Russian New Generation Warfare

Deterring and Winning the Tactical Fight

James Derleth, PhD

In the twenty-first century we have seen a tendency toward blurring the lines between the states of war and peace. …

… The very "rules of war" have changed. The role of nonmilitary means of achieving political strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. …

… Frontal engagements of large formations of forces at the strategic and operational levels are gradually becoming a thing of the past. …

… Asymmetrical actions have come into widespread use, enabling the nullification of an enemy´s advantages in armed conflict. Among such actions are the use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected. …

… The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased.

—Gen. Valery Gerasimov,
Chief of the Russian General Staff

The Russian view of deterrence is based on the integrated use of nonmilitary, conventional, and nuclear instruments.[1] In contrast, the traditional Western conceptualization of deterrence is based on the deployment and employment of conventional and nuclear forces.[2] A crucial difference is that Russia does not believe deterrence stops after the outbreak of conflict. It will continue to apply these instruments throughout all stages of a political-military crisis in an attempt to control escalation and ensure conditions favorable to Russia. Therefore, to foster deterrence and to prevail if deterrence fails, the United States must have the capability to counter instruments across all areas (nonmilitary, conventional, nuclear), at all levels (tactical, operational, strategic), and throughout all phases of a conflict.[3] Although the U.S. Army faces complex, dynamic, multi-domain challenges in the contemporary operational environment (OE), it has largely focused its education and training on deterring, and if necessary, defeating near-peer adversaries in large-scale combat operations (LSCO). As seen from Crimea to Georgia, the focus on higher-level conventional and nuclear forces' deterrence has allowed Russia to achieve its national objectives through a variety of nonlethal instruments.

Since employment of conventional and nuclear systems is already part of the Army's education and training, it is important to note that nonlethal instruments such as information warfare (IW) have not been integrated into education and training; however, they would significantly affect the ability of tactical formations to deter or win if conflict occurs.[4] Traditionally, in U.S. military doctrine, information activities have been viewed in a supporting role by facilitating and enabling

"I took this photo while on a mission to Georgia that coincided with the anniversary of VE Day. In Russian, I asked the pensioners if they spoke English. They didn't. I then asked how they could make a sign in English if they didn't speak English. They said 'friends' made the signs for them. For me, a very powerful image showing the pervasiveness of Russian information warfare. What would our forces do if confronted by this group while supporting Georgia in a conflict against Russia?"

—James Derleth

A pro-Russian, anti-NATO demonstration on Victory in Europe (VE) Day 9 May 2019 in front of The Joseph Stalin Museum in Gori, Georgia. (Photo by author)

combat operations. In contrast, Russia has always had a holistic and integrated approach to IW.[5] The revolution in information technology has only strengthened this perspective. Russian military leaders believe that a conflict's decisive battles are in the information domain and that information operations in the early phases are more decisive than later conventional warfare. IW, as the decisive form of maneuver, targets an adversary's vulnerabilities and center of gravity, with lethal operations executed to produce an information effect rather than delivering a lethal effect.[6] In this way, the roles of the two domains have been reversed. Rather than a supporting operation, information campaigns have become the supported operation.[7] Consequently, information superiority is central to enhancing the utility of tools across all domains in all phases of a conflict.[8] Without it, it is impossible to prevail in combat. IW can create or leverage local military and political support, discredit leadership, slow decision-making, nurture dissent, shape public opinion, foster or manipulate local sources of instability, and mobilize local populations against foreign forces; all of these minimize the likelihood of lethal engagements or improve their likelihood of success.[9] In summary, IW

can be a prelude to armed conflict, a preparation of the battlefield preceding the deployment of forces, or an end in itself, through which Russia and other adversaries weaken superior U.S. forces without firing a shot.

Although Army doctrine notes that "in modern conflict, information has become as important as lethal action in determining the outcome of operations," soldiers in tactical formations have a limited ability to understand or influence the information environment (IE).[10] Notably, doctrine is based on the assumption that IW will only be executed at operational or strategic levels. This is questionable given the contemporary threat environment.[11] Since tactical formations will be significantly impacted by enemy IW regardless of the phase of the conflict, they must have the capability to understand and influence the IE. Without this capability, adversaries will continue to frame the conditions of future competition and conflict.

The Threat: A Vignette

A national election in Estonia saw a nationalist pro-Estonian party take control of the government.[12] Frustrated by the election outcome and lack of citizenship, the ethnic Russian minority—20 percent of the population—demonstrated against the government. The Russian government released statements of support; launched a covert campaign to shape perceptions with more than two hundred thousand Twitter accounts sending 3.6 million tweets using #protectRussiansinEstonia; and initiated snap exercises by Russian ground, naval, and air forces in the region.

A week later, a group of demonstrators gathered in the town square of Narva, a town in eastern Estonia on the border with Russia. Complaining their human rights had been violated, the demonstrators demanded autonomy for Narva, official status for the Russian language, and Estonian citizenship. When Estonian police moved in to break up the demonstration, they were confronted by an armed group of Russian-speaking, military-age men. Fearing the loss of innocent lives, the police left the area. At the same time, a group of armed demonstrators attacked the Estonian border post with Russia, forcing it to be abandoned. A third group of demonstrators took over the local telecommunications center (cutting internet, radio, telephone, and television traffic to and from Narva), surrounded the police station, and stormed the town hall, forcing Mayor Tarmo Tammiste to resign. Georgi Zhukov, a spokesman for the demonstrators, declared the establishment of the Narva People's Republic. He asked Russia for assistance "to ensure peace and public order against nationalists and fascists." These actions were supported by a series of cyberattacks that overwhelmed the Estonian government, economy, news, telecommunication, and military networks throughout the country. The cyberattacks crippled the government's command-and-control capability as well as its ability to communicate with its population and allies. The cyberattacks included the release of videos that purportedly showed Estonian security forces massacring Estonian residents of Russian descent. These products proliferated across the internet via bots, stoking anti-Estonian and anti-U.S. opinion among Russian-sympathetic and nonaligned populations across Europe. The Estonian government declared the establishment of the Narva People's Republic illegal and demanded the return of control to elected officials.

A week after the border post was abandoned, Estonian intelligence estimated that a few hundred people in military uniforms without insignia entered the region from Russia. In response, the Estonia government called an emergency meeting of the North Atlantic Council (NAC) to invoke the collective defense provision (Article 5) of the North Atlantic Treaty. The NAC refused Estonia's request due to a lack of clarity regarding the nationality of the armed group and origins of the cyberattacks. Despite the NAC's refusal, the United States agreed to deploy the 2nd Cavalry Regiment (2CR) to Estonia. Its mission was to support the Estonian army,

James W. Derleth, PhD, is the senior interagency training advisor at the Joint Multinational Readiness Center in Hohenfels, Germany. His responsibilities include educating and training civilian and military personnel in Russian new generation warfare, stability operations, and civil-military operations; integrating contemporary security challenges into exercises; and interacting with diplomatic missions, international organizations, and nongovernment organizations to integrate them into training. He earned an MA from The American University and a PhD from the University of Maryland in 1990.

local security forces, and the local government in achieving the following four objectives:

- preserve Estonian territorial integrity,
- support Estonian government legitimacy,
- foster internal security, and
- prevent the conflict from escalating.

As 2CR prepared to roll out of its garrison in Vilseck, Germany, several videos, purportedly showing the sexual assault of several underage German nationals by U.S. personnel, surfaced on social media. The videos appeared to implicate key leaders within the regiment, prompting German political authorities to call for an investigation. Local citizen protests erupted outside the gates of the 2CR garrison, delaying the unit's deployment.

During 2CR's road march, there were electronic warfare attacks on its communication network that limited its soldiers' abilities to communicate among themselves and with local security forces. Targeting U.S. and European antiwar groups, untraceable "patriotic" social media posted videos of ethnic Russians' livestock and crops being damaged and the disruption of essential services (water, electricity, sewerage) in Narva. These messages shifted U.S. and European public opinion from opposing aggression to supporting citizenship and the use of Russian language for minority residents of Estonia.

Upon its arrival in Estonia, 2CR moved to its cantonment area in Jõhvi, fifty kilometers northwest from Narva. The day after 2CR arrived, an unidentified, unmanned aerial vehicle was spotted overflying the 2CR base. Shortly afterward, soldiers' cell phones were unable to access the local cellular network, and they began receiving text messages telling them to leave the area to prevent their "destruction."

In summary, *before* 2CR reached its cantonment area, the enemy had executed multi-domain operations that established information dominance, created local and international opposition to its presence, limited its ability to communicate with the local government or its formations, fostered civil unrest, and controlled key infrastructure. Russia's decisive operation of IW began as 2CR, with its limited IW capabilities, training, and education, arrived with their lethally focused formations. In other words, 2CR forfeited the initiative to Russia before the first Stryker rolled out the gate. This significantly limited the 2CR commander's combat power and ability to execute his or her mission.

> "The roles of the two domains have been reversed [lethal operations versus information operations]. Rather than a supporting operation, information campaigns have become the supported operation."

This is not a hypothetical threat! The relationship between contemporary warfare and IW can be clearly seen in the Russian takeover of Crimea in February 2014. IW operations included engaging local people through interviews, "surveys," referendum rallies, and pro-Russian gatherings; mass dissemination of posters, brochures, leaflets, and text messages; severing fiber-optic cables; taking control of the Simferopol internet exchange point; disabling Ukrainian television facilities and replacing them with Russian channels; electronic warfare attacks on Ukrainian military communications; defacement of Ukrainian and NATO websites; the release of telephone recordings and email correspondence between Ukrainian, European Union, and U.S. officials; the creation of fake websites in which Russia targeted Ukrainian military units using soldiers' social media accounts; the use of real websites (Facebook, Twitter, Odnklassniki, Vkontakte) to spread panic and rumors; and distributed denial-of-service attacks that sent thousands of text messages and telephone calls to military and civilian leaders' cell phones to prevent them from communicating and responding to Russian actions. This information dominance also ensured that only Russian-sourced information was available, resulting in a significant percentage of the population welcoming Russian troops. These actions, combined with nonlethal Spetsnaz reconnaissance and destabilization actions, broke the morale and combat effectiveness of the Ukrainian military, leading to the surrender of sixteen

thousand soldiers.[13] This was an excellent example of multi-domain operations extending across the entire information spectrum. Consequently, Russia was able to manipulate Ukrainian perceptions, prevent a military response, influence its decision-making process, foster distrust in the government, and limit its strategic behavior while minimizing the use of lethal force.

Challenges

The Army has belatedly realized the next generation warfare challenge and is reorganizing Army Cyber Command to synchronize Army capabilities in order to "change how we conduct Information Warfare."[14] This will be accomplished by "integrating and employing Intelligence, Information Operations, Cyber, Electronic Warfare, and Space capabilities to provide Combatant Commanders with options to compete below the level of armed conflict."[15] While important goals, there are many challenges to implementing this guidance at the tactical level. Based on observations at the Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany, they include the lack of understanding of the IE; failure to integrate the IE into the operations process; inability to integrate force multipliers; ineffective civilian partner coordination; reluctance to acknowledge that physical actions have informational effects; and a lack of doctrine, education, and training that would allow formations to mitigate enemy actions in order to regain tactical and operational initiative.

Lack of understanding of the IE. While formations are adept at identifying lethal threats, they have a limited understanding of nonlethal ones that can have an even larger impact on maneuver. Future conflicts will occur in and among a connected population in a complex IE. Without improving situational awareness, combat power will be degraded. Although commanders need to understand and influence the IE, the staff section tasked with understanding the OE (intelligence) is focused on enemy groups and actions that could have lethal consequences. Consequently, the IE is neglected. Commanders do not establish priority intelligence requirements or use standard templates to understand the IE. They rationalize this by simplifying the battlespace and applying a narrow view of the worst-case scenario that has enemy forces overrunning their own formations. Unfortunately, modern conflict is not a simple "either/or." Formations that do not understand the IE are "blind" as to how they are perceived by the population and how they are portrayed by the enemy. This blindness limits a formation's ability to gain information about enemy forces and positions and to identify enemy supporters or special operations forces behind the space where ground troops operate. As an illustration, to protect its communications, a rotational unit (RTU) in a recent JMRC training exercise decided to use the Secret Internet Protocol Router Network (SIPRNet) as its primary communication medium. The result was that while the unit could communicate securely internally, because unclassified information systems had been neglected, the RTU had no understanding of the local environment. This lack of understanding resulted in local demonstrations that restricted the unit's main supply routes, internally displaced people interfering with its maneuver, and forewent a wealth of actionable information gathered by internally displaced people as they fled from the enemy. This lack of visibility and understanding of the IE directly impacted the RTU's combat power.

Failure to integrate the IE into the operations process. The goal of the operations process, as stated in Army Doctrine Publication 5-0, *The Operations Process*, is to understand, visualize, and describe the operational environment; make and articulate decisions; and direct, lead, and assess military operations.[16] Observations from JMRC continue to show that tactical formations are unable to integrate an understanding of the IE into operations. This is the result of commanders not understanding the IE or viewing their actions only through a physical lens.[17] This lack of understanding is compounded by a platform-centric, enemy weapon system/lethality-focused staff structure. For example, a staff can easily target an enemy tank formation but is challenged to target an enemy social media site that is instigating demonstrations on main supply routes. Consequently, formations cannot identify or support friendly information-related capabilities (IRC), identify and target enemy IRCs, or integrate this information into operations and plans. This is part of a larger institutional challenge, namely, that "victory" can only be won with lethal combat operations.

Inability to integrate force multipliers. U.S. Army doctrine emphasizes the commanders' responsibility for operating across all domains, including the IE. However, tactical formations lack many organic

Russia's "little green men" facilitating the annexation of the Ukrainian peninsula of Crimea in February 2014. Armed with modern Russian small arms and equipment, these personnel were a mix of Russian special forces and other elite Russian units who wore unmarked green uniforms. Russia initially claimed that the little green men were local Ukrainian patriotic militias sympathetic to Russia's claims regarding Crimea. They seized and occupied the Simferopol Parliament and numerous Crimean military bases, and blockaded the Simferopol International Airport to prevent the arrival of Ukrainian government forces. Simultaneously, Russia engaged in a broad hybrid warfare global campaign using a wide variety of instruments including diplomacy, economic warfare, electronic warfare, cyberattacks, propaganda, and focused violence to achieve its objectives. Western countermeasures and responses have been largely ineffective against the Russian fait accompli. (Screenshot from Hromadske.tv)

information-related capabilities. When deployed, tactical formations are given force multipliers such as civil affairs (CA) and psychological operations (PSYOP) units. However, these and other force multipliers (public affairs officers [PAO], electronic warfare officers [EWO], etc.) are often unable to influence the IE. There are several reasons for this situation, but two stand out:

1. Force multipliers do not work with tactical formations until an exercise or deployment. Since they are not organic to the staff and have had limited interaction with it, it is a challenge for them to integrate their knowledge of the OE knowledge into operations. This is partially the result of home-station training areas and ranges not replicating the multifaceted, dynamic, IE found in modern conflicts. Typically, commanders create their own opposing forces that lack enemy information warfare capabilities. Thus, they do not understand how force multipliers can facilitate their operations. The consequence: units that live, eat, and breathe lethality at home are immersed into drastically different, realistic environments during exercises or deployments. However, they have no or limited training to win in them.
2. Force multipliers do not create products linked to the commander's intent and operational goals. Too often, force multipliers' products are linked to their narrow military operational specialty rather than to a commander's end states.[18] For example, the

civil affairs annex that should doctrinally "describe how civil affairs operations, in coordination with other military and civil organizations, supports the concept of operations described in the base plan or order" often simply lists aspects of the civil situation (areas, structures, capabilities, organizations, people, and events).[19] Since commanders do not see these things tied to their intent, force multipliers are often assigned other duties such as guarding the tactical operations center or emplacing obstacles. A related challenge is the inability of force multipliers to break out of their "cylinders of excellence." At JMRC, we often notice that because they define their missions narrowly, the IRCs (CA, PAO, PSYOP, etc.) do not synchronize their activities, limiting their effect. In contrast, the United Kingdom's 77th Brigade combines these capabilities in information, activity, and outreach teams that "support the military objectives of Commanders … using non-lethal engagement and legitimate non-military levers as a means to adapt behaviours of the opposing forces and adversaries."[20]

Ineffective civilian partner coordination. Russian IW is focused on delegitimizing adversaries' military and political structures. However, because of operational timelines, limited technical competence, and lack of legal authority, U.S. tactical formations are often unable to mitigate the effects of enemy IW. To mitigate these limitations, a whole-of-government approach is required. International organizations, nongovernmental organizations, local governments, media, and marketing agencies can all support and/or execute tactical information activities. The failure of tactical formations to identify civilian partners (CP) and integrate their knowledge and expertise into operations limits their ability to maneuver and consolidate gains. Although there are numerous reasons for this situation, key factors include not identifying CP in the OE and not understanding CP capabilities and capacities.

Reluctance to acknowledge that IW impacts maneuver. There has been a dramatic shift in contemporary military operations as a result of globalization, diffusion of military-related technologies, and an information revolution. Despite that, the current emphasis on LSCO has caused commanders to focus on the maneuver aspects of offensive and defensive operations. Even though the manipulation of information can create denial effects and is doctrinally a form of fires, commanders have not applied the necessary staff resources and leadership emphasis to the cognitive aspect of operations.[21] This lack of applied resources can have numerous consequences that limit the ability to conduct multi-domain operations. This includes allowing the enemy to set conditions, neutralizing military superiority, limiting the ability to employ force, and creating a negative public image for both friendly and enemy audiences.

Lack of counter-new generation warfare (NGW) education and training. Traditional and contemporary Army education and training is focused on major combat operations against the armed forces of a peer or near-peer state. Notwithstanding, despite the lack of success in Vietnam, Afghanistan, Iraq, Libya, Mindanao, Syria, and trans-Sahel, there is a continuing belief that if the Army can effectively execute LSCO, it can win any conflict. This belief has three significant flaws. First, as those conflicts showed, applying LSCO education and training in non-LSCO operations invariably forces widespread and costly adaptation, endangering mission success. Second is the common assumption that the next clash will be a great-power conventional conflict. As former Secretary of Defense James Mattis was fond of pointing out, the enemy also "gets a vote." Aware their militaries cannot win a conventional battle against the United States, adversaries such as China, Iran, and Russia are heavily investing in asymmetrical resources to exploit American vulnerabilities. Third, the Army's desire to focus on traditional threats does not change the reality that a host of nonstate actors continue to foster unrest throughout the world, undermining regional stability and threatening U.S. interests. Data shows that most armed conflicts today are internationalized civil or substate conflicts rather than conventional interstate wars.[22]

To win tomorrow's conflicts, the Army must revise its education and training. Although some combat training centers have created and integrated a complex and dynamic IE into their exercises, too often it is ignored or its value is diminished so it does not "interfere with other training objectives." Consequently, RTUs are not receiving a realistic training experience. A good rule of thumb for measuring progress would be assessing whether an RTU is expending equal or greater resources to IE operations as physical operations. While this would be a measure of performance rather than a measure of effect, it would at least force commanders to try and integrate IE operations into planning.[23]

Sgt. Camille Coffey (*left*), Spc. Victorious Fuqua (*center*), and Spc. Mark Osterholt, all cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), conduct offensive cyber operations as part of the Cyber-Electromagnetic Activities Support to Corps and Below program 18 January 2018 during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center Rotation 18-03 at Fort Irwin, California. (Photo by Steven Stover, 780th Military Intelligence Brigade Public Affairs)

Another challenge is the lack of counter-NGW education to train leaders to defeat multi-domain operations like Russia's annexation of Crimea. Other than a course created at JMRC, the author is unaware of any other U.S. or NATO course that trains tactical formations to defeat NGW tactics.

Understanding and Influencing the IE

While many of these challenges are the result of decisions and polices made at higher levels, tactical formations will have to deal with their ramifications. Consequently, what can they do to win in the contemporary information environment? There are many things that can be done, including home-station education, force multiplier integration at the Leadership Training Program (LTP), predeployment IE analysis, modifying the task organization, integrating CP into staff processes, putting a senior leader in charge of integrating force multipliers and CP, and fostering commander involvement.

Home-station education. Realizing that RTUs lack counter-NGW warfare training, JMRC created a three-day program of instruction and a mobile training team to deliver it at home station. Unfortunately, most RTUs decline the opportunity, which means they have limited or no experience understanding OE or defeating nonlethal threats before their deployments to training centers or to real-world missions. Formations that do not train for realistic contingencies put themselves at a tremendous disadvantage. Similar to the situation during the Afghanistan and Iraq wars (when a counterinsurgency mobile training team was sent to every deploying brigade), a simple fix would mandate that every RTU take the counter-NGW or a regionally based variant course before going to a combat training center. This is especially important since NGW is based on a state of permanent conflict.

Students from Resident Elective Course A350, Decisive Action Tactical Application, plan large-scale combat operations in a class exercise 14 May 2019 at the Command and General Staff College (CGSC) at Fort Leavenworth, Kansas. There is a continuing belief that if the Army can effectively execute large-scale combat operations, it can win any conflict. (Photo by M. Shane Perkins, CGSC instructor)

Foster enabler integration at the Leadership Training Program. Since many of the force multipliers are reservists, they are often not included in rotational unit LTPs. Therefore, they do not start working with their supported unit until they are deployed. This makes it difficult for them to synchronize with brigade staffs and demonstrate their value to commanders focused on lethal threats. To mitigate this challenge, the 353rd Civil Affairs Command mandated that all of its formations (1) must take JMRC's counter-NGW course before deployment to the Europe Command theater and (2) representatives from the deploying battalion must attend rotational planning conferences and the LTP. This allows them to start working with their supported unit early and show their value to the team.

Predeployment information environment analysis. Just as units should identify enemy formations in their OE before they deploy, they should also identify enemy information operations that have been shaping the OE before they arrive. At a minimum, this analysis should include key allied and enemy IRCs, information on how the enemy is influencing OE, possible courses of action to negate enemy activities that could impact combat operations, and measures of effect that would show the success of counter-information operations.

Modifying the task organization. Since the IE is global and constantly evolving, understanding it is a more complex challenge than understanding the physical environment. Thus, more staff resources must be dedicated to understanding the IE. Focusing on the "effect" to be achieved (e.g., degrading enemy combat power, fostering freedom of maneuver, and prioritizing information-related priority intelligence requirements) will facilitate change. During an OE after action review, the RTU commander who used SIPRNet as his or her communication medium realized SIPRNet had numerous unintended consequences that limited his or her combat power. To mitigate this problem, the commander created an "engagement cell" that included not only the usual suspects (PAO, CA, EWO, PSYOP) but also intelligence and operations. The engagement cell included staff members to ensure the former's information was included in planning and targeting. To foster integration and improve the ability to target nonlethal threats, the commander also had JMRC's mobile training team deliver their counter-NGW course to the cell.

Integrating civilian partners into staff processes. Because CP will already be operating in areas where a unit will deploy, they will have local contacts, expertise, and capabilities to shape or counter-shape the IE. However, too often this opportunity is wasted because formations fail to identify CP and integrate them into operations. A simple way to mitigate this challenge is to ensure they are included in the staff processes. For example, doctrinally, there should be an Information Operations Working Group (IOWG) at brigade. Integration into the IOWG would allow CP to identify the enemy narrative and develop messaging to defeat it as well as to identify nonlethal targets for the targeting process. CP involvement in operations can also be facilitated through the existing fires architecture. When commanders want to deliver lethal effects, they simply tell their fires coordinator the effect they want to achieve. The well-established system then executes the task. If commanders provided the same guidance for nonlethal/information effects, and since brigades lack capability and capacity in the information space, the fires coordinator would have to use the CP and force multipliers to achieve the desired effect.

Putting a senior leader in charge of nonlethal activities. RTUs who have had the most success in multi-domain operations have tasked a senior leader—usually the deputy brigade commander or brigade executive officer, to oversee the integration of information into operations. While other staff officers are doubtless capable, they lack the rank to integrate force multipliers and CP into brigade operations.

Involve commanders. The most important way to win the information war is to ensure commanders at all levels know that this battle is the "commanders' business." Leaders must understand how the IE can either facilitate—or limit—their ability to conduct the multi-domain operations required to achieve desired end states. A good place to start would be evaluating commanders not only on their gunnery scores but also on their ability to execute multi-domain operations in the contemporary OE.

Summary

The dichotomy of war and peace is no longer a useful construct for thinking about national security or tactical operations. We are in a state of competition and conflict that is continuous and dynamic. As a number of adversaries have demonstrated, they can achieve their national interests short of conflict with nonlethal operations centered around information warfare. Writing in the Russian journal *Military Thought*, I. Vorobyev and V. Kiselyov noted, "Information is now a type of weapon. It does not simply compliment fire strikes and maneuvers, it transforms and unites them." Thus "information is becoming *an armed struggle in its own right* [emphasis in the original]."[24] To defeat multi-dimensional threats, U.S. tactical formations must be able to understand and influence the IE. Although the Army has belatedly started to realize the existence of the information competition/conflict continuum, it has focused its attention and resources in support of LSCO.[25] However, the nature of emerging threats (e.g., precision long-range fires, multilayered air defense systems, drones, electronic warfare, cyberattacks, etc.) suggests that future military operations will be conducted by tactical units. That is why in contrast to U.S. policy, Russia has been modifying its force structure away from divisions to lower-level (brigade and battalion) formations. Russia believes that success in the contemporary operating environment requires lower-level formations to have a degree of autonomy and capability to perform a variety of missions as the factors noted above will severely limit the ability of higher echelons to support them. This includes "psychological warfare and information confrontation sub-units."[26] Until the Army recognizes that the information space is not only a domain of conflict but also the center of gravity, we will face two stark alternatives: tolerate nonconventional challenges or escalate them to armed conflict. This leaves the United States at a tremendous disadvantage against adversaries who have weaponized information to influence and shape interactions across domains in support of integrated tactical combined arms maneuver. ■

Notes

Epigraph. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Voyenno-Promyshlennyy Kurier* (Military-industrial courier), 26 February 2013, accessed 12 May 2020, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

1. Russian Federation Ministry of Defence, *Military-Encyclopedic Dictionary* (2015), accessed 28 May 2020, http://encyclopedia.mi1.ru/encyclopedia/dictionaryIdetails_rvsn.htm ?id=14206@morfDictionary, cited in K. Ven Bruusgaard, "Russian Strategic Deterrence," *Survival: Global Politics and Strategy* 58, no. 4 (2016). See also Okke Geurt Lucassen, "In Between War and Peace: The Conceptualization of Russian Strategic Deterrence," UPTAKE Working Paper No. 16/2018 (Tartu, Estonia: University of Tartu Press, 2018), 10, accessed 28 May 2020, http://www.uptake.ut.ee/wp-content/uploads/2019/03/Okke_Lucassen_WP2.pdf. Strategic deterrence "is the collective of instruments, using soft and hard power, by employing (dis-)information, cyber, economic, military, and political tools, both offensively and defensively, continuously regardless of peace or war-time, in pursuit of deterring violent conflict, de-escalation (or early cessation) of military conflict, or stabilizing military-political situations in (potential) adversary (coalitions of) states of interest, on favorable conditions for the Russian Federation."

2. Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

3. Gerasimov, "The Value of Science Is in the Foresight." Gerasimov notes that contemporary operations follow a roughly 4:1 ratio of nonmilitary and military measures with nonmilitary competition under the control of military formations using information operations, private military organizations, special operations forces, and internal protest potential. This view has two significant ramifications: first, the West considers nonmilitary measures as ways to avoid war while Russia considers them weapons of war (see Charles Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 [2016]: 34); and second, tactical formations will be faced with a myriad of nonlethal challenges that will affect their combat power and ability to maneuver.

4. See Catherine Theohary, "Information Warfare: Issues for Congress," Congressional Research Service (CRS) Report No. R45142 (Washington, DC: CRS, 2018), accessed 28 May 2020, https://crsreports.congress.gov/product/pdf/R/R45142/5. Unlike information operations (IO), information warfare (IW) is not defined in U.S. military doctrine. This article uses IW to describe the execution of offensive and defensive actions in the information domain to compel opponents to succumb to one's will through the use of cyber operations, psychological operations, electronic warfare, operations security, and military deception.

5. "Convention on International Information Security," Ministry of Foreign Affairs of the Russian Federation, 27 September 2011, accessed 20 May 2020, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666. See also *On Russia's Information War Concepts before the House Armed Services Subcommittee on Emerging Threats and Capabilities*, 115th Cong., 1st sess. (2017) (statement of Timothy Thomas), accessed 20 May 2020, http://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf. A 2011 Russian strategy document, the "Convention on International Information Security," defines IW as a "conflict between two or more States in information space with the goal of inflicting damage to information systems, processes, and resources, as well as to critically important structures and other structures; undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents." In the military realm, the goal of IW is to (1) to achieve political objectives without the use of military force and (2) shape a favorable international response to the deployment of its military forces, or military forces with which Moscow is allied. Information "weapons" are the technology, means, and methods used in information warfare.

6. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 2012, incorporating Change 1, 2014), ix. According to the doctrine, Information operations are "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." Per this definition, IO is focused on coordination and synchronization only during military operations and relies on other capabilities to deliver effects. Monica Ruiz, "Impacts of Russian Information Operations: Technical and Psychological Aims," International Centre for Defence and Security, 24 October 2017, accessed 13 May 2020, https://icds.ee/impacts-of-russian-information-operations-technical-and-psychological-aims/. In contrast, Russia's holistic approach to IW is divided into two components: "information-technical," which aligns with the Western definition of electronic and cyberwarfare and is centered on technical capabilities; and "information-psychological," which resembles the NATO concept of strategic communications and psychological operations, centered on influence operations.

7. Keir Giles, "Delivery of Information Effects by Russian Special Forces and Intelligent Agencies" (working draft).

8. Sergei Modestov, "Strategicheskoe sderzhivanie na teatre informatsionnogo protivoborstva," *Vestnik Akademii Voennykh Nauk*, no. 1 (2009): 26, cited in Dmitry (Dima) Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy," Proliferation Papers 54 (Paris: Institut français des relations internationales [ifri], November 2015), accessed 13 May 2020, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. In the Russian view, the information campaign blurs the line between war and peace, front and rear, levels of war (technical, operational, strategic), forms of warfare (offense and defense), and forms of coercion (deterrence and compellence).

9. See Adamsky, "Cross-Domain Coercion," 24; Gerasimov, "The Value of Science Is in the Foresight"; Margarita Jaitner, "Russian Information Warfare: Lessons from the Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cyber Defence Centre of Excellence, 2015), 91, accessed 13 May 2020, https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf. This can be accomplished with disinformation, misinformation, cyberattacks, digital sabotage, etc. The importance of gaining information superiority in warfare can be seen in how much time and resources have been spent in creating official, semiofficial, and unofficial sources of war-related information, including dedicated YouTube channels.

10. Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2017), para. 2-113. For additional information, see JP 3-13, *Information Operations*, ix–x.

11. It is not clear how cyberattacks, electronic warfare, long-range precision fires, drones, etc., would allow higher echelons to communicate with, let alone execute tactically relevant information warfare operations.

12. Adapted from "Weaponized Information: One Possible Vignette," *Mad Scientist Laboratory* (blog), U.S. Army Training and Doctrine Command, 7 November 2019, accessed 13 May 2020, https://madsciblog.tradoc.army.mil/190-weaponized-information-one-possible-vignette/.

13. See Vladimir Sazonov, Kristiina Müür, and Igor Kopõtin, "Methods and Tools of Russian Information Operations Used Against

Ukrainian Armed Forces: The Assessment of Ukrainian Experts," ENDC Occasional Papers No. 6/2017 (Tartu, Estonia: Estonian National Defence College [ENDC], 2017): 59; Oscar Jonsson and Robert Seely, "Russian Full Spectrum Conflict: An Appraisal After Ukraine," *Journal of Slavic Military* Studies 28, no. 1 (2015): 15; Jaitner, "Russian Information Warfare: Lessons from the Ukraine," 91; Gleb Pakharenko, "Cyber Operations at Maidan: A First-Hand Account," in Geers, *Cyber War in Perspective*, 61; Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corporation, 2017), 5–31, accessed 13 May 2020, https://www.rand.org/pubs/research_reports/RR1498.html.

14. A note on definitions. Emerging and somewhat ambiguous contemporary threats, many of which fall short of the threshold historically consider "war," have been referred to as hybrid warfare (United States and NATO), new generation warfare (Russia), unrestricted warfare (China), and gray-zone competition (various). The lack of a common definition allows various entities to choose a definition that fits their world view or bureaucratic mandate. This allows the rationalization of preconceived notions and more importantly, limits our understanding of the actual threats. In an attempt to mitigate this challenge, this article uses the following definitions:

Hybrid threat. ADP 3-0, *Operations*, describes a hybrid threat as "a diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefiting effects." It is important to note that this view is focused on military threats, not a type of warfare and that hybrid threats can be defeated by the application of military power. Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. GPO, 2019), 1-3.

New generation warfare (NGW). NGW seeks to bring about political or military outcomes without resorting to overt conventional military means, although the latter is not excluded. In NGW, the main battlespace is the mind. As a result, contemporary conflict is dominated by information warfare to achieve superiority by morally and psychologically demoralizing an enemy's military personnel and civilian population before and, if necessary, during hostilities. This reduces the need to deploy lethal military power, making the opponent's military and civilian population support the attacker to the detriment of their own government. Consequently, the Russians have placed the idea of influence at the center of their operational planning. This is relevant for understanding its strategic significance since the operationalization of NGW cannot be characterized as a military strategy in the traditional Western sense. For example, hybrid warfare can be part of NGW but should not define it. This description is based on Russian actions in Ukraine, as well as speeches and writings from Russian military leaders and researchers. See Jānis Bērziņš, "Not 'Hybrid' but New Generation Warfare," in *Russia's Military Strategy and Doctrine*, ed. Glen E. Howard and Matthew Czekaj (Washington, DC: Jamestown Foundation, 2019), accessed 13 May 2020, https://jamestown.org/wp-content/uploads/2019/02/Russias-Military-Strategy-and-Doctrine-web.pdf?x30898&x87069; see Gerasimov, "The Value of Science is in the Foresight"; S. G. Chekinov and S. A. Bogadanov, "On the Nature and Content of a New-Generation War," *Voennaia Mysl* [Military thought], no. 10 (2013), accessed 13 May 2020, https://pdfs.semanticscholar.org/c887/4593b1860de12fa40dadcae8e96861de8ebd.pdf.

Unrestricted warfare. Unrestricted warfare is based on the belief that globalization acts as a force multiplier for less traditional nonmilitary methods like diplomatic warfare (alliance building), economic warfare (trade sanctions), cyberwarfare (hacking attacks), or environmental warfare (man-made natural disasters). Thus to achieve strategic goals, China must move beyond the purely military force power spectrum and operate in multiple domains. In 2003, China issued the "Political Work Guidelines of the People's Liberation Army." It described "three warfares," which are to be applied during peacetime and military operations. The first, "psychological warfare," is the application of military, diplomatic, and economic pressure to weaken adversaries' will. The second, "public opinion warfare," is focused on the overt and covert manipulation of information to influence international and domestic audiences. The third, "legal warfare," refers to the exploitation of international norms to accomplish Chinese objectives. See Nan Li, "Unrestricted Warfare and Chinese Military Strategy" (Singapore: Institute of Defence and Strategic Studies, 2002), accessed 28 May 2020, https://www.rsis.edu.sg/wp-content/uploads/2014/07/CO02022.pdf; Sergio Miracola, "Chinese Hybrid Warfare," Italian International Institute for Political Studies, accessed 13 May 2020, https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853.

Gray-zone competition. This is defined as "covert or illegal activities of nontraditional statecraft that are below the threshold of armed organized violence; including disruption of order, political subversion of government or non-governmental organizations, psychological operations, abuse of legal processes, and financial corruption as part of an integrated design to achieve strategic advantage. This competition among and within state and non-state actors falls between the traditional war and peace duality and is characterized by ambiguity about the nature of the conflict, opacity of the parties involved, and uncertainty about the relevant policy and legal frameworks." Notably, all three descriptions feature gray-zone competition. See Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism* 7, no.4 (2018): 36; Philip Kapusta, "The Gray Zone," *Special Warfare* 28, no. 4 (October-December 2015): 18–25, accessed 13 May 2020, https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf.

Summary. In contrast to the Russian and Chinese descriptions of contemporary warfare, which are based on multi-domain operations facilitated by information warfare occurring simultaneously covertly and overtly below the traditional threshold of war; the U.S. view is focused on overt military threats that can be defeated by the application of military power. As Frank Hoffman notes, embracing this narrow conventional conception of conflict does not prepare future leaders for the range of emerging threats. It is also not conducive to developing doctrine and training: "A myopic focus on conventional threats obscures the complexity of the phenomena and oversimplifies the challenges. It may also be a way of overemphasizing a preferred mission set for a conventional, big war paradigm, which narrows our cognitive understanding of conflict." Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly*, no. 52 (2009, 1st Quarter): 34–59, accessed 13 May 2020, https://smallwarsjournal.com/documents/jfqhoffman.pdf.

15. Sydney Freedberg Jr., "The Golden 5 Minutes: The Need for Speed in Information War," Breaking Defense, 21 October 2019, accessed 13 May 2020, https://breakingdefense.com/2019/10/the-golden-five-minutes-the-need-for-speed-in-information-war/.

16. Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 2019), v.

17. "Information Warfare Foundational Study (Working Draft)" (Fort Gordon, GA: U.S. Army Cyber Command, 10 July 2019), 8.

18. Jen Judson, "Army Learning How Cyber Support Plays Role in Tactical Operations," DefenseNews, 10 November 2015, accessed 13 May 2020, http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-

FUTURE WARFARE WRITING PROGRAM

Call for Speculative Essays and Short Works of Fiction

Military Review calls for short works of fiction for inclusion in the Army University Press Future Warfare Writing Program (FWWP) for 2020. The purpose of this program is to solicit serious contemplation of possible future scenarios through the medium of fiction in order to anticipate future security requirements. As a result, well-written works of fiction in short-story format with new and fresh insights into the character of possible future martial conflicts and domestic unrest are of special interest. Detailed guidance related to the character of such fiction together with submission guidelines can be found at https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/Future-Warfare-Writing-Program-Submission-Guidelines/. To read previously published FWWP submissions, visit https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/.

Army University Press

in-tactical-operations/75545442/. During a pilot exercise, which attempted to incorporate cyber support into an infantry brigade, an observer noted that "while we provided some very technically smart folks, they weren't able to communicate with the brigade commander and staff in terms that they were able to easily understand, what capabilities we are providing and how best to integrate those capabilities."

19. FM 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. Government Printing Office, 2014), Annex D.

20. "77th Brigade Influence and Outreach," British Army, accessed 13 May 2020, https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/. The 77th Brigade is a combined Regular and Army Reserve unit formed in 2015. Its missions include audience, actor and adversary analysis, information activity and outreach, counteradversarial information activity, support to civilian partners, collecting media content, disseminating media, monitoring the IE, evaluating the IE, advising and training on human security (emphasizing the security of people and their social and economic environment rather than the security of the state), and providing support to current operations.

21. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense [DOD], 2020), accessed 13 May 2020, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf. Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) or manipulation that leads to physical domain denial are considered a form of fires.

22. Alexandra Evans and Alexandra Stark, "Bad Idea: Assuming the Small Wars Era is Over," Defense 360, Center for Strategic and International Studies, 13 December 2019, accessed 14 May 2020, https://defense360.csis.org/bad-idea-assuming-the-small-wars-era-is-over/.

23. "Information Warfare Foundational Study," 35.

24. I. Vorobyov and V. Kiselyov, "Russian Military Theory: Past and Present," *Military Thought* 22, no. 1 (2013): 56.

25. For example, the U.S. Army is planning on creating two new integrated intelligence, information, cyber, electronic warfare, and space battalions to help shape the operational environment, monitor information streams, and conduct information operations or cyber missions.

26. "В Белоруссии начались учения 'Нерушимое братство-2016'" [In Belorussia begins the exercise Unbreakable Brotherhood 2016], RIA, 23 August 2016, accessed 14 May 2020, https://ria.ru/world/20160823/1475032583.html, cited in Giles, "Delivery of Information Effects by Russian Special Forces and Intelligent Agencies." Consecutive exercises in 2016 included the use of "psychological warfare and information confrontation sub-units."