Russian Information Warfare
& Implications for Deterrence Policy

by Media Ajir, Shelby Haas, & Bethany Vailliant

with special thanks to Harrison Johnson

Abstract

The following research project explores the advancing threat of a Russian disinformation campaign against Western democracies and the United States in particular. It explores the evolution of anti-Western propaganda from the Soviet period to an overview of today's tools such as the proliferation of Russian state-funded media, hiring Western PR firms, and utilization of the global internet network, specifically social media. It will also include an in-depth examination of cyber warfare capabilities to complement Russia's various forms of disinformation tactics. We conclude by recommending several means to combat this threat, including analysis of deterrence theory and its applicability to the domains of information warfare and cyberspace. This research will conduct a single case study analysis on Russia and its offensive warfare to deliberately undermine the political stability of the United States.

Methodology

This paper asks the question, "What are Russia's strategies for information warfare and how can the United States use deterrence policy to combat it?" It was written using a thorough review of open source literature of military and original source government documents. Additionally, secondary-source information from the Russian Federation and the United States was also used. This paper includes a qualitative analysis of developments of information warfare. It is also supported by interviews with subject matter experts, who have and are currently operating in the fields of cyber security and intelligence.

Table of Contents

"U.S. intelligence analysts are in the midst of a historic transformation, twenty years in the making and with no end in sight. By the mid-1990s, the IC saw the growing interconnectedness of networking moving information, culture, technology, capital, goods, and services with unprecedented speed and efficiency around the world and across the homeland. Globalization was recognized as the defining reality of our age, providing mankind with unprecedented opportunities to do good and with unparalleled capacity to do evil."

~ John C. Gannon

Introduction

This paper will seek to establish that current use of information warfare operations by the Russian Federation simply represent a modern, internet-age version of already well-established Soviet reality-reinventing tactics. It will argue that America has failed to deter Russia's information warfare campaign, and that addressing this requires exploring different ways in which Russian and American strategists conceptualize and understand the use of IW. Secondly, it will seek to define some of the primary information warfare concepts that Russia integrates into their national security and foreign policy agendas. Thirdly, the study will demonstrate that Vladimir Putin, taking leads from his communist and tsarist predecessors, has implemented a high-level, modernized propaganda effort with four main developments:

1. Unprecedented budgets for its propaganda efforts
2. Modernized propaganda machinery employed by all modern media in the Kremlin's message
3. Sophisticated technical expertise of the Kremlin's information warfare allowed them access to a greater variety of foreign audiences
4. Utilization by the Kremlin of the relative openness of the Western media world for the Russian propaganda offensive[1]

Furthermore, Russia has developed capabilities for information warfare such as computer network operations, electronic warfare, psychological operations, and deception activities.[2] In the information age, Russian analysts have recognized that information technologies can be used in coming conflicts where there will be no clearly drawn battle lines and the fighting will take place in several dimensions and arenas. There is a new "race" moving into the sphere of technology.[3] Disinformation, propaganda, and cyber capabilities are now employed in the new Russian influence campaigns. Information age techniques include internet trolls and social media use, and

[1] Van Herpen, Marcel. *Putin's Propaganda Machine*. Lanham, ME: Rowman & Littlefield, 2016, pg. 202.

[2] Swedish Defense Research Agency. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* By Rolan Heickero. Stockholm, 2010.

[3] Ibid.

cyber-attacks.[4] We conclude this research with proposals to apply deterrence methods to future strategic moves.

Conventional Theories Applicable to Information Warfare

Theories of conventional warfare are often applied to cyber warfare. To a certain extent, these strategies do parallel cyber and information warfare strategies, but even these theories have their limits. In this section, we seek to compare the theories of two strategists to cyber approaches in which the Russian Federation controls, blocks, and guides information. Cyber Warfare both multiplies the force capabilities in conventional conflict, but also has the potential to set objectives well outside of them.

Clausewitz's theory of the Fog of War[5] suggests that cyber and technological capacities can be used as tools of uncertainty to magnify the fog of war, rather than lifting it. "Actors looking to engage in information warfare need to seriously consider creating the ability to blind/jam the information flow within a target to (1) create a fog of war which creates friction for their ability to operate and (2) to effectively break the ability of a targeted actor to act at all." In this way, Russia uses their cyber arsenal to control the flow of information to and in the Western world. The perpetrator of cyber espionage or warfare benefits from Clausewitz's "fog of war," while the victim is disoriented, scrambling to attribute blame to an enemy.

Similarly, the IW techniques used by Russian agents to disseminate propaganda and influence NGOs and PR firms, which will be explained later in this paper, reflects effective clandestine strategies. Russian agents are able to block and guide discourse on the web, blackmail, and threaten leaks of sensitive information. They understand the importance of deception, avoiding attribution, and creating a fog of war when it comes to information warfare conducted through cyber capabilities.

Nobel laureate economist Thomas Schelling described Cold War deterrence in defensive terms saying, "Successful threats are those that do not have to be carried out."[6] He mainly argued the threat of credible punishment, showing one's retaliatory abilities, deters enemy attacks. George F. Kennan also believed Soviets could be deterred. "If the adversary has sufficient force and makes clear his readiness to use it, he rarely has to do so."[7]

On the other hand, promoting an offensive approach is Robert Jervis, co-editor of the Cornell Studies in Security Affairs and expert on nuclear proliferation, explains that a spiral of mutual distrust creates an environment in which a strong defense is accomplished by achieving a

[4] McCauley, Kevin. *Russian Influence Campaigns Against the West: From the Cold War to Putin.* North Charleston, SC, 2016. Pg. 86 (Kindle Edition)

[5] Clausewitz states that ""War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth" Carl von Clausewitz, Vom Kriege, Book 1, Chapter 3.

[6] Schelling, Thomas C. "Arms and Influence." Harvard University Center for International Affairs. New Haven: Yale University Press, 1966.

[7] Rojansky, Matthew. "George Kennan Is Still the Russia Expert America Needs." Foreign Policy. Last modified December 22, 2016. http://foreignpolicy.com/2016/12/22/ why-george-kennan-is-still-americas-most-relevant-russia-expert-trump-putin-ussr/.

strong offense. In other words, "A country engaged in a war of defense might be obliged for strategic reasons to assume the offensive.”[8] This is the position Russia has taken.

Unlike conventional warfare and offensive-defensive theories, “in asymmetrical conflicts, the attackers have an advantage over the defenders; they can launch the offensive any time, and the attack may be discovered years after the threat actor completed its mission.”[9] This is the point at which we no longer apply past theories to the new domain of cyber, which achieves the goals of conventional warfare faster, easier, cheaper, and more covertly.

Russian v American Understanding of Use of Information Warfare: Soft v Hard Power

This section seeks to demonstrate that Russia and the United States are on different sides of an important conceptual dispute about the nature of information warfare. To the United States, it is a hard power tool reserved for wartime. Studies that consider the strategic effects of information war conclude that for the West, “information war is almost by definition counter command and control warfare.”[10] Subversion, deception, and the like are all ‘force multipliers’ to combat arms, not forces in their own right.[11]

On the other hand, Russia views information warfare as a soft power tool to be used in both peacetime and wartime. According to an original source document from the Russian government, “The leadership and the command staff of all levels directly participate in the organization of the activity in the information space during peacetime and in wartime.”[12] Most Americans do not understand that Russia already believes that it is in a “soft war” with the West - a war without bullets during times of “peace.” Against the United States in particular, they use disinformation, propaganda, and cyber operations.[13]These three concepts comprise the main analyses of this research and are articulated by retired Gen. Vladimir Shamanov, head of the lower house’ defense affairs committee when he stated, “We must stop offering excuses and force the West into the defensive by conducting operations to expose its lies.” [14]

The different types of international frameworks adopted by each nation for governing appropriate behavior in cyberspace serve to illustrate this point. The West, overall, has extended traditional principles of already-established international law to the new realm of cyber. In

[8] Jervis, Robert. *Cooperation under Security Dilemma*. 1978. World Politics. Vol 30. No.2

[9] *Cyber Warfare: From Attribution to Deterrence*. InfoSec Institute. October 3, 2016.

[10] Blank, Stephen. "Can information warfare be deterred?" *Defense Analysis,* August 2001, 121-38

[11] Galleoti, Mark. "Hybrid, ambiguous, and non-linear? How new is Russia’s ‘new way of war’?" *Small Wars & Insurgencies* 27, no. 2 (March 21, 2016).

[12] Russian Federation. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. NATO CCD, 2000; Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9, September 2000.

[13] Farkas, Evelyn. "Trump Needs a Russia Policy, or Putin Will Force One on Him." *Foreign Policy,* February 15, 2017.

[14] O’Connor, Tom. “Russia Forms Cyber Warfare Branch amid Military Buildup.” IBT. February 22, 2017.

general, this means that they have extended Article 2(4) of the United Nations Charter[15] and Article 51,[16] which prohibit the use of force unless acting in self-defense in response to a physical attack. These articles regulate both the laws of *Jus ad Bellum* (law to war) and *Jus in Bello* (Law of War). In other words, when it is acceptable to go to war and what is acceptable once war has been entered.

One example of how this operates is the *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[17] which was created in 2013 as a response to a series of denial of service attacks in Estonia in 2007. While not officially signed, or adopted, this is an example of the framework under which the United States operates in terms of its defining of what counts as a cyber-attack. The International Group of Experts who released this *Tallinn Manual* declared that, at a minimum, any cyber operation that causes harm to individuals or damage to objects qualifies as a use of force. Conversely, they agreed that cyber operations that **merely cause inconvenience (such as information warfare) or irritation do not qualify as use of force.**[18] This way of viewing cyber operates under the assumption that it should be conducted and punished in the same way as conventional, hard power warfare.

Diagram 1 illustrates this concept. Only the red arrow, or actions causing physical destruction, qualify as “attacks” deserving of retribution. Nuisance behavior might constitute website defacement, for example, while cybercrime is defined any crime that uses a computer that is a global problem affecting the government, corporations, and individuals. Furthermore, espionage involves cyber spying, theft of industrial technology, and state secrets. Also in this arrow is significant, non-disruptive disruption. This classification is very important for this paper, as we will argue that information warfare can reach this level of impact. The effects of disruption can be equated to those of destruction caused by traditional armed force. For example, a weeklong cyber-attack that shuts down the national grid, and thus leaves millions of people without electricity, cripples the financial market and the transport system, and prevents government communications is likely to be treated as a use of force, whether or not physical damage ensues.[19] This level is about impact and intention, not about actual physical results. Lastly, while somewhat disputed, most agree that physical destruction at least includes death, injury, destruction of critical infrastructure, or targeting the military.

[15] Article 2(4) of the UN Charter states, “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”

[16] Article 51 states, “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”

[17] Please note that the manual is not a NATO directive as commonly thought. The project's conclusions are the opinions of the authors in their private capacities, and not a statement of official policy by NATO, any of its member governments, or any other participating organization.

[18] "Tallinn Manual on the International Law Applicable to Cyber Warfare." *Council on Foreign Relations*. 28 Mar. 2013. Web.

[19] Roscini, Marco. Cyber Operations and the Use of Force in International Law (p. 62). Oxford University Press. Kindle Edition.

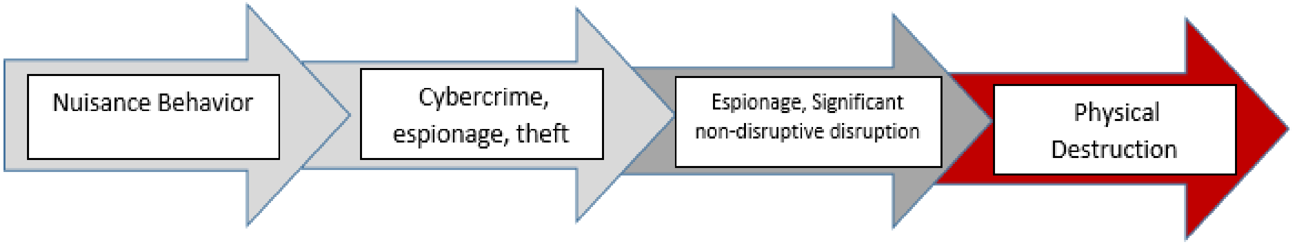

Nuisance Behavior
Cybercrime, espionage, theft
Espionage, Significant non-disruptive disruption
Physical Destruction

Diagram 1: Spectrum of potential acts in cyberspace[20]

In contrast, the six member nations[21] of the Shanghai Cooperation Organization adopted the SCO Information Treaty of 2009. This treaty is considered a means for exerting **soft power** and information geopolitics to support foreign policy and security objectives.[22] China and Russia do not have the military or economic strength to directly counter the United States, so they rely on non-confrontational methods of power to ward off U.S. normative influence. The Shanghai Cooperation Organization is one way of inserting "soft" or "normative" dimensions to counter U.S. hard power.[23]

According to Fiona Hill, Director of the Center for the United States and Europe, "Putin's and Russia's biggest problem is that, in trying to ensure its security against the United States and the entire West, its resources are far inferior in conventional military and economic terms. So, in an "asymmetric" struggle, Putin and Russia have to be innovative, catch the West off guard, and fight dirty."[24] Moscow, whether controlled by the Soviets or President Putin, has executed centralized, coordinated, sustained, and well-funded influence campaigns against the West to weaken and undermine with an indirect, low-risk strategy[25] to accomplish "strategic tasks."[26]

The United States traditionally had great difficulty in developing a sophisticated understanding of Soviet motivations and of the inner workings of the Soviet system, and this difficulty is still being experienced today. The goals, beliefs, and practices of the two countries are often diametrically opposed, but even the meaning assigned to words or concepts, which we would assume to be cognates, are often very different.[27] In fact, according to Keir Giles, the Director of Conflict Studies Research Center, and Andrew Monaghan, a Research Fellow in the Russia and Eurasia Program at Chatham House, "Many in the United States and allied policy or

[20] Spectrum of Potential Acts in Cyberspace. Credit goes to Liam Nevill and Zoe Hawkins in "Deterrence in Cyberspace: Different Domain, Different Rules."

[21] Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.

[22] Giles, Keir, and Andrew Monaghan. "Legality in Cyberspace: An Adversary View." In *Terrorism: Commentary on Security Documents*, 89-112. Vol. 140. NY.

[23] Ferguson, Chaka. *Soft Power as the New Norm: How the Chines - Russian Strategic Partnership (Soft) Balances American Hegemony in an Era of Unipolarity*. Florida International University. Accessed March 28, 2011.

[24] Hill, Fiona. "Putin: The One-man Show the West Doesn't Understand." *Bulletin of the Atomic Scientists*, 2016. Taylor & Francis.

[25] McCauley, Kevin. *Russian Influence Campaigns against the West: From the Cold War to Putin.* North Charleston, SC, 2016. Pg. 72 (Kindle Edition).

[26] Giles, Kier. *Handbook of Information Warfare*. NATO Defense College. 2016. Pg. 5.

[27] Chotikul, Diane. *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: Preliminary Study*. Technical paper no. Ocm84392904. Naval Postgraduate School. Monterey, 1986.

academic communities remain sharply unaware that there is a view that diverges sharply from the one they are accustomed to."[28] The extent to which Russian concepts and approaches to IW and cyber differ from Western ideas should not be underestimated. To effectively respond to an adversary, it is first and foremost important to understand their way of thinking. All advanced collection specialists must be able to see the world through the eyes of their adversary, the populace, and their respective cultural prisms… in order to anticipate what [they] could do. Specialists cannot abdicate their responsibility in this matter, because their mission success depends upon achieving a viable state of foreknowledge of enemy activities through anticipation.[29]

Moreover, the distinction between "cyber" and "information warfare" to the Russians is an artificial one. For example, distributed denial of service attacks (DDoS), advanced (cyber) exploitation techniques and RT television are all considered tools of IW.[30] Searches for "cyber" in Russian sources primarily return references to Western doctrine and thinking.[31] Instead of cyberspace, Russia refers to "information space," which includes both computer and human information processing.[32] The closest Russian thinking comes to separating cyber from other activities is the division of the information-technical and information-psychological domains.[33] The key concept here is "information." In the Russian conceptual framework, information in the media, on TV, or in someone's mind is all subject to the same targeting procedures as a computer. Furthermore, uploading corrupted data to a computer is no different to them from spreading disinformation through the media.[34] Consistent with the ideas of information warfare, a destructive real-world impact is not necessary to operate in the cyber domain. According to Professor V. Lisovoy, speaking at a Swedish Defense Research Agency in Stockholm in 2010, "Influencing the transfer and storage of data means that the physical destruction of your opponent's facilities is no longer required." The important thing to take away from this is that while Russia does not separate IW and cyber, ultimately cyber means are being used as a method of conducting the spread of information warfare across the globe. In order to fight the information war, the United States must engage in the fight against the misuse of cyber.

There is little doubt that Putin views himself and Russia in a continuing and fierce competition with the Western world, and in particular with the United States. Since he has taken power in Russia, Putin has largely developed a new nationalist ideology. Unlike the Cold War, Putin is no longer bound to promote Communism. Instead, he only needs to undermine American democratic principles and exploit divisions in the West.[35]

[28] Giles, Keir, and Andrew Monaghan. "Legality in Cyberspace: An Adversary View." In *Terrorism: Commentary on Security Documents*, 89-112. Vol. 140. NY.

[29] Hall, Wayne, and Gary Citrenbaum. *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments*. Santa Barbara, CA: Princeton University Press, 2012.

[30] American Foreign Policy Council. *How Russia Harnesses Cyberwarfare*. By D.J. Smith. Vol. 4. 2012. Pg.8.

[31] Giles, Kier. *Handbook of Information Warfare*. NATO Defense College. 2016. Pg. 8.

[32] Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Studies* 17 (2004): 243. Taylor & Francis.

[33] V. Kvachkov, Опецназ России, (Russia's Special Purpose Forces), op. cit.

[34] Giles, Kier. *Handbook of Information Warfare*. NATO Defense College. 2016. Pg. 10.

[35] Mak, Tim. "U.S. Preps for Infowar on Russia." *The Daily Beast*, February 6, 2017.

Russia's primary aim is to influence the political bodies of their targeted countries. For example, U.S. agencies allege that the DNC was an attack on U.S. democracy and sovereignty - principles the United States takes pride in. The content of the leaked emails suggests a calculated ploy to leverage the election so that Russia's foreign policy goals are more attainable.

With respect to perceptions of cyber-attacks and Russia, we wish to point out the measurable differences in American society as a result of Russian influence following the hacking of the Democratic National Committee. After the hack, Republicans became less concerned about cyberattacks (dropping from 78 percent to 67 percent), while Democrats became more concerned. Republicans also became less concerned about Russia's power and influence as a major threat (From 46 percent to 41 percent), as compared to now 67 percent of Democrats. Currently, 49 percent of Republicans hold favorable views of Putin, compared to only 21 percent of Democrats.[36]

In conjunction to political hacking, an NSA cyber tool set was leaked by the Shadow Brokers, which may have been leaked to share U.S. developed software and cyber capabilities or expose "digital footprints" to the world. These warnings constitute a form of deterrence, or threat of punishment. Russia's cyber capabilities in hacking personal and commercial information, disseminating, and exploiting information is a perfect example of information warfare under the subset of cyber espionage, the modern and cost-efficient form of virtually-derived HUMINT.

Information warfare that can be conducted through the cyber dimension provides Russia with the ideal set of opportunities to continue its campaign against the West. Recognition that Russia cannot compete directly in conventional terms has led to persistent emphasis in public statements and in annual budgets on finding asymmetric responses.[37] Information warfare does this in two important ways. First, IW is a significantly less costly method of conducting operations since it replaces the need for conventional military forces. According to Putin himself, "We must take into account the plans and directions of development of the armed forces of other countries… Our responses must be based on intellectual superiority; they will be asymmetric, and **less expensive.**" Second, Russia recognized that cyber operations are a critical gap in the West, leaving space for Russian to become superior. Colonel Sergey Chekinov, head of the Centre for Military Strategic Research of the Russian General State Academy, states that:

> "*Wars will be resolved by a skillful combination of military, nonmilitary, and special non-violent measures that will be put through by a variety of forms and methods and blend of political, economic, informational, technological, and environmental measures, primarily takes advantage of* **information superiority.***"*[38]

What is important to highlight is that while Western democracies are concerned with cyber deterrence against Russian entities, Russian intelligence services are increasingly worried about the potential detrimental effects on their national security arising from connection to the internet. In fact, the vast majority of Russian writing on cyber conflict is defensive in tone, and is

[36] PEW Research Center. "The World Facing Trump: Public Sees ISIS, Cyberattacks, North Korea as Top Threats." January 12, 2017.

[37] Ibid.

[38] S.G. Chekinov and S.A. and S.A. Bagdanov, "Прогнозирование характера и содержания во н будущего: проблемы и суждения" (Forecasting the nature and content of wars of the future: problems and assessments, No. 10, 205, pg. 44-45.

focused on information security and information assurance.[39] In the original source document "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space,"[40] it says that:

> *"Due to the vulnerability of the information and communication systems towards radioelectric and software effects, the information weapons that have cross-border adverse factors were created and started quickly spreading in the world, and the role of the information war has substantially grown. The Russian Federation, which is rapidly moving in the direction of the informatization of all spheres of the vital activity of the society, is currently facing a serious threat arising from the global information space."*

According to Stephen Blank and Richard Weitz of the U.S. Army War College, "We often underestimate the impact of the Russian leadership's perception that Russia is intrinsically at risk, and in some sense under attack from the West."[41] In the Russian view, the internet particularly is a method for the Western world to "attack" them, but less for inflicting crippling blows than as a way to spread unacceptable ideas, norms, practices, and behavior.[42] For example, at a UN disarmament conference in 2008, a Russian Ministry of Defense representative proposed that whenever a State promotes ideas on the internet with the intention of undermining another State's government, including in the name of democracy, this would qualify as "aggression" and interference in internal affairs.

The web has especially become a source of concern as Putin's government has been clamping down on dissent. While indirectly tied to Russia, the opinion that political change in North Africa as a result of the Arab Spring was caused by a Western IW and cyber conspiracy, which would be turned against Russia, made the Russian government suspicious of foreign meddling in Russian elections in 2011-2012.[43] This sort of fear has further increased Russia's use of censorship. The Foreign Intelligence Service of the Russian Federation (SVR) has invested in programs to monitor blog postings and social networks in order to determine where information originates and how it spreads. A senior FSB official cited the uncontrolled use of Skype, Gmail, and Hotmail as potential security threats. In 2013, Putin even gave the FSB responsibility for the "detection, prevention, and liquidation" of cyber-attacks.[44]

Differing definitions of cyber and information warfare, continuing conflict with the West, feelings of inferiority, cost-effectiveness, and issues of security have all combined to create the conditions in which Russia views IW as beneficial to advancing its position in world affairs.

[39] CCD COE. *Proc. of International Conference on Cyber Conflict, Conflict Studies Research Centre*. By Kier Giles. Oxford: CCD COE Publications. 45-60.

[40] Russian Federation. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. NATO CCD, 2000.

[41] Blank, Stephen, and Richard Weitz. *Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. U.S. Army War College. Strategic Studies Institute. 2010. Pg. 3.

[42] Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*. By Patrick Morgan. Irvene: National Academy of Sciences, 2010.

[43] 4th International Conference on Cyber Conflict. *Russia's Public Stance on Cyberspace Issues*. By Keir Giles. Oxford, UK: NATO CCD COE Publications, 2012.

[44] Lowenthal, Mark. *Intelligence: From Secrets to Policy*. 7th ed. Thousand Oaks: Sage Publications, 2017. Pg. 518.

Russian Information Warfare Concepts

Active Measures

Information warfare, according to the Russian government document *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, is defined as confrontation between two or more states in the information space for damaging the information systems, processes, and resources. These are of critical importance to undermine the political, economic, and social system, through what Russia deems "massive brainwashing" of the population to destabilize the society and the state. It also forces the state to make decisions in the interests of the confronting party.[45] However, this is nothing new; the Soviet regime also utilized information weapons to help them achieve these greater long-term goals. The first known use of the words "active measures" was in a Bolshevik document in 1919. Active measures involve influencing events and behavior in, and the actions of, foreign countries.[46] The Soviet intelligence active measures budget was reportedly $3-4 billion annually and employed well over 15 thousand personnel. Active measures were employed to influence nations around the globe, however, the United States was always considered the main enemy, and they did not differentiate between peacetime and war.[47] The Soviets had created the most threatening influence of its kind in the modern world.[48] Diagram 2 shows how disinformation plays into the grand scheme of active measures. It begins with the overall goal of achieving an advantage in political warfare. There are several ways to operationalize this objective, of which disinformation is only one. The actor then must choose between overt of covert disinformation tactics. To break it down even further, depending on which option is chosen, there is a set of options by which to accomplish these methods as well.

[45] Russian Federation. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. NATO CCD, 2000.

[46] McCauley, Kevin. *Russian Influence Campaigns against the West: From the Cold War to Putin*. North Charleston, SC, 2016. Pg. 121 (Kindle Edition).

[47] Ibid.

[48] U.S. Information Agency. *Soviet Active Measures in the "Post-Cold War" Era 1988– 1991*. 1992.

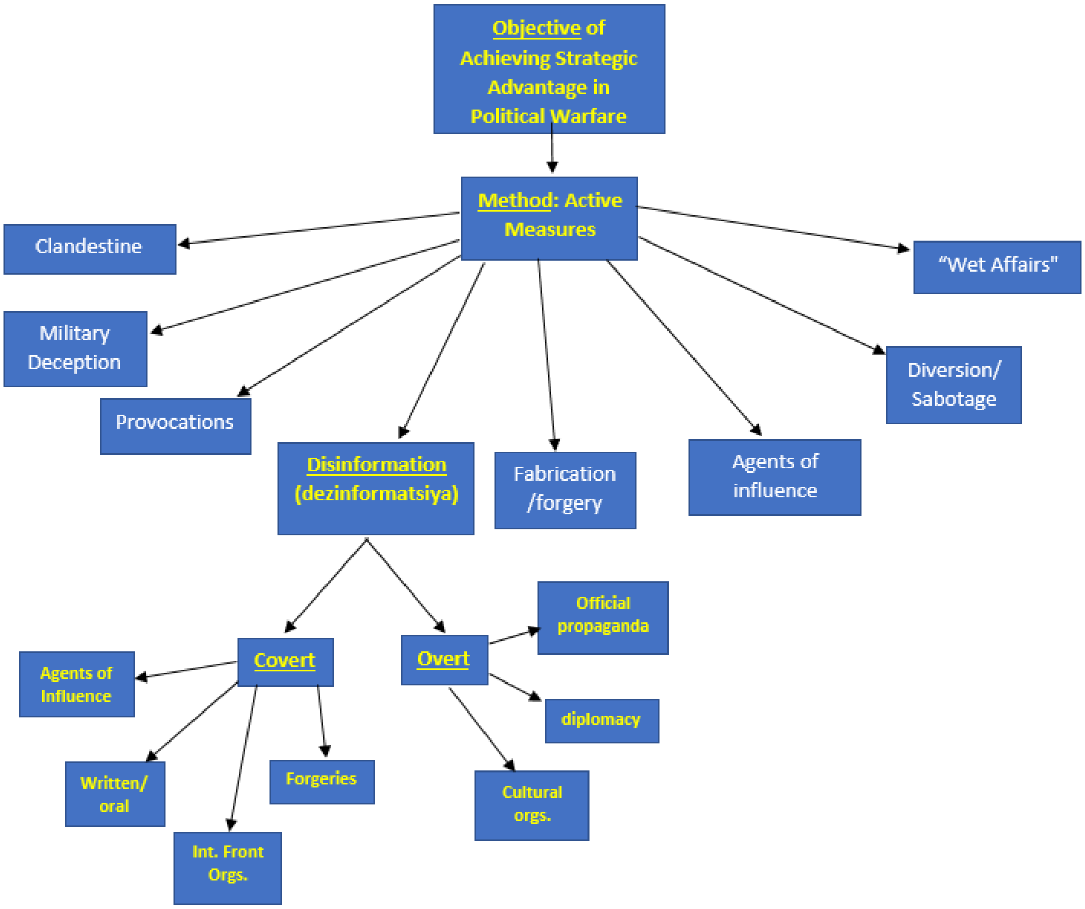


Diagram 2: Active Measures

Reflexive Control Theory

Active measures that focused on disinformation represented a carefully constructed false message secretly introduced into the opponent's communication system in order to deceive the decision maker and the public. "Reflexive control theory" is a term used to describe the practice of predetermining an adversary's decision by altering key factors in the adversary's perception of the world.[49] It takes the concept of disinformation one-step further in that the crafted information message is inserted into an adversary's decision-making process to guide the opponent into making pre-determined decisions and actions that are unfavorable to himself.[50] The central focus of reflexive control is on the less tangible enemy's inner nature, his ideas, and concepts, which is the filter through which passes all data about the external world.[51] During the Cold War, for

[49] Giles, Kier. *Handbook of Information Warfare*. NATO Defense College. 2016. Pg. 19.

[50] McCauley, Kevin. *Russian Influence Campaigns against the West: From the Cold War to Putin*. North Charleston, SC. 2016. Pg. 215 (Kindle Edition).

[51] Leonenko, Sergey. *Refleksivnoe upravlenie protivnikom [Reflexive control of the enemy]*. Vol. 8. Armeiskii sbornik (Army Collection), 1995. Pg. 28.

example, the Soviets used reflexive control to attempt to alter U.S. perceptions of its missile capabilities by parading fake ICBMs to deceive intelligence officers into believing that the missiles carried more warheads than they did.[52] Russians have upgraded these tactics into the sphere of information technologies to use in a similar fashion today.

Therefore, reflex requires the study of another's filter and the exploitation of it for one's own ends. The Soviet and Russian Armed Forces have studied the use of reflexive control theory for nearly 40 years. Over these years, many intellectual "giants" have emerged in the field of reflexive theory in the military, academic, and civilian sectors of society. They did so particularly at the tactical and operational levels, both for deception and disinformation purposes, and to control the enemy's decision-making processes.[53] It is important to note that the target for reflexive control activity is not limited to key decision-makers, but can include broader sections of the population as well, including mass and individual cognitive domains.

Russian Information Warfare Toolbox

1) Propaganda Tactics in Western Media

The Kremlin's peculiar definition of "soft power" has more to do with official state propaganda and less with the accustomed standard of results of attractive policies. While remembering the history of Russian information warfare, it is important to note that Soviet propaganda had almost no access to the Western mass media as it does today. After the collapse of the Soviet Union, Russia gained access to Western markets, also benefitting from the oil boom, leading to an increase in Russian wealth, which paved the way for buying space in the West. By 2011, "The Russian government will spend $1.4 billion on international propaganda (through media)."[54] The openness of the Western media has found itself hostage to this new tactic. The Kremlin has effectively been able to adapt its message with great freedom and flexibility to selective audiences worldwide.[55] In reality, the Kremlin has twisted one of our most fundamental and cherished values of liberal democratic societies, free speech and free press, into validation for its behavior. This section outlines the numerous ways in which Russia has weaponized this new form of soft power.

A version of this broad strategy can be found in a Russian primary military source - "The primary methods of manipulating information used by the mass media in the interests of information-psychological confrontation objectives are:

[52] Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Studies* 17 (2004): 253. Taylor & Francis.

[53] Ibid.

[54] Harding, Luke. *Mafia State: How One Reporter Became an Enemy of the Brutal New Russia*. London: Guardian Books, 2011.

[55] Van Herpen, Marcel. *Putin's Propaganda Machine*. Lanham, ME: Rowman & Littlefield, 2016, pg. 1863 (Kindle Edition).

- *Direct lies for the purpose of disinformation both of the domestic population and foreign societies;*
- *Concealing critically important information;*
- *Burying valuable information in a mass of information dross;*
- *Simplification, confirmation, and repetition (inculcation);*
- *Terminological substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events;*
- *Introducing taboos on specific forms of information or categories of news;*
- *Image recognition: known politicians or celebrities can take part in political actions to order, thus exerting influence on the worldview of their followers;*
- *Providing negative information, which is more readily accepted by the audience than positive*[56]

The real-world consequences of these objectives are identified through several forms of attack.

The first is through disseminating official Russian state propaganda abroad via foreign language news channels as well as Western media. Most notably is the creation of the very successful government-financed international TV news channel, Russia Today (RT). The content began as aiming to improve Russia's image abroad by stressing the nation's positives such as "its unique culture, its ethnic diversity, its role in World War II, and so on."[57] It was not until 2009 that the channel shifted from a defensive soft power tool to an offensive one. To do so, it began to extensively cover the negative aspects of the West, zeroing in on the United States. Examples of topics included mass unemployment, social inequality, and the banking crisis; furthermore, it became a platform for American conspiracy theorists explicitly questioning the September 11 attacks, the terrorist attack on the Boston Marathon, and Barack Obama's birth location. An Economist article titled "Russia Today Goes Mad" defines the channel's programs as "weirdly constructed propaganda" characterized by "a penchant for wild conspiracy theories."[58] Russia Today is not the only state-sponsored television channel, and its other media outlets have waded into overt attempts at political disruption in foreign governments.

The Lisa Affair is a recent example of how Russian State TV perpetuates confusion and disinformation. In the summer of 2016, a 13-year-old Russian immigrant in Eastern Germany claimed to have been raped by a group of "immigrants."[59] Channel One, an English language TV station funded and directed by the Russian Government, picked up the story before local authorities had time to verify the allegations. Only days later, after police questioning, the girl admitted that the story had been a fabrication. Russian State TV and on their social media sites then accused German police of covering up the assault. Ethnic Russians immediately took to the streets demanding "justice." Far-right political groups also capitalized on the incident for their anti-immigration rhetoric. The most baffling part was Russian Foreign Minister Sergey Lavrov appearing in a press conference also doubting the veracity of German authorities, implying a cover-up was underway. The coordination from the state television services in Germany to the

[56] Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare in Modern Conditions, *op. cit.*, p. 107.

[57] Van Herpen, Marcel. *Putin's Propaganda Machine*. Lanham, ME: Rowman & Littlefield, 2016, pg. 71.

[58] "Airwaves Wobbly- Russia Today Goes Mad." *The Economist*, July 6, 2010.

[59] "German media worries about Russian-led disinformation campaign." Deutche Welle. February 19, 2016.

Foreign Ministry of Russia, implemented a process to instigate political instability. The level of success is debatable; while protests were widespread, they generally were not large.

The second form of attack is takeover of Western newspapers. One method used is by buying space in its publications to manipulate Western readers. Once a month, an eight-page Russian supplement, "Russia Beyond the Headlines" is added to a list of established and influential Western newspapers including: the *Washington Post*, the *New York Times*, the *Daily Telegraph* (United Kingdom), *Le Figaro* (France), *Repubblica* (Italy), *El Pais* (Spain), and the *Suddeutsche Zeitung* (Germany), with arrangements in more countries currently being made. The two main maneuvers employed that beguile readers consist of: 1) subsiding cognitive dissonance by "adapting the contents and the style of the articles to fit their 'critical' Western mind."[60] These "critical" articles "would never stand a chance of being published in their mother paper, *Rossiyskaya Gazeta*; their only function is to give the Kremlin a "liberal" image."[61] And 2) applying the two-step flow of communication theory which implies that information to the public through mass media is not directly inherited but rather channeled indirectly through opinion leaders.[62]

Another method used has been to purchase papers in foreign countries, in an attempt to create popular, far right, Kremlin-friendly publications. It is important to note the lack of economic incentive in buying these loss-making papers, but rather the strategic reasons behind it. One notable example of this was the acquiring of the dying French newspaper *France-Soir* by the son of Russian oligarch Alexander Pugachev in 2009. Although it ultimately failed by 2012, it had succeeded in changing the image of the far-right nationalist, anti-EU, anti-NATO, and pro-Putin party of Marine Le Pen: The National Front. An even more chilling example is Russian oligarch, and former KGB lieutenant colonel Alexander Lebedev (who had worked undercover at the Soviet embassy in Britain), who bought two loss-making British newspapers in 2009 and 2010. It was "an astonishing moment in British press history, the first time a former member of a foreign intelligence service has owned a British title."[63] Trying to uphold and maintain a reputation as a semi dissident of the Kremlin, his critics have been able to outline several reasons to oppose this reputation. For example, his endorsement of Putin's Popular Front coalition in May 2011.

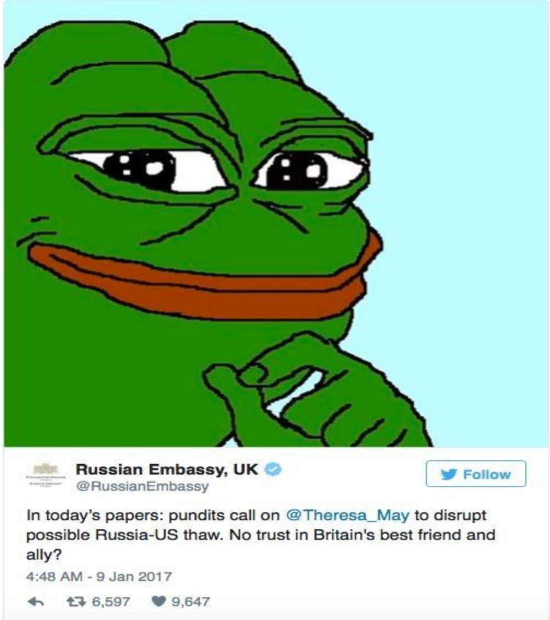
[60] This tactic illustrates what is known as "indirect strategy" - in that propaganda at home and abroad may differ. (Andre Beaufre, *Introduction a la strategie.* Paris: Librarie Armand Colin, 1965.)

[61] Van Herpen, Marcel. *Putin's Progaganda Machine: Soft power and Russian foreign policy.* Lanham, ME: Rowman & Littlefield, 2016.

[62] Theory by sociologist Paul Lazarsfeld; states that "the mass media does not find its way directly to the broader public but is rather channeled indirectly to it via opinion leaders." (Putin's Propaganda Machine, p.75).

[63] Harding, Luke. "Russian Oligarch Alexander Lebedev to Buy London Evening Standard." The Guardian. January 14, 2009.

The third is by obtaining power and projecting disinformation through social media, whether it be Twitter, Facebook, YouTube, etc. There are countless examples of this, including the recycling and spreading of a YouTube video of Russian soldiers with the title "Punitive Ukrainian National Guard Mission throwing dead bodies near Kramatorsk (Donetsk region) on 3 May 2014."[64] Social Media's new and highly accessible platform has paved way to accounts with large networks and numbers of followers. These groups are currently "engaged in establishing their credibility, and developing tactics for defeating analytical methods used to identify false personae,"[65] particularly to generate followers and interaction from genuine accounts through tailored and sophisticated features. An example of a sophisticated feature includes a marketing technique that maximizes the visibility of disinformation; "Twitter accounts can follow this pattern, with examples of accounts that were originally set up to generate revenue as click bait now repeating Russian disinformation, with profiles providing links to RT."[66]



Russian Embassy, UK
@RussianEmbassy

In today's papers: pundits call on @Theresa_May to disrupt possible Russia-US thaw. No trust in Britain's best friend and ally?

4:48 AM - 9 Jan 2017

Figure 1.

Another example involves the Twitter accounts of Russian embassies, who have taken an active role in using propaganda and unusual content in their tweets - something the typical foreign embassy account would not engage in. An example of this behavior is illustrated in this photo (left), when the Russian Embassy based in London, Tweeted during Prime Minister Theresa May's first state visit to the United States during the Trump presidency. The obvious goal here was to convince sympathetic Americans that Theresa May should not intervene in Russia-U.S. relations, seemingly with a condescending tone to undermine U.S. relations with its greatest ally, Great Britain.

Of equal importance is the concept of social media solely within Russia itself; it's equivalent to Facebook is called VKontakte, taking place as Russia's biggest social network. Known as the "King of the Internet" in Russia, Alisher Usmanov owns about 70 percent of it. This includes having stakes in Mail.ru, the search engine. Yandex, and of course, Vkontakte. Today, 88% of VKontakte's shares are in the hands of Kremlinfriendly individuals.[67] According to one of the social media's former main stakeholders,

[64] Van Herpen, Marcel. *Putin's Progaganda Machine: Soft power and Russian foreign policy.* Lanham, ME: Rowman & Littlefield, 2016.

[65] Giles, Keir. "V. Kvachkov, Спецназ России (Russia's Special Purpose Forces)." *Handbook of Information Warfare*. Rome: NATO Defense College, 2016. 19-20. Print.

[66] Ibid.; "Private correspondence with Joonas Vilenius, CIO of WG Consulting, a social media intelligence consultancy.

[67] The chronological order of buying and selling shares in Vkontakte to reflect today's owners is a long and complicated chain of events. Further information can be found in "Putin's Propaganda Machine" pg. 90-92.

> *"We [VKontakte] have already worked together for some years with the FSB and the 'K' department of the Ministry of Internal Affairs, engaged in supplying information on thousands of users on our site."*[68]

He goes on to admitting VKontakte's active role in countering opposition initiatives during the 2012 anti-government rallies in Moscow, by formulating fake profiles on opposition group's pages, with the aim of creating fake information on fake rallies. The FSB's ability to monitor VKontakte virtually unrestricted, means reaching even beyond the borders of the Russian Federation to millions of users who live in former Soviet republics. This "offers the FSB unprecedented opportunities to watch closely- and subsequently manipulate events in the neighboring republics."[69] While this sort of control has not yet come to life within the United States or its allies, the Kremlin has found other ways to use social media abroad.

Russian troll[70] campaigns and bots,[71] otherwise known as the Kremlin Troll Army, were created specifically to sow discord, interacting directly with the audience of a range of media. In order to establish subtle, permissive environments that illustrate an impression of consensus, trolls and bots may seek to divert and suppress any debate in opposition to the Russian version of events while perpetuating disinformation through false accounts. Their presence leaves mainstream media outlets unsure as to whether or not the comments pages are filled with real accounts or trolls with an agenda. To put it into perspective, "each troll is expected to post 50 news articles daily and maintain six Facebook and 10 Twitter accounts, with 50 tweets per day."[72] This form of information warfare capability is often oversimplified and underestimated, and therefore leaves the target audience to exploitation through already existing vulnerabilities. In the Russian primary source, "Bulletin of the Academy of Military Sciences." One author states:

> *"The victim country does not even suspect that it is being subjected to information- psychological influence. This leads in turn to a paradox: the aggressor achieves his military and political aims with the active support of the population of the country that is being subjected to influence."*[73]

Furthermore, reporting on these tactics have been met with retaliation campaigns filled with harassment and insults, set to destroy careers of several journalists, academics, and experts by

[68] Rukovodtso 'VKontakte': My uzhe neskolko let sotrudnichaem s FSB i otdelom "K" MVD, operativno vydavaya informatsiyu o tysyachakh polzovateley nashey seti," Novaya Gazeta (March 27, 2013). This claim was made in a letter on behalf of Pavel Durov, although he denied it after it became public. Durov later fled Russia after being dismissed as CEO of Vkontakte; he had refused to give information on Ukrainian users of the social media website over to the FSB.

[69] Van Herpen, Marcel. *Putin's Progaganda Machine*: *Soft power and Russian foreign policy* Lanham, ME: Rowman & Littlefield, 2016, pg. 93.

[70] Definition: Online personae run by humans. Original internet meaning of the word is to simply provoke argument and confusion along with sowing discord.

[71] Definition: Online personae run by automated processes.

[72] Van Herpen, Marcel. *Putin's Propaganda Machine*: *Soft power and Russian foreign policy* Lanham, ME: Rowman & Littlefield, 2016.

[73] Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare In Modern Conditions: Theory and Practice), *Vestnik Akademii Voyennykh Nauk* No.1 (46), 2014, pg.106

vilifying them and denouncing them as delusional. This has essentially deterred many other journalists on the reporting of trolls in order to avoid falling victim to reputational damage.

2) Using Western Lobbies and Civil Society

Incentivized to weaken democracy abroad and increase political influence, Russian businessmen, especially ex-Soviets, have long been attempting to generously finance campaigns of Western politicians and/or political parties. Areas of weakness in Western democracies have been identified to be taken advantage of, such as the "lack of strict regulations concerning party funding,"[74] along with secret lobbying measures. These are both particularly high-risk in relation to corruption. A most notable example of this buying of elite political opinion is the influential group "Conservative Friends of Russia." This initiative was launched in August 2012, and has engaged with countless Tory party MPs and Tory peers of the UK government. They were even invited on a ten-day trip to Moscow and St. Petersburg, where they attended a number of gala dinners and "in between, they had meetings with politicians of Putin's United Russia Party. Their trip was paid for by Rossotrudnichestvo, the Kremlin's new soft-power organization."[75]

Another tactic can be seen with the usage of NGOs and civil society groups after realizing the central role they played during the "Orange Revolution." This tactic was developed to rival ideologies supported by existing NGOs with its own "counterrevolutionary" ideology through think tanks, roundtables, conferences, etc. to export its own brand of political and economic influence.[76] A primary Russian source summarizes this idea clearly:

> "*It is preferable to have a foreign nonprofit nongovernmental organization (NGO) that could best contribute to the attainment of the goal of a hybrid operation. It can be established beyond the Russian Federation under the rules of a foreign country and can draw its members from residents of the disputed territory and its political objectives will include discrediting the current government agencies, eroding the prestige and public standing of the law enforcement agencies, particularly the armed forces, buying up mass media and conducting information operations purportedly to protect democracy, and nominating delegates for local government elections, and infiltrating them into the elected government authorities.*"[77]

Examples of umbrella organizations that covertly channel funds to Russia-friendly NGOS include the Institute of CIS Countries, as well as Russian World.

The last tactic is the hiring of Western lobbying firms to improve the Kremlin's image abroad. While this strategy is not a new one in the world of politics, it has been something new for post-Soviet Russia. The Kremlin's newfound wealth has given them the ability to reach out to the most prestigious lobbying and communication firms, firms that "possess the necessary

[74] Van Herpen, Marcel. *Putin's Propaganda Machine*: *Soft power and Russian foreign policy* Lanham, ME: Rowman & Littlefield, 2016, pg. 100.

[75] Ibid.

[76] Popescu and Wilson, "The Limits of Enlargement-Lite," pg. 29.

[77] I. N. Vorobyov and V. A. Kiselev, "Гибридные операции как новы вид военного противоборства" (Hybrid operations as a new form of armed conflict), *Voyennaya mysl'*, No. 5 2015, pp. 41-49.

know-how...because they often employ former politicians, ambassadors, and other highly placed officials, who have direct personal access to government circles."[78]

Former Secretary of State Henry Kissinger is an example of a prominent lobbyist in good favor with the Kremlin, with a mutual admiration for Putin. This is to the fact that he abstains from asking questions about democracy and human rights. This is particularly an asset to Putin's objectives. Kissinger's private lobbying firm, called Kissinger Associates, published a report in 2009 to influence the then new President Obama's foreign policy goals, specifically with Russia. The following are excerpts from the report:

> "*America's essential goal is not securing NATO's long-term future as the central element of our engagement with Europe, no matter how valuable an instrument of U.S. Policy in Europe NATO has been in the past. The United States should stop criticizing Russia on human rights and the lack of democratic standards. Issues of democratic development should be raised in a non-confrontational and non-accusatory manner" because Russia "is deeply sensitive about any appearances of interference in its domestic affairs."*[79]

This report, on balance, perfectly exemplifies the way in which Kremlin-U.S. public-private ties have given a platform for pro-Russian sentiment in the United States. The reader could easily believe the report was written by a Kremlin pundit, or by Putin himself.

Another Western lobbyist hired by the Kremlin is in accordance to a New York-based firm, Ketchum. Hired in 2006, they have consistently attempted to improve the Kremlin's image, even when it has been at historical lows, such as during the war with Georgia or the annexation of Crimea. Despite criticism from within, the firm persisted on helping make Russia more attractive to investors, which meant "helping them disguise all the issues that make it unattractive: human rights, invasions of neighboring countries, etc."[80] Ketchum also played a main role in the publication of Putin's highly political op-ed piece in the *New York Times* in September 2013.[81] One can also classify this move as a soft power play through western newspapers as discussed before.

3) Cyberspace Means of Information Warfare

Cyberspace takes the lead as the Federation's means of influence in information operations, as its development and deployment does not require extensive resources or critical infrastructure. Cyber platforms have given the Kremlin capabilities to accomplish political foreign policy goals that would not otherwise be capable of doing with just a troll army. A common development of state actors with less defense resources have been to develop domains that have low-cost high-impact (LCHI) tools. Understanding Russia's unified campaign to achieve its foreign policy influence in using cyber techniques requires an examination of those tools.

[78] Van Herpen, Marcel. *Putin's Propaganda Machine*: *Soft power and Russian foreign policy* Lanham, ME: Rowman & Littlefield, 2016, pg. 48.

[79] Thomas Graham, "Resurgent Russia and U.S. Purposes: A Century Foundation Report," Century Foundation, New York and Washington (2009).

[80] Somaiya, Ravi. "P.R. Firm for Putin's Russia Now Walking a Fine Line." *The New York Times*, August 31, 2014.

[81] Putin, Vladimir. "A Plea for Caution from Russia." *The New York Times*, September 11, 2013.

Hacking Group Strategies and Targets

Cozy Bear, an advanced persistent threat affiliated with the FSB, targeted the White House, Department of State, the U.S. Joint Chief of Staff and successfully hacked the DNC. They also recently targeted the Norwegian Labour Party, defense and foreign ministries, intelligence service (PST).[82] Another group, Fancy Bear infiltrated the German parliament (Bundestag) and French channel TV5 Monde. American intelligence suspects links between Fancy Bear and the GRU, Russia's military intelligence agency. Both hacking groups combine carefully crafted viruses and sophisticated targeting mechanisms to reach the targets and infect secretly. Both use spear phishing and malware to gain access to users' passwords and information. These groups display remarkable capabilities of exploiting zero-day vulnerabilities.[83]

These Russian-linked hackers are able to infiltrate media, as seen in the United Kingdom, where Fancy Bear penetrated an unnamed television channel, remaining "dormant" for over twelve months.[84] Hackers obtained near unrestricted access to the media outlet's network. This potentially provides Russian intelligence with the ability to target sources or journalists that disagree or present facts that embarrass Russian officials. Russia has indeed targeted journalists, including one Russian analyst at the Atlantic.[85] Whether the Kremlin wishes to inject propaganda, coerce, or gather data from individuals, these cyber capabilities hold the potential to influence multiple strata of society. These information warfare methods are cost-effective, difficult to attribute, and accessible from any location.

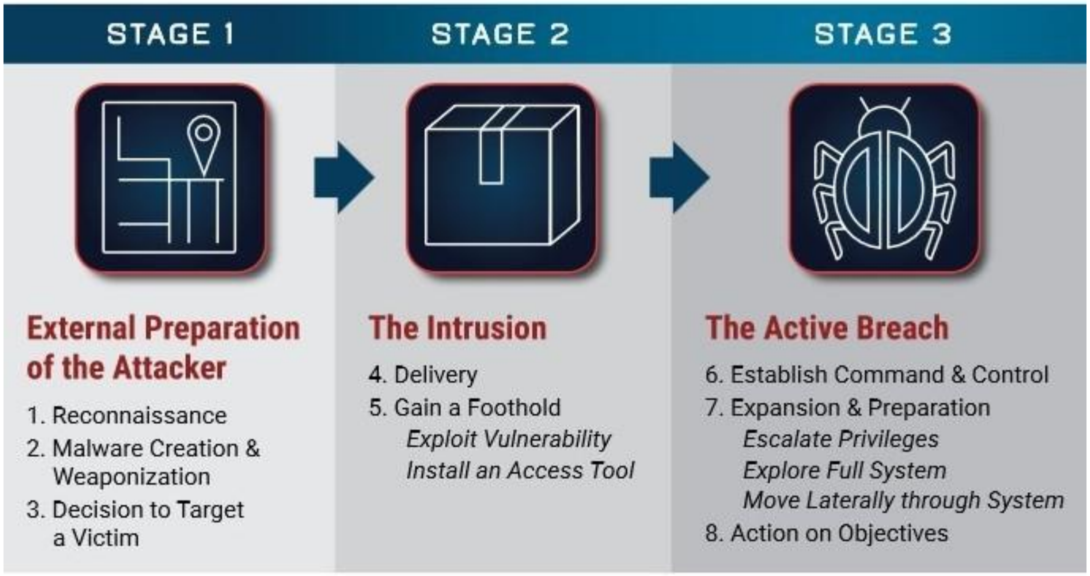


Figure 2.[86]

[82] "Norway institutions 'targeted by Russia-linked hackers'" BBC News. February 3, 2017.

[83] *Bears in the Midst: Intrusion into the Democratic National Committee*. Crowdstrike, 2016.

[84] Murdock, Jason. "Russia-linked Fancy Bear hackers had access to UK television station for 'almost a year'" International Business Times. January 26, 2017.

[85] Lippman, Daniel. "State-sponsored hackers targeting prominent journalists, Google warns" POLITICO. February 10, 2017.

[86] Ibid.

Crowdstrike, an American cybersecurity company, counts Cozy Bear as one of the most advanced hacking groups, rivaling OPSEC and technical expertise seen in nation-states. The more targeted hacking operations reflect F3EAD (Find, Fix, Finish, Exploit, Analyze, and Disseminate). For a basic model of cyber targeting equivalent of F3EAD, see Figure 2. From the Center for Cyber and Homeland Security detailing the Cyber Kill Chin Model originally developed by the DoD.

In August 2016, the NSA found its own hacking tools doxed online, tools that infiltrate firewalls and exfiltrate data. The doxing appeared to contain real NSA tools, according to former employees of the Tailored Access Operations (TAO) and emanated from a group called the Shadow Brokers who utilized file-sharing websites like BitTorrent and DropBox. They threatened to release NSA cyber weapon systems to the public if they were not paid or if the United States retaliated for the alleged hacking of DNC emails and other cyber intrusions.[87] The result was that the NSA tools were leaked. The affiliation of this group to Russia is not concrete; however, their objectives are the same as other Russian-linked groups.

Private Companies: The New Arms Dealers

Director of Central Intelligence, Michael Hayden, once commented on the availability of hacking software to commercial and private buyers:

> *"A lot of the weapons in our toolbox were harvested in the wild from the Web...But some of these exploits could be pretty ugly so they had to be modified to meet our operational and legal requirements."*[88]

The Italian company, Hacking Team, deemed the "Blackwater of surveillance,"[89] sells RCS (remote control system) spyware that is by technical definitions, undetectable. It is designed to infiltrate antispyware, antivirus programs, and firewalls. Also known as Da Vinci, it can turn on computer cameras and microphones and download emails, security credentials, Skype conversations, web-browsing activities, and various instant messenger platforms. Existing data on the hard drives is vulnerable to exploitation.[90] Because this technology is sold to intelligence agencies and governments around the world, one can deduce that similar products exist on the market to non-state actors, as well as much more advanced products via commercial backchannels. Although Hacking Team does not sell to "repressive regimes," the abuse of this type of software occurred in the 2014 targeting of Ethiopian journalists by the Ethiopian state.[91] More recently in 2014, a Russian firm linked to the FSB reportedly purchased Hacking Team's iPhone hacking software, nullifying their export license.[89]

[87] Lipton, Eric, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." *The New York Times*, December 21, 2016.

[88] Nye, Joseph. "International Security." *MIT Press Journals* 41, no. 3 (February 1, 2017): 44-71.

[89] Kushner, David. "Fear this Man." *Foreign Policy,* April 26, 2016.

[90] *Hacking Team and the Targeting of Ethiopian Journalists*. Munk School of Global Affairs. University of Toronto. February 12, 2014.

[91] Zetter, Kim. "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments." *Wired Magazine,* May 4, 2014.

In February 2017,[92] news reports announced that Fancy Bear acquired iPhone malware in light of United States Army Special Operations Command and United Kingdom MoD switching from Android to iPhone platforms for secretive communication.[93] This illustrates their highly adaptive nature of keeping up with technologies used by adversaries. It further ties Fancy Bear to the FSB, who coincidentally uses the same hacking software, even though the software is no longer being sold on the market. We assume that Fancy Bear acquired the software from the FSB, or that the FSB and GRU control both Cozy Bear and Fancy Bear.

A Russian computer programmer, Alexandr Vyarya, explained that in 2015 he was invited by Vasily Brovko - a high ranking official from Russian military contractor Rostec to Bulgaria for a demonstration of an offensive DDoS attack software; Mr. Vyarya was asked to improve the capabilities of this offensive software. The very same day, the demo targeted the Ukrainian Ministry of Defense (MoD) and the Russian news Slon.ru reported a network disruption. Mr. Vyara refused the proposition and had to flee Moscow after being surveilled.[94]

The dangerous applications of these tools threaten Western or American media, private companies, government, military, and intelligence. Like arms dealers, these private companies such as Hacking Team, have the potential to give states tools that have significant law enforcement, state security, and defense capabilities with continued expansion of R&D of state and non-state actors. The proliferation of hacking tools on the net has created an environment for the arm's race for cyber tools and weapons in this ever-changing cyber sphere.

Effects

Apart from the explicit immediate effects of the tactics explained above, the general overall implication of Russian propaganda and disinformation has led to a process of dysfunctional political upheaval in the West. These tactics are prime examples of the Russian's modern-day use of the past method of reflexive control used by the Soviets. It begins with an offensive propaganda and disinformation strategy, leading to a climate of confusion among the masses of the target state, leading them to believe these thoughts are coming from within rather than from without. This then perpetuates distrust in the target state's government officials and political system; in this case, our Western values of democracy. One might then safely assume the direct correlation between this sort of discontent for the current state of affairs and mainstream politicians at home with the rise of abnormal admiration for a non-Western political figure such as Putin and the Russian Federation.[95] Diagram 3 illustrates this chain of events that lead to such an outcome. It is important to note that the Kremlin has never been under any ideological compulsion to accomplish its purposes in a hurry. Because they do not feel that they must reach their goal at any given period, they do not have any qualms about retreating in the

[92] Fox-Brewster, Thomas. "DNC Hackers Are Using Apple Mac Spyware Code from FBI Surveillance Vendor, Claims Ex-NSA Researcher." *Forbes*, February 16, 2017.

[93] Owen, Malcom. "Insufficient Samsung security forces UK military communications project to switch to modified iPhone 7." Applesider. January 2017.

[94] Kramer, Andrew. "How Russia Recruited Elite Hackers for Its Cyberwar." *The New York Times*, December 29, 2016.

[95] It is worth noting that Putin's favorability in the U.S. at the time of this writing is 32%, according to a Gallup poll. Find more information at http://www.gallup.com/poll/204191/putin-image-rises-mostly-among-republicans.aspx

face of superior forces or due to failure. The main thing has always been that there should always be pressure, unceasing constant pressure, toward the desired goal.[96] After all, the Soviets did not consider the influence campaigns as having immediate results, but as having a cumulative long-term effect.

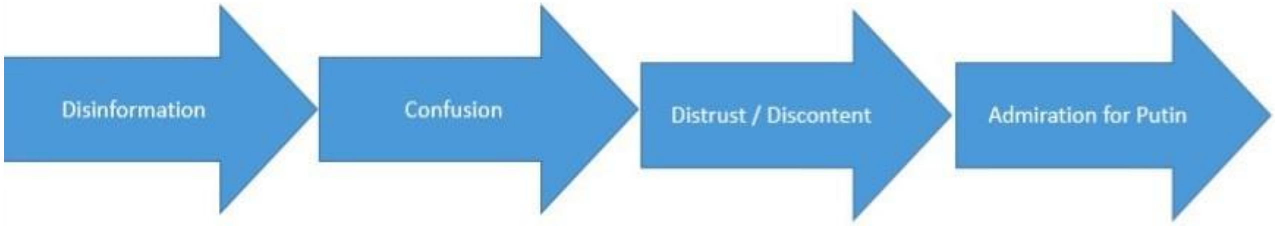


Diagram 3.

Recommendations

Technology has gotten ahead of policy in the domain of cyber warfare.[97] While information warfare most definitely falls below the threshold of causing physical damage, that does not mean the harms of these actions against a nation are not real or end in non-tangible results. We have addressed many of these harms throughout our paper. Until international law changes, these will remain unaddressed harms on the global level. However, given the unlikely prospect of legal solutions to the problems posed by cyber, there is an ever-growing body of domestic legislations to govern interstate cyber activities. It is unlikely that the United States will have the unilateral force enough to change international law. Even if it did, international law may not result in the changing behavior of states. Therefore, the next section will give recommendations on how the United States should address this new brand of information warfare, which do not meet the requirements of physical destruction, on a national level.

Deterring Disinformation

Due to basic values of Western democracies on freedom of expression, and their requisite legal foundations, limiting access to disinformation will be problematic and ultimately ineffective. We must pursue adaptation policies to deal with the spread of disinformation and implement our own counter-propaganda. Mirroring a country like Finland, which has effectively countered the propaganda attempts from their neighbor, a society more conscious and educated **can** help to combat targeted disinformation attacks.[98]

[96] Kennan, George (X). "The Sources of Soviet Conduct." *Foreign Affairs*, July 1947.

[97] Yoo, Christopher. *Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures*. University of Pennsylvania Law School. 2015.

[98] Standish, Reid. "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*. 01, March 2017. Web. 02 Mar. 2017.

A key measure recently taken by the U.S. Department of State was forming the Global Engagement Center based on the Countering Foreign Propaganda and Disinformation Act of 2016.[99] The House and Senate's key mandates include:

- *"Establish a framework for the integration of critical data and analysis on foreign propaganda and disinformation efforts into the development of national strategy."*
- *Establish a process for integrating information on foreign propaganda and disinformation efforts into national strategy, and*
- *Coordinate the sharing among government agencies of information on foreign government information warfare efforts,*
- *Develop and synchronize interagency activities to expose and counter foreign information operations directed against U.S. national security interests and advance narratives that support U.S. allies and interests.*

An important element of this strategy should be to dedicate government resources to promote an independent press in countries that are vulnerable to foreign disinformation while developing a fact-based strategic narrative. There exists a wealth of knowledge about marketing and messaging in the private sector that the GEC is also leveraging. This is not the first time the United States has taken an approach like this, but while the communications landscape has changed, we must continuously adapt to be successful. While the United States has many good messages to tell, the U.S. Government is not always the most effective messenger when it comes to countering propaganda.

Deterrence in Cyberspace

The lack of agreed behavioral standards in cyberspace poses an increasingly acute threat to stability. Norms offer a solution to this issue, offering the potential to bring 'predictability, stability, and security to the international environment.'[100] However, creating new norms in cyberspace on the international level has proven very difficult. Thus, it is our recommendation that the United States focus on a combined deterrence policy that involves both deterrence by punishment and denial to thwart enemy advances.

The Problem of Attribution: Solved, or Solutions

While nuclear armament was regulated by the International Atomic Energy Agency (IAEA) and the Treaty on the Nonproliferation of Nuclear Weapons, cyber weapons are not set to the same standard. Compared to nuclear-armed, the possibilities are seemingly endless with cyber, as no amount of GEOINT, SIGINT or even MASINT can detect and attribute a string of code. It can take weeks of investigation and once attributed to a source, may not be attributable to a national actor. Due to these time constraints, punishment becomes even more difficult. Furthermore, the immediacy of a punishment directly correlates with its effectiveness in establishing a deterrent. The longer the time lapse between the crossing of a red line and the

[99] House Bill: https://www.congress.gov/bill/114th-congress/house-bill/5181; Senate Bill: https://www.congress.gov/bill/114th-congress/senate-bill/3274

[100] Nevill, Liam, and Zoe Hawkins. *Deterrence in Cyberspace: Different Domain, different rule*s. Report. International Cyber Policy Centre, Australian Strategic Cyber Institute. 2016.

associated retribution, the less apparent the connection between the two for both the punished actor and the punisher. Thus, a defender's ability to establish deterrence by punishment in cyberspace is inhibited by the challenges of detecting serious infractions quickly enough.[101]

Russia knows attribution is a difficult and lengthy process; these complications permit Russia to continue achieving their foreign policy goals. U.S. Deputy Secretary of Defense William Lynn declares, "In cyberspace, the offense has the upper hand." He argues that defensive software will always be vulnerable to offensive capabilities. Just like propaganda tactics, Russian strategy is to gain the upper hand in this cyber domain, and achieve their best defense as a good offense.[101]

However, despite the obvious problems with attribution, even if it cannot be solved, it can be managed. FireEye, a company that operates globally with private and government actors, prevents attacks via defensive software and investigating cyber-attacks. A senior analyst specializing in cyber espionage informed our research team that they are able to attribute using a multi-layer approach to evidence (timestamping, digital forensics, target history, etc.), resulting in a confidence interval as to who the state-actor is.[102] Performing attribution well is at the core of all forms of coercion and deterrence. The bottom line is that the quality of attribution rises as the number of intelligence sources increases. Attribution is too large and too complex for any single person to handle, therefore broad skills and a wide range of tactical activities are required to address it.[103] For example, Moonlight Maze, an FBI inquiry into a cyberattack against the United States, demonstrates the importance of all-source intelligence initiative. In this situation, foreign spies targeted the U.S. Department of Defense (DoD), Department of Energy, National Aeronautics, and Space Administration (NASA), National Oceanic and Atmospheric Administration (NOAA), various defense contractors, and universities to steal information. The FBI took on this case but was overwhelmed, so the DoD began supporting them, as did the Joint Task Force Computer Network Defense. This collaboration led them to be able to attribute Moonlight Maze to Russia. A second example is when Crowdstrike, an American cyber security technology company attributed Sony cyberattacks within 48 hours. A national actor can be identified and implicated not only by increasing the number of investigating bodies, but also by also mounting evidence:

- Digital Forensics

Investigators can identify original IP addresses, malware, traces of Russian language, defining characteristics in strings of code and "specific names, MD5 hashes, timestamps, custom functions, and encryption algorithms. Their backdoors may have command and control IP addresses or domain names embedded" After forensic investigation, intelligence agencies and private cybersecurity firms attributed these APT groups to Russia based on "digital fingerprints" and common methods of entry. Crowdstrike employs Falcon, a software that acts as an airplane black box. It replays and retrospectively records the internal operations of a computer system.

[101] Farrell, Henry. "The political science of cybersecurity III – How international relations theory shapes U.S. cybersecurity doctrine." *The Washington Post*, February 20, 2014.

[102] McNamara, Luke. Interview by Shelby Haas. Telephone Interview. Omaha, NE, Date March 1, 2017.

[103] Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (December 23, 2014).

- Temporal Deduction

Analysts can determine approximate locations by the timestamp of the attack. For example, Crowdstrike identified the DNC hacks occurring during workday hours in Moscow's time zone, UTC+04:00[104]

- Level of Sophistication

Analysts can measure the level of sophistication by the methods and tools used by the adversary. For example, Crowdstrike categorized the DNC hacking by "superb" tradecraft, with "nation-state level capabilities"[105] Fancy Bear software is so extremely calibrated and risk-averse to security and detection by the host that the infiltration employs a different tool when at risk of detection.

- Targeting History

The targets of these hacking groups suggest the Russian Federation in its geopolitical goals: they focused mainly on political and foreign entities. The security firm Volexity found the targets of Cozy Bear included American NGOs and policy think tanks such as "RAND Corporation, Radio Free Europe/Radio Liberty, the Atlantic Council, and the State Department."[106] Fancy Bear targets include the Georgian Ministry of Internal Affairs and Ministry of Defense, Ukrainian artillery (D-30 Howitzers hacked by Android malware[107]), and according to an official list as quoted from ESET[108]:

- *Ministries of Defense in Turkey and Ukraine*
- *Political leaders and heads of police of Ukraine*
- *Members of NATO institutions*
- *Members of the People's Freedom Party, a Russian liberal democratic political party [15]*
- *Russian political dissidents*
- *Shaltay Boltai", an anonymous Russian group known to release private emails of Russian politicians [16]*
- *Journalists located in Eastern Europe*
- *Academics visiting Russian universities*
- *Chechen organizations*

[104] Go to http://www2.fireeye.com/rs/fireeye/images/rpt-apt28.pdf for more information.

[105] *Bears in the Midst: Intrusion into the Democratic National Committee*. Crowdstrike, 2016.

[106] Paganini, Pierluigi. "Cozy Bear launched new spear-phishing attacks against US policy think-tanks aiming to infect their systems with a malware." Security Affairs. November 12, 2016.

[107] Meyers, Adam. "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units." Crowdstrike. December 22, 2016.

[108] *Approaching the Target*. Report. En Route with Sednit. Vol. 1. 2016. 1-40.

Deterrence by Denial

Denial is the best line of defense **when attribution is not possible**. It is a way of denying the enemy of any benefits it may receive by building a higher wall and increasing the time and effort to scale that wall. The Trump administration has yet to speak on the continuation of these initiatives; therefore, we urge the necessity and value of such development in the cybersecurity sector. We recommend four pathways to support this method:

1. **Strengthening government/private relationships to promote cyber threat information sharing.**

Most private network providers today consider it their responsibility to defend their own networks. The role of the government, then, should be to incentivize collective action through some combination of incentives or regulation. Both U.S. policymakers and business leaders see the need to bridge the gap between the independent cybersecurity demands of commercial enterprise and the collective security imperatives of a nation protecting its vital infrastructure. Therefore, the government and industry should develop best practices collaboratively rather than top-down prescriptions from federal regulators.[109]

In February 2015, the White House formed the Cyber Threat Intelligence Integration Center (CTIIC) as a part of the ODNI. Former President Obama requested the private sector to share cyber threat information at the White House Summit on Cybersecurity and Consumer Protection. His administration aimed to form Information Sharing and Analysis Centers (ISACs), to be “authorized by the Department of Homeland Security to share classified information across business sectors that could help thwart cyberattacks.”[110]

Furthermore, the idea of information sharing should be extended to our Intelligence agencies nationwide, in order to maintain high quality results and be able to conduct accurate attribution. A senior analyst at FireEye who spoke to us on cyber means of information warfare, said that with such an evolving field, government-private information sharing and military-academic and synergies are increasingly of importance as the risks and complexities in cyber skyrocket.[111]

2. **Sharing cyber threats and training the next generation in academic capacities ensures our spot as a strong competitor.**

The Centers on Academic Excellence, joint sponsored by the DHS and NSA is an academic-government partnership to recruit and train students in order to fill the growing number of cyber-security positions with graduates from programs of high cybersecurity academic standards.[112] Aside from this, The FBI Cyber Division’s Cyber Initiative and Resource

[109] Masters, Jonathan. "Confronting the Cyber Threat." Council on Foreign Relations. May 23, 2011.

[110] White House Cyber Deterrence Policy. December 2015.

[111] McNamara, Luke. Interview by Shelby Haas. Telephone Interview. Omaha, NE, Date March 1, 2017.

[112] For more information visit https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae [113] FBI. *Cyber Crime*.

Fusion Unit (CIRFU) works with the National Cyber-Forensics & Training Alliance (NCFTA), which draws its intelligence from the hundreds of private sector NCFTA members, as well as Carnegie Mellon University's Computer Emergency Response Team (CERT).[113]

3. National legislation needs to be updated to accurately reflect the pace of military technological advancement.

The rapid evolvement of cyber warfare is leaving a gap between the military's capabilities and legal controls over digital combat. General Keith B. Alexander of USCYBERCOM "has warned Congress that policy directives and legal controls over digital combat are outdated and have failed to keep pace with the military's technical capabilities."[113]

4. Investing in security software innovation

First, human error remains the common denominator of most successful hacking operations. Since this issue remains after various spearfishing-training programs, our next best line of defense relies on our development of advanced technological capabilities. Strong and adaptive defenses, resilient networks, and the use of other advanced techniques and technology can reduce the perceived value of attempted malicious behavior from the adversary. Security technologies that prevent or detect network entry and protect critical data include network monitors that shoot down intruders like THAAD systems or honeypots, which lure intruders to their demise. More of these active defense measures are included in Figure 3.[114]

As a baseline, we need passive defenses, such as firewalls, but we also need a range of these active defense measures to both deter an adversary by denial and protect our systems. Based on Figure 3, deterrence by denial will keep us in The Gray Zone, while moving into offensive cyber capabilities sets up deterrence by punishment.

[113] Reich, Pauline, Stuart Weinstein, Charles Wild, and Allan Cabanlong. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity." *European Journal of Law and Technology* 1, no. 2 (2010).

[114] *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: Center for Cyber and Homeland Security, 2016.

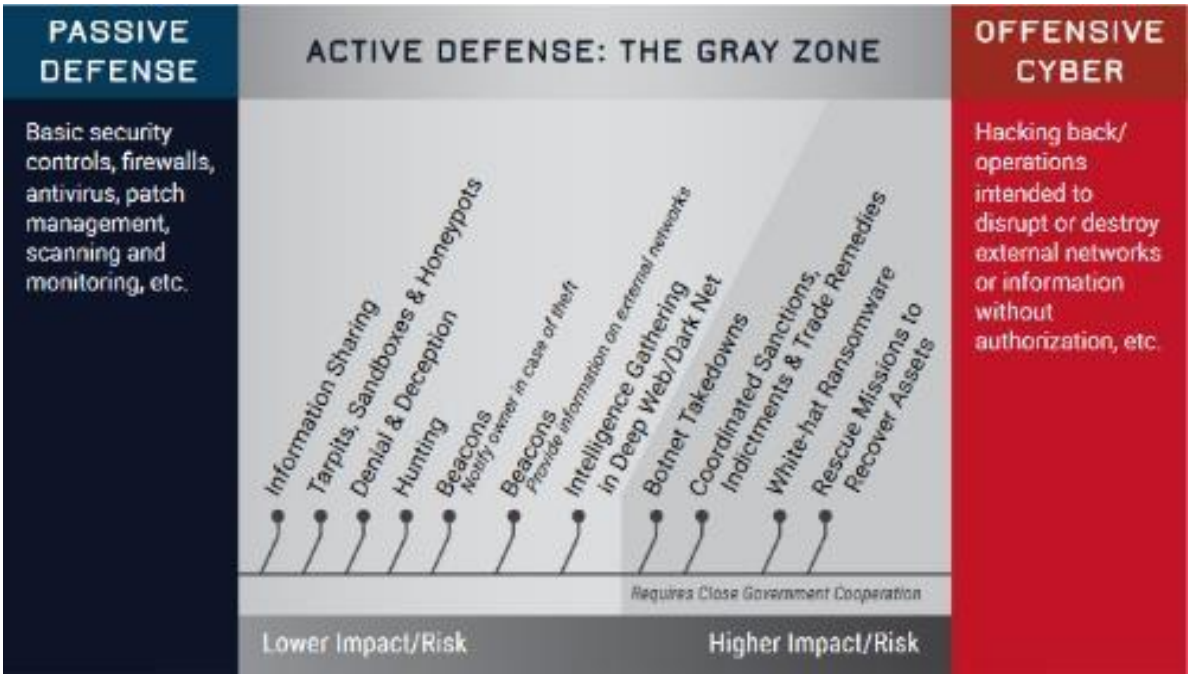

PASSIVE DEFENSE
ACTIVE DEFENSE: THE GRAY ZONE
OFFENSIVE CYBER
Basic security controls, firewalls, antivirus, patch management, scanning and monitoring, etc.
Information Sharing
Tarpits, Sandboxes & Honeypots
Denial & Deception
Hunting
Beacons Notify owner in case of theft
Beacons Provide information on external networks
Intelligence Gathering in Deep Web/Dark Net
Botnet Takedowns
Coordinated Sanctions, Indictments & Trade Remedies
White-hat Ransomware
Rescue Missions to Recover Assets
Requires Close Government Cooperation
Lower Impact/Risk
Higher Impact/Risk
Hacking back/ operations intended to disrupt or destroy external networks or information without authorization, etc.

Figure 3.

Deterrence by Punishment

Deterrence by punishment is the idea that nations will not commit offenses because they are worried about being caught,[115] and the subsequent punishment. It is the most difficult to achieve reliably due to correctly attributing the act to a particular actor. However, as described above, attribution is possible. To successfully deter an adversary, both attribution and punishment are necessary components, one does not exist without the other, and generally, the threat of punishment has to be credible to serve as a deterrent.

A deterrence strategy requires both hard limits or “red lines” and softer policies, which allow for maneuverability. In a world where there is an overwhelming amount of information and cyber activities happening daily, with limited resources available, prioritization based on the incurred damage, or potential damage, is necessary. A lack of perceived damage can short-circuit the attribution process before it even starts.[116] The analysis of damage should go beyond a single event and determine if a particular nation is causing great enough harm through a culmination of smaller acts. This is the case with Russia - they are consistent in their use of information warfare through the use of cyber means against the United States. While each incident may not seem worthy of a reaction in and of itself, the end result of their campaign is much greater than the sum of its parts, and therefore would be worth incurring costs to counter it. Russian’s long-term behavior indicates a strategy of pushing its adversaries bit by bit, not ever quite enough to warrant a response. If the cyber-attack was a standalone one that instantaneously produced its damaging effects, a reaction in self-defense would probably not be necessary. If, on the other

[115] Office of Justice Programs. National Institute of Justice. *Five Things about Deterrence*.

[116] Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (December 23, 2014).

hand, the cyber-attack is continuing or is formed by a series of smaller-scale cyber-attacks, the likelihood that clear and convincing evidence can be collected would considerably increase (in order to justify retaliatory action).[117] In some cases, however, such as the DNC hack of the U.S. election, a single event can in fact reach the level of significant non-destructive disruption (discussed above), as the impact on the United States political system (which could be considered a critical infrastructure) is tremendous.

Lawmakers and administration officials should begin drafting policies that clearly define and establish available responses. This method of deterrence can be utilized to take a hard, domestic stance against a culmination of lower-level cybercrimes and espionage, to include information warfare. Articulating a clear distinction between acceptable and unacceptable behavior is essential to define the boundaries of deterrence policy and to establish clear-cut norms.[118] Proportionality has been identified as an important principle for cyberspace interactions; however, without agreement on what constitutes an appropriate response to cyber acts of differing severity or even how to distinguish between them, international cyber norms remain fluid and unpredictable.[119]

The softer policies should be made to surround cyber intelligence gathering, cyberattacks on non-critical networks or infrastructure, and disinformation efforts. Disinformation efforts, depending on the severity, should be met with contradiction and dismissal on the lowest level possible. To avoid the equivalence problem by presenting disinformation as though it were a political debate and worthy of academic merit, efforts should focus broadly on vetting and discrediting narratives designed to cause political instability. In some instances, such as the Lisa Affair, diplomatic repercussions may be effective and necessary to apply cost to the Kremlin's actions.

However, efforts to disrupt and disable critical infrastructure, in addition to computer networks should be met with serious diplomatic repercussions and the possibility of reciprocal actions. Additionally, pervasive disinformation that exploits an ongoing crisis, or instigates political instability that may result in serious damage, may amount to information warfare and require a severe response. For instance, if state-sponsored, or affiliated news programs release false and misleading information during a natural or civil disaster that results in damages or real risks to Americans, the United States should consider a "red line" that requires a strong unmistakable response. Depending on the severity, diplomatic, and economic sanctions are appropriate, and even military options should be explored. Diagram 4 demonstrates what a hypothetical proportional response framework might look like.

[117] Roscini, Marco. Cyber Operations and the Use of Force in International Law (p. 102). Oxford University Press. Kindle Edition.

[118] Nevill, Liam, and Zoe Hawkins. *Deterrence in cyberspace: Different domain, different rules*. Report. International Cyber Policy Centre, Australian Strategic Cyber Institute. 2016.

[119] Michael Schmidt (ed.), *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2009, p. 61.

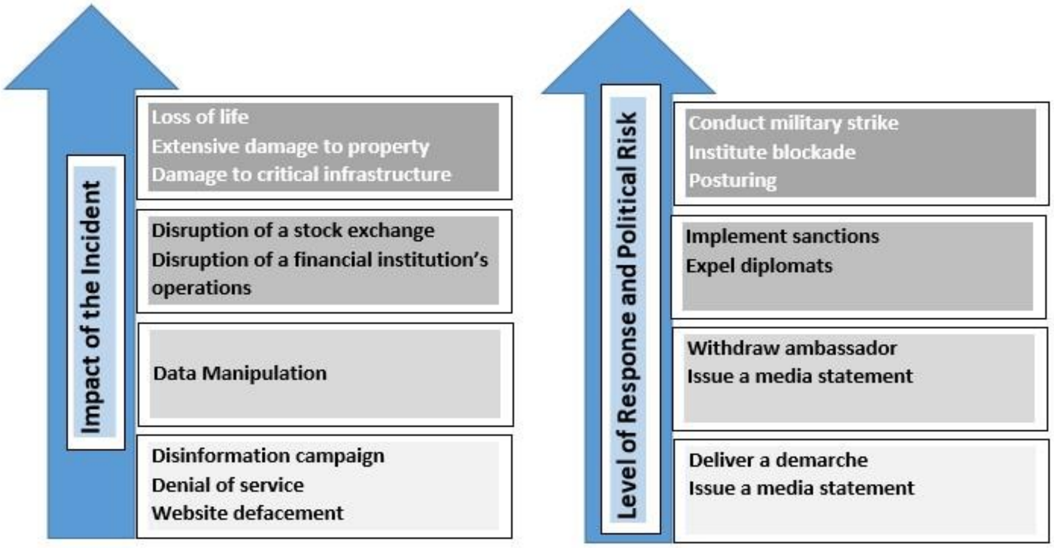


Diagram 4: Hypothetical Proportional Response Framework[120]

Conclusion

Russia utilizes a variety of disinformation and cyber enabled tools to facilitate their operations. They use their media outreach to inspire nationalist Russian sentiment and identify loyalists and supporters. Their cyber capabilities give them unequal access to sensitive government, commercial, and political information. Their financial and ideological support of domestic nationalist parties give them pervasive vector for exporting Russia's worldview. Finally, their vast use of traditional intelligence operations has given them an asymmetric advantage in the availability of political/military tools. Russia uses these capabilities to achieve different objectives in each target country.

The United States needs to levy the greater resources available to combat the cyber-enabled disinformation efforts by hostile actors like the Russian Federation. We need to bring to the greatest extent possible, private resources that are already cyber defense oriented. We must actively develop our academic resources to ready the next generation to secure our networks. This requires government resources to be aligned to specifically address threats by creating interagency task forces and providing continued support. Legislation needs to be crafted by policy makers that realize the modern cyber battlefield.

The U.S. deterrence strategy should be clear when an adversary takes actions that harm U.S. national interests. They should combine policies that both allow for wide ranges of reactions, but also strict limits that engender harsh responses. Information warfare that causes actual political instability should be treated in the deterrence formula and all applicable actions, to include military. Lastly, international and national policy should be changed to reflect the new deterrence theaters, which will also communicate expectations. It is time to accept the hard realities of soft power.

[120] Policy responses to escalating state-sponsored cyber incidents. Credit goes to Liam Nevill and Zoe Hawkins in "Deterrence in Cyberspace: Different Domain, Different Rules."

Bibliography

4th International Conference on Cyber Conflict. *Russia's Public Stance on Cyberspace Issues*. By Keir Giles. Oxford, UK: NATO CCD COE Publications, 2012.

"Airwaves Wobbly- Russia Today Goes Mad." *The Economist*, July 6, 2010.

American Foreign Policy Council. *How Russia Harnesses Cyberwarfare*. By D.J. Smith. Vol. 4. 2012.

Approaching the Target. Report. En Route with Sednit. Vol. 1. 2016.

Bears in the Midst: Intrusion into the Democratic National Committee. Crowdstrike, 2016.

Blank, Stephen. "Can information warfare be deterred?" *Defense Analysis*, August 2001.

Blank, Stephen, and Richard Weitz. *Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. U.S. Army War College. Strategic Studies Institute. 2010.

Carl von Clausewitz,_Vom Kriege, Book 1, Chapter 3.

CCD COE. *Proc. of International Conference on Cyber Conflict, Conflict Studies Research Centre*. By Kier Giles. Oxford: CCD COE Publications.

Chotikul, Diane. *The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: Preliminary Study*. Technical paper no. Ocm84392904. Naval Postgraduate School. Monterey, 1986.

Cyber Warfare: From Attribution to Deterrence. InfoSec Institute. October 3, 2016.

Farkas, Evelyn. "Trump Needs a Russia Policy, or Putin Will Force One on Him." *Foreign Policy*, February 15, 2017.

Farrell, Henry. "The political science of cybersecurity III – How international relations theory shapes U.S. cybersecurity doctrine." *The Washington Post*, February 20, 2014.

Ferguson, Chaka. *Soft Power as the New Norm: How the Chines - Russian Strategic Partnership (Soft) Balances American Hegemony in an Era of Unipolarity*. Florida International University. Accessed March 28, 2011.

Fox-Brewster, Thomas. "DNC Hackers Are Using Apple Mac Spyware Code from FBI Surveillance Vendor, Claims Ex-NSA Researcher." *Forbes*, February 16, 2017.

Galleoti, Mark. "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?" *Small Wars & Insurgencies* 27, no. 2 (March 21, 2016).

"German media worries about Russian-led disinformation campaign." Deutche Welle. February 19, 2016.

Giles, Kier. *Handbook of Information Warfare*. NATO Defense College. 2016.

Giles, Keir, and Andrew Monaghan. "Legality in Cyberspace: An Adversary View." In *Terrorism: Commentary on Security Documents*, Vol. 140. NY.

Giles, Keir. "V. Kvachkov, Спецназ России (Russia's Special Purpose Forces)." *Handbook of Information Warfare*. Rome: NATO Defense College, 2016. Print.

Hacking Team and the Targeting of Ethiopian Journalists. Munk School of Global Affairs. University of Toronto. February 12, 2014.

Hall, Wayne, and Gary Citrenbaum. *Intelligence Collection: How to Plan and*

Execute Intelligence Collection in Complex Environments. Santa Barbara, CA: Princeton University Press, 2012.

Harding, Luke. *Mafia State: How One Reporter Became an Enemy of the Brutal New Russia*. London: Guardian Books, 2011.

Harding, Luke. "Russian Oligarch Alexander Lebedev to Buy London Evening Standard." The Guardian. January 14, 2009.

Hill, Fiona. "Putin: The One-man Show the West Doesn't Understand." *Bulletin of the Atomic Scientists*, 2016. Taylor & Francis.

I. N. Vorobyov and V. A. Kiselev, "Гибридные операции как новы вид военного противоборства" (Hybrid operations as a new form of armed conflict), *Voyennaya mysl'*, No. 5 2015.

Into the Gray Zone the Private Sector and Active Defense Against Cyber Threats. Report. Center for Cyber & Homeland Security, The George Washington University.

Jervis, Robert. *Cooperation under Security Dilemma*. 1978. World Politics. Vol 30. No. 2

Kennan, George (X). "The Sources of Soviet Conduct." *Foreign Affairs*, July 1947.

Kramer, Andrew. "How Russia Recruited Elite Hackers for Its Cyberwar." *The New York Times*, December 29, 2016.

Leonenko, Sergey. *Refleksivnoe upravlenie protivnikom [Reflexive control of the enemy]*. Vol. 8. Armeiskii sbornik (Army Collection), 1995.

Lipton, Eric, and Scott Shane. "The Perfect Weapon: How Russian Cyber Power Invaded the

U.S." *The New York Times*, December 21, 2016.

Lowenthal, Mark. *Intelligence: From Secrets to Policy*. 7th ed. Thousand Oaks: Sage Publications, 2017.

Mak, Tim. "U.S. Preps for Infowar on Russia." *The Daily Beast*, February 6, 2017.

Masters, Jonathan. "Confronting the Cyber Threat." Council on Foreign Relations. May 23, 2011.

McCauley, Kevin. *Russian Influence Campaigns Against the West: From the Cold War to Putin.* North Charleston, SC, 2016. (Kindle Edition)

McNamara, Luke. Interview by Shelby Haas. Telephone Interview. Omaha, NE, Date March 1, 2017.

Meyers, Adam. "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units." Crowdstrike. December 22, 2016.

Murdock, Jason. "Russia-linked Fancy Bear hackers had access to UK television station for 'almost A year'" International Business Times. January 26, 2017.

Nevill, Liam, and Zoe Hawkins. *Deterrence in Cyberspace: Different Domain, different rule*s. Report. International Cyber Policy Centre, Australian Strategic Cyber Institute. 2016.

"Norway institutions 'targeted by Russia-linked hackers'" BBC News. February 3, 2017.

Nye, Joseph. "International Security." *MIT Press Journals* 41, no. 3 (February 1, 2017).

O'Connor, Tom. "Russia Forms Cyber Warfare Branch amid Military Buildup." IBT. February 22, 2017.

Office of Justice Programs. National Institute of Justice. *Five Things about Deterrence*.

Owen, Malcom. “Insufficient Samsung security forces UK military communications project to switch to modified iPhone 7.” Applesider. January 2017.

Paganini, Pierluigi. "Cozy Bear launched new spear-phishing attacks against US policy think-tanks aiming to infect their systems with a malware." Security Affairs. November 12, 2016.

Patrick Morgan. Irvene: National Academy of Sciences, 2010.

PEW Research Center. “The World Facing Trump: Public Sees ISIS, Cyberattacks, North Korea as Top Threats.” January 12, 2017.

Popescu and Wilson, “The Limits of Enlargement-Lite.”

Putin, Vladimir. "A Plea for Caution from Russia." *The New York Times*, September 11, 2013.

Reich, Pauline, Stuart Weinstein, Charles Wild, and Allan Cabanlong. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity." *European Journal of Law and Technology* 1, no. 2 (2010).

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (December 23, 2014).

Rojansky, Matthew. "George Kennan Is Still the Russia Expert America Needs." Foreign Policy. Last modified December 22, 2016.

Roscini, Marco. Cyber Operations and the Use of Force in International Law. Oxford University Press. Kindle Edition.

Rukovodtso ‘VKontakte’: My uzhe neskolko let sotrudnichaem s FSB i otdelom “K” MVD, operativno vydavaya informatsiyu o tysyachakh polzovateley nashey seti,” Novaya Gazeta (March 27, 2013).

Russian Federation. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. NATO CCD, 2000; Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9, September 2000.

S.G. Chekinov and S.A. and S.A. Bagdanov, “Прогнозирование характера и содержания во н будущего: проблемы и суждения” (Forecasting the nature and content of wars of the future: problems and assessments, No. 10, 205.

Schmidt, Michael. (ed.), *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2009.

Sechser, Todd D, *A Bargaining Theory of Coercion*. University of Virginia. http://faculty.virginia.edu/tsechser/Sechser-Bargaining-Theory-of-Coercion.pdf

Somaiya, Ravi. "P.R. Firm for Putin’s Russia Now Walking a Fine Line." *The New York Times*, August 31, 2014.

Spectrum of Potential Acts in Cyberspace. Credit goes to Liam Nevill and Zoe Hawkins in “Deterrence in Cyberspace: Different Domain, Different Rules.”

Standish, Reid. "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*. 01, March 2017. Web. 02 Mar. 2017.

Swedish Defense Research Agency. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* By Rolan Heickero. Stockholm, 2010.

"Tallinn Manual on the International Law Applicable to Cyber Warfare." *Council on Foreign Relations.*, 28 Mar. 2013. Web.

Thomas, Graham. "Resurgent Russia and U.S. Purposes: A Century Foundation Report," Century Foundation, New York and Washington (2009).

Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Studies* 17 (2004). Taylor & Francis.

U.S. Information Agency. *Soviet Active Measures in the "Post-Cold War" Era 1988– 1991*. 1992.

Van Herpen, Marcel. *Putin's Propaganda Machine*. Lanham, ME: Rowman & Littlefield, 2016.

V. Kvachkov, Опецназ России, (Russia's Special Purpose Forces), op. cit.

White House Cyber Deterrence Policy. December 2015.

Yoo, Christopher. *Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures*. University of Pennsylvania Law School. 2015.

Yu. Kuleshov et al., "Информационно-психологическое противоборство в современных условиях: теория и практика" (Information-Psychological Warfare in Modern Conditions, *op. cit.*

Zetter, Kim. "American Gets Targeted by Digital Spy Tool Sold to Foreign Governments." *Wired Magazine*, May 4, 2014.