

School of Advanced Warfighting

*United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico VA 22134*

FUTURE WAR PAPER

INFORMATION WARFARE


U.S. Countermeasures on the Battlefields of the Future

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

Major Jonathan S. Joseph

AY 2018-19

Mentor: Dr. Daniel Marston

Approved: _____


Date: _____
5/25/2019

School of Advanced Warfighting

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT

School of Advanced Warfighting

I. Introduction

The 21st Century has experienced substantial development in both the digital and the information environments. The world's population, through the advancement and access to technology, can now transmit and receive thoughts, opinions, and ideas regardless of geographic location. Internet access introduced a delivery platform to communicate information globally and at previously unseen speeds. Additionally, it now allows unrestricted contact with the world's population regardless of demographic. This advancement in technology has allowed malign actors to access previously inaccessible data by targeting information available through digital profiles and on-line personas. Specifically the ability to target populations, cultivate ideas, and subsequently harvest information, factual or fictitious, has made America's military increasingly vulnerable to Russian's utilization of information as a weapon.

The Russian use of Information Warfare (IW)¹ is not a new phenomenon. The Russian State has used some variation of IW for over a hundred years, dating back to the era of the Czar. Imperial Russia used the Okharana, the state's secret police, to target, disrupt, discredit, and with some frequency silence the Bolsheviks and other revolutionary groups during the later part of the 19th century and into the early portion of the 20th century. During the Soviet era, the state actively used IW in the form of both Reflexive Control² and what is referred to as Active Measures³ to wage Political Warfare⁴ against both internal and external threats to the Soviet Union. The term reflexive control is further defined and expanded upon throughout this essay. The use of disruption, deception, subversion, and active disinformation were main staples of Soviet doctrine and more importantly is currently a major component of modern Russian strategy. If the Russian State has used IW for over a hundred years, why is the United States substantially more

School of Advanced Warfighting

vulnerable today than it was in the past? Furthermore, how and why is Russia able to influence the opinion of American citizens and additionally shape the effects that impact U.S. society as a whole? The above belief has been strongly articulated by James Clapper the former Director of National Intelligence along with other influential intelligence experts within the U.S. intelligence community.⁵

The aforementioned aspects of information transcend all environments and are equally important to recognize when applied to a military confrontation on America's current and future battlefields. The fight for information and the information space is so important that the U.S. military recently identified it as a separate domain for military operations. Though there has always been an information aspect to warfare, it has become increasingly important based on what is accessible, what can be circulated, and at what speed information can be transmitted. Of additional importance is the evolving characterization of the information domain's battlefields. IW is directly challenging the military's definition and perception of what constitutes a battlefield. Where is the U.S. military fighting for information, what defines the information objectives, how are these objectives affected through tactical actions and operational and strategic goals, and how does the military prepare for this role against a future adversary such as Russia?

Russia's use of IW reappeared on the world stage in the beginning of the 21st century with the leadership and direction of Vladimir Putin. As Russia moved to reassert its sphere of influence, the international community witnessed an uptick in the use of IW. IW played a major role against Estonia in 2007 and during the conflict with Georgia in 2008. Russia again employed it

School of Advanced Warfighting

throughout the annexation of Crimea, in March of 2014, and continues to use it in her war with Ukraine. Russian use of IW is further explored in the following Crimean case study.

The annexation of Crimea, though an offensive, unprovoked military campaign, exposed the international community to the clever use of IW. The marriage of IW and offensive maneuver, the use of “Little Green Men”, soldiers appearing to be void of national identity or allegiance, in conjunction with a cunning manipulation of information, allowed Russia to achieve its military objectives.⁶ Russian IW in the form of deception, disinformation, and denial paralyzed world leaders as they attempted to sort through what was fact from fiction in the rapidly unfolding situation on the Crimean Peninsula. This artificially manufactured environment of informational chaos prevented states from taking action against Russia and provided the time and maneuver space necessary for Russia to carry out the territorial annexation of a sovereign nation.⁷

Russia’s campaign in Crimea is a sobering case study for Information Operations (IO).⁸ Effective use of information is predicated on an understanding of the adversary’s decision-making calculus, on who or what is targeted, on what information is transmitted, and how to deliver the information. During its campaign in Crimea, Russia’s ability to control information masked her actions and left the international community dumbfounded. This was accomplished by painting the conflict as a civil war between pro-Russian factions rejecting oppressive Ukrainian governance. In reality the Russians manufactured the conflict.⁹ She used both Russian special operations forces and mercenaries to represent the pro-Russian forces to disrupt the rule of law and pave the way for Russian intervention. This low cost, high payoff form of warfare was challenging to detect and even harder to counter effect.¹⁰

School of Advanced Warfighting

An open society such as the U.S. is vulnerable to IW. In response to this vulnerability and in preparation for future conflict the U.S. military needs to have a clear understanding of its role in the information domain and how to prepare for this form of conflict in the future.

II. Russian Use of Information and Political Warfare Dating Back to the Czar

Russia's contemporary employment of IW is linked to its historic use of disinformation.

Throughout the history of imperial Russia, secret police organizations existed to inform and protect the royal family. In 1881, as a result of the assassination of Czar Alexander II the Okharana was established to protect the Czar and ultimately the imperial ruling system. The scope of the Okharana expanded with time to cover influence, disinformation, penetration, and subversion operations. The Okharana's focus became Russian political and revolutionary groups both domestically and abroad. ¹¹

By 1883 the Okharana's operations had international reach with foreign field offices established abroad and a network of informants and operatives working throughout Central and Western Europe. Additionally the Okharana established mutually beneficial relationships with the French and British national police forces. This outsourcing of assets allowed the agency to influence and infiltrate dissident populations of Russian revolutionaries residing in major European cities from Paris to Berlin. ¹² During this period, the Okharana began to modernize its use and employment of human intelligence, which led to its application of IO against threats to Imperial Russia. The Okharana also began to transition from police/detective work to international intelligence and counterintelligence operations, disinformation campaigns, and

School of Advanced Warfighting

penetration activity. This period has served as a part of the foundation for contemporary Russia's use of IW.

The Okharana mastered the art of infiltrating groups through the use of penetration, source operations, and asset development and employment. Their ability to intercept, monitor, and alter personal communication between key leadership within the numerous revolutionary groups was well developed and continually refined. A major source of information came from the Okharana's ability to intercept mail between targeted groups and individuals. Their activities became so successful that they were referred to as the, "gendarme of Europe"¹³ based on their steady, accurate, and up to date flow of actionable information. There are many reoccurring themes between the various Russia intelligence and military organizations that existed during the 19th and 20th century. The extensive human intelligence networks both inside and outside of Russia, the penetration of governments and organizations perceived as threats to the state, and the ability to continuously refine the application of IW.¹⁴ Most notably is that each continued to build upon their predecessor's established practices in IW. The Bolshevik's secret police, the Soviet NKVD and KGB¹⁵, and ultimately the FSB all adopted techniques used by the Okharana.

16

The Okharana specialized in eliciting personal information related to the opinions and activities of targeted social revolutionary groups. This ability to penetrate courier systems and intercept correspondence proved effective in the disruption of oppositional groups and was adopted by the Soviet security services for future use inside Russia as well as abroad.¹⁷ As an example, the Okharana would systematically interdict mail destined for delivery to suspected threats to the state. From the intercepted information the Okharana were able to conduct both the link analysis

School of Advanced Warfighting

necessary to understand the structure of the targeted revolutionary groups and use the information for future coercion and blackmail. Additional association dating back to the Okharana is the use of disinformation campaigns in the pursuit of national objectives.¹⁸

The Okharana organized and carried out very effective intelligence and information operations. However, it was never as brutal as its Soviet counterparts and from an historic perspective, though its operations were ground breaking, they were ultimately unsuccessful in preventing the Russian revolution and the toppling of the Romanov family from power. According to Ben B. Fischer's essay, "Okharana: The Paris Operations of the Russian Imperial Police," both Lenin and Stalin viewed the Okharana's methodologies as not brutal enough. Though impressive in their manipulation of public opinion and distortion of contemporary current events they were unable to prevent a small group of revolutionaries from violently overthrowing the government of the Czar. The Soviets would be forever influenced by the effectiveness of manufacturing and promoting false information for consumption by the masses. Russia's use of disinformation and IW is traceable to the 19th century. As we look at current and future operations much may be learned from Russia's historic past.¹⁹

III. Soviet employment of Information Warfare and Reflexive Control

The Imperial Russian understanding of IO evolved into an extensive and effective system to collect, inform, influence, and disrupt groups identified as threats to the Czar. The Soviets further refined IO and its application for subsequent use against internal and external threats to both the Soviet Union and her satellite states.

School of Advanced Warfighting

The Soviet employment of Information and Political Warfare is rich with history. However, the volume of Soviet techniques and case studies is too vast to adequately cover within this essay.

With this understanding, the Soviet use of Reflexive Control will be briefly discussed.

Reflexive control is defined as, “a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.”²⁰ The Okharana pioneered the theory in the early 20th century and it has subsequently been refined by both the Soviets and modern-day Russia. Reflexive control is a key component in the Russian application of Information Warfare. Its use is aimed at controlling or influencing an adversary’s decision-making process. Reflexive control techniques are used to target either human or computer based decision makers to influence their perception of a situation. The end result is that the targeted decision maker, whether a commander on the battlefield, a computer based sensor, or a civilian leader is influenced into unknowingly making a decision favorable to the opposition. The application of Reflexive Control Theory has been universally used by the Russians to influence positive outcomes in the furtherance of their national interests. Its use has not only transcended from the tactical to the strategic levels of war but has also been applied to shape various national and international narratives both domestically and abroad. An example of Reflexive Control is the Russian display of fake inter-continental ballistic missiles (ICBM) at military parades through out the Cold War. This form of deception was designed to mislead western powers regarding Soviet military capabilities. The goal was to persuade NATO to divert resources in the pursuit of information and research about systems that did not exist.²¹ A further Russian philosophical belief is that Reflexive Control is a more lethal and effective weapon at achieving national interests than firepower. This ties into the Russian

School of Advanced Warfighting

indirect approach to conflict and the belief that the most effective form of war is the variety that does not involve armies engaging in direct combat. Dating back to the Cold War, segments of Russian society placed great emphasis on the efficacy of Reflexive Control and its potential to outpace and out perform kinetic operations.

Russian philosophy currently promotes the belief that Reflexive Control is capable of playing a pivotal role in disrupting and ultimately defeating nation states.²² This theory dates back to the U.S. Strategic Defense Initiative (SDI) and the role it played in the collapse of the Soviet Union.²³ The SDI whether intentionally or not, influenced the Russians, who at the time were in economic turmoil, to dedicate financial resources to match the U.S. program. Russian belief is that this was a form of Reflexive Control aimed at influencing an already financially strained nation to pursue a program that would ultimately bankrupt the Russia economy and lead to the collapse of the Soviet Union.

Reflexive Control complements IW through the process of gleaning, understanding, and inserting information about the enemy, its culture, its personalities, its beliefs, its capabilities and any other factors that may influence its decision-making cycle. The reflexive aspect understands when to imitate the adversary's reaction. This understanding aids in predicting actions and reactions and how and when to inject information to elicit desired responses. The ability to apply reflexive control successfully hinges on the understanding of the culture, philosophy, economic status, and capabilities of the adversary. How and when will they react, how do they make decisions, what motivates them, what influences them. All of the above require a rigorous study of culture and a concerted effort to understand human behavior and dynamics.²⁴

School of Advanced Warfighting

The Russians have historically outpaced the U.S. through their emphasis on understanding and studying the culture and decision making process of Americans. In Diane Chotikul's "The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study," she explores the amount of effort that Soviet researchers put into understanding American culture in an effort to imitate and in turn predict American responses to Russian actions. Ms Chotikul's study explored the Soviet indirect approach and the Soviet's ability to understand and influence the American decision-making process. Her key takeaways were that the Russians emphasized avoiding the temptation to mirror image. That the true importance is understanding who your adversary really is not who you want them to be.²⁵

IV. Contemporary Russian Information Warfare

Over the past 20 years the world has witnessed Russia's increased use of IW. Targeted nations have varied from the Ukraine and Crimea to Estonia and Georgia. The use of the cyber realm and the speed and reach of accessing and penetrating information reservoirs and systems has modernized as has the ability to conduct disinformation campaigns to achieve national objectives. However, the playbook that post modern Russia is using was collectively written by the nation's Soviet and Imperial Russian forefathers. The previous example of the Okharana's mail interdiction operations has been modernized into the form of email interdiction, same concept new platform.²⁶

Russia's current leader Vladimir Putin is a product of the KGB but also of the Soviet Union of the 1970s and 80s. This time period saw a revival of Russian nationalism and Soviet

School of Advanced Warfighting

conservatism. For context, the 70s and 80s gave birth to the idea that the Second World War was the Russian “Great Patriotic War”²⁷ and that Joseph Stalin, “built a modern, industrialized Soviet superpower feared by the West.”²⁸ The 70s and 80s also saw the aggressive employment of IW in the form of Soviet Active Measures and extensive disinformation operations (dezinformatsiya). This period not only shaped the Soviet Union but also had a lasting impression on Vladimir Putin.

For the purpose of this essay Active Measures are defined as:

“Different to espionage and counter-intelligence and included written and spoken disinformation, efforts to control the media in foreign countries, the use of foreign communist parties and front organizations controlled by the Communist Party’s International department, clandestine radio stations, blackmail and political influence through collaborative elites. The means for the USSR to pursue active measures included forgeries (a well-known example was that of a US military manual and ‘secret’ diplomatic letters), rumors, insinuations and ‘altered facts’ and lies.”²⁹

The Soviets turned disinformation operations into something of an art form. Their ability to manipulate the news, alter photographic images, and promote narratives, was remarkable. It was used, in the parlance of the Soviet intelligence services, to “frame”³⁰ history, current events, or first hand accounts of observed behavior or actions. A well-documented example of this technique was the Soviet manufactures narrative that the U.S. military had created the AIDS virus and was using it on the world stage as a weapon.³¹ Whether true or untrue did not matter

School of Advanced Warfighting

as long as the information was consumed and partially or completely believed to influence a planned reaction or outcome. Many of the Soviet themes used during this time period, for example anti-western sentiment, xenophobia, anti-Semitism, and Russian nationalism have been recycled by the Putin administration, as has the approach. The only difference is that it has taken on a new moniker. Instead of referring to it as propaganda, disinformation, or active measure, it is now referred to in the west as alternative facts or fake news.³²

This modernized approach has nuanced differences that are worth examining to prepare for future offensive and defensive IO. Based on technology the Russians are able to transmit disinformation on multiple mediums and have a global reach and speed that was not available to their Soviet predecessors. They are able to saturate multiple information mediums with a volume of data that has the potential to eclipse accurate information and place doubt as to the legitimacy of targeted actions. The byproduct of this approach is latent paralysis based on the inability to distill fact from fiction or useless action based on faulty information. Either reaction is beneficial to the initiator. Russia's investment in the modernization and application of IW is based on a long history of using information as a weapon, the Russian indirect approach to conflict, and the low cost high payoff benefits.³³

Russia's view of conflict varies greatly from that of the U.S. Their use of overt denial, disinformation, and deception are foreign concept to most Americans. Additionally Russian military campaigns are complimented by parallel social, political, psychological and economic campaigns. Two final factors for consideration when analyzing current and future conflict with the Russians are worth further exploration. They are the stark cultural and ethical differences

School of Advanced Warfighting

and a divergent approach to long term planning, national strategy, and control of the nation's citizenry. The below excerpt from Diane Chotikul's 1986 study on reflexive control is used to illustrate the stark cultural and ethical differences between U.S. and Soviet society.³⁴

"The difference between Western and Soviet society is much deeper than usually assumed: this difference touches upon the fundamental structure connecting the categories of good and evil. The first system, as exemplified by the U.S., as one in which the compromise between good and evil is viewed as evil; where ethical compromise is discouraged, but compromise in human relationships is encouraged. In the second ethical system, as represented by the U.S.S.R., just the opposite holds true. There, the compromise between good and evil is viewed as good: ethical compromise is encouraged, but compromise in human relations discouraged. The Soviet Union is the most developed society in the world whose culture is based on this second ethical system."³⁵

Simply stated, we are two very different societies that view interaction and conflict through dissimilar lenses. This point is key as we look at potential future Russian conflict.

Russia's military campaigns in the Ukraine and in Crimea are extraordinary examples to study in preparation for future operations in the information domain. In an effort to use information to discredit and disrupt the 2004 Ukrainian presidential elections Russia employed a "directed chaos"³⁶ approach using Soviet era active measures to plant and cultivate disinformation depicting unfavorable candidates as fascists, anti-Russians, U.S. puppets, and neo-Nazis. This

School of Advanced Warfighting

use of directed chaos is incredibly effective as it saturates the media and the citizenry with information that requires time to validate. That time works against the target and slows and or distorts the ability to make informed decisions. Fundamental to this Russian approach is the deliberate use of denial, disinformation, and deception. This is an example of where culturally the U.S. and Russia are diametrically opposed in their approach to conflict. During the invasion of Crimea, Russian military forces surreptitiously crossed onto the peninsula, seized key infrastructure, and shut down media platforms. Russian forces were reported by the now famous description as polite “Little Green Men.” When publicly asked if they were Russian troops, Vladimir Putin responded, “There are many military uniforms. You can find them in any shop.”

³⁷ The masquerading of an overt Russian military invasion and the subsequent annexation of sovereign territory was orchestrated through a coordinated use of weaponized information in concert with a planned offensive ground operation.

Once Crimea was annexed, the 2014 invasion of the Donbas in eastern Ukraine followed. Russian information warfare promoted pro Russian, anti Ukrainian “protests” that were staged and thoroughly covered by state media. These protests, supported by Russian backing evolved into armed revolt and eventually a staged and funded pro Russian fake insurgency. As this charade continued it began to appear that Ukrainian government forces were on the verge of defeating the Russian proxy force. Russia stepped in and escalated the conflict in support of their proxy formations and the make believe Russian backed anti Ukrainian insurgency continues today.³⁸

School of Advanced Warfighting

V. Future Conflict with Russia in the Information Domain

Postmodern Russia's use of IW differs in approach from that of the Soviets. Today's Kremlin employs a targeted method to divide alliances, erode public trust in national institutions, and confuse and distract populations with the end goal being the, "intensification of geopolitical, economic and ideological competition in areas that are crucial to U.S. interests."³⁹ Russian information warfare is sophisticated, disciplined, and well funded. It is also a key component within what is referred to as Russian Hybrid Warfare. Russian Hybrid Warfare, as articulated by the Russian Chief of the General Staff of the Army General Valery Gerasimov, is a "combination of political, economic, information, technological and ecological campaigns."⁴⁰

The United States currently has an economic and military advantage over Russia. However, it is unprepared to effectively recognize and respond to Russia's targeted information operations. Additionally it lacks the adequate institutional knowledge, training, and resources to fight for and employ information as a weapon. In order to prepare for and counter this threat, the U.S. military needs to perform a paradigm shift. The U.S. military is very comfortable in the realm of direct confrontation dealing with overt threats that can be addressed with technological or tactical solutions. However, as discussed earlier in this essay it is not comfortable with indirect approaches to conflict such as working in the ambiguous environment of IO.⁴¹

Preparation for war with Russia is nothing new. America dedicated over 40 years of training to prepare for a potential military confrontation with the Soviet Union. As the U.S. military plans for future conflict in the information environment, a focus on Russian societal history is required. In her study of Soviet reflexive control, Diane Choikul assessed that during the Cold War an

School of Advanced Warfighting

American shortfall was its ethnocentric approach to the Soviet Union. In direct contrast, the Russians studied American culture, American society, and the American approach to decision making. The effort that was dedicated to understanding the American thought process tied into the Soviet's ability to effectively employ IO.⁴² Postmodern Russia continues with this practice to their benefit.⁴³ If the U.S. military is to compete with Russia in the information environment, service members need to intimately understand the decision-making calculus of the adversary. The fight in the information arena needs to center on the social, ethnic, economic, religious and political aspects of Russians.⁴⁴ This cultural understanding will greatly increase U.S. military efficacy and lethality in the information domain.

Current U.S. military capabilities to generate and counter act propaganda pale in comparison to what they were during the Cold War. Additionally non-military government organizations such as the U.S. Information Agency and the Active Measures Working Group no longer exist. To successfully initiate and counter Russian information warfare an interagency approach is required. The targeting of military commanders and troops is directly connected to targeting population centers and specific demographic groups. A linkage between civilian government agencies that focus on information operations in civilian population centers supports the capabilities of military operations. It generates a greater understanding of parallel operations and additionally enhances the military's understanding of full spectrum IW targets.

During the Cold War the U.S. military studied Soviet doctrine. Since the collapse of the Soviet Union the U.S. military has lost its focus on the Russian threat. For the future fight in the information environment the American military once again needs to study the Russian playbook.

School of Advanced Warfighting

Current Russian IW themes have a common narrative. They use “conspiratorial discourse and a strategic use of disinformation to trash the information space, break trust, increase polarization and undermine the public space for democratic debate.”⁴⁵ Interestingly, these themes are eerily similar to the themes used by the Okharana against revolutionary groups in the early 20th Century and by the NKVD and KGB as they levied active measures against threats to the Soviet Union.

As with all forms of military operations the IW of the future will involve a symbiotic relationship between the offense and the defense. It may initially require analysis more so than direct action. To effectively counter Russian IO, military units will have to have the ability to analyze why an audience was targeted and gauge the reaction. Based on the above factors an initial offensive response may not be appropriate. The counter messaging information strike must be targeted and relevant, with a clearly defined purpose if not it becomes ineffective, stray rounds on an information battlefield. Additionally, U.S. military units will have to have the ability to identify and analyze Russian disinformation and have quick fire responses. Depending on the situation the transition from defense to offense may require speed and the need to saturate an area or a targeted audience with information to drown out, discredit, or expose the identified Russian disinformation. Key to this challenge is having the ability to monitor social media, news outlets, and local and national personalities and leadership.⁴⁶

For future operations in the information environment, U.S. military units should look to emulate the capabilities of organizations similar to the Ukrainian group StopFake. StopFake originated in Ukraine after the Russian incursion and annexation of Crimea as a response to Russia’s aggressive disinformation campaign. Its strategy centers on identifying Russian “myths”⁴⁷

School of Advanced Warfighting

across the electromagnetic spectrum and rapidly exposing them as disinformation. U.S. military formations will require a similar capability dedicated to aggressively identify disinformation, conducting accurate analysis, and rapidly launching clear counter messages. This ability to monitor and target wide swaths of the information domain is still in its infant stages and relies heavily on new technology to scan the inter-web and other mediums to identify Russian activity. Time, research, analysis, training, and experience will enable these capabilities.

VI. Conclusion

Russia's use of information warfare has existed for over a hundred years. History provides the U.S. military with a deep archive of evidence and analysis that illuminates the foundational origins, philosophy, and techniques used by the various Russian and Soviet organizations in their employment of information as a weapon. As the U.S. military prepares for future conflict with Russia in the information domain, history is the greatest resource. While the delivery systems and the Russian national objectives have evolved the tactics and employment of information warfare have remained relatively constant. Following the collapse of the Soviet Union and the end of the Cold War, the U.S. military lost its focus on the Russian threat and subsequently became increasingly vulnerable to Russian information warfare. Though the resident knowledge is not where it was, the archival information is relevant and accessible. Additionally, Russian actions in Central and Eastern Europe have provided the U.S. and its allied partners with a front row seat to the latest Russian actions in the information domain. Russian ability to target populations, cultivate ideas, and subsequently harvest information has made the U.S. military increasingly vulnerable to this utilization of information as a weapon. The initiative to counter this threat will set the stage for future success against a hardened and experienced adversary such

School of Advanced Warfighting

as Russia. The U.S. military needs to increase its information warfare capabilities to address and match the Russian threat. If not, America will continue to be outpaced and out performed by the Russian disinformation machine.

Word Count: 4775

School of Advanced Warfighting

End Notes

¹ Information Operations – 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. JP 1-02, DOD Dictionary of Military and Associated Terms

² Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

³ Mitrokhin, Vasili, Andrew, Christopher. *The Mitrokhin Archive The KGB in Europe and the West*. Penguin, 2000

Active measures is a term for the actions of [political warfare](#) conducted by the [Soviet and Russian security services \(Cheka, OGPU, NKVD, KGB, FSB\)](#) to influence the course of world events, in addition to collecting intelligence and producing "politically correct" assessment of it. Active measures range "from [media manipulations](#) to special actions involving various degrees of violence. They were used both abroad and domestically. They included [disinformation](#), [propaganda](#), [counterfeiting](#) official documents, [assassinations](#), and [political repression](#), such as penetration into churches, and persecution of political dissidents.

⁴ Smith, Paul A. "On Political War ". Washington: National Defense University Press, 1989
Political warfare is the use of political means to compel an opponent to do one's will, based on hostile intent. The term political describes the calculated interaction between a government and a target audience to include another state's government, military, and/or general population. Governments use a variety of techniques to coerce certain actions, thereby gaining relative advantage over an opponent. The techniques include [propaganda](#) and [psychological operations](#) (PSYOP), which service national and military objectives respectively. Propaganda has many aspects and a hostile and coercive political purpose. Psychological operations are for strategic and tactical military objectives and may be intended for hostile military and civilian populations.

⁵ McClintock, Bruce. "Russian Information Warfare: A Reality That Needs a Response." *U.S. News & World Report*, July 21, 2017.

⁶ The belief as to why Putin annexed Crimea may be broken down into three categories. First deals with Russia's attempt to prevent the Ukrain from joining NATO and in turn evicting Russia's Black Sea Fleet from its port in Sevastopol. The second deals with Russia's aim of reasserting themselves within their former Soviet states. And the third belief is that Putin reactive impulsively to political discourse inside Ukrain where he feared the current government would reject contemporary Russian influence.

⁷ Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova and Damon Wilson. "Hiding in Plain Sight: Putin's War in Ukraine." Atlantic Council, May 2015

⁸ Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova and Damon Wilson. "Hiding in Plain Sight: Putin's War in Ukraine." Atlantic Council, May 2015

⁹ Lucas, Edward, Peter Pomeranzev. "Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe."

School of Advanced Warfighting

¹⁰ Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

¹¹ Fischer, Ben B. “Okhrana: The Paris Operations of the Russian Imperial Police.” *History Staff Center for the Study of Intelligence*, Central Intelligence Agency, 1997

¹² Ibid

¹³ Ibid

¹⁴ Ibid

¹⁵ Library of Congress.

<https://www.loc.gov/exhibits/archives/secr.html>

NKVD - From the beginning of their regime, the Bolsheviks relied on a strong secret, or political, police to buttress their rule. The first secret police, called the Cheka, was established in December 1917 as a temporary institution to be abolished once Vladimir Lenin and the Bolsheviks had consolidated their power. The original Cheka, headed by Feliks Dzerzhinskii, was empowered only to investigate “counterrevolutionary” crimes. But it soon acquired powers of summary justice and began a campaign of terror against the propertied classes and enemies of Bolshevism. Although many Bolsheviks viewed the Cheka with repugnance and spoke out against its excesses, its continued existence was seen as crucial to the survival of the new regime. Once the Civil War (1918–21) ended and the threat of domestic and foreign opposition had receded, the Cheka was disbanded. Its functions were transferred in 1922 to the State Political Directorate, or GPU, which was initially less powerful than its predecessor. Repression against the population lessened. But under party leader Joseph Stalin, the secret police again acquired vast punitive powers and in 1934 was renamed the People's Commissariat for Internal Affairs, or NKVD. No longer subject to party control or restricted by law, the NKVD became a direct instrument of Stalin for use against the party and the country during the Great Terror of the 1930s.

KGB- The KGB [Russian](#): Komitet Gosudarstvennoy Bezopasnosti [English](#): Committee for State Security, was the main [security agency](#) for the [Soviet Union](#) from 1954 until its break-up in 1991. As a direct successor of preceding agencies such as [Cheka](#), [NKGB](#), [NKVD](#) and [MGB](#), the committee was attached to the [Council of Ministers](#). It was the chief government agency of “union-republican jurisdiction”, acting as [internal security](#), [intelligence](#) and [secret police](#). Similar agencies were constituted in each of the [republics of the Soviet Union](#) aside from [Russia](#), and consisted of many ministries, state committees and state commissions.

¹⁶ Fischer, Ben B. “Okhrana: The Paris Operations of the Russian Imperial Police.” *History Staff Center for the Study of Intelligence*, Central Intelligence Agency, 1997

¹⁷ LtGen Pacepa, Ion Mihai, and Prof Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*.

¹⁸ LtGen Pacepa, Ion Mihai, and Prof Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*.

¹⁹ Fischer, Ben B. “Okhrana: The Paris Operations of the Russian Imperial Police.” *History Staff Center for the Study of Intelligence*, Central Intelligence Agency, 1997

²⁰ Thomas, Timothy L. “Russia’s Reflexive Control Theory and the Military.” *Journal of Slavic Military Studies*, 2004

School of Advanced Warfighting

²¹ Ibid

²² Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

²³ “Strategic Defense Initiative.”

Atomic Heritage Foundation, July 18, 2018

²⁴ Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

²⁵ Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

²⁶ Kuzio, Taras, Paul D’Anieri. “The Soviet Origins of Russian Hybrid Warfare.”

²⁷ Kuzio, Taras, Paul D’Anieri. “The Soviet Origins of Russian Hybrid Warfare.”

²⁸ Ibid

²⁹ Ibid

³⁰ LtGen Pacepa, Ion Mihai, and Prof Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism.*

³¹ Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

³² Ibid

³³ Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

³⁴ Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

³⁵ Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

³⁶ Kuzio, Taras, Paul D’Anieri. “The Soviet Origins of Russian Hybrid Warfare.”

³⁷ Ibid

³⁸ Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova and Damon Wilson. “Hiding in Plain Sight: Putin’s War in Ukraine.”

Atlantic Council, May 2015

³⁹ Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

⁴⁰ Ibid

⁴¹ Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

⁴² Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study. C3CM Joint Task Force

⁴³ Bergmann, Max, Carolyn Kenney. “War by Other Means: Russian Active Measures and the Weaponization of Information.” Center for American Progress, June 6, 2017

⁴⁴ Darczewska, Jolanta. “Russia’s Armed Forces on the Information War Front.”

OSW: Center for Eastern Studies

School of Advanced Warfighting

⁴⁵ Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

⁴⁶ Giles, Keir. “Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power.”

⁴⁷ Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

School of Advanced Warfighting

Bergmann, Max, Carolyn Kenney. "War by Other Means: Russian Active Measures and the Weaponization of Information."

Center for American Progress, June 6, 2017

Chotikul, Diane. *The Soviet Theory of Reflexive Control in Historical and Psycho Cultural Perspective: A Preliminary Study*. C3CM Joint Task Force

NPS55-86-013. Monterey, California: Naval Postgraduate School, July 1986

Connell, Mary Ellen and Ryan Evans. "Russia's 'Ambiguous Warfare' and Implications for the U.S. Marine Corps." CNA Analysis & Solutions, May 2015

https://www.cna.org/cna_files/pdf/dop-2015-u-010447-final.pdf

Czuperski, Maksymilian, John Herbst, Eliot Higgins, Alina Polyakova and Damon Wilson. "Hiding in Plain Sight: Putin's War in Ukraine."

Atlantic Council, May 2015

http://www.atlanticcouncil.org/images/publications/Hiding_in_Plain_Sight/HPS_English.pdf

Darczewska, Jolanta. "Russia's Armed Forces on the Information War Front."

OSW: Center for Eastern Studies

Warsaw, Poland. June 2016

Fischer, Ben B. "Okhrana: The Paris Operations of the Russian Imperial Police."

History Staff Center for the Study of Intelligence, Central Intelligence Agency, 1997

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/okhrana-the-paris-operations-of-the-russian-imperial-police/5474-1.html>

Giles, Keir. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power."

Chatham House, The Royal Institute of International Affairs. 2016.

Kronenbitter, Rita T. "The Illustrious Career of Arkadiy Harting."

Studies in Intelligence, CIA, September 22, 1992

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/okhrana-the-paris-operations-of-the-russian-imperial-police/art2.pdf>

Kronenbitter, Rita T. "Paris Okhrana 1885-1905."

Studies in Intelligence, CIA, September 22, 1992

<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/okhrana-the-paris-operations-of-the-russian-imperial-police/art1.pdf>

Kuzio, Taras, Paul D'Anieri. "The Soviet Origins of Russian Hybrid Warfare."

E-International Relations, June 17, 2018

<https://www.e-ir.info/2018/06/17/the-soviet-origins-of-russian-hybrid-warfare/>

School of Advanced Warfighting

Lucas, Edward, Peter Pomeranzev. “Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.”

Center for European Policy Analysis, August 2016

https://cepa.ecms.pl/files/?id_plik=2715

LtGen Pacepa, Ion Mihai, and Prof Ronald J. Rychlak. *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. Washington, DC: WND Books, Inc, 2013

McClintock, Bruce. “Russian Information Warfare: A Reality That Needs a Response.”

U.S. News & World Report, July 21, 2017.

<https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html>.

McKew, Molly K. “The Gerasimov Doctrine: Its Russia’s New Chaos Theory of Political Warfare. And it’s Probably Being Used on you.”

Politico, September 10, 2017.

<https://www.politico.eu/article/new-battles-cyberwarfare-russia/>

Monaghan, Andrew. “Putin’s Way of War: The ‘War’ in Russia’s ‘Hybrid Warfare.’

Army War College (2016):

http://ssi.armywarcollege.edu/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf

Thomas, Timothy L. “Russia’s Reflexive Control Theory and the Military.”

Journal of Slavic Military Studies, 2004

https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

“Strategic Defense Initiative.”

Atomic Heritage Foundation, July 18, 2018

<https://www.atomicheritage.org/history/strategic-defense-initiative-sdi>

Treisman, Daniel. “Why Putin Took Crimea: The Gambler in the Kremlin”

Foreign Affairs, May/June 2016

<https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea>