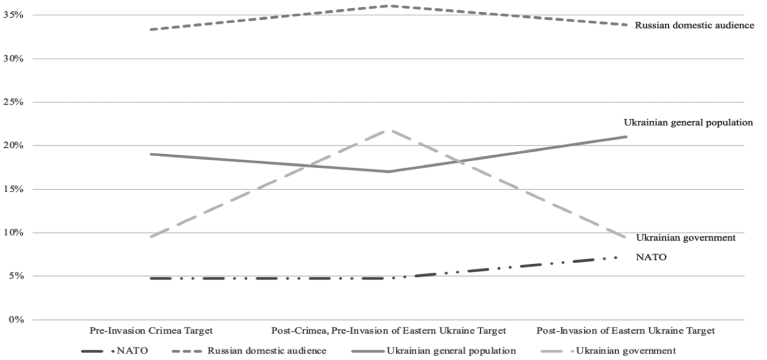

Figure 3. Target by Phase of War

Vulnerability Pre-Crimean Invasion	Vulnerability Post-Crimea, Pre-Eastern Ukraine	Vulnerability Post-Eastern Ukraine Invasion
Government Legitimacy	Government Legitimacy	Russia's Narratives to Citizens
Economic Dependence	Russia's Narratives to Citizens	Government Legitimacy
Reputation of US	Command and Control	Russian Legitimacy for Intervention

Table 5

Russia's IW largely targeted Ukrainian government legitimacy throughout all phases of the war, with post-Eastern Ukraine seeing a rise in Russia's emphasis on its domestic narratives, as noted in Table 5. Ukraine's economic dependence was exploited in the IPW, as was the US's reputation. As Russia consolidated control throughout the war, it targeted vulnerabilities within its society and sought to legitimize the war.

United States

Table 6

Form Pre-Election	Form Post-Election
Pressure	Pressure
Suggestion	Suggestion
Division	Division

The ongoing nature of Russia's IW campaign on the US created just two phases of warfare. Table 6 lays out the lack of change in IW form, and Table 7 shows some nuance between phases. Pressure made up 23 percent of the form for all events pre-2016 election, with suggestion at 16 percent and division at 13 percent, as shown in Table 7. These percentages changed slightly, post-election, with pressure at 20 percent, suggestion at 19 percent, and division at 17 percent. The largest change between forms by stage of the IW campaign was evidenced in the increased use of provocation post-2016 election, which increased from two to seven percent. Division saw a similar increase. Distraction fell from eight percent to one percent post-2016 election.

Table 7

Form	Pre-Election Percentage	Post-Election Percentage	Change
Pressure	23%	20%	-3%
Suggestion	16%	19%	3%
Division	13%	17%	5%
Deception	11%	12%	1%
Overload	9%	9%	0%
Exhaustion	9%	10%	1%
Distraction	8%	1%	-7%
Paralysis	6%	5%	-1%
Deterrence	2%	0%	-2%
Provocation	2%	7%	5%
Pacification	1%	0%	-1%

Tactics before and after the 2016 election differed, as Table 8 and Figure 4 confirm. While the primary tactic used was code-based, use of polemics and amplification grew the most, by five and seven percent, respectively. Conversely, leaks were less utilized post-2016 election, shrinking by nine percent. Table 9 compiles the change in tactic between the phases of the IW campaign.

Table 8

Tactic Pre-Election	Tactic Post Election
Code-based	Code-based
Political Legitimacy	Polemics
Leak	Amplification
Political Action	Political Legitimacy

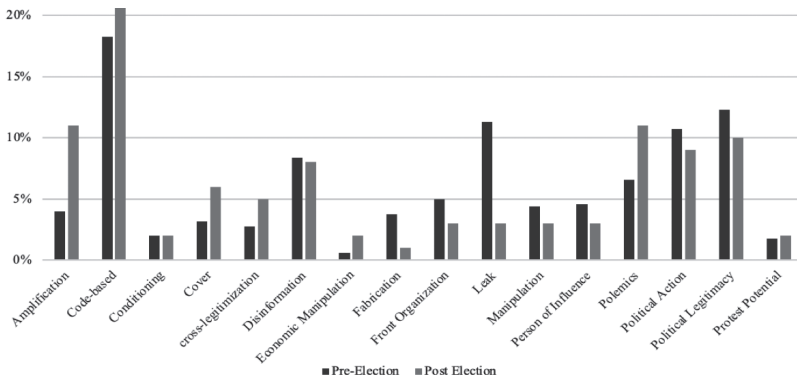

Figure4. Tactic Used Over Time

Table 9

Tactic	Change
Amplification	7%
Polemics	4%
Cover	3%
Code-based	3%
Cross-legitimization	2%
Economic Manipulation	1%
Manipulation	-1%
Person of Influence	-2%
Political Action	-2%
Front Organization	-2%
Political Legitimacy	-2%
Fabrication	-3%
Leak	-8%

Table 10

Target Pre-Election	Target Post-Election
US Public	US Public
US Policy Elites	Civil Society
Media	Media
Russian Domestic Audience	US Policy Elites

Table 11

Vulnerability Pre-Election	Vulnerability Post-Election
US Elites	Civil Society
Media	Media
Civil Society	US Reputation
US Reputation	US Elites

Table 12

Vulnerability	Pre-Election Percentage	Post-Election Percentage
US Elites	29%	13%
Media	18%	22%
Civil Society	18%	26%
US Reputation	17%	19%

The consistent IW target was the US public, holding 34 percent and 19 percent of the share of events before and after the election, respectively, as illustrated in Table 10. Although US policy elites were heavily targeted pre-2016 election with 24 percent of all events directed at them, this decreased to 11 percent post-election as the campaign moved toward targeting the media and civil society, which grew five and ten percent, respectively.

Russian IW saw vulnerabilities within US elites, the media, the US's reputation, and civil society throughout the IW campaign. Table 11 shows that the vulnerabilities did not change, but there was a different hierarchy of priorities in each stage. US elites were seen as less vulnerable following the election and were replaced by the media. Civil society was the most vulnerable part of American society post-2016 election, with 26 percent of all events directed toward it.

DISCUSSION

Use of Bagge's DOPES Methodology

This case study clearly shows that Bagge's DOPES analysis usefully delineates Russian IW forms and tactics. Indeed, DOPES analysis is perhaps the first of its kind to characterize Russian IW forms and tactics, and future scholars will find it useful for known Russian information interference, in categorizing events by form and tactic to discern patterns and emphases of Russian IW campaigns. The benefits of DOPES is clear. First, the forms and tactics Russia employs reveal a picture of how Russia views the reflexive system, and can be used in an offensive counterintelligence manner. Second, knowing the forms and tactics enables resources to be adequately distributed. Finally, the analyst is better informed to recommend measures to inhibit or mitigate Russian IW attempts.

DOPES delineates the evolving nature of Russia's forms of IW throughout the Ukrainian conflict, and reveals the flexibility of the Russian IW doctrine. Russia was interested in preventing Ukraine from joining NATO and the EU, sought control over Ukrainian policy, and needed Ukraine for domestic ideological purposes.[32] As each stage of warfare unfolded, Russia could assess whether and how those goals could be met by the context on the ground and was flexible in the tactics and forms used to achieve the goals.[33]

While categorizing helps practitioners, the data itself will enable a fine-tuned understanding of Russian IW. The events data for this case study were compiled over a short period and are not exhaustive. Future research should apply DOPES to larger events data sets that have multiple researchers cross-categorizing events. Finally, DOPES should be strengthened by incorporating other analytical processes such as Hammond-Errey's information influence and interference framework, thereby adding considerable depth to conclusions from events data.[34]

Ukraine

The effectiveness of Russia's IW campaign in Ukraine revolves around its understanding of Ukraine's reflexive system. Pressure, which DOPES defines as disseminating information that delegitimizes or destabilizes the government, is the main form of IW in Ukraine throughout all stages of warfare. The Ukrainian government has a reputation for corruption, incompetence, and general lack of ability and is one of the weakest links in the decision-making network within Ukraine. By heightening these exploitable elements within Ukraine through political action, disinformation through the media, and economic manipulation to decrease support for the government, Russia effectively pressured the Ukrainian government and outside elements into delayed reaction. Ukraine's will to resist diminished over time because Russia effectively targeted communication infrastructure and people of influence within the media and politics.[35]

Post-invasion of Crimea, Russia turned to suggestion and distraction to validate its military incursion to its domestic audience. Code-based tactics, cover, and electronic warfare were the most common tactics during this stage and enabled a broad implementation of suggestion and distraction and also inhibited an international response.

Russian forces consolidated control of military installations, the media, the internet, and cellular networks through electronic warfare tactics. Consolidation of control in the information sphere enabled Russia to utilize the tactic of cover entities across the media spectrum and within local organizations to distract observers from its activities. Specifically, television is still the primary source of information dissemination in Ukraine and Crimea, and 74 percent of the population derives information mainly from television. One leading Russian television station in Ukraine is associated with the Institute of CIS Countries' director who is a proponent of Novorossiya.[36] Essentially, Russia used consolidation of control over the media to implement both suggestion and distraction concerning the invasion of Crimea while also legitimizing its actions.

Post-Eastern Ukraine, the form of IW changed, and deception was implemented on a massive scale to rewrite the origins of the conflict, alter beliefs about facts on the ground, and manipulate the allocation of resources in a manner that fostered positive decision-making

outcomes for Russia, mainly in the form of a lack of Western intervention and the inability of the Ukrainian government to mount an effective response. Indicative of this is the report that in 2019 one in three Ukrainians was confused as to who started the war in Crimea.[37] Also, external governance has become an accepted narrative in eastern regions, illustrating the effectiveness of focusing on suggestion pre-invasion of Eastern Ukraine.[38]

At this point, the conflict became frozen, one of many outcomes favorable to Russia. High levels of disinformation, primarily enabled by the consolidation of control over the media, telecommunications system, and strategically placed elites parroting Russian narratives, achieved deception and pressure in the final stage. Amplification and cross-legitimization were used between media sources to normalize disinformation and achieve deception.

Russia's use of paramilitary forces in Ukraine was vital, but was hardly the most surprising aspect of warfare. More surprising was Russia's ability to "coordinate military and non-military means, including the information warfare aspects."[39] It did this by dividing the population early on, distracting international entities that could interfere, and placing high economic, diplomatic, and social pressure on Ukraine. Russia then vilified the leadership as fascist, claimed that government actions were unconstitutional, posited itself as the defender of a created victim group, and suggested that the West backed the protesters.[40] Finally, all that was left was to continue distraction through heightening disinformation levels, effectively paralyzing the decision-making capabilities of Ukrainians and Western diplomats, and corrupting the reflexive system.

Russia also used code-based tactics throughout the periods of war examined here. Russian IW doctrine consistently uses information-technology approaches throughout an IW campaign, and the events data show effective implementation of the doctrine. Since code-based tactics support any form of IW, it is understandable to see it as one of the most used tactics in Ukraine. Code-based tactics enabled other tactics to delegitimize the Ukrainian government, amplify disinformation, spread ideas, and consolidate control.

DOPES highlights a western misunderstanding that the most effective period of IW is the beginning of the war.[41] IW was vital through all stages of warfare, including throughout the kinetic stage. Western analysts assuming that Russia intends IW to be carried out linearly in a war setting underestimate Russia's IW strategy.

Russia's flexible IW doctrine enabled it to achieve international paralysis and increased federalism, and therefore Russian influence, in the region. The outcome raises doubts about whether specific plans are necessary when using reflexive control and IW or just broad directions.[42] Furthermore, Russia's deep understanding of the cultural and reflexive system, and all the previous long-term leg work associated with co-opting it, proved vital for the demoralization of the target. The exact progression of forms and tactics will be implemented

differently in future Russian IW campaigns. However, scholars and practitioners should acknowledge that Russia understood the target society and exploited its vulnerabilities and that the Russian implementation of IW aligns with its stated doctrine.

The United States

Whereas Ukraine lies within Russia's traditional sphere of influence and holds a unique position within Russia's national heritage, the US is the dominant democratic state espousing the liberalism that most threatens Russia, and the IW campaigns in these two states were quite different. As Sokolsky and Stronski explain, the key aims against the US were to delegitimize institutions, disintegrate the coalition of Western states through division, and destroy the supranational organizations that undergird democratic values.[43] Flake notes that Russia pushes a narrative of a "corrupt and failing" US democratic system, building on pre-existing ideas in specific segments of the US population.[44] Russia targets these groups in order to amplify, disseminate, and normalize its narrative.

DOPES shows that pressure is the most commonly used form in the US campaign. Pre-election, Russia used suggestion and division to attack the moral legitimacy and value system that drove decision-makers within the US reflexive system. Leaks, political action campaigns, and attacks on the political legitimacy of policy elites were common tactics. Undergirding these tactics was the specific targeting of the US media enterprises, a primary source of legitimacy within US civil society. The tactics align with known Russian IW doctrine, which attempts to destabilize countries through psychological attacks and undermine political, economic, and social systems.[45]

Kuleshov, Zhutdiev, and Fedorov explain that Russia's goal is to use psychological influence to encourage important resources to be "handed over voluntarily, since this is seen not as the result of aggression, but as a progressive movement toward democracy and freedom."[46] The tactics Russia used pre- and post-election illustrate this use of reflexive control. For example, the pre-election emphasis on leaks and attacks on political legitimacy enabled Russia to foster and amplify divisions post-election. Polemics further destabilized and disintegrated trust in media sources, with a recent Gallup poll noting that only 21 percent of Americans have "a great deal" or "quite a lot" of trust in newspapers.[47] In essence, Russia focused its IW campaign on driving a push for perceived progress toward a better democracy while at the same time hollowing out and co-opting the very elements of a healthy democratic system.

The pre-2016 election focus was on political elites. Post-election, Russia began targeting general civil society, hoping to funnel public discontent and division from the elites to general citizens. Easy US targets for Russia during the IW campaign included racism and immigration, both subjects with large numbers of activists to co-opt into increasing the state's instability. Russia can exaggerate the extent of racism in the US because of real discrimination

that exists.[48] Again, this aligns with an understanding of the reflexive system of the US, where political elites rely on mass perception, which civil society perpetuates.

Some scholars have highlighted the trend of Russia embedding itself within social media networks, learning how to interact successfully, and then manipulating the narrative and the actual network.[49] Persistent, long-term use of #blacklivesmatter by Russian agents within online African American networks illustrates this manipulation and co-option.[50] Scholars have also noted the Russian emphasis "to divide America by further polarizing an already polarized political climate."[51]

DOPES facilitates analysis of both of these trends, and the events data illustrates how the tactics employed can change while the form stays the same because the IW's target has changed. The change reflects a Russian understanding of the origins of US government legitimacy and Russia's technical ability to creatively and quickly build on trends evidenced in the target society to achieve successful outcomes from IW campaigns.

Comparison

The overarching aim of IPW is information superiority in the reflexive system, and Russian IW campaigns have implemented this doctrine across a wide range of cases, of which this study focused on two. The data illustrates Russia is clearly capable of running simultaneous IW campaigns that span the globe. In addition, one of the best-used methods for achieving information superiority includes the co-option of the mass media, military command-and-control processes, elite decision-makers, and the public in democratic states.[52]

Moreover, the DOPES forms and tactics align with the goal of RC.[53] Critics of Russia's work in Eastern Ukraine say there was no clear doctrine, but DOPES illustrates a flexible doctrine with clear and consistent categories of forms and tactics regardless of the target. This flexible and broad doctrine benefits Russian decision-makers who may fail to achieve tactical victories because it enables a wide range of follow-on options to achieve the broader mission.[54]

Russia aims to induce paralysis in both Ukraine and the US, identify and co-opt groups with anti-systemic leanings, and create alternative realities that they can later reinforce through Russian-backed entities.[55] The progression from division to suggestion and distraction in Ukraine illustrates this process. The evolution of tactics from political action and leaks to polemics and amplification in the US is a similar illustration. Vorobyov and Kiselev explain that this process often presents as buying up mass media, creating a perception of protecting democracy, infiltrating local government elections, and using nonprofit organizations.[56] These tactics are used in both Ukraine and the US campaigns, as the events data illustrate.

Russia knows it cannot destroy the US, but the US can destroy itself. The Leninist concept of disintegration provides the historical conceptualization for Russia to implement a campaign where "every manifestation of discontent" is utilized.[57] Disinformation becomes a potent weapon of societal disruption.[58] Russia achieves this by undercutting the government's legitimacy, deeming individuals and institutions hypocritical or morally repugnant, and co-opting language.[59]

In a 2017 US Senate hearing, it was noted that Russian IW is not so much about manipulating groups into trusting Russia but instead encouraging groups to legitimize their ideas and delegitimize all others, which is the Marxist idea of repressive tolerance.[60] Through the modern implementation of RC, groups come to view one another as adversaries who have no common ground, leading to group conflict.[61]

The flexibility of Russia's IW encourages use of different forms and tactics in different states. Russia will not likely replicate the Crimea model or even the US model. Instead, its IW will reappear with different combinations of tactics and forms which can be altered and redirected within the campaign based on new developments within the specific reflexive system.

RECOMMENDATIONS

The US must address its shortcomings from multiple directions if it desires to regain the strategic advantage or even successfully defend itself against Russian IW forms and tactics. Military involvement is a necessary but incomplete step; hyper-focus on a military solution will create an inadequate response to IW.

Recommendation 1: Bolster human networks, which are imperative for both offense and defense.

Human-centered strategies should identify and disrupt the human networks engaged in propagating IW, create networks to launch our IW campaigns, and facilitate durable and robust counterintelligence. From the counterintelligence perspective it means identifying connections between those within a decision-making loop and outside entities, such as Kremlin-linked think tanks and oligarchs, who are pressured in IW campaigns through illicit finance and investment.[62] The US must identify and disrupt these flows.

Recommendation 2: Regain institutional knowledge of Russian IW.

The US Intelligence community should target the Russian institutions that provide a bedrock for developing Russian IW doctrine and RC. For example, one widely understood element of effective RC is encouraging unpredictability. DOPES analysis can help counter this.[63] Clearly identifying the elements of Russian IW will lead to possible avenues of mitigation.

Recommendation 3: Consolidate and coordinate IW in the US.

The US must professionalize IW human capital and then decentralize and disperse the implementation of strategic goals through these individuals. Furthermore, consideration of recreating the Active Measures Working Group (AMWG) to identify Russian IOs may be beneficial.[64] The organization could "identify and expose" Russian disinformation and there could be a classified and public version of the group.[65]

Recommendation 4: Bolster Counterpropaganda.

Counterpropaganda should highlight Russia's illiberalism toward particular groups, outing the corruption of Russian elites and oligarchs, amplifying dissident stories within Russia, and the potential use of the Orthodox community, which today is strongly aligned with the Russian state. Each of these forms was used successfully by Russian counterpropagandists in Ukraine during World War II, as laid out by Kudinova.[66]

Recommendation 5: Acknowledge a necessary culture shift at home.

The priority as to combating tactics, especially disinformation and polemics, should be objectivity more than balance.[67] Objectivity and resilience are perhaps the two most important methods to combat Russian IW, although both of these would require a change in current American cultural norms. A society under attack needs to endure the present chaos with patience and fortitude until the facts can be found.[68] Society also must be resolved first to understand the facts before rushing to conclusions. Unfortunately, current means of mass communication in the US engender neither resilience nor objectivity. Indeed, they heighten impatience.

Recommendation 6: Set standards for online privacy and data protection.

IW abuses the lack of individual privacy afforded by the current regulatory measures in the digital space.[69] The data collected on an individual, which the US government cannot use, is sold and used by adversaries to launch IW campaigns to persuade or modify an individual's behavior.[70] Regulating who can collect personally identifiable data, its stored duration, how it is to be stored, and how it can be disseminated are all key avenues of regulation by the federal government.[71]

CONCLUSION

The goal of Russian IW is not to create a war; it is to prepare the ground in case of war and assist war once in process. Information warfare need not convince anyone; it simply needs to generate noise and destroy the idea of objective truth.[72] Essentially, it comes down to convincing those you can and confusing those you cannot. Russia's narratives are appealing because they tell a linear story that is flexible and straightforward, two elements that draw in "unwitting naïve idealists."[73]

Ultimately, Russia's use of IW is flexible, and it uses whichever tactics are most appropriate for the timing and context.[74] However, when combined, the effect can become fatal for a society.[75] Ukraine and the US bear witness to this process. Each tool used by the Russians is meant as one aspect of a cumulative, long-lasting campaign to create, direct, and support a particular framework beneficial to Russia's geopolitical goals. Bagge's DOPES methodology is a valuable tool to identify the forms and tactics of Russian IW as they occur in real-time while also providing evidence of Russia's ability to adhere to and implement its IW doctrine in multiple ways simultaneously. The US requires an ever nimble and robust response to mitigate Russian IW.

DISCLAIMER

NOTES

1. Daniel Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (New York, New York: Defense Press, 2019), 27.
2. Sandor Fabian, "The Russian Hybrid Warfare Strategy-Neither Russian Nor Strategy," *Defense & Security Analysis* 35 no. 3, (2019): 308-325.
3. Timothy Thomas. Th*inking* Like *a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War* (US Army Training and Doctrine Command, 2016), 38.
4. Timothy Thomas, "Russian Military Thought: Concepts and Elements," *MITRE Corporation* (US European Command, 2019): 12-3.
5. Katherine Costello, "Russia's Use of Media and Information Operations in Turkey: Implications for the United States," (RAND Corporation, 2018), 3, http://www.jstor.com/stable/resrep19906.
6. Bagge, *Unmasking Maskirovka*, 72, 85.
7. Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory," *Strategic Studies Quarterly* Fall (2018): 70-89; Conor Cunningham, "A Russian Federation Information Warfare Primer." *The Henry M. Jackson School of International Studies* (November 12, 2020), 2, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/.
8. Vladimir A. Lefebvre, *Conflicting Structures*, trans. Victorina D. Lefebvre (Los Angeles: Leaf & Oaks Publishers, 2015).
9. Lefebvre, *Conflicting Structures*, 12.
10. Lefebvre, *Conflicting Structures*, 55.
11. Sergey G. Chekinov and S. A. Bogdanov, "Strategic Deterrence and Russia's National Security Today," *Voennaya Mysl' (Military Thought)*, 3 (2012): 11-20; Stanislav Ermak and Aleksandr Raskin, "Are All Methods Good in Battle? On Some Aspects of Reflexive Control of the Enemy," *Armeyskiy Sbornik (Army Journal)* 7 (2002): 44; V. N. Karankevich, "How to Learn to Deceive the Enemy," *Voennaya Mysl' (Military Thought)* 15 (2006): 135-152.
12. Bagge, *Unmasking Maskirovka,* 53.
13. Ministerstvo Oborony Rossiyskoy Federatsii (Ministry of Defense of the Russian Federation), *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space* (2011), www.ens.mil.ru.
14. Makhmut Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, trans. Yakov Vladimirovich Fomenko (Abingdon: Routledge 1998), 53.
15. Bagge, *Unmasking Maskirovka*; C. Kamphuis, "Reflexive Control: The Relevance of a 50-year-old Russian Theory Regarding Perception Control," *Militaire Spectator* 187, no. 6 (2018): 329; Kevin N. McCauley, *Russian Influence Campaigns Against the West: From the Cold War to Putin (*North Charleston, South Carolina: CreateSpace Independent Publishing Platform, 2016); Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.
16. Keir Giles, *The Next Phase of Russian Information Warfare (*NATO Strategic Communications Centre of Excellence, 2016): 3; Keir Giles, *Handbook of Russian Information Warfare,* Research Division (NATO Defense College, 2016), 23.
17. Giles, *Handbook of Russian*, 9.
18. Ulrik Franke, *War by Non-Military Means: Understanding Russian Information Warfare*, Russia Studies Programme, March (Swedish Defense Research Agency, 2015), 20; Giles, *The Next Phase* (2016): 4.
19. Bagge, *Unmasking Maskirovka*, 46; Giles, *Handbook of Russian*, 9.
20. Bagge, *Unmasking Maskirovka,* 63.
21. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Voyenno-Promyshlennyy Kuryer* (2013).
22. Giles, *The Next Phase.*
23. Giles, *The Next Phase.*
24. Jolanta Darczewska, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study* (OSW Centre for Eastern Studies, 2014), 6.
25. Thomas, *Thinking Like a Russian*, 15.
26. Sergey G. Chekinov and S. A. Bogdanov, "The Strategy of the Indirect Approach: Its Impact on Modern Warfare," *Voennaya Mysl' (Military Thought)* (2011): 4; Chekinov and Bogdanov, "Initial Periods of War," 27; Gerasimov, "The Value of Science."

NOTES

27. Giles, T*he Next Phase* (2016).
28. Cunningham, "A Russian Federation," 5.
29. Thomas, *Thinking Like a Russian,* 30.
30. S. A. Komov, "About Methods and Forms of Conducting Information Warfare," *Military Thought* (English edition), 4 (July-August 1997), 18-22.
31. Costello "Russia's Use of;" Darczewska, *The Anatomy of,* 26; Rid, *Active Measures*, 133, 147.
32. Maria Snegovaya, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War (2015), 15.
33. Snegovaya, "Putin's Information Warfare," 15.
34. M. Hammond-Errey, "Understanding and Assessing Information Influence and Foreign Interference," *Journal of Information Warfare* 18, no. 1 (2019): 1-22.
35. Franke, *War by Non-Military*, 45.
36. Oleksandra Tsekhanovska and Liubov Tsybulska, *Evolution of Russian Narratives About Ukraine and Their Export to Ukrainian Media Space* (Ukraine Crisis Media Center, 2021), 4, 6, https://uacrisis.org/en/russian-narratives-about-ukraine7.
37. Detector Media, *Sources of Information, Media Literacy, and Russian Propaganda: The Results of the All-Ukrainian Public Opinion Poll*, March 2019, 10.
38 Detector Media, "On the Other Side of the Screen: An Analysis of Media Consumption and Disinformation in the Ukraine's Information Environment," May 18, 2021, https://detector.media/infospace/article/188115/2021-05-18-on-the-other-side-of-the-screen-an-analysis-of-media-consumption-and-disinformation-in-the-ukraines-information-environment/
39. Franke, *War by Non-Military*, 44.
40. McCauley, *Russian Influence Campaigns,* 354.
41. Snegovaya, "Putin's Information Warfare," 17.
42. Kristiina Muur, et al., "Russian Information Operations Against the Ukrainian State and Defense Forces: April-December 2014 in Online News," *Journal on Baltic Security* 2, no. 1 (2016): 63.
43. R. Sokolsky and P. Stronski, *The Return of Global Russia: An Analytical Framework*, Carnegie Endowment for International Peace, December 14, 2017, https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003.
44. Lincoln Flake, "Russia and Information Warfare: A Whole-of-Society Approach," *Lithuanian Annual Strategic Review* 18 (2020): 168.
45. Gareev, *If War Comes*, 53; Ministry of Defense of the Russian Federation, *Conceptual Views* on.
46. E. Kuleshov, B. B. Zhutdiev, and D. A. Fedorov, "Information-Psychological Confrontation Under Contemporary Conditions: Theory and Practice," *Vestnik Academia Voennykh Nauk* (*The Journal of the Academy of Military Science*) 1 (2014): 108.
47. Megan Brenan, "Americans' Confidence in Major U.S. Institutions Dips," *Gallup*, July 14, 2021, https://news.gallup.com/poll/352316/americans-confidence-major-institutions-dips.aspx.
48. Oleg Kalugin, *Spymaster* (New York: Basic Books, 2009), 54.
49. David M. Beskow and Kathleen M. Carley, "Characterization and Comparison of Russian and Chinese Disinformation Campaigns," in *Disinformation, Misinformation, and Fake News in Social Media,* (2020), 63-81.
50. Beskow and Carley "Characterization and Comparison;" Patrick Savage, *Social Media Information Operations: How Russia Has Used Social Media to Influence US Politics* (American Security Project, 2017).
51. Beskow and Carley "Characterization and Comparison."
52. Sergey G. Chekinov and S. A. Bogdanov, "Initial Periods of Wars and Their Impact on a Country's Preparations for a Future War," *Voennaya Mysl' (Military Thought)* 4 (2012): 27.
53. Bagge, *Unmasking Maskirovka*; Kamphuis, "Reflexive Control," 329; McCauley, *Russian Influence Campaigns; Rid, Active Measures*; Thomas, "Russia's Reflexive Control."
54. Muur, et al., "Russian Information Operations, 69.
55. Todd C. Helmus, et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (RAND Corporation, 2018), 9.
56. I. Vorobyov and V. Kiselev, "Hybrid Operations as a New Form of Armed Conflict," *Voyennaya Mysl* 5 (2015): 41-49.

NOTES

57. Vladimir Lenin, *What Is to Be Done?* (New York: International Publishers, 1929), 84.
58. McCauley, *Russian Influence Campaigns,* 22.
59. United States Senate, "Russian Influence and Unconventional Warfare Operations in the 'Gray Zone': Lessons From Ukraine," hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, March 29, 2017 in Washington D.C., 5, http://www.fdsys.gov.
60. Ibid.
61. Marek N. Posard et al., *From Consensus to Conflict: Understanding Foreign Measures Targeting* U.S. Elections, RR-A704-1 (RAND Corporation, 2020), https://doi.org/10.7249/RRA704-1.
62. Heather A. Conley et al., *The Kremlin Playbook 2: The Enablers,* Center for Strategic and International Studies, March (2019), https://www.csis.org/features/kremlin-playbook-2.
63. Giles, *Handbook of Russian,* 53.
64. Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 10.
65. Abrams, "Beyond Propaganda," 10, 11.
66. L.V. Kudinova, "The Role of Soviet Counter-Propaganda in Countering the Voluntary Departure of the Population from the Occupied Ukrainian Territories to Work in Germany," *Gileya* 110 (2016): 81-85.
67. Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power,* Russia and Eurasia Programme, March (Chatham House: The Royal Institute of International Affairs, 2016).
68. Snegovaya, "Putin's Information Warfare," 18.
69. Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review Winter,* 6, no. 1 (2021): 65.
70. Dawson, "Microtargeting as Information, 69, 71.
71. Jessica Dawson. Presentation at SECR 6982: Information Warfare class, Augusta University, Augusta, GA, November 2, 2021.
72. Steven Wilson, "What Are Russia's Goals with Disinformation on Social Media? Professor Steven Wilson Explains," *BrandeisNow* October 22, 2020.
73. McCauley, Russian Influence Campaigns, 66; Ben Nimmo, *Anatomy of an Info-War: How Russia's Propaganda Machine Works and How to Counter It*, Strategy Council (Central European Policy Institute, 2015).
74. Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare: Ukraine," *CEPA January* 29, 2021.
75. Roy Godson et al., *Soviet Active Measures, People-To-People Contacts, and the Helsinki Process* (New York: Ramapo Press, 1986).