Russia's Information Warfare
Exploring the Cognitive Dimension

Blagovest Tashev, PhD; Lieutenant Colonel Michael Purcell (Ret); and Major Brian McLaughlin (Ret)

Abstract: The U.S. military increasingly invests in capabilities to meet challenges from the growth of strategic competition in the information environment, which is aimed at influencing and disrupting adversaries and other groups. By analyzing Russia's approach to information warfare, this article adds to the current understanding of the Russian modus operandi in the information environment. The article argues that the success of competitive strategies in this domain requires not only investment in its technical and informational dimensions but also deep knowledge of its most important one—the cognitive dimension. The article concludes with recommendations to incorporate cognitive dimension considerations in Marine Corps operations in the information environment.

Keywords: information warfare, Russia, cognitive dimension, deputy commandant for information, culture, Marine Air-Ground Task Force (MAGTF) information operations, operations in the information environment

The U.S. military is increasingly investing in structures and capabilities to meet the challenges resulting from the exponential growth of strategic competition in the information environment. However, U.S. military

Blagovest Tashev has expertise in Eastern Europe and Eurasia and currently works in the Translational Research Group at Marine Corps University's Center for Advanced Operational Culture Learning (CAOCL). LtCol Michael Purcell is a former armor officer and Eurasian foreign area officer with extensive operational experience in the former Soviet space. Maj Brian McLaughlin is a former infantry officer, Eastern European foreign area officer, and crypto-linguist, who is focused on Ukrainian security and politics and developing curriculum at CAOCL to ensure deploying forces are better prepared to operate among foreign populations. The views presented in this work are the authors' own.

MCU Journal vol. 10, no. 2
Fall 2019
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.2019100208

professionals continue to face difficulties addressing the intangible elements inherent to this form of confrontation. Success in this realm requires not only effectiveness in the physical and informational dimensions but also intimate knowledge of the cognitive dimension of the information environment. Russia's approach to information warfare provides valuable insights into the complexity of this issue for military and national security professionals.

The purpose of this article is to advise information operations professionals and improve their understanding of the cognitive dimension. This article addresses the evolving role of information warfare in Russia's strategy for interstate power competition and argues that, to successfully counter it, American military professionals must come to terms with Russia's philosophically different understanding and approach to the cognitive dimension in the information environment.

In the last decade, Russia has reemerged as a significant power player capable of exerting influence beyond its immediate neighborhood. Starting with the invasion of Georgia in 2008, Russia gradually expanded its military presence in Central Asia, annexed Crimea from Ukraine in 2014, provoked and supported an ethnic Russian insurgency in Eastern Ukraine, and intervened militarily in support of the ruling regime in Syria.[1] Simultaneously, Russia broadened security cooperation missions in the greater Middle East region, Africa, Asia, and South America, while Russia's Aerospace Forces and the Navy are increasing their long-range patrols. This widened presence abroad was made possible by massive military modernization at home.[2] The country has reformed both the structure and the capabilities of its armed forces and has successfully used them as a credible instrument of national power. Russia's return to global politics has been a long process. Yet, it was the annexation of Crimea and the revelation of Moscow-directed interference in the U.S. presidential elections in 2016 that thrust this process into public discourse, which seems to have shifted Washington's attitude toward Russia's reemergence as a global player. Accordingly, U.S. national security documents, including the *National Security Strategy* (NSS) in 2017 and the *National Defense Strategy* (NDS) in 2018, identified Russia, along with China, as a threat to national security.

One particular aspect of Russia's expanding power that has garnered considerable attention is its use of information warfare. While Western national security professionals have noted Russia's use of information in the short Russia-Georgia war in 2008 and in the wake of Russia's intervention in Ukraine starting in 2014, the American public and Washington, DC, in general have become obsessed with this after Russian interference in the 2016 U.S. presidential elections. Since then, the national security elite and the public have begun to pay more attention to Russia's information operations in Europe and elsewhere.[3] Russia's information warfare feeds into U.S. concern about the growing impact of stratagems employed by states to control the narratives surrounding their operations while aiming to influence the decision making and behavior of other actors. The trend is facilitated by the proliferation of technologies and the growing use of the internet and social media as well as changing human habits of acquiring and using information. Accordingly, both the NSS and NDS highlight threats to U.S. security stemming from the use of information by adversaries.

The growing emphasis on threats emanating from the information environment prompted the creation of a seventh warfighting function by the Chairman of the Joint Chiefs of Staff in 2017. Accordingly, the U.S. Marine Corps added a deputy commandant for information to synchronize the efforts of those disparate functions related to the information environment already organic to the Marine Corps. U.S. Department of Defense publications providing doctrine for information operations identify the information environment as including the physical, informational, and cognitive dimensions.[4] *Information Operations*, Joint Publication 3-13, describes the information environment as consisting of the human-centric cognitive dimension, the data-centric information dimension, and the tangible physical dimension.[5] It goes on to explain the cognitive dimension as encompassing "the minds of those who transmit, receive, and respond to or act on information."[6] The *Marine Air Ground Task Force Information Environment Operations Concept of Employment* lays out the approach to fighting and winning through and in the information environment.[7] According to the publication, the cognitive dimension includes "the knowledge, attitudes, beliefs, and perceptions of people."[8] In the same section, elements of the cognitive dimension are represented as a list of possibilities, "such as the decisionmaker's culture, life experiences, relationships, outside events, ideology, and the influences of those inside and outside of [a] decisionmaker's group."[9]

While organizing, equipping, and training to face the more tangible physical and informational dimensions of the information environment, the U.S. Marine Corps is only beginning to realize the difficulties of the least tangible dimension. This article first offers a short analysis of the elevation of information warfare as a powerful instrument of national power as reflected in Russia's national security documents and thinking about warfare. It then proceeds to address some issues with the Western analysis of Russia's way of competition in the information environment. In the next section, we offer several factors that need to be included in the analysis of Russia's information warfare. The article concludes with recommendations about the Marine Corps' approach to countering Russian information warfare and more specifically about addressing the cognitive dimension—the most important dimension in the information environment.

A Terminology Issue

The use of the term *information warfare* in American public discourse to describe Russia's interference in the internal political affairs of other countries is problematic. Like other terms, such as *hybrid warfare*, information warfare has no doctrinal definition and is correspondingly ambiguous. Its meaning is further diluted or outright misused by practitioners at the operational level in fields that would be better considered as subsets of the term information warfare. The general notion of information warfare as a "strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations" as described by the Congressional Research Service (CRS), is often used liberally to describe narrower activities, such as network operations, psychological operations, electronic warfare, operations security, and military deception.[10]

This conflict is in part due to the operationalization of information warfare in the United States, which is bound by the confines of legal and cultural barriers. In practice, "much of the current information warfare doctrine and capability resides with the military."[11] However, the U.S. military's doctrine, capabilities, and functions (a.k.a. information operations) do not address the strategic level, but rather the operational and tactical ones. In addition, as the report of the CRS points out, Title 10 U.S.C. § 2241 prohibits the Department of Defense (DOD) from domestic "publicity or propaganda."[12] Although the U.S. military is expected to be involved in information warfare, there are barriers to its ability to influence beyond the operational level of war. At the same time, there seems to be no other institution in the U.S. government entrusted with a role in information warfare at the strategic level.

It has been pointed out by others that the U.S. military used to have a more comprehensive and holistic approach to information warfare and at some points even involved coordination and synchronization of policies and actions by military and nonmilitary agencies and structures.[13] Gradually, however, the various information-related functions and organizations went in different directions. Very importantly, information warfare was increasingly associated with the military and warfighting, divorcing it from any broader—civilian, nonmilitary, and peacetime—efforts in the information environment.

This is a critical point, as the discussion below will indicate that Russia not only faces fewer legal and cultural barriers to influence at the operational and strategic level during both war and peace, but it also has philosophically different approaches and goals while operating in the information environment. The multiple issues with the definition of information warfare in the United States notwithstanding, even the most expansive understanding of the term fails to capture the nature of the approach adopted by Russia. As Timothy Thomas observed, what is really different in the Russian approach "is the conceptual understanding of an information operation from a cultural, ideological, historical, scientific, and philosophical viewpoint."[14] As the rest of this article will point out repeatedly, the distinct nature of Russia's approach is so different from the American approach that many argue for adopting a new term that better captures Russia's way and avoids mixing it with the Western conceptualization of operations in the information environment. One author, for example, calls for adopting IPb, a shorthand for the Russian term информационное противоборство, loosely meaning "information confrontation."[15] For the purpose of this article, however, we will continue to use the term information warfare, despite its shortcomings.

Russia's Elevation of Information Warfare

Through its strategic documents, Russia consistently indicates that it seeks to adopt a comprehensive and coordinated approach to gaining security and successfully advancing its interests. This effort is envisioned as the integration of multiple instruments of power and the involvement of both national institutions and nongovernmental actors. In fact, the body of strategies, doctrines, and government-promoted narratives suggests that the successful promotion of Russia's national interests requires the involvement of the entire society. Russia has also increasingly placed emphasis on nonmilitary means as a way to gain security, even as the country is involved in an ambitious military modernization.[16] According to General Valery V. Gerasimov, chief of the General Staff of the Armed Forces of the Russian Federation, the ratio of nonmilitary to military measures in the modern security environment is 4:1, even as nonmilitary competition comes under the aegis of the military.[17] To the best of our knowledge, this is the only reference Gerasimov, or any other high-ranking Russian military official, has made to this ratio. One can reasonably suspect that the chief of the General Staff is paying lip service to the increasingly large role nonmilitary measures are playing in confrontations between states; the Russian military elite is still focused on preparing the armed forces to prevail in a kinetic confrontation with other states. There is little doubt, however, that the Russian military recognizes the utility of nonmilitary measures in interstate confrontation, especially during what would be considered peacetime.

This way of thinking is leading to an evolution in the Russian way of warfare; while the military is not necessarily departing from the big-war paradigm, decision makers in Moscow are increasingly focusing on how defense structure and posture, along with nonmilitary instruments, shape the strategic environment in line with Russia's preferences.[18] Accordingly, information warfare is increasingly central to a state's arsenal to use against other states in confrontation, wherein countries' elites and public perceptions are becoming the center of gravity in determining confrontation outcomes. The goal of information warfare is to influence both the adversary's strategic calculus and the public's behavior.[19] As Aleksander Dvornikov, commander of Russia's Southern Military District, points out in the Russian publication *Military-Industrial Courier*, "Now states achieve their geopolitical goals through the application of complex non-military measures, which often are more effective than the military ones. The main goal of these measures is not the physical destruction of the enemy but the complete submission of his will."[20] He goes on to argue that without information operations, Russia would not have succeeded in many operations in Syria.

Not surprisingly, Russia is implementing policies and practices designed to promote information warfare to a level of parity with nuclear and conventional power. This struggle to shape other states' perceptions and calculus is constant, even during peacetime and periods of cooperation; thus, the lines between peace, conflict, and war are blurred. As General Gerasimov puts it, "military conflicts have not gone beyond the bounds of the conventional nature of war; their components are types of struggle such as direct armed struggle, political struggle, diplomatic struggle, information struggle, et al." [21] While the U.S. approach to warfare, largely conditioned by political and legal constraints, makes a relatively clear distinction between war and peace and restricts methods and capabilities accordingly, Russian thinking displays a willingness to harness the power of all national institutions in a continuous struggle with its opponents, both current and potential. Ironically, Russian strategists see the elevation of informational instruments of influence, the blurring of the line between peace and war, and even hybrid warfare as innovations advanced and practiced by Western powers.[22] Hence, Russia is simply adapting to the new type of warfare. While the enemy's economy and state command and control system will continue to be priority targets, the information sphere becomes a new critical operating environment.[23]

Of course, one should not take what we pointed out as the American proclivity to make a clear-cut distinction between war and peace to the extreme. This is simply a tendency. There is already evidence that this is changing. Most recently, the DOD released *Competition Continuum*, Joint Doctrine Note 1-19, which points out that the joint force traditionally "employs many constructs and procedures that reflect an artificial distinction between an environment of armed conflict and peace." Instead, it calls for the adoption of a "competition continuum," a construct that better describes "a world of enduring competition conducted through a mixture of cooperation, competition below armed conflict, and armed conflict."[24] This is a step in the right direction. However, changing long-established, historically, culturally, and doctrinally shaped attitudes in the U.S. military toward warfighting will take years. The growing popularity of terms such as *hybrid war*, *political warfare*, and *gray zone conflict* in the United States also point out American attempts to rationalize what is seen as a new type of confrontation between states (of course one should also ask if this is a new political phenomenon). Russia, conversely, has long seen relations between states as inherently and constantly competitive.

Russia's attention to changing trends in the information environment is reflected in official security-related documents. The Russian 2015 *National Security Strategy* (NSS) identifies informational security as one of the components of national security along with the state, public, environmental, economic, transportation, energy, and individual components.[25] The Russian NSS goes on to point out that the United States and its allies are attempting to contain Russia by exerting political, economic, military, and informational pressure on it. In general, Russia sees an intensifying confrontation in the global information arena as some states (meaning the West) use information and communication to achieve their geopolitical objectives.

Russia's NSS is specifically concerned with Western attempts to use information as a tool to interfere in Russia's domestic affairs to weaken "traditional Russian spiritual and moral values" and to threaten the "unity of the Russian Federation's multinational people."[26] Likewise, *The Foreign Policy Concept of the Russian Federation* pledges to respond to these challenges by continuing to focus on traditional measures to ensure strategic deterrence.[27] Internally, the state also tasks itself with implementing policies "aimed at strengthening and augmenting traditional Russian spiritual and moral values," in other words, creating resilience against foreign cultural influences. This focus on traditional Russian values is not new. In a wide-ranging series of interviews in 2000, when asked what the country needed most, then-acting President Vladimir Putin responded, "moral values."[28]

The Military Doctrine of the Russian Federation also acknowledges the changing nature of warfare, especially the integrated use of military force, political, economic, informational, and other nonmilitary measures. Accordingly, it calls for the "development of forces and means of information warfare."[29] While the United States has struggled to define information warfare and formulate a comprehensive approach to confrontation in the information space, Russian institutions, security professionals, and analysts seem to have reached a consensus on the nature of the confrontation. According to Russia's Ministry of Defence:

> Information War is the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psy-

> chological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.[30]

Similarly, in a political-military dictionary, edited by Russia's former ambassador to NATO, Dmitry Rogozin, *information warfare* (информационная война) is defined as an "intensive struggle in the information environment with the aim of achieving informational, psychological and ideological superiority, damaging information infrastructure, undermining political and social systems, as well as psychologically shaping military personnel and populations."[31] The entry suggests a philosophical approach to information warfare quite different from that in the West, which not only aims to influence the consciousness of groups in society but also to change their knowledge about basic social and natural phenomena, weakening their will to counter aggression. As this definition indicates, but also as numerous publications of Russian defense analysts attest, Russia's approach to information warfare is very different from the American approach to information operations.[32] It is based on different cognitive, ethical, legal, and cultural norms and practices.

Russia's distinct approach to information warfare is informed by a view on the nature of conflict in the international system that starkly contrasts with that of the United States. The roots of the Russian security elites' thinking have been subject to lengthy and sophisticated debate, but there is little doubt that one of the most dominant narratives in Russia's collective consciousness is one of a country standing alone without enduring alliances, constantly targeted by malign foreign designs.[33] Although Russia has a history of balancing external threats by alliance formation—most recently through the Warsaw Pact (1955 Treaty of Friendship, Cooperation, and Mutual Assistance) during the Cold War—the country currently sees itself as dangerously exposed and alone. This conception is of course founded on a long history of conflict with Western peoples, such as the Poles, French, Germans, and Americans, as well with those from the East, such as the Mongols and Japan.

This outlook was reinforced by the Marxist-Leninist ideology, particularly dialectical and historical materialism, with its emphasis on human history as the result of a constant struggle between social classes and states. In this view, while socialist states were free of domestic and external conflicts because they were classless, the capitalist countries, in contrast, were always involved in domestic and foreign conflicts. That made the international system inherently conflictual, a condition that would disappear only when the entire world became socialist.[34] Even when various Soviet leaders embraced "peaceful coexistence" or "détente" with the capitalist camp, those were considered tactical pauses in the inevitable showdown between the socialist states and imperialists.[35] While Marxist-

Leninist ideology was arguably not the most important source of Soviet foreign policy, generations of Russians were educated and socialized in its teachings[36] The use of terms such as *imperialism*, *exploitation*, *world domination*, and *fascism* introduced in the social lexicon through education and social discourses during Soviet times—are still frequently employed to describe Russia's opponents. One does not have to look hard to find outlooks in modern Russia that harken back to Soviet beliefs about the nature and extent of confrontation between states. Addressing the audience at a conference organized by the Russian Academy of Military Sciences, for example, General Valery Gerasimov pointed out that the increased struggle between states is caused by the U.S. quest for global dominance. This struggle involves political, economic, and informational tools, and encompasses all spheres of social activity including diplomacy, science, sport, and culture. Although this struggle is mostly nonmilitary, war cannot be excluded as an instrument. In his words, the confrontation is total.[37]

Marxism-Leninism influenced another aspect of the Soviet (and by extension Russian) approaches to information warfare. In this school of thought, the working masses possessed revolutionary potential in their struggle with the capitalist class. However, this potential needed to be translated into a political program; it was the role of the professional revolutionaries organized in a vanguard party (later to be known as the Communist Party) that organized, educated, and provided direction. The party needed to organize the masses with purpose and direction. That required that party members go among the classes as theoreticians, propagandists, agitators, and organizers.[38] The working class had to be trained in political consciousness, in understanding their true interests, and in embracing the revolutions as the way to liberation from exploitation. The Communist Party's efforts to actively shape the consciousness of the masses did not end with the assumption of power. Instead, it became a permanent activity, part of the party's goal of creating a new person—the Soviet man—whose consciousness and behavior aligned with ideological end states.[39] While the influence of Marxism-Leninism only partly explains the Russian approach to information warfare, it adds some understanding of the Soviet and Russian experience in targeting people's minds. In other words, better understanding requires exploration of the ideological foundations of Russia's long military tradition of information warfare.

But How Do They Do It?

A note of caution is in order at this point. Russian politicians, military leaders, and analysts talk and write about information warfare. However, most of their analyses seem to be their reading of how the West is conducting information warfare against Russia and others. Such analyses almost always include a description of the information threats Russia is facing and multiple examples of how the West is conducting information warfare. What is absent, however, is a description or prescription of how Russia is conducting or should conduct information warfare. This paradox is evident even in Russian strategic documents. They include long lists of information threats faced by the country and the armed forces but provide little insight into how the country or the armed forces should respond to those threats and conduct their own operations at the strategic, operational, and tactical level. While U.S. doctrinal publications related to information warfare, including information operations, psychological operations, public affairs, civil-military operations, etc., are available to the public, similar Russian documents, if they exist, are neither available nor discussed in public forums.[40] What little is publicly available provides no insights into strategy, tactics, techniques, and procedures. Russia's *Information Security Doctrine of the Russian Federation*, for example, is long on identifying national interests, threats to those interests in the information space, and calls for action, but there is little about how Russia operates in this sphere. Nevertheless, these documents are useful as they provide insight into Russian thinking about the information environment in general.[41]

Russia's traditional lack of openness on security and defense issues has led Western analysts on a quest to come up with concepts and terms that best capture Russia's approach to information warfare and its place in the country's overarching strategy. Accordingly, terms such as *hybrid warfare*, *Gerasimov doctrine*, *gray zone activities*, *reflexive control*, and *political warfare* have been introduced or borrowed in attempts to capture the nature of Russia's activities in the information space, and more generally Russia's overall strategy.[42] The proliferation of concepts notwithstanding, there is limited evidence that they provide substantial analytical value in the attempts to gain knowledge in Russia's strategy and more specifically in Russian information warfare. The result of this approach to the analysis is that the nature and meaning of Russia's actions are determined by the logic of those concepts and terms. If the hybrid war concept is used, for example, any Russian actions will be seen as a hybrid war action and a goal that may have nothing to do with the actual Russian intent and goal. Similarly, although one can come across multiple articles written in the West on the concept of "reflexive control" as the basis of Russian information warfare, one fails to find studies providing evidence and case studies of the application of reflexive control above the tactical and arguably the operational level.[43]

Rather than design a new one, or modify an existing concept that fully captures Russia's way of information warfare, it is more practical to look at how exactly the Russians approach interaction in the information space and attempt to understand the logic of their approach from the Russian perspective. There are historical, philosophical, cultural, military, and ethical rationales for the nature of Russia's approach. We need to accept that the logic of this approach is not necessarily similar to the logic that dominates the Western approach, lest we are to fall into the psychological traps of confirmation or selection bias in our understandings of Russian approaches.

On the Nature of Russia's Information Warfare

Rather than fit Russia's approach to information warfare into a neat, all-encompassing concept, one should start off with several considerations that inform a systematic analysis of Russian actions. What follows are the considerations, in no particular order, as each one must be analyzed in the context of a unified Russian strategic approach.

The Russian approach is holistic. It aims to not only affect the target state and its armed forces' ability to manage information and exercise effective command and control functions but also to achieve desired effects in the mind of target populations' perceptions and decision-making processes that favor Russia's interests and goals. This is a two-pronged approach that seeks to affect both the physical and the cognitive dimensions of the information environment. At the physical level, what the Russians call the *digital-technological level*, they seek to disrupt and compromise the physical dimension of the information environment by penetrating, manipulating, and destroying information networks and command and control systems. In the last decade, the Russian military has deployed multiple new electronic warfare systems, completing a similar modernization in agencies outside the armed forces, including the intelligence services.[44] Russia's increasing emphasis on information warfare is reflected in its growing investments in information warfare capabilities and structures. In 2017, Russia acknowledged the establishment of a new branch of the military—information warfare troops.[45] At the same time, at the cognitive level, the Russians have already demonstrated the ability to integrate actions in the physical dimension of operations in the information environment with actions intended to affect perceptions and decision-making processes; in other words, they are achieving effects in the cognitive dimension.[46]

Russia has a whole-of-government approach to information warfare. While information operations in the United States are seen as mostly a military activity, Russia uses a more expansive approach, including multiple government bodies and agencies and both military and nonmilitary methods and instruments. In addition, Russia considers information warfare to be an effort that involves nongovernmental players, in fact, requiring the efforts of all of society.

According to the Russian view, not just the state but the entire society is the target of foreign-led information warfare, so the society must be protected and must participate in actively resisting foreign information campaigns. The whole-of-government approach has important consequences for the nature of the Russian method. While the American military tends to focus on the capabilities of a foreign military, this approach underestimates Russia's information warfare capabilities as most of them are not organic to the Russian armed forces. While the armed forces certainly possess information warfare capabilities, particularly electronic and cyber warfare capabilities, the bulk of Russia's capabilities to target the cognitive dimension of a population and key decision makers with culturally and politically sophisticated information and messaging are to be found outside the military. And, of course, one should always include the Russian military as a whole as an information warfare tool. Military modernization, snap readiness checks, large military exercises—including multinational ones—security cooperation events with foreign militaries, and increased military presence abroad are used not only to increase readiness but also to communicate, demonstrate, and intimidate. In short, the military is not only a tool to win in a force-on-force confrontation but also a tool to affect the strategic calculations of key foreign decision makers and the attitudes and beliefs of civilian populations.[47] This is an example of the use of the military at the strategic level of information warfare.

The use of the military in shaping the strategic calculus of other states as discussed above brings about another important point. Ultimately, both the Russian and the U.S. approaches to deterring each other is about shaping the other side's thinking. The communication to the other side, however, is viewed through the perspective of the communicating country. The value of this communication depends entirely on the effect it has on the other side. Very often, however, what one side communicates to the other—through words, actions, postures, etc.—is not what the other side hears. This is why knowledge of the cognitive dimension matters—understanding the opposite side's interests, frames of reference, outlooks, and thought processes not only increases effectiveness in confrontation in the information space but also avoids dangerous misunderstandings and conflict escalations.

Russia's approach is very flexible and adaptable. Many have tried to discern patterns in how the Russians conduct information warfare as an attempt to anticipate and predict future operations. It is becoming clear that these attempts provide limited predictive value. If anything, the Russian approach does not seem to be married to a doctrine. Instead, what is evident is innovation, flexibility, adaptability, and no fear of failure. When an approach seems to be failing, the Russians quickly adopt another one.

Above all, the whole-of-government approach allows for the fourth aspect that must be taken into consideration. That is, the Russians will quickly resort to kinetic action when they see that nonkinetic methods, including those using information operations, do not work.[48] What also makes the flexible use of kinetic and nonkinetic methods possible is the Russian system of governance that, while lacking in transparency and institutional checks and balances, allows for short decision-making cycles. Of course, this type of decision making also makes it prone to miscalculations and failure to anticipate second- and third-order effects of selected courses of action.

The discussion of the Russian flexibility in the use of kinetic and nonkinetic actions is an appropriate place for a note of caution. Although information warfare is becoming an increasingly prominent method in the pursuit of national interests, the Russians have in no way forsaken the use of force as an instrument of national power. While the attention the West is paying to growing Russian activity in the information space is fully deserved, one must never ignore the fact that the most significant development in Russia's growing national power is the country's successful military modernization and the transformation of the armed forces into an effective instrument of national power. In fact, one might plausibly argue that Russia's growing military power allows it to use information warfare methods more aggressively as it feels confident enough the military possesses enough power to deter other states from responding more aggressively to information campaigns.

Russian information warfare is uninterrupted and constant, meaning that it is waged during both war and peace. While Western states tend to make a distinction between war and peace, in the Russian thinking, states are constantly engaged in a struggle for security, influence, and resources. Accordingly, even absent war, states engage in an information struggle trying to influence each other's perceptions and decision making, while also targeting populations, both domestic and foreign, trying to influence their consciousness. It is therefore no surprise that Russia sees the promotion of human rights, democracy, and Western preferences for international order as a form of warfare, targeting Russian interests and the state's social cohesion and resilience. The Russian political and military elite, for example, see any attempts to promote democracy in its neighborhood, or anywhere else for that matter, as only initial Western steps to prepare the ground for regime change that will lead to Western expansion, including a military one, in these states.

The strong strain of conspiratorial thinking that traditionally runs through Russian attitudes toward the West also promotes a normalization of information warfare as a legitimate and necessary tactic of the state. Almost anything Americans—and the West in general—say and do is often perceived as part of a nefarious propaganda campaign designed to promote Western interests and undermine Russia.[49] This campaign is believed to be constant and widespread, using diverse instruments of influence ranging from diplomatic, economic, cultural, and informational.[50] This campaign requires a Russian response, including in the information space. In a discussion on the global information environment organized by the St. Petersburg International Economic Forum in 2018, Margarita Simonyan, RT's editor-in-chief, pointed out that the global media environment has long been dominated by "Anglo-Saxon media outlets."[51] However, she asserted that the appearance of alternative media voices, including Russian ones, has challenged that status quo. This, she argued, explains why these alternative outlets have become targets of Western intelligence services and private media with ties to intelligence services.[52] Russia sees itself as being at a disadvantage, what some call "information inequality," a situation that justifies the steps taken to address this weakness, such as the proliferation of Russian state-sponsored television and radio channels (e.g., RT, Sputnik) and institutions promoting the official Russian point of view abroad.[53] The increasing Russian presence in the international information space is seen as part of Russia's return as a global power. Understanding this dynamic explains why those who hope to see an end of Russian presence in America's information space are badly misguided.

Because the Russians have a long tradition of waging information warfare, conduct it constantly, and have flexibility without many checks and balances does not automatically mean that they are very successful practitioners. It is high time we engage in a sober assessment of Russia's information warfare's effectiveness. Much of the writing on the subject tends to exaggerate the effectiveness of Russian information warfare. This is perhaps understandable in the political climate created by Russia's interference in the 2016 presidential elections. Instead, a careful study of Russia's multiple information operations must be completed in the United States and abroad. Our own study of Russian actions, granted they are confined to observations in several countries in Europe, tentatively leads us to believe that Russia has achieved only mixed successes while failures are abundant.[54]

Knowledge and information about Russian information warfare in various countries are valuable lessons; however, those lessons might not amount to a pattern that provides analytical value. The Russians tailor their approach according to their understanding of the varying vulnerabilities of target populations, context, and intended end results. How they approach a target population in Ukraine, in the European Union, and in the United States, for example, will differ. This is a good indicator that the Russians take the cognitive dimension seriously—adopting a course of action that takes into consideration the cultural, historical, ideological, and contextual factors relevant to the target population and the goals of the Russian actions.

Russia might be actively exploiting the cognitive vulnerabilities in foreign states and groups, but the country also has its own vulnerabilities. In fact, that explains why the state is active in the information environment—it sees other states and groups targeting the Russian state and society's vulnerabilities. While the West sees Russia as conducting offensive campaigns in the information space, Russia sees its actions as defensive measures. The existence of perception and misperceptions on both sides notwithstanding, the Russian state and society do have multiple cleavages and frictions that could be exploited by outside actors.

Recommendations for the Marine Corps

As the Marine Corps adapts to increase the effectiveness of its operations in the information environment, especially regarding the cognitive dimension, it is vital to study Russia's approach toward information warfare.

When confronting Russia, the Marine Corps must understand that it is not dealing solely with the Russian armed forces—let alone with one of its components—but rather with the Russian state. In addition to addressing the threats posed by information warfare capabilities organic to the Russian military, it is facing an information campaign waged by the state's intelligence services, the Ministry of Foreign Affairs, and nongovernmental actors, including the Russian Orthodox Church, patriotic organizations, independent and contracted cyber hackers and trolls, business people with ties to the Kremlin or seeking the Kremlin's favors, and criminal groups with ties and no ties to state agencies. Addressing all these actors is a tall order and the Marine Corps should not aim to do that. Instead, the focus should be to see Marine Corps information warfare efforts as an element in a larger United States, NATO, and European Union effort to confront Russia's information warfare campaigns. This also is a tall order, but the only viable option.

Furthermore, since Russian information warfare efforts target multiple populations, the Marines should be prepared to work with populations exposed to those efforts. Allied military personnel and civilian populations, too, are targets, and Marines need to develop knowledge and information about the target populations' vulnerabilities and resilience levels regarding Russian information warfare threat as well as the local institutions' own capabilities and methods to affect Russian perceptions and decision making. Simply put, knowing the Russian way of information warfare is not sufficient; the Marines must have knowledge and information about how the Russians target specific groups among the military partner or friendly population in the Marines' area of operations and how partners, in turn, fight back in the information space.

Successful operations in the information environment require mastering its most important dimension—the cognitive one. Above all, that means gaining knowledge and information about target groups' culture, history, ideologies, experiences, relationships, and influences that affect those populations' decision-making processes. Developing this knowledge is a time-consuming and expensive process, one that the military cannot hope to achieve in isolation and integrate it as an organic capability. However, there are ways to integrate the military's limited capabilities in this area with ones existing in government and nongovernmental agencies and actors.

Notes

1. Sultan-Khan Zhussip, "Russia Expands Its Military Presence in Central Asia," Radio Free Europe/Radio Liberty, 12 November 2008. It must be pointed out that after the disintegration of the Soviet Union, Russian troops never left Moldova, Georgia, and Tajikistan, where they were active participants in civil wars and after cease-fire agreements stayed as peacekeepers.
2. *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017).
3. There is a growing body of research into Russia's information warfare, along with attempts to conceptualize the country's approach. See, for example, Timothy L. Thomas, *Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations* (Fort Leavenworth, KS: Foreign Military Studies Office, Center for Army Lessons Learned, 1998); Timothy L. Thomas, "Russia's Reflexive Control: Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56, https://doi.org/10.1080/13518040490450529; Timothy L. Thomas, *Crafting an Information Warfare and Counter-propaganda Strategy for the Emerging Security Environment*, 115th Cong. (15 March 2017) (hearing before the Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services); Donald N. Jensen and Peter B. Doran, *Chaos as a Strategy: Putin's "Promethean" Gamble* (Washington, DC: Center for European Policy Analysis, 2018); Stephen Blank, "Cyber War and Information War à la Russe," in *Understanding Cyber Conflict: 14 Analogies*, ed. George Perkovich and Ariel E. Levite (Washington, DC: Georgetown University Press, 2017), 81–98; Dmitry (Dima) Adamsky, "From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture," *Journal of Strategic Studies* 41, nos. 1–2 (2018): 33–60, https://doi.org/10.1080/01402390.2017.1347872; Charles K. Bartles, "Getting Gerasimov Right," *Military Review* (January–February 2016): 30–38; Keir Giles, *Handbook of Russian Information Warfare*, Fellowship Monograph No. 9 (Rome, Italy: NATO Defense College, 2016); Keir Giles, *The Next Phase of Russian Information Warfare* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016); Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Center for Strategic and International Studies, 2016); Heather A. Conley et al., *The Kremlin Playbook 2: The Enablers* (Washington, DC: Center for Strategic and International Studies, 2019); Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: Rand, 2018), https://doi.org/10.7249/RR1772; Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: Rand, 2018), https://doi.org/10.7249/RR2237; Bettina Renz and Hanna Smith, *Russia and Hybrid Warfare—Going Beyond the Label* (Helsinki, Finland: Kikimora Publications, 2016); and Keir Giles, *Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (London, UK: Royal Institute of International Affairs, Chatham House, 2016).
4. *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: Department of Defense, 2010), 110.
5. *Information Operations*, JP 3-13 (Washington, DC: Department of Defense, 2014), figure I-1, p. I-2.
6. *Information Operations*, figure I-1, p. I-2.
7. *Marine Air Ground Task Force Information Environment Operations Concept of Employment* (Quantico, VA: Headquarters Marine Corps, 2017), 22.
8. *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, 22.

9. *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, 24.
10. *Defense Primer: Information Operations* (Washington, DC: Congressional Research Service, 2018); and Catherine A. Theohary, *Information Warfare: Issues for Congress* (Washington, DC: Congressional Research Service, 2018).
11. Theohary, *Information Warfare*, 7.
12. Title 10 Armed Forces, U. S. C. § 2241 (2012).
13. Conrad Crane, "The United States Needs an Information Warfare Command: A Historical Examination," *War on the Rocks* (blog), 14 June 2019. See also Conrad C. Crane et al., *A Return to Information Warfare* (Carlisle, PA: Historical Services Division, U.S. Army Heritage and Education Center, U.S. Army War College, n.d.).
14. Timothy L. Thomas, "Dialectical versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," *Journal of Slavic Military Studies* 11, no. 1 (1998): 40–62, https://doi.org/10.1080/13518049808430328.
15. Olga Vartanova, *Gerasimov Doctrine as an Active Measure of Russian IPb* (Quantico, VA: Marine Corps Intelligence Activity, 2017).
16. Valeriy Gerasimov, "Ценность науки в предвидении," *Военно-промышленный курьер*, 26 February 2013.
17. Gerasimov, "Ценность науки в предвидении."
18. Adamsky, "From Moscow with Coercion," 33–60.
19. Adamsky, "From Moscow with Coercion," 40–41.
20. Aleksandr Dvornikov, "Штабы для новых войн," *Военно-промышленный курьер*, 23 July 2018.
21. Gen Valery Gerasimov, Russian Federation Armed Forces, "Contemporary Warfare and Current Issues for the Defense of the Country," trans. Dr. Harold Orenstein, *Military Review* (November–December 2017): 24.
22. Gen Valery Gerasimov "Мир на гранях войный," *Военно-промышленный курьер*, 13 March 2017.
23. One may argue that the American concept of gray zone conflicts (a.k.a. competitive zones) is a partial attempt to address the Russian understanding of the struggle between states, which makes no clear-cut distinction between peace and war as it exists in Western military thinking.
24. *Competition Continuum*, Joint Doctrine Note 1-19 (Washington, DC: Joint Chiefs of Staff, 2019). See also *Joint Concept for Integrated Campaigning* (Washington, DC: Joint Chiefs of Staff, 2018).
25. *Russian National Security Strategy* (Moscow: Russian Federation, 2015).
26. *Russian National Security Strategy*, 21–22.
27. *The Foreign Policy Concept of the Russian Federation* (Moscow: Ministry of Foreign Affairs, 2016).
28. Vladimir Putin et al., *First Person: An Astonishingly Frank Self-Portrait by Russia President Vladimir Putin*, trans. Catherine A. Fitzpatrick (New York: PublicAffairs, 2000).
29. *The Military Doctrine of the Russian Federation*, No. Pr.-2976 (Moscow: Russian Federation, 2014).
30. *Russian Federation Armed Forces' Information Space Activities Concept* (Moscow: Ministry of Defence of the Russian Federation, 2000).
31. Dmitrii Rogozin et al., "Информационная война," in *Война и Мир в Терминах и Определениях* (Bucharest, Romania: Veche Publishing House, 2011) (authors' translation).
32. See for example, Leonid Savin, "Информационная война. Исторический экскурс и позиция России," *Gepolitika*, 21 March 2018.
33. For an excellent summary of Russia's strategic thinking, see Dmitri Trenin, "Russia's Threat Perceptions and Strategic Posture," in R. Craig Nation and Dmitri Trenin, *Russian Security Strategy under Putin: U.S. and Russian Perspectives* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2007): 35–47. See also Dmitry Gorenburg, "Circumstances Have Changed Since 1991, but Russia's Core Foreign Policy Goals Have Not," *PONARS Eurasia*, January 2019.

34. Vladimir Ilyich Lenin, *Imperialism: The Highest Stage of Capitalism* (Rookhope, UK: Aziloth Books, 2018).

35. Very early on, Soviet leaders recognized that taking on capitalist states head-on might be a tall order and adopted foreign policy accordingly while still believing in the inevitable violent clash with the capitalist world. See Jon Jacobson, *When the Soviet Union Entered World Politics* (Berkeley, CA: University of California Press, 1994).

36. Frederic J. Fleron Jr. et al., eds., *Classic Issues in Soviet Foreign Policy: From Lenin to Brezhnev* (New York: Aldine de Gruyter, 1991).

37. Viktor Hudoleev, "Военная наука смотрит в будущее," *Krasnaya Zvezda*, 26 March 2018.

38. See chapter 3 in Vladimir Ilyich Lenin, "What Is to Be Done?: Burning Questions of Our Movement," Marxists Internet Archive, 1999.

39. The 22d Congress of the Communist Party of the Soviet Union, for example, adopted the "Moral Code of the Builder of Communism," the foundation of a superior ethical system aimed at further instilling Communist morality among citizens. See Deborah A. Field, "Moral Code of the Builder of Communism," Seventeen Moments in Soviet History. See also Herschel and Edith Alt, *The New Soviet Man: His Upbringing and Character Development* (New York: Bookman Associates, 1964); and Jay Bergman, "The Idea of Individual Liberation in Bolshevik Visions of the New Soviet Man," *European History Quarterly* 27, no. 1 (1997): 57–92, https://doi.org/10.1177/026569149702700103.

40. For a few examples, see *Department of Defense Strategy for Operations in the Information Environment* (Washington, DC: Department of Defense, 2016); *Joint Concept for Operating in the Information Environment (JCOIE)* (Washington, DC: Joint Chiefs of Staff, 2018); *Information Operations*; and *Military Deception*, JP 3-13.4 (Washington, DC: Department of Defense, 2012).

41. *Information Security Doctrine of the Russian Federation*, No. 646 (Moscow: Ministry of Defence of the Russian Federation, 2016).

42. See, for example, Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks* (blog), 11 March 2016.

43. See, for example, Margarita Levin Jaitner and Harry Kantola, "Applying Principles of Reflexive Control in Information and Cyber Operations," *Journal of Information Warfare* 15, no. 4 (Fall 2016): 27–38; and Thomas, "Russia's Reflexive Control Theory and the Military," 237–56.

44. On the modernization of the Russian electronic welfare capabilities, see Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Eesti, Estonia: International Centre for Defence and Security, 2017).

45. Vladimir Isachenkov, "Russia Military Acknowledges New Branch: Info Warfare Troops," Associated Press, 22 February 2017.

46. See, for example, a report by Col Liam Collins on examples of Russia's successful use of fires and information operations. Col Liam Collins, "Russia Gives Lessons in Electronic Warfare," Association of the United States Army, 26 July 2018, 18–19.

47. Russia's large Vostok-2018 military exercise, which also included Chinese troops, was meant to demonstrate close ties between the two countries, both of which see the United States as a threat. The message was not lost on the West. See "Russia and China Hold the Biggest Military Exercises for Decades," *Economist*, 6 September 2018.

48. Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: Rand, 2017), https://doi.org/10.7249/RR1498.

49. Serghei Golunov and Vera Smirnova, "Proliferation of Conspiracy Narratives in Post-Soviet Russia: The 'Dulles' Plan' in Social and Political Discourses," *Acta Slavica Iaponica*, no. 37 (2016): 21–45.

50. *Doctrine of Information Security of the Russian Federation*.

51. RT is a Russian international television network funded by the Russian government.

52. "«Сбалансировать картину мира»: в рамках ПМЭФ проходит обсуждение современных источников информации," RT, 24 May 2018, 1:18:26 video.

53. “Информационное неравенство: как сбалансировать информационную картину мира,” St. Petersburg International Economic Forum 2018, 24 May 2018.

54. See, for example, Ben Nimmo, “Failures and Adaptions: Kremlin Propaganda in Finland and Sweden,” Foreign Policy Centre, 21 March 2017.