STRATEGIC STUDIES QUARTERLY

Russian Information Warfare: Implications for Deterrence Theory

Media Ajir and Bethany Vailliant

Abstract

The advanced threat of Russian disinformation campaigns against Western democracies and the United States in particular begs the questions: What are Russia's strategies for information warfare, and how can the United States combat them? This article explores the evolution of anti-Western propaganda coming from Russia in three ways: state-funded global social media networks, controlling Western media outlets, and direct lobbying of Western society. Recommendations to combat these threats include analysis of deterrence theory and its applicability to the domain of information warfare.[1]

✵✵✵✵✵

Having struggled to establish its place in the world, Russia has increasingly moved away from its short stint with democracy and toward its past authoritarianism. Formerly bound to promote Communist ideology, Russia is now a nation characterized by statism. Vladimir Putin and his cronies have largely defined this path. Since taking power in 2000, Putin has developed a strong nationalistic narrative, especially since his third term as president. This narrative incorporates traditional values at the individual level and a focus on returning the glory of the Soviet Union on the national level. To restore Russia's greatness, Putin has focused on solidifying his own power within Russia as well as returning to imperialist

Media Ajir is instructor of political science and international relations at the University of Nebraska–Omaha and Bellevue University. She holds a master of science degree in political science and a certificate in intelligence and national security from the University of Nebraska–Omaha. She is the recipient of the 2017 USSTRATCOM General Larry D. Welch Deterrence Writing Award.

Bethany Vailliant is a researcher for the National Strategic Research Institute (NSRI) and an instructor of international relations at the University of Nebraska–Omaha. She holds a master of science degree in political science and a certificate in intelligence and national security. She is a two-time winner of the USSTRATCOM General Larry D. Welch Deterrence Writing Award.

tendencies to grab land and people in the Russian "near-abroad" (the former Soviet Union states that have now gained their independence).

However, his ability to hold on to power and forays into Russia's near-abroad have not been enough. Russia continues to view itself in an ongoing and fierce competition with the Western world—and in particular the United States. For example, incidents such as the release of the Panama Papers, the annexation of Crimea, the passing of the Magnitsky Act, and the Olympic doping scandal have all inflamed the tension between Russia and the US. Therefore, Putin's recent power plays are made with a zero-sum mentality. Put simply, destabilization of the West is a means by which Putin pursues his goal of restoring Russia's lost greatness and holding on to power.

While it is a common perception in the West that Russia is acting offensively, there lies explanatory power as well in understanding that the Russians view their actions as being defensive in nature. In the Russian view, technology is a particular method the West uses to "attack" it—but less for inflicting crippling blows than as a way to spread unacceptable ideas, norms, practices, and behaviors. Russian intelligence services are increasingly worried about the potential detrimental national security effects arising from the internet. In fact, the vast majority of Russian writing on information conflict is defensive in tone and focused on information security due to their perception of the global information space as a serious threat to Russian sovereignty. The original Russian source government document "Doctrine of Information Security of the Russian Federation" states that there is a trend in foreign media to publish biased information about Russian state policy and that there is discrimination against Russian mass media. Additionally, they observe what they perceive as increasing pressure on the Russian population through Western propaganda efforts that "erode Russian traditional and spiritual and moral values."[2] The belief that the West was heavily involved in the color revolutions and in the Arab Spring, as well as with the protests preceding Putin's reelection in 2012, is a deeply held one. In response, Russia views the media and the internet as tools to defend its authoritarian state and ideology both at home and abroad through dissemination of its own views and propaganda efforts. To understand this fully, one must first consider Russian information warfare concepts before examining three specific Russian information warfare tools.

Russian Information Warfare Concepts

Information warfare, according to the original Russian government document *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, is defined as confronting a state in the information space by damaging information systems, processes, and resources. These are of critical importance to undermine any political, economic, or social system, through what Russia deems "massive brainwashing" of the population to destabilize the society and the state. It also forces the confronted state to make decisions in the interests of the confronting party.[3] However, this is nothing new; the Soviet regime also used information weapons to help achieve these greater long-term goals. The first known use of the words "active measures" was in a Bolshevik document in 1919. By definition, active measures involve influencing events and behavior in, and the actions of, foreign countries.[4]

The Soviet intelligence active measures budget was reportedly $3–4 billion annually and employed well over 15,000 personnel. Active measures were employed to influence nations around the globe; however, the United States was always considered the main enemy, and the Soviets did not differentiate between peacetime and war.[5] Today, the same logic is employed. According to 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."[6]

The Soviets created the most threatening influence of its kind in the modern world.[7] To capture this, figure 1 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. Active measures that focused on disinformation represented a carefully constructed false message secretly introduced into the opponent's communication system to deceive decision makers and the public.

The next concept to understand is reflexive control theory—a term used to describe the practice of predetermining an adversary's decision-response by altering key factors in the adversary's perception of the world.[8] It takes the concept of disinformation one step further in that the crafted information message is inserted into an adversary's decision-

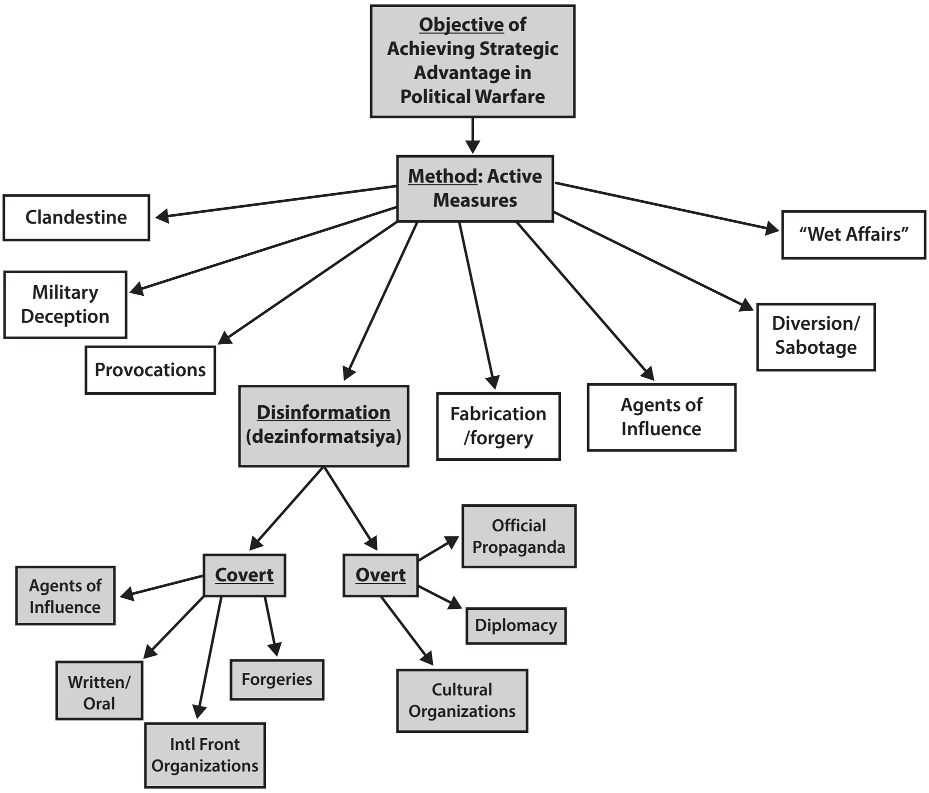

Figure 1. Disinformation dissemination as subset of active measures. "Agents of Influence" are used both as a subset of active measures and a subset of disinformation. (Source: Kevin McCauley, *Russian Influence Campaigns against the West: From the Cold War to Putin* [North Charleston, SC: Amazon Digital Services, 2016], 94, Kindle edition.)

making process to guide the opponent into making predetermined decisions and actions that are unfavorable to himself.[9] The central focus of reflexive control is on the less tangible aspects of decision making, such as the enemy's inner nature—his ideas and concepts—which is the filter through which passes all data about the external world.[10] Therefore, reflexive control 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 for nearly 40 years. Over these years, many intellectual "giants" have emerged in the field of reflexive control theory in the military, academic, and civilian sectors of society. They've done so particularly at the tactical and operational levels, both for deception and disinformation purposes and to control the enemy's decision-making processes.[11] 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.

There is a distinct continuity of Soviet active measures and reflexive control into the present day practices of the Russian Federation. However, the advent and rapid progress of technology has enabled the Russians to be far more successful in their disinformation campaigns than the Soviets ever were. The Russian distinction between "cyber" and "information warfare" is an artificial one. Instead of cyberspace, Russia refers to it as the "information space," which includes both computer and human information processing.[12] Today, information in the media, on TV, on the computer, or in someone's mind is all subject to the same targeting procedures.

Russia 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 to support the Kremlin's message,
3. sophisticated technical expertise of the Kremlin's information warfare that allowed access to a greater variety of foreign audiences, and
4. utilization by the Kremlin of the relative openness of Western media for the Russian propaganda offensive.[13]

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.[14] Information warfare does this in two important ways. First, Russia recognizes that information operations offers an opportunity to achieve a level of dominance. Second, it provides a significantly less costly method of conducting operations since it replaces the need for conventional military forces. According to Putin, "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."[15] Russia makes these concepts effective by using a multitude of information warfare tools.

Russia's Information Warfare Tools

A common development of state actors with fewer defense resources has led to the development of tools that are low cost and high impact (LCHI). Since Russia does not have the military or economic strength to directly counter the United States, it relies on nonconfrontational and asymmetric methods of power to ward off US normative influence. Some of the tools Russia relies upon to fulfill its asymmetric information warfare campaign include state-funded global social media, control of Western media outlets, and direct lobbying of Western society.

Exploiting Global Social Media

Cyber platforms have given the Kremlin capabilities to accomplish political foreign policy goals it would not otherwise be capable of. 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 and are cost effective, difficult to attribute, and accessible from any location.

Current use of information warfare operations by the Russian Federation simply represents a modern, internet-age version of already well-established Soviet reality-reinventing tactics. 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, including disinformation and propaganda.[16] Russia has therefore developed multiple capabilities for information warfare, such as computer network operations, electronic warfare, psychological operations, deception activities, and the weaponization of social media, to enhance its influence campaigns.[17]

Of particular importance is the injection of propaganda through social media as the nexus of information operations and cyberwarfare, whether it be through Twitter, Facebook, or YouTube. 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."[18] 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 when the Russian

Embassy based in London tweeted "pundits call on @Theresa_May to disrupt possible Russia-US thaw. No trust in Britain's best friend and ally?" 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-US relations, seemingly with a condescending tone to undermine US relations with its greatest ally, Great Britain.

A more technical approach to social media propaganda allows for Russian troll campaigns and bots, otherwise known as the Kremlin Troll Army, to sow discord, spread fear, influence beliefs and behaviors, discredit institutions, diminish trust in the government, and ultimately destroy the possibility of using the internet as a democratic space. According to Lt Col Jarred Prier, this "hinges on four factors:

1. a message that fits an existing, even if obscure, narrative;
2. a group of true believers predisposed to the message (when presented with information within one's belief structure, bias is confirmed and propaganda is accepted easily);
3. a relatively small team of agents or cyber warriors; and
4. a network of automated 'bot' accounts." These factors allow a proactive approach to spreading a narrative at an extremely fast rate, what Prier has defined as "commanding the trend."[19]

This 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 this 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." In 2014, Twitter estimated that only 5 percent of accounts were bots; that number has grown along with the total users and now tops 15 percent.[20] For example, "Following the first presidential debate, the #TrumpWon hashtag quickly became the number one trend globally. Using the TrendMap application, one quickly noticed that the worldwide hashtag seemed to originate in Saint Petersburg, Russia."[21]

As future conflicts come into existence in the technological and cyber domain, "He who controls the trend will control the narrative- and ultimately, the narrative controls the will of the people."[22] This form of information warfare capability is often oversimplified and underestimated and therefore leads the target audience to exploitation through already existing vulnerabilities. The Russian *Bulletin of the Academy of Military Sciences* 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,"[23] fulfilling the objectives of reflexive control theory.

Controlling Western Media Outlets

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, paving the way for buying space in the West. By 2011, Russia had spent $1.4 billion on international propaganda,[24] a massive increase from the old Soviet era. 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.[25] In reality, the Kremlin has twisted one of the most fundamental and cherished values of liberal democratic societies, free speech and free press, into validation for its behavior, exploiting a very real vulnerability. Furthermore, Russia has in numerous ways weaponized this new form of soft power.

A version of this broad strategy can be found in the Russian primary military source *Information-Psychological Warfare in Modern Conditions* and includes:

- 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[26]

The real-world repercussions 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 notable 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."[27] 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."[28] Russia Today is not the only state-sponsored television channel; its other media outlets have waded into overt attempts at political disruption in foreign governments as well.

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."[29] 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 under way. The coordination from the state television services in Germany to the Foreign Ministry of Russia, launched a process to instigate political instability.

The second form of attack is takeover of Western newspapers. One method used is 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 to beguile readers consist of, first, mitigating cognitive dissonance by "adapting the contents and the style of the articles to fit their 'critical' Western mind."[30] 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."[31] The second maneuver is applying the two-step flow of communication theory, which implies that information provided to the public through mass media is not directly inherited but rather channeled indirectly through opinion leaders.[32] To do this, a handful of newspapers have been purchased 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 unprofitable papers and highlight the strategic reasons behind them. A notable example of this was the acquisition 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."[33]

Lobbying Western 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,"[34] along with overt and covert 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 10-day trip to Moscow and Saint 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."[35] 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, and conferences to export its own brand of political and economic influence.[36] Examples of umbrella organizations that covertly channel funds to Russia-friendly NGOs include the Institute of CIS Countries, as well as Russian World. 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.[37]

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 it the ability to reach out to the most prestigious lobbying and communication firms that "possess the necessary know-how . . . because they often employ former politicians, ambassadors, and other highly placed officials, who have direct personal access to government circles."[38]

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. He abstains from asking questions about democracy and human rights, making him an excellent 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."[39]

This report, on balance, perfectly exemplifies the way in which Kremlin-US 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 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 in 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."[40] 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.[41] One can also classify this move as a soft power play through western newspapers.

Long-Term Implications and Recommendations

Clausewitz's fog of war theory has been a useful term in a traditional sense for conveying the lack of situational awareness, and it has become a useful concept in information warfare as well. Russia has found an incredibly effective way to marry the ideas of disinformation, psychological warfare, reflexive control, and technology to create a very powerful fog of war that has disoriented the West. Their success in this endeavor has led to a climate of confusion, leading many to believe that problems are internal rather than external. This is because in some ways, they are. Russia merely has had to exploit an existing narrative—that is, the divisions in the West created by the fundamental principles of democratic societies: the freedom of individuals to attach themselves to a group they identify with and choose political leaders accordingly.

The implications of this are truly daunting. In the long term it serves to create distrust by the public in democratic institutions. It also elevates distrust in the press, in technology, in social media platforms and the businesses that are involved in creating them. This quite literally creates a modern fog of war. Scrambling to determine the truth as well as whom to blame, political disagreements transcend into extreme polarization and fuel tribalism that can tear a country apart.

In past conflicts, there has often been a "rally around the flag" effect where the nation comes together, despite differences, against a common enemy. However, an information war that uses disinformation as its weapon of choice destroys this unification by bringing the war directly into our homes and our minds.

Rethinking the Applicability of Deterrence

On 31 May 2018, the State Department released "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats." While the document recommends "a fundamental rethinking" of deterrence policy, the proposed strategies merely touch upon old ideas and fail to encompass a larger problem. The report continues to view information operations exclusively within the cyber domain, particularly because cyberspace has not yet been categorized as distinct and separate parts, as conventional warfare has been (that is, land, sea, air, and space). Due to the fact that modern times have forced us to move from a purely physical space into a virtual one, and because information warfare has been made so much more effective within the virtual space, it seems that multiple types of information warfare are artificially being lumped together under the cyber domain. Instead of rethinking deterrence, we recommend rethinking the applicability of deterrence to cyber domain of warfare.

Introducing a Sixth Domain

Therefore, the evolution of military operations must include a sixth official domain of warfare, psychological, overlapping but distinctly separate from cyber. Vulnerabilities in cyberspace are concerned with malicious activity of a kind that needs to be separate from a psychological domain. For example, cyber focuses heavily on computer network defense and defense of critical infrastructure, among other malicious cyber activities within information security. On the other hand, psychological warfare focuses on the more human-related aspects of abstract information processing. It is critical that we differentiate this type of activity from particular tools of disinformation that Russia has used to wage war on the human psyche throughout the West.

The weaponization of information changes the application of deterrence, both within the cyber domain and in a psychological domain. There is currently plenty of scholarly research on the former. Although both of these dimensions can operate at a level beneath the use of force, there are disinformation operations that simply do not fall within the category of cyber, and we are left with nowhere to place them. In this article we have identified several tools Russia has used to enhance its information campaign in the West—social media, Western media outlets, and lobbying of civil society—all of which have the capacity to manipulate the human mind, but all of which do not necessarily benefit from virtual space exclusively.

We do not wish to undermine the valuable nature of cyberspace in spreading psychological disinformation campaigns. It has undoubtedly created a particularly ideal set of opportunities for Russia to accomplish its goal of destabilizing the West to increase its own power. While information warfare can operate independently from the cyber domain, it is important to note that it also benefits greatly from realities of virtual spaces to disperse its message. Social media platforms, for example, are a way for our adversaries to cost effectively and asymmetrically reach broad audiences of average people, tailoring active measures and reflexive control to achieve their objectives on a massive scale. This is, essentially, how Russia classifies this domain. It does not distinguish between cyber and information warfare. The problem is that this ignores the reality of information operations as two-fold: both virtual and non-virtual. This means we are not creating a complete picture of the human dimension of information warfare, which only serves to limit the discussion on how deterrence theory can be modified to address all types of warfare.

Figure 2 illustrates the differences and similarities between the traditional perceptions of deterring conventional threats and achieving deterrence in cyberspace compared to our proposed psychological domain. While there are unchanging deterrence elements and concepts that allow deterrence to function in all domains, the applicability of these elements does not look the same across domains.

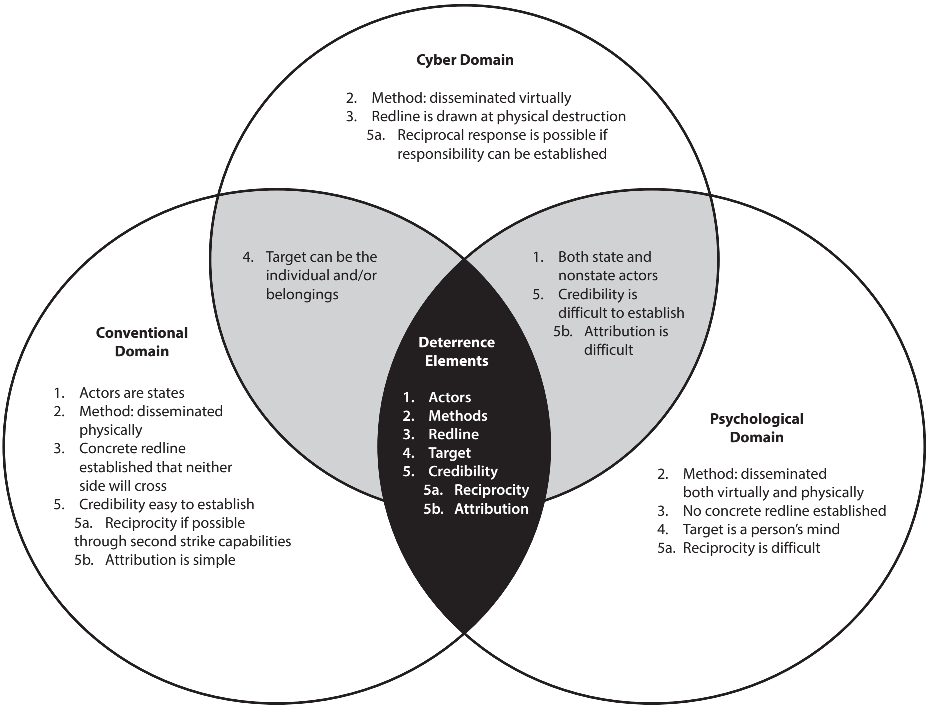
Cyber Domain
2. Method: disseminated virtually
3. Redline is drawn at physical destruction
5a. Reciprocal response is possible if responsibility can be established
4. Target can be the individual and/or belongings
1. Both state and nonstate actors
5. Credibility is difficult to establish
5b. Attribution is difficult
Conventional Domain
1. Actors are states
2. Method: disseminated physically
3. Concrete redline established that neither side will cross
5. Credibility easy to establish
5a. Reciprocity if possible through second strike capabilities
5b. Attribution is simple
Deterrence Elements
1. Actors
2. Methods
3. Redline
4. Target
5. Credibility
5a. Reciprocity
5b. Attribution
Psychological Domain
2. Method: disseminated both virtually and physically
3. No concrete redline established
4. Target is a person's mind
5a. Reciprocity is difficult

Figure 2. **A comparison of domain characteristics in relation to deterrence theory**. (Note: the numbers within the circles correlate with the numbers of the deterrence elements in the black center.)

Specifically, five areas of difference exist:

Actors. First, cyber has allowed nontraditional actors, such as individuals or transnational criminal organizations, to play an active part in destabilization. As the world moves away from traditional, black-and-white norms concerning the sovereignty of states due to globalization, so too our ability to deter threatening actors has had to accept as reality the breakdown of the state as a concept. Therefore, while nuclear deterrence fits nicely into a traditional state-centric international relations framework, the more one moves into the cyber and psychological domain with the inclusion of nonstate actors, the less relevant the state becomes.

Methods. Warfare in the conventional domain consists of specific methods of attack, being those that cause physical destruction. Those in the cyber domain consist of virtual dissemination and destruction. Lastly, the psychological domain consists of multiple approaches, both physical and virtual. This illustrates the increasing complexity of the latter domains.

Redlines. Traditional deterrence strategy has been effective because a distinct redline generally exists that both sides are unwilling to cross based on the simple cost-benefit analysis of mutually assured destruction (MAD). The same cannot be said about the cyber and psychological domains, as Russia's actions have highlighted. While the nuclear redline is clear, the cyber redline becomes more obscure. Currently, the redline in cyber is drawn at any sort of physical harm, which is then considered to be an act of war. Anything short of this, however, is merely considered a nuisance. This line becomes even more obscure in the psychological domain because no physical line exists, despite the incredible amount of destruction and confusion it can cause.

Target. The object of conventional domain attacks can be the individual and/or possessions. In a strictly cyber domain, the target is normally a person's belongings (information, hardware, money). However, in the psychological domain the target is a person's mind.

Credibility. Credibility is a critical component of ensuring successful deterrence. To be deterred, an adversary must believe its actions will incur a cost. Credibility relies on two important factors: reciprocity and attribution.

Reciprocating an attack relies on quantifying or measuring the level of destruction incurred to determine proportionality. While this is relatively easy to do in the conventional domain, it is challenging but possible within the cyber domain dependent on establishing those responsible behind an attack. It becomes even more difficult in the psychological domain due to the inability to measure effects and respond in kind.

Attribution becomes increasingly difficult as one moves outside of the physical world into a virtual and cognitive space. Attributing a physical attack is much simpler than attributing a virtual act to a state actor, and the involvement of nonstate actors in the cyber and information realms only seems to complicate this issue. This begs the question: can we deter an adversary we cannot identify? This problem degrades the ability to create credibility, along with the ability to follow up with requisite punishment.

In sum, given an increase in actors and methods, along with the blurring of redlines and sophistication of the targets, Clausewitz's fog of war is exponentially increased, which reflects the difficulty presented in reciprocity and attribution. The closed and carefully censored nature of Russia's society inhibits a proportional response by the West, since the media is primarily a tool of the Russian state. Conversely, the openness of democratic societies creates an opportunity for exploitation. Due to basic values in Western democracies for freedom of expression and their requisite legal foundations, limiting access to disinformation will be problematic and ultimately ineffective as a form of punishment. If we cannot fully reciprocate or attribute an attack correctly, we cannot threaten punishment, which leads to a decrease in overall credibility. And while the impact that can be had on a human's psyche is by no means new, it has only recently reached a level of magnitude that surpasses any other time in history.

However, this is not an argument against the establishment of a sixth domain. Instead, this strengthens the need for one. Given the difficulties that arise when information warfare is conducted on the human psyche, it is important to distinguish types of attacks as clearly as possible rather than lumping all of them under one category, as Russia has done. Russia is essentially viewing information itself as the weapon as well as a "space" (or domain) of warfare. In contrast, the US should see the cyber and psychological domains as being the space within which information is being used as the weapon of choice. Doing so will allow the US to create new and more specifically targeted deterrence policies, giving us an upper hand in future warfare. Information warfare should be classified under two separate domains of warfare: the cyber domain (virtual) and a psychological domain (cognitive).

Conclusion

While we have certainly moved beyond the days of a nuclear arms race with the Soviet Union and deterrence has subsequently evolved, our views of deterrence still rest upon nuclear and conventional forces to avoid escalation of conflict. Russia's recent emergence into the global dialogue among nations has been one of antagonism and active hostility, emphasizing its motives to be an established power on its own with a zero-sum mentality. This means reemergence as a world power while keeping the West out of its internal affairs of nationalistic authoritarianism. The means to this end include destabilizing their adversaries in the West, NATO, and the EU, using a variety of disinformation and cyber-enabled, low-cost, high-impact tools to facilitate operations. These capabilities are used to achieve different objectives in each target country with an asymmetric advantage. An underlying theme in Russia's success in this war is the rise of technology, allowing for the reinvention of old Soviet tactics. Propaganda, whether in the form of social media, traditional media outlets, or lobbying, is easily dispersed with the help of twenty-first-century machinery.

Today, conventional battlefield tactics remain a necessary component for deterring our adversaries, but we must now move away from traditional measures and transcend our thinking to reflect modern warfare. This includes accepting and understanding a new domain and how to navigate it to successfully deter Russian information warfare. We cannot, as a nation, create viable defense policies based on an old understanding of the application of deterrence theory. Furthermore, there has been no evidence to date to suggest that outside powers will not continue to exploit our vulnerabilities as a Western democratic nation. Therefore, we must take a proactive approach in confronting this new kind of weapon. Though Russia has been engaging in nonconfrontational methods of attack, it is time the US shifts from a pacifist stance to a more dynamic one in the psychological domain. SSQ

Notes

[1] This research uses a thorough review of open-source literature of military and original source government documents. Secondary-source information from the Russian Federation and the United States was also used. It includes a qualitative analysis of developments in information warfare.

2. Russian Federation, “Decree of the President of the Russian Federation,” The Ministry of Foreign Affairs of the Russian Federation, 5 December 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

3. Russian Federation, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9 September 2000, NATO Cooperative Cyber Defence Center of Excellence, 2000, http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

4. Kevin McCauley, *Russian Influence Campaigns Against the West: From the Cold War to Putin* (North Charleston, SC: Amazon Digital Services, 2016), Kindle edition, 121.

5. McCauley, 121.

6. Russian Federation, *Conceptual Views.*

7. McCauley, *Russian Influence*, Kindle edition, 109.

8. Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016), 19.

9. McCauley, *Russian Influence Campaigns*, 2015.

10. T. L. Thomas, “Russia’s Reflexive Control Theory and the Military,” *Journal of Slavic Military Studies* 17 (2004): 237–56, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

11. Thomas, “Russia’s Reflexive Control.”

12. Giles, *Handbook*, 8.

13. Marcel Van Herpen, *Putin’s Propaganda Machine*: *Soft Power and Russian Foreign Policy* (Lanham, MD: Rowman & Littlefield, 2016), 202.

14. Giles, *Handbook*, 5.

15. Giles, 3.

16. Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm: Swedish Defense Research Agency, 2010), 15, http://www.highseclabs.com/data/foir2970.pdf.

17. McCauley, *Russian Influence Campaigns*, 86.

18. Van Herpen, *Putin’s Propaganda Machine*.

19. For more information on how to command the trend, see Lt Col Jarred Prier, “Commanding the Trend: Social Media as Information Warfare,” *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): 50–85, http://www.airuniversity.af.mil/SSQ/Display/Article/1349602/volume-11-issue-4-winter-2017/.

20. Alex Lubben, “Twitter’s Users Are 15 Percent Robot, but That’s Not Necessarily a Bad Thing,” VICE News, 12 March 2017, https://news.vice.com/story/twitters-users-are-15-percent-robot-but-thats-not-necessarily-a-bad-thing.

21. Prier, “Commanding the Trend,” 74.

22. Prier, 81.

23. 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* 46, no.1 (2014): 106.

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

25. Van Herpen, *Putin’s Propaganda Machine*, 1863.

26. Yu. Kuleshov et al., “ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ПРОТИВОБОРСТВО В СОВРЕМЕННЫХ УСЛОВИЯХ: ТЕОРИЯ И ПРАКТИКА” (“Information-Psychological Warfare in Modern Conditions”), 107.

27. Van Herpen, *Putin's Propaganda Machine*, 71.

28. "Airwaves Wobbly—Russia Today Goes Mad," *Eastern Approaches* (blog), *The Economist*, 6 July 2010, https://www.economist.com/eastern-approaches/2010/07/06/airwaves-wobbly.

29. "German Media Worries about Russian-Led Disinformation Campaign," Deutsche Welle, 19 February 2016, http://www.dw.com/en/german-media-worries-about-russian-led-disinformation-campaign/a-19061955.

30. 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: Librairie Armand Colin, 1963).

31. Van Herpen, *Putin's Propaganda Machine*, 79.

32. Theory by sociologist Paul Lazarsfeld, which 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." Quoted in Van Herpen, *Putin's Propaganda Machine*, 75.

33. Luke Harding, "Russian Oligarch Alexander Lebedev to Buy London Evening Standard," *The Guardian*, 14 January 2009, https://www.theguardian.com/media/2009/jan/14/russian-oligarch-alexander-lebedev-buy-london-evening-standard.

34. Van Herpen, *Putin's Propaganda Machine*, 100.

35. Van Herpen, 100.

36. Nicu Popescu and Andrew Wilson, *The Limits of Enlargement-Lite: European and Russian Power in the Troubled Neighbourhood*, Policy Report 14 (London: European Council on Foreign Relations, June 2009), 29.

37. 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): 41–49.

38. Van Herpen, *Putin's Propaganda Machine*, 48; and Thomas Graham, *Resurgent Russia and U.S. Purposes: A Century Foundation Report* (New York: Century Foundation, 2009), http://russiaotherpointsofview.typepad.com/files/graham_resurgent_russia.pdf.

39. Graham, *Resurgent Russia*.

40. Ravi Somaiya, "P.R. Firm for Putin's Russia Now Walking a Fine Line," *New York Times*, 31 August 2014, https://www.nytimes.com/2014/09/01/business/media/pr-firm-for-putins-russia-now-walking-a-fine-line.html.

41. Vladimir Putin, "A Plea for Caution from Russia," *New York Times*, 11 September 2013, https://www.nytimes.com/2013/09/12/opinion/putin-plea-for-caution-from-russia-on-syria.html.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil