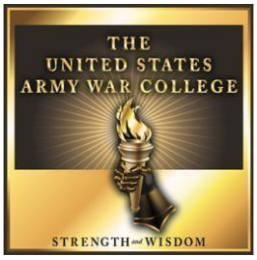
Strategy Research Project

The Russian Battlespace of the Mind

by

Lieutenant Colonel Joshua Kennedy
United States Army

Under the Direction of:
Professor Catherine Hill-Herndon



United States Army War College
Class of 2017

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2017	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
The Russian Battlespace of the Mind

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Joshua Kennedy
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Catherine Hill-Herndon

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Approved for Public Release. Distribution is Unlimited.

To the best of my knowledge this SRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** ☒ **PA:** ☒

13. SUPPLEMENTARY NOTES
Word Count: 5452

14. ABSTRACT

The Russian Federation's use of information as a weapon is not a new phenomenon. Interest in the subject has grown amongst U.S. foreign policy and defense practitioners following Russia's 2014 annexation of Crimea and especially the attempted manipulation of the 2016 presidential election in the United States. An objective analysis reveals a lack of institutional memory in the United States rather than a significant change in Russian strategy. Russian leaders since the tsars used false information, propaganda, and deception to control their internal population as well as influence external audiences. An understanding of the Soviet system of active measures and the United States countermeasures shed light on the challenges and opportunities in the new information environment. Russia updated its information tools, so must the United States.

15. SUBJECT TERMS
Active Measures, Disinformation, Information Operations, Propaganda, Political Warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	27	

The Russian Battlespace of the Mind

(5452 words)

Abstract

The Russian Federation's use of information as a weapon is not a new phenomenon. Interest in the subject has grown amongst U.S. foreign policy and defense practitioners following Russia's 2014 annexation of Crimea and especially the attempted manipulation of the 2016 presidential election in the United States. An objective analysis reveals a lack of institutional memory in the United States rather than a significant change in Russian strategy. Russian leaders since the tsars used false information, propaganda, and deception to control their internal population as well as influence external audiences. An understanding of the Soviet system of active measures and the United States countermeasures shed light on the challenges and opportunities in the new information environment. Russia updated its information tools, so must the United States.

The Russian Battlespace of the Mind

"[T]he Russian view of modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare."[1] – Janis Berzins, National Defense Academy of Latvia

While modern scholars may be learning this anew, it would not surprise Russian or Soviet historians who have long known this to be true. Czarist, Soviet, and post-Soviet leaders placed a premium on the use of information for both internal control and external influence. This assessment of the Russian Federation's view of modern war has been on full display during the last several years and is an essential aspect of Russia's foreign policy and defense strategy. After the dissolution of the Soviet Union in 1991, outside of a relatively small community of diplomats and Russia specialists, Russia was viewed as a defeated power. The world neglected to pay it much serious security attention. Assuming that it was on the path to democracy, partnership, and a free market economy, Russia became the preserve of western academics assisting with democratic transition and businessmen benefitting from market reform. Nations have a national character and history that shape their interaction with the world, particularly in the areas of diplomacy and security. As Russia struggled through the 1990s it increasingly felt itself threatened by loss of its territory, alliances, economic security, status, and by what it viewed as increasing encroachment and threats from the West, especially the United States and the North Atlantic Treaty Organization. Seriously weakened in the diplomatic, military, and economic elements of national power, Russia chose to maximize the use of information as a weapon to combat its adversaries and

regain its great power status in the world. Regrettably, it took the invasion of Crimea in 2014 to renew the full attention of Western Europe and the United States.

The central thesis of this strategy research project is that the Russian Federation's use of information as a weapon to advance its national interest is not a new phenomenon. The United States and the liberal democratic international order it established after World War II were, and remain, the primary targets of Russian falsehoods. The strategies and policies the United States developed to counter Soviet disinformation during the Cold War were effective and can serve as models for 21st century action. The paper will briefly compare the concepts of information operations as used in United States doctrine as well as that of the Russian Federation. Next, Russia's use of information will be placed in historic context alongside the Cold War response of the United States. Finally, the paper will examine Russia's current policy and information activities and will propose several recommendations to mitigate Russia's information strategies.

Definitions

The United States and Russia view and define information operations differently. To begin a discussion of strategic information operations, key doctrinal distinctions require clarification. U.S. Department of Defense Joint Publication 1 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."[2] The focus is clearly on activities conducted during *military operations* against a threat, suggesting a state of hostilities or conflict. "Information related capabilities" include strategic communication, joint interagency coordination groups, public affairs,

civil-military operations, cyberspace operations (CO), information assurance, space operations, military information support operations (MISO), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations, and key leader engagement.[3] The specific definitions of each of these terms is beyond the scope of this project, however, the important concept is that IO is a broad array of activity conducted by the military during conflict against a threat.

U.S. information operations are wholly separate from public diplomacy efforts which doctrine defines as “overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad.”[4] Admittedly, the U.S. does attempt to influence foreign audiences but does so based on shared understanding, open and truthful communications, and relationships.

The Russian Federation does not have a single definition of information operations, at least not one that is known to western analysts. Analysts comb through numerous published doctrines, academic journals, and the writings and speeches of Russian officials to determine the Russian approach to information and are able to develop a rather clear understanding of their doctrine. All of the information related capabilities of U.S. IO doctrine are found in Russian concepts. There are three key differences, however, that have important implications.

First, in the Russian context, there is no distinction between use of the information space in peace or war. Russia considers itself in a state of information war

at all times and believes that other nations, especially the United States, are as well; therefore it justifies all actions as defensive measures.[5] Second, the two concepts of information operations and public diplomacy are combined and expanded to include the Russian population. Neither U.S. information operations nor public diplomacy are principally directed at U.S. citizens and according to U.S. law it is illegal to do so. Russia practices defensive information warfare by tightly controlling its domestic information and media environment. By isolating the Russian public from alternative views that do not support the government's message, the Kremlin is able to effectively manipulate Russian public opinion in its favor.[6] The information itself is the important object and control of the information is vital to success. The third distinction, the concept of truth, is also of critical significance. Russian information strategies are not reliant on, or bound by, the use of true information. In U.S. doctrine the truth is paramount and those practicing IO or public diplomacy are lawfully required to be truthful, except in the application of approved military deception operations.

Historical Context

As the West works to understand how Russia uses information in the modern context, Heidi Tworek provides a valuable reminder that "[e]ach political system yields different forms of political communications, because political communications build on the logic of the system."[7] Russian tsarist and Soviet legacies shape the current system, and its approach to information operations. James Sherr, in his book on Russian foreign policy, points out that modern Russian leaders "have made it clear that they regard this historical experience as a source of legitimacy and inspiration for the state."[8] Past actions are often a good indicator of future actions.

Russia has a long history of authoritarian governance. The subordination of the individual, and society, to the state began early in Russian history and is a key factor in understanding how Russians see themselves and approach information.[9] Censorship, the invention of lies, the deception of others, and the creation of false realities were all well-established practices in tsarist Russia and even considered an integral part of Russian society.[10] In the mid-19th century, a French nobleman, Marquis Astolphe de Custine, published a book of his observations of Russian society and declared that "to refute a lie, to contradict a political claim…is an attack on the security of the state."[11] As the state was the ultimate authority, this created a society "where from birth minds are adapted to dissimulation."[12] The tsars used fakes, forgeries, staged events, and the agents and informers of the secret police to attempt to control the population. The Bolsheviks adopted their methods and developed formal policies and institutions to greatly expand the authoritarian nature of the state.

The Soviet Union's main tool of information operations was known as active measures. In Soviet terminology, active measures referred to a wide array of deceptive techniques designed to influence foreign populations and leaders. Like the modern Russian concept of information operations, there was no exact definition of active measures. They can, however, be broadly characterized as influence activities designed to strengthen allies, weaken opponents, and shape the environment to create conditions favorable to Soviet goals. There is general consensus that they did not include classic espionage and counterintelligence operations, which were activities designed to collect or protect Soviet intelligence.[13] Overt active measures included the work of numerous media outlets, diplomatic relations, cultural diplomacy, and international think tanks.

Covert activities included such things as establishing and funding front groups, covert propaganda of all forms, disinformation, agents of influence, and forgeries.[14] A study by the Central Intelligence Agency determined that the long-term, strategic objectives were to: influence world and American public opinion against U.S. objectives and programs, demonstrate that the United States is an aggressive power, isolate the United States from its allies, weaken U.S. standing in the developing world, discredit, weaken and expose U.S. intelligence activities, create conditions favorable for Soviet foreign policy, and undermine the political resolve of the United States and allies from defending against Soviet encroachment.[15]

Because of the highly centralized nature of the Soviet regime, the conduct of active measures was a truly “interagency” activity because it utilized the entire state apparatus for support. Numerous analysts describe active measures as one of three types; white (overt), black (covert) or gray (a mix), all managed by different agencies but centrally controlled by the Politburo. The International Information Department of the Communist Party of the Soviet Union (CPSU) controlled white active measures such as diplomatic, trade, aid, and information efforts. Examples include the TASS and Novosti news agencies, *Pravda*, Radio Moscow, information departments of Soviet embassies, and other open outreach activities. Department A (for *aktivnyye meropriatia*, active measures) of the KGB controlled black activities such as covert agents of influence, false rumors, forgeries, and propaganda. Gray activities, including communist fronts, foreign communist parties, Soviet NGOs, and foreign policy think tanks, were controlled by the International Department of the CPSU. Examples include the World Peace Council, World Federation of Trade Unions, Christian Peace Conference, the Academy

of Sciences, and publications such as the *World Marxist Review*. The International Department established the themes of active measures but left implementation up to the KGB and the International Information Department. All the departments received guidance and direction from, and reported back to, the CPSU Secretary.[16] While all KGB officers received training in active measures techniques and were encouraged to submit ideas for implementation, according to Major General Oleg Kalugin, the highest ranking KGB defector, "active measures were well integrated into Soviet policy and involved virtually every element of the Soviet party and state structure, not only the KGB".[17] It is estimated that the regime employed more than 15,000 people directly working active measures.[18]

U.S. Response

Early in the Cold War, the United States recognized that ideological confrontation was a key component of the struggle with the Soviet Union. Not only was the West competing with a nation state, but also with the international communist ideology espoused and exported by the Soviet Union. While it took many forms around the world, at its root, the Cold War was an ideological battle between democracy and communism in which both sides consciously used information as a weapon.

The Truman Doctrine and the Marshall Plan were already in place in April 1948 when George Kennan, while serving as the Director for Policy Planning at the State Department, outlined a strategy to conduct political warfare against the Soviet Union. He defined political warfare as "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."[19] He acknowledged that the United States had been conducting overt political warfare "in part consciously

and in part unconsciously." The purpose of the memorandum was to acknowledge the need for, and broad outline of, a coherent strategy for overt and covert actions and propose an organization in the U.S. government to conduct political war against the Soviet Union. The first element of the strategy was to form liberation committees. These were to be American civic organizations that would organize public support for "resistance to tyranny in foreign countries".[20] The second element was paramilitary operations, many of which remain classified, that included guerrilla forces, saboteurs, and other subversive activities in the Soviet Union and Eastern European countries.[21] The third element was support to indigenous anti-communist elements in threatened countries of the free world. Finally, Kennan proposed preventative direct action in free countries "only in cases of critical necessity… to prevent vital installations, other material, or personnel from being (1) sabotaged or liquidated or (2) captured intact by Kremlin agents or agencies".[22] He proposed the creation of a new organization to coordinate U.S. government efforts in political warfare and received approval to create the innocuously named Office of Policy Coordination (which was later moved to the CIA).

U.S. Congressional leaders also recognized the need for an overseas outlet to explain U.S. actions and counter Soviet messaging activity. A Congressional delegation sent to Europe in 1947 to assess the information activities of the State Department reported that "Europe had become 'a vast battlefield of ideologies in which words have to a large extent replaced armaments as the active elements of attack and defense.'"[23] This dire assessment led to the passage of the Smith-Mundt Act in 1948 (officially the U.S. Information and Educational Exchange Act of 1948) which, for the first time,

created an overt, global public affairs program run by the State Department. To improve the effectiveness of interagency information efforts, President Eisenhower created the United States Information Agency in 1953 to centralize “America’s public affairs operations under one agency, one leader, and one Congressional appropriation.”[24] In theory, the State Department became the policymaking body for public diplomacy, while the USIA became the operational component. The USIA’s mission was to “understand, inform, and influence foreign publics in promotion of the [U.S.] national interest, and to broaden the dialogue between Americans and U.S. institutions, and their counterparts abroad.”[25] USIA conducted educational and cultural exchanges, such as the Fulbright Scholar program, ran information resource centers in foreign countries, published electronic and printed materials and broadcast multiple radio and television stations to achieve effects. While not without its faults and critics, this dual arrangement with information responsibilities shared between USIA and the State Department continued throughout the Cold War. Believing that the ideological war with Russia was over, Congress dismantled the USIA in 1999 and merged most of its operations back into the State Department.

For much of the Cold War, the United States did not have an organization specifically chartered and designed to expose and challenge Soviet active measures in an overt manner. A key component of President Reagan’s approach was to directly confront all aspects of Soviet strategy including the information domain. Created in 1981, the Active Measures Working Group (AMWG) was an interagency organization that focused its efforts on exposing Soviet disinformation. Led by the State Department Bureau of Intelligence and Research (INR), with participants from the Central

Intelligence Agency, Department of Defense, United States Agency for International Development, Federal Bureau of Investigation, Department of Justice, the Arms Control and Disarmament Agency, the Defense Intelligence Agency, and the National Security Council staff, amongst others, the working group developed a methodology to collect, analyze and confront Soviet disinformation.[26] The working group met weekly in an unclassified forum to review the disinformation, forgeries, and media stories collected throughout the world by the CIA, State Department, USIA, and other organizations.[27] The group produced reports and held press conferences to publicize its findings and ensure the exposure of the false information. The AMWG eventually began to travel to foreign nations to meet with U.S. embassies, foreign governments, and the press to provide briefings on its findings. Positive feedback from friendly nations and condemnation from the Soviets and other hostile governments and organizations served as an early indicator of success. The understanding of the importance of active measures to Soviet strategy grew as the groups work became well known. The work proved so effective that Soviet leaders eventually reigned in the KGB and disinformation campaigns in an effort to improve U.S.- Soviet relations.[28]

Current Situation

Many in Russia view the end of the Soviet Union primarily as the loss of an information war with the West. Igor Panarin, a prominent intellectual, former KGB agent, and professor at the Diplomatic Academy of the Foreign Ministry, authored a book entitled *The First Global Information War- The Collapse of the USSR* in which he accuses the West, specifically the United States and Great Britain, of waging a decades long information war that resulted in the dissolution of the Soviet Union. His theory posits that Russia was, and is still, attacked not only militarily and economically, but

through the West's strategic use of information. His perspective directly informs the 2016 Doctrine for the Information Security of the Russian Federation which clearly describes a Russia under assault from other states "use of information technology for the purpose of causing damage to the sovereignty, territorial integrity, and political and social stability of the Russian Federation."[29] Russian elites believe the activities of western governments in post-Soviet countries are acts of war, "whose goal is to weaken or even topple the Russian government."[30] This widely held belief provides a convenient cover for a wide range of aggressive actions and supports Panarin's argument that any use, or misuse, of information on the part of Russia is now justified as defensive in nature.[31]

Coupled with this belief are advances in military thought. Since the annexation of Crimea in 2014, western analysts have spent considerable time and effort studying the operation in light of a 2013 article written by General Valery Gerasimov, the Chief of the Russian General Staff. In the article "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," he described his observations on the past, present and future of war. Although he was explaining how he thinks other nations, particularly the United States, conduct war in the modern era, since the annexation of Crimea his thoughts have become known as the "Gerasimov doctrine" in the West. Dozens of international think tanks and military organizations now believe that the new doctrine was the template for the seizure for Crimea and for future Russian action.[32] Gerasimov wrote, "The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force

of weapons in their effectiveness."[33] During an associated speech to the Russian Academy of Military Sciences in 2013, he was even more explicit in his description of 21st century warfare. In his view, political goals "are no longer to be attained through conventional firepower but through the 'widespread use of disinformation, of political, economic, humanitarian, and other non-military measures deployed in connection with the protest potential of the population'"[34] In retrospect, such language was a signal of what was to come as the Russian Federation captured Crimea without violence, but with a referendum. Now alternatively known as hybrid war, gray zone conflict, non-linear warfare, next generation warfare, or a host of other terms, Russia clearly prioritizes the use of information in concert with its other elements of power.

The collapse of the Soviet Union, coupled with advances in technology, increased the desire and ability of Russia to conduct active measures style operations. The decade of the 1990s destroyed much of the power of the former Soviet Union and exposed the weaknesses of the state. While not able to fully compete militarily or economically, and grasping to maintain relevance diplomatically, Russia discovered that it could still wield considerable power through influence. Russia is not stuck in a 20th century Cold War mindset as some argue; it has instead built on its history to create a modern information warfare approach "designed to work within the limitations of the 21st century strategic environment and within Russia's budget constraints".[35] Russian 21st century active measures are incredibly similar to their Soviet counterparts, though they lack the central direction of the CPSU. There does not appear to be a formal structure for modern information warfare outside of the Ministry of Defense (at least not yet identified), but it is clear that unity of effort exists amongst a wide swath of Russia's

ruling class. During the tumultuous years after the Soviet Union, many of the 800,000 KGB officers reorganized themselves into the Federal Security Service (FSB) while "expanding and absorbing other instruments of power, including criminal networks, other security services, economic interests, and parts of the political elite".[36] It is estimated that nearly 80% of Russian elites have ties to the security services and many are former KGB agents themselves, meaning that they have training, a worldview and a mode of operating that is in concert with each other.[37]

The Kremlin has many propaganda outlets and maintains control of the majority of media sources in the country. Most famously, it runs the international RT (formerly Russia Today) television and YouTube channel which reaches millions of people around the world with its message of "Question Everything." Sputnik, which produces radio, social media and news in 34 countries, is another media platform offering the Russian alternative worldview. These outlets, along with Russian officials in formal statements, seek to separate allies, particularly NATO, the EU and the U.S. by exaggerating or falsifying divisions in alliances. Russia's Compatriots policy, the Institute for Democracy and Cooperation, the Russkiy Mir Foundation, the Orthodox Church (wittingly or not), the Russian International Affairs Council and the Gorchakov Foundation represent the many Russian NGOs, think tanks, and cultural outreach organizations that foster Russian propaganda and harken back to their Soviet predecessors.

Meddling in the 2016 U.S. Presidential election is the most recent, visible, and audacious interference in the politics of the United States, but it is not a new tactic for Russia. Nor is the United States the only target, however, and 2017 will prove to be a

pivotal year in European politics as eight nations will hold parliamentary or legislative elections, five nations will hold presidential elections, and several nations will hold local elections. The results of these elections are of critical importance to the future of the European Union (EU) and the North Atlantic Treaty Organization (NATO). As with the 2016 U.S. election, Russia is actively attempting to influence outcomes through propaganda, networks of influence, economic pressure, and cyber and social media activities. Russia is attempting to weaken the EU and NATO as well as discredit Western style liberal democracy. Eurosceptic parties, particularly in France, Germany, and the Netherlands, are poised to make stunning gains during the year and force United Kingdom Brexit-style referendums on leaving the EU in many countries. Such actions could pose a significant threat to the future of the EU, NATO, and stability in Europe as well as the global economy. Many of these Eurosceptic parties and organizations receive funding and support from Russia or its front organizations.[38]

European Intelligence agencies are actively reporting on the threat to their countries. For example, the Security Information Service of the Czech Republic describes Russia's actions as intended to weaken the strength of Czech media, strengthen the information resistance of the Russian audience while exerting influence on the perceptions and thoughts of the Czech audience, weaken society's will for resistance or confrontation, create or promote inter-societal and inter-political tensions in the Czech Republic, and, disrupt the coherence and readiness of NATO and the EU.[39] Germany's internal intelligence chief recently described "increasingly aggressive cyber espionage" against German political parties ahead of the 2017 elections.[40] Some analysts fear that the sizable Russian ethnic minorities in the Baltic nations are

susceptible to Russian information campaigns and will provide the pretext to a military conflict similar to Ukraine.

The greatest difference between Soviet active measures and the modern Russian version is the significance of truth for foreign target audiences. Soviet propagandists, forgers, and agents went to great lengths to convince foreigners that its disinformation efforts were the truth. With limited budgets, language barriers, and rigid publication standards in the Western media, disinformation had to be believable to be effective. A member of Putin's election campaign remarked that in the Soviet Union the "concept of truth was important. Even if they were lying they took care to prove what they were doing was 'the truth'. Now no one even tries proving the 'truth.' You can just say anything."[41] Coupled with what RAND analysts refer to as the "firehose of falsehoods"- incessant lies and propaganda across multiple mediums- it is now even more difficult to stop, manage, and correct misinformation.[42] There are four characteristics of this fire hose model: "high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions" as well as its rapid, continuous, and repetitive nature and lack of consistency.[43]

The diffusion of technology and the proliferation of the internet allow the Kremlin to reach new audiences and at a higher volume than in the Soviet era. Thousands of Russian "trolls" work around the clock, under fake identities, to flood the internet and social media with disinformation, lies, or pro-Russian stories causing confusion and the proliferation of "fake news". The effect is that the average internet user is often confused about what is fake and what is real. It also sows seeds of doubt in numerous areas of western culture and politics, undermining liberal democratic values. No longer tied to

communist ideology, Russia now cooperates with virtually any group, politically left or right, that it can use to weaken the international democratic order.[44]

Recommendations

Research for this project reveals good news that Western governments, societies, and media organizations are already taking action to combat and mitigate Russia's information operations strategies. The following recommendations seek to propose areas of further study and increased action:

Understanding

Robert Seely's extensive study of information warfare has led him to conclude that active measures "describes a form a warfare practiced by the USSR in the second half of the 20th century which is likely to become one of the most important forms of warfare in the 21st century, indeed it may become the single most practiced form of war between states."[45] The first step to combat Russian actions is to understand the history, context, and aims of the Russian use of information. "Ignorance of the precedents, fears, and ambitions that inform" Russia's actions will lead to further miscalculation, ineffective responses, and possibly tragic consequences.[46] U.S. policy makers, in all sectors of power and society must renew and rebuild expertise about Russia. During the Cold War thousands of Americans became Sovietologists and developed a deep knowledge of Russia and the Soviet regime. It is now time for Kremlinologists to replace them and focus on the modern Russian Federation. The United States, and the West more broadly, must also understand the Russian target audiences, information dissemination networks, and the messages that resonate and stick.[47] Only then can it design, develop, and distribute effective counter-messages. The public outcry about

direct Russian interference in the 2016 election is already proving to be a powerful motivator for action.

Not a New Cold War

In his manuscript, *A 'New Cold War'? Abusing History, Misunderstanding Russia*, Dr. Andrew Monaghan makes an important case that the current conflict with Russia is not a "new Cold War."[48] While there are many similarities, there are also incredible differences. If the West defaults to a Cold War discussion it will traps itself in simplistic and deterministic thinking and miss the many ways Russia is adapting. Not every tool or tactic employed in the Cold War is appropriate for today's conflict. The West cannot refight the Cold War with the same methods and believe that it will be successful.

Counter Unconventional Warfare/Political Warfare

Section 1097 of the U.S. Government's National Defense Authorization Act (NDAA) of 2016 tasked the Secretary of Defense to submit a strategy to counter unconventional warfare (UW) threats.[49] This is a substantial recognition of the threat and a welcome validation of the importance of unconventional warfare strategies at the national level. Although tasked to the Secretary of Defense, unconventional or political warfare requires a coordinated effort across all agencies of the government. It is already driving a robust discussion of political warfare and interagency actions amongst UW practitioners. There is a broad discussion occurring amongst Special Operations organizations, and the United States Army Special Operations Command has held numerous workshops and wargames with political war and UW as the subject. Two of the immediate outcomes were the 2014 *USASOC Counter-Unconventional Warfare White Paper* as well as the 2015 *SOF Support to Political Warfare White Paper*.[50] The

increasing discussion of gray zone conflicts in academia, senior service colleges, think tanks, and in Congress should drive a robust political warfare debate at the National Security Council along the lines of President Eisenhower's Project Solarium.[51]

Counter Propaganda Efforts

Section 1287 of the 2017 NDAA included the Countering Foreign Propaganda and Disinformation Act of 2016 which re-charters the existing State Department Global Engagement Center to, "lead, synchronize, and coordinate efforts of the federal government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining U.S. national security interests."[52] It also authorizes the center to "provide grants to support civil society groups, media content providers, nongovernmental organizations, federally-funded research and development centers, private companies, or academic institutions in analyzing, reporting on, and refuting foreign disinformation efforts."[53] Congress recognizes the need for such an effort and organization, now it should appropriate the funds necessary for the work.

Unity and Civilizational Confidence

Finally, one of the greatest threats to democracy is citizens lack of understanding about, and confidence in, themselves, their institutions and their system of government. This is Russia's primary line of attack against the western, liberal democratic order. Molly McKew provides a grim assessment of Russia's successful weakening of western civil society:

> The Kremlin's campaign of disruption has succeeded in deepening divides in our society, tarnishing a considerable cross-section of our leadership, eroding faith in our institutions and propelling Russia to the center of our political life. It has helped turn us against each other and our allies, and

> made us distrust the very tools and institutions that can give us clarity on the threats we face.[54]

The “Firehose of Falsehoods” contributes to the West questioning beliefs in liberal democratic principles and institutions. In many ways U.S. citizens no longer know what or whom to believe and are left with “weakened moral immunity to propaganda”, and “weakness of confidence in sources of knowledge”.[55] The most effective way to negate disinformation is with accurate information. The more citizens of democracies disagree amongst themselves the more they enable Russia’s propagandists. Perhaps the most basic place to start is to establish agreement on the problem.

Conclusion

Russia seeks to weaken the existing liberal world order while avoiding a direct military confrontation with the United States and believes that its best defense is in a strong information offense. This challenge is not new. The character and tools of the information may have changed but the essential nature of the conflict has not. “The major propaganda themes directed against the West consistently have sought to characterize U.S. military and political policy as the cause of most international conflict; to demonstrate that the United States is an aggressive, militaristic, and imperial power; and to isolate Washington from its allies and friends.”[56] This description, written more than 30 years ago, is still an accurate characterization of Russian objectives. Until very recently policy makers, defense organizations, and the American public did not remember Soviet active measures, accept that Russia may still be employing them, or demonstrate the willingness to aggressively counter their actions. The United States cannot neglect the importance of the information domain. As Rand Waltzman, a former program manager at the Defense Advanced Research Projects Agency, succinctly

describes, “U.S. military doctrine is primarily kinetically oriented. Our opponents are becoming less kinetically oriented by the day.”[57]

The United States and the West have a Russia problem, not a Putin problem. The use of disinformation is a characteristic of Russian foreign policy and internal politics and has been employed by every Russian leader since the tsars and there is no reason to believe the next Russian leader will be different. The current Russian information warfare strategy, while not identical to active measures, is remarkably similar. No strategy or organization can possibly refute every falsehood, but it is vital to defend the values of the United States from the most egregious lies. A strategy, and a model of an interagency organization that achieved success in the past, exists. It is time to update it for the 21st Century. The United States can no longer concede the “battlespace of the mind”.

Endnotes

[1] Janis Berzins, *Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Policy Paper 2 (Riga, Latvia: National Defense Academy of Latvia, April 2014), 5, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP 02-2014.ashx (accessed December 5, 2016).

[2] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 110.

[3] U.S. Joint Chiefs of Staff, *Information Operations,* Joint Publication 3-13 (Washington, DC: U.S. Joint Chiefs of Staff, November 27, 2012, Incorporating Change 1, November 20, 2014), xi.

[4] U.S. Joint Chiefs of Staff, *Dictionary of Military and Associated Terms*, 192.

[5] Kier Giles, *The Next Phase of Russian Information Warfare* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, May 20, 2016), http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles (accessed December 5, 2016).

[6] Kier Giles, *Russia’s “New” Tools for Confronting the West* (London: Chatham House, March 2016), 33, https://www.chathamhouse.org/publication/russias-new-tools-confronting-west (accessed December 10, 2016).

[7] Heidi Tworek, *Political Communications in the "Fake News" Era: Six Lessons for Europe*, Policy Brief No. 1 (Washington, DC: Transatlantic Academy, February 2017), http://www.academia.edu/31629897/Political_Communications_in_the_Fake_News_Era_Six_Lessons_for_Europe (accessed February 20, 2017).

[8] James Sherr, *Hard Diplomacy and Soft Coercion: Russia's Influence Abroad* (London: Chatham House, 2013), 17.

[9] Thomas Graham, "The Sources of Russian Conduct," *The National Interest*, November 27, 2016, http://nationalinterest.org/feature/the-sources-russian-conduct-17462 (accessed December 15, 2016).

[10] Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Lanham, MD: Rowman and Littlefield, 2016), 3.

[11] Ibid.

[12] Ibid.

[13] Richard J. Heuer, "Soviet Organization and Doctrine for Strategic Deception," in *Soviet Strategic Deception,* ed. Brian Dailey and Patrick Parker (Lexington, MA: Lexington Books, 1987), 23.

[14] Richard H. Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington, DC: Pergamon-Brassey's International Defense Publishers, 1984), 2.

[15] Heuer, "Soviet Organization and Doctrine for Strategic Deception," 25; Shultz, *Dezinformatsia*, 40.

[16] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016): 5-31, 12, https://connections-qj.org/article/beyond-propaganda-soviet-active-measures-putins-russia (accessed November 12, 2016); Shultz, *Dezinformatsia,* 20-25; Heuer, "Soviet Organization and Doctrine for Strategic Deception," 26-29.

[17] Abrams, "Beyond Propaganda," 7, 13.

[18] Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Special Report of The Interpreter (New York: Institute of Modern Russia), http://imrussia.org/en/research (accessed December 10, 2016).

[19] George Kennan, *Policy Planning Staff Memorandum* (Washington, DC: U.S. Department of State, May 4, 1948), https://history.state.gov/historicaldocuments/frus1945-50Intel/d269 (accessed December 20, 2016).

[20] Ibid.

[21] Lowell H. Schwartz, *Political Warfare against the Kremlin: US and British Propaganda Policy at the Beginning of the Cold War* (New York: Palgrave Macmillian, 2009), 108.

[22] Kennan, *Policy Planning Staff Memorandum.*

[23] Schwartz, *Political Warfare against the Kremlin*, 109.

[24] Matthew Armstrong, "The Past Present and Future of the War for Public Opinion," *War on the Rocks*, January 19, 2017, https://warontherocks.com/2017/01/the-past-present-and-future-of-the-war-for-public-opinion/ (accessed January 20, 2017).

[25] U.S. Information Agency, *USIA Overview 1998* (Washington, DC: U.S. Information Agency 1998), http://dosfan.lib.uic.edu/usia/usiahome/oldoview.htm#overview (accessed January 5, 2017).

[26] Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference* (Washington, DC: National Defense University Press, 2012), 34, 39.

[27] Ibid., 39.

[28] Ibid., 100.

[29] Vladimir Putin, *Presidential Decree of December 5, 2016, No 646, On Approval of the Doctrine of Information Security of the Russian Federation* (Moscow: The Kremlin), http://kremlin.ru/acts/bank/41460/page/1 (accessed February 10, 2017).

[30] Stefan Meister, *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign*, German Marshall Fund of the United States 2015-2016 Paper Series, No. 6. (Washington, DC: German Marshall Fund of the United States), 5, http://www.gmfus.org/publications/isolation-and-propaganda-roots-and-instruments-russia's-disinformation-campaign (accessed December 15, 2016).

[31] Van Herpen, *Putin's Propaganda Machine*, 8.

[32] RAND, Chatham House, Atlantic Council, Transatlantic Academy, Institute for the Study of War, Center for Strategic and International Studies, NATO, the European Union and others all produced reports about the Gerasimov doctrine and its application in Crimea and its future use elsewhere.

[33] Valery Gerasimov, *"*The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,*" Military Review*, January-February 2016, 23-29.

[34] Meister, "Isolation and Propaganda," 3.

[35] Maria Snegovya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russia Report 1(Washington, DC: Institute for the Study of War, September 2015) 9, http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare (accessed December 15, 2016).

[36] Molly Mckew, *"*Putin's Real Long Game," *Politico Magazine*, January 1, 2017, http://www.politico.com/magazine/story/2017/01/putins-real-long-game-214589 (accessed January 2, 2017).

[37] Abrams, “Beyond Propaganda,” 17. See also Sherr, *Hard Diplomacy and Soft Coercion,* 47.

[38] Alina Polyakova et al., *The Kremlin's Trojan Horses* (Washington, DC: Atlantic Council, November 25, 2016), http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses (accessed December 20, 2016).

[39] “Russian Intelligence Waging Information War, Says Czech Security Service,” *The Atlantic Council,* blog entry posted September 2, 2016, http://www.atlanticcouncil.org/blogs/natosource/russian-intelligence-waging-information-war-says-czech-security-service (accessed December 20, 2016).

[40] Anni Piiparinen and Geysha Gonzalez, *“*Russia’s Old Tricks against New Targets,*” The Atlantic Council*, blog entry posted December 19, 2016, http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-s-old-tricks-against-new-targets (accessed December 22, 2016).

[41] Pomerantsev, “The Menace of Unreality,” 9.

[42] Christopher Paul and Miriam Matthews, *The Russian ‘Firehose of Falsehood’ Propaganda Model* (Santa Monica, CA: RAND, 2016).

[43] Ibid., 1.

[44] Pomerantsev, *The Menace of Unreality*, 6.

[45] Robert Seely, “Russia’s New Warfare Tools and the Link to Soviet Active Measures,” *Georgian Review,* September 2015, http://georgianreview.ge/wp-content/uploads/2015/09/bob-pdf.pdf (accessed January 20, 2017).

[46] Sherr, *Hard Diplomacy and Soft Coercion*, 18.

[47] Patrick Tucker, “The US is Losing at Influence Warfare. Here’s Why,” *Defense One*, December 5, 2016, http://www.defenseone.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/?oref=search_influence%20warfare (accessed December 6, 2016).

[48] Andrew, Monaghan, *A ‘New Cold War’? Abusing History, Misunderstanding Russia* (London: Chatham House, May 2015).

[49] *National Defense Authorization Act for Fiscal Year* 2016, Public Law 114-92, 114th Cong., Section 1097 (November 25, 2015).

[50] U.S. Army Special Operations Command, *USASOC Counter Unconventional Warfare White Paper* (Fort Bragg, NC: U.S. Army Special Operations Command, September 26, 2014); U.S. Army Special Operations Command, *SOF Support to Political Warfare* (Fort Bragg, NC: U.S. Army Special Operations Command, March 10, 2015).

[51] In 1953 President Eisenhower ordered a full review of containment strategy in an exercise called Project Solarium. The project resulted in National Security Policy 162/2 which increased the role of diplomacy, economic and political efforts. A brief summary can be found by Tyler Nottberg, *Solarium for Today* (Gettysburg, PA: Eisenhower Institute at Gettysburg

College), http://www.eisenhowerinstitute.org/about/living_history/solarium_for_today.dot (accessed March 20, 2017).

[52] *National Defense Authorization Act for Fiscal Year* 2017, Public Law 114-328, 114th Cong. Section 1287 (December 23, 2016).

[53] Ibid.

[54] Molly K. McKew, "Russia is already Winning," *Politico Magazine*, January 18, 2017, http://www.politico.com/magazine/story/2017/01/russia-is-already-winning-214648 (accessed January 18, 2017).

[55] Leon Aron quoted in Giles, *The Next Phase of Russian Information Warfare,* 6.

[56] Shultz, *Dezinformatsia*, 188.

[57] Tucker, "The US is Losing at Influence Warfare. Here's Why."