



People hold a banner reading "We demand a referendum" as they shout slogans during a pro-Russian rally 8 March 2014 in Donetsk, Ukraine, and as Russia was reported to be reinforcing its military presence in Crimea. (Photo by Sergei Grits, Associated Press)

Expanding Tolstoy and Shrinking Dostoyevsky



How Russian Actions in the Information Space are Inverting Doctrinal Paradigms of Warfare

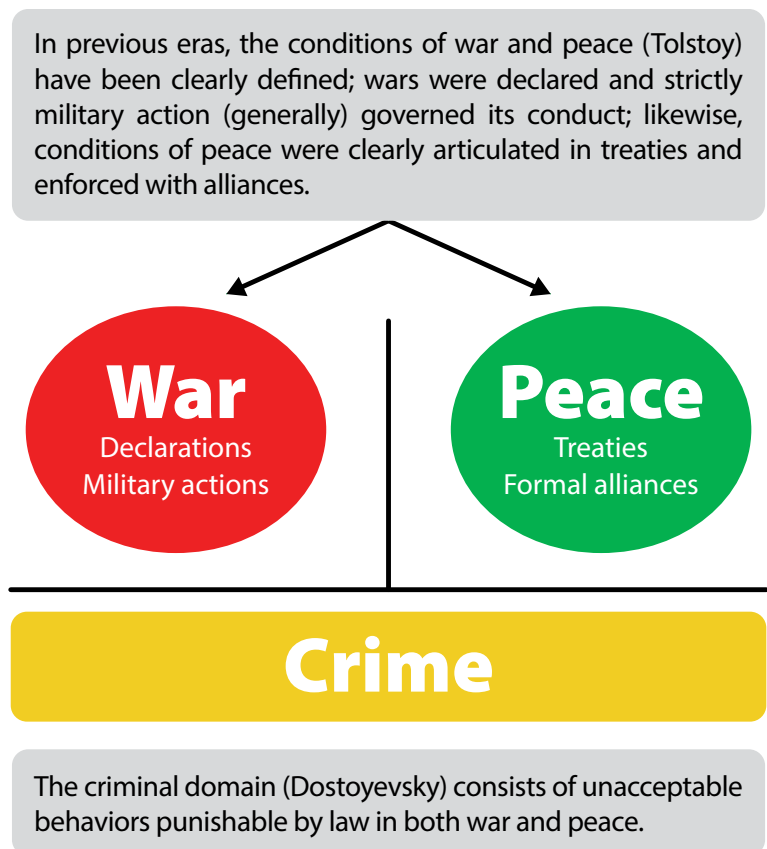
Maj. Scott J. Harr, U.S. Army

In February 2013, Russian Chief of Staff Valery Gerasimov published “The Value of Science is in the Foresight,” which describes a twenty-first century battlefield replete with new methods, capabilities, and applications of war that transcend accepted contemporary definitions and uses of military power.¹ Subsequent Western debate on Gerasimov’s discourse (dubbed the “Gerasimov Doctrine”) often focuses on whether Gerasimov’s ideas represent old or new ways of war and whether Gerasimov intended to describe a distinctly Russian style of warfare for the twenty-first century.²

To be sure, the evolution of military thought and science is an ongoing discussion within Russia that involves not just Gerasimov, but other prominent Russian military officers as well. So, as retired Lt. Col. Timothy Thomas points out, it is wise for Western military analysts to not exclusively categorize trends in Russian warfare.³ However, the Gerasimov Doctrine represents the most powerful and relevant current adaptation of Russian military thought, and it describes a new type warfare that emphasizes Russian development of capabilities to defend and win in the cyber and information domains as the critical domains of future warfare (vice actual kinetic combat).⁴ In any case, Russian actions on the international stage have demonstrated a style of warfare that comprehensively integrates all instruments of national power (in militaristic ways) to achieve strategic objectives countering Western influence. The title of the renowned Russian novelist Leo Tolstoy’s masterpiece *War and Peace* alludes to discrete conditions of the modern Russian approach to warfare. Like Western concepts of the “gray zone,” the Tolstoyan concept expands the spectrum between war and peace to include levels of conflict that satisfy neither of the extremes—yet remain viable arenas to promote strategic interests using force. Likewise, akin to the boundaries of criminality that timeless Russian author Fyodor Dostoyevsky explored in his classic work *Crime and Punishment*, current Russian modes of warfare have shrunk the criminal boundaries of

war and blended the rules of warfare to enable more interaction among the instruments of national power to pursue strategic interests.

In a metaphorical sense, depicted in figures 1 and 2 (page 41), Russian actions in warfare under the Gerasimov Doctrine have “expanded Tolstoy” (i.e., created more fluid conditions between war and peace) while “shrinking Dostoyevsky” (i.e., reducing the crimi-

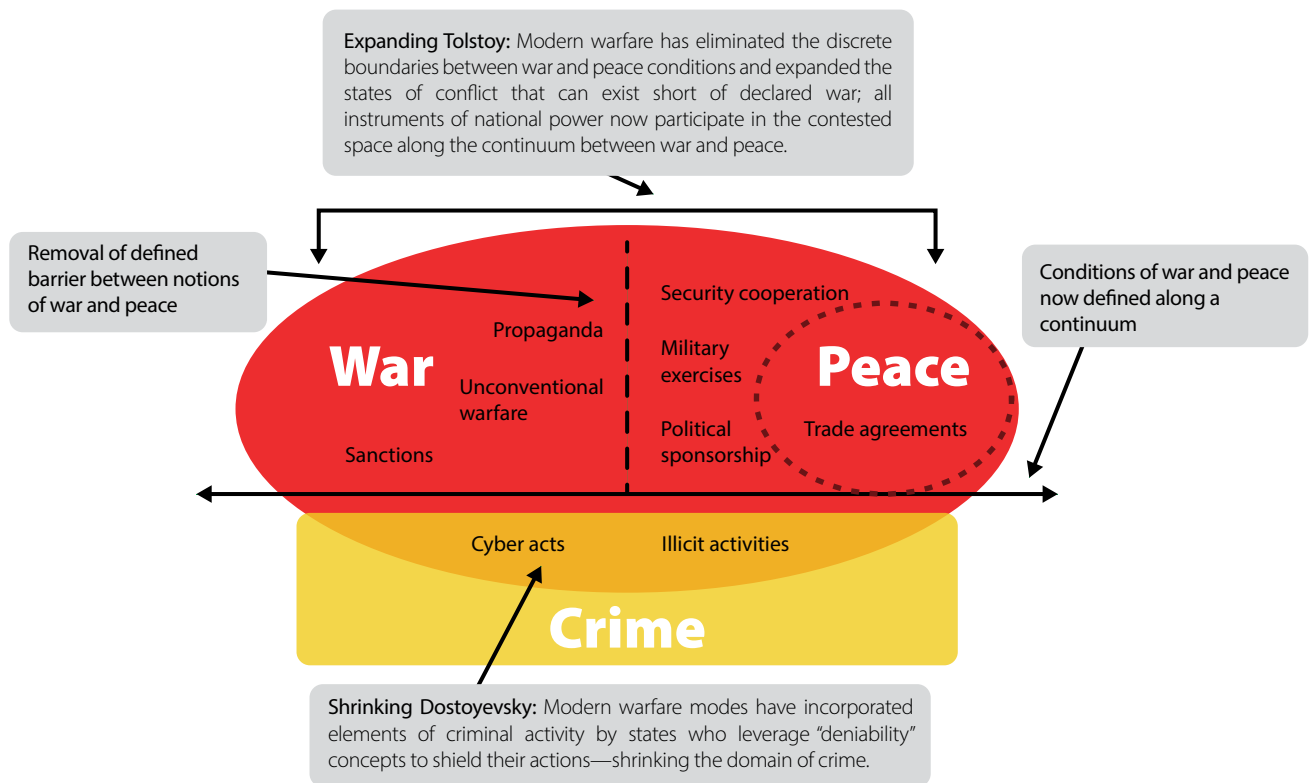


(Graphic by author)

Figure 1. Expanding Tolstoy and Shrinking Dostoyevsky Construct Explained

nal boundaries of national activities to prosecute war). As a linchpin that increasingly knits the contemporary modes of Russian warfare together, the broad range of information operations (IO) has played a major role in Russian actions, inverting the paradigms of warfare espoused by U.S. doctrine and thus presenting the U.S. joint force with significant challenges.

Given the above discussion, the intent of this paper is to outline the major ways that recent Russian IO



(Graphic by author)

Figure 2. Expanding Tolstoy and Shrinking Dostoyevsky in Terms of Contemporary Understanding of War

actions (as part of the Gerasimov Doctrine) have inverted commonly held U.S. paradigms of warfare. Upon illuminating the role of IO in forging new applications of war that depart from U.S. notions, this paper distills the major implications for the U.S. joint force in terms of policy, doctrine, and capabilities. On this basis, recommendations can be made regarding how to populate, train, and equip the joint force (especially Army forces) to counter and proactively guard against Russian IO actions that undermine or deliberately target U.S. interests in contested areas.

Paradigm Inversions: Three Ways Russian IO Actions Challenge American Conceptions of War

One long-held paradigm of U.S. approaches to warfare necessitates that combat power be dedicated toward the destruction of the enemy. Modern joint doctrine still speaks of the Clausewitzian concept of center of gravity as the main source of an enemy's power that should be attacked with the full force of combat capabilities to

ensure an enemy's defeat.⁵ This paradigm appears as simple and obvious as the front plate on a Claymore mine that reads "Front Towards Enemy." However, Russian IO actions, as a Gerasimov Doctrine application of combat power, demonstrate that in the era of limited "wars of choice," concerted and weaponized IO efforts can be directed toward *friendly* audiences and centers of gravity to deliver decisive effects cultivating and sustaining public opinion supporting government and/or military action. According to analyst Stephen Blank, Russia can use the decisive force of IO on its own domestic population because Russia has "securitized" the information instrument of national power.⁶ That is, Russia has convinced its population that information is a national security matter and the government therefore has a compelling interest in controlling it. Russian actions controlling the information that it feeds to its population have been on full display during the Russian annexation of the Crimea, where political scientist Ioana-Nelia Bercean notes that domestic support of Russia's actions remains high.⁷ The combat potential of Russia's paradigm inversion is clear



when juxtaposed against the influence of public opinion in recent American military efforts: while public support for American campaigns in Iraq and Afghanistan dwindled over time to induce massive strategy shifts, Russia continues to target its own population with IO actions that preserve and monopolize public opinion justifying its counter-Western actions contending with American strategic objectives in Europe.

Another time-honored paradigm of Western war (from the Clausewitzian tradition) frames *war as an extension of politics*. Reflecting this dynamic, the joint force under U.S. law serves its civilian political masters in executing national strategy and foreign policy delineated by elected political elites. Russia's IO actions, on the other hand, delve into and rely heavily on political messaging and political tampering to achieve strategic ends. In this sense, its IO actions treat *politics as an extension of war*. Such actions have found fertile ground in the former Soviet states of Eastern Europe. The Republic of Moldova serves as a striking current example of the effects of Russian political IO actions. According to Moldovan military reports, many political parties in Moldova have been infiltrated by pro-Russian personalities who have overt links to Moscow and regularly visit Russian leaders.⁸ The direct input from the Russian information machine to Moldovan politicians exerts pressure on Moldovan

Moldovans protest a NATO summit 9 July 2016 in Warsaw, Poland. Moldovans of ethnic Russian descent together with pro-Russian ethnic Moldovans increasingly act in concert in organized efforts such as demonstrations to put pressure on the Moldovan government to acquiesce to Russian government policy demands. Reportedly cultivated and supported by Russian agents, these efforts specifically promote agitation against Moldova to decrease that country's association with the European Union and NATO. (Photo by Denis Bolotsky, Sputnik)

society in the form of anti-Western statements or pro-Russia endorsements from political pulpits. Russia's treatment of politics as an extension of war has had positive effects reshaping Moldovan public opinion, as recent polling figures suggest a significant drop in support of the European Union and NATO.⁹ Perhaps more famously (and distinctly more ominously), Russian political IO actions have been implicated and heavily investigated in the tampering and release of information associated with recent U.S. presidential election processes.¹⁰ If true (or perhaps even if untrue), the inversion of the Western paradigm specifying the relationship between politics and war portends foreboding consequences for sovereign states, as IO operations can seemingly influence regime changes without the firing of a single bullet.

Finally, a paradigm of U.S. joint warfare frames all operations within the context of "legitimacy" that,

accordingly, identifies the imperative that all operations be perceived as legitimate and credible. Joint Publication (JP) 3-0, *Joint Operations*, elevates the concept of legitimacy into one of the principles of joint operations and defines it as a “decisive factor of operations” based on the “actual and perceived legality, morality, and rightness” of an operation.¹¹ In this paradigm, to ignore legitimacy is to sacrifice the purpose and effects of the operation. Russian IO actions have demonstrated a penchant for inverting this paradigm so that legitimacy does not validate operations, but rather operations validate their legitimacy. Russian manipulation of social media and the cyberspace realm of IO provides the most pertinent example of Russian efforts in this space. Scholar Jessikka Aro notes how a modern component of Russian information warfare consists of government paid commentators who troll social media sites and post propaganda, fake news, and overtly pro-Russian messages designed to confuse audiences or reinforce pro-Russian information themes.¹² This aspect of information warfare plays on the twin concepts of deniability and attribution to create chaos. As analyst Oliver Fitton puts it, efforts in cyberspace and social media are difficult to conclusively attribute to official Russian instruments of power and therefore give the Russian apparatus deniability in these operations.¹³ Without the burden or imperative of being perceived as legitimate or credible, Russian IO actions can spin, craft, and create narratives that suit their objectives by continually flooding the information space with messages that advance their interests.

Overmatch: The Limits of Joint IO Doctrine and Policy

Russian IO actions employ and integrate all instruments of national power to exploit seams and gaps in U.S. joint IO doctrine and overarching policy. By turning the propaganda effects of their IO actions against their own people to control public opinion, Russian actions trespass into areas of manipulation that the democratic principles that undergird joint policy and doctrine cannot (with good reason) emulate. Indeed, both policies that govern the conduct of IO—Department of Defense Directive 3600.01, *Information Operations*, and Chairman of the Joint Chiefs of Staff Instruction 3210.01C, *Joint Information Operations Proponent*—strictly and explicitly prohibit IO activities “intended to manipulate audiences,

public actions, or opinions in the United States.”¹⁴ In democracies, the ends cannot justify the means, which, while potentially ceding a critical IO advantage to Russia, actually reinforces civil society and suggests an effective counter-IO strategy that will be discussed in the next section.

JP 3-13, *Information Operations*, characterizes IO as “the integrated employment, *during military operations*, of IRCs [information related capabilities] [emphasis added].”¹⁵ This makes it clear that, institutionally, the joint force generally views IO as a force multiplier for military actions. But Russian IO efforts, under the “securitized” concept mentioned earlier, have expanded the scope of what constitutes a “military operation” into all domains of national power that far outpaces U.S. joint doctrine conceptions of IO applications. To illustrate, the instruments of national power are doctrinally represented in JP 3-0 in terms of the separate domains of diplomacy, information, military, and economic, commonly depicted using the acronym “DIME.” For Russia, however, the separate block letters of DIME do not capture the roles and level of integration between their instruments. Rather, a cursive depiction of DIME—with connected letters—better captures the highly integrated Russian approach, and the term “national instruments of war” (not power) better articulates the blended construct of the Russian securitized environment. Figure 3 (on page 45) visually depicts the different constructs of national power. The Russian construct integrates IO actions across all instruments and provides venues for action that joint doctrine and policy cannot legally

Maj. Scott J. Harr,
U.S. Army, is a Special Forces officer serving in 5th Special Forces Group (Airborne). He holds a BS in Arabic language studies from the U.S. Military Academy and an MA in public policy—Middle Eastern affairs from Liberty University, and he is a recent graduate of the Command and General Staff College, Fort Leavenworth, Kansas. He has served in multiple tours in Afghanistan and locations throughout the U.S. Central Command area of responsibility as an infantry platoon leader and Special Forces detachment commander. He most recently deployed as an operations officer supporting special operations forces for Operation Inherent Resolve.

or operationally follow without undermining the same liberal democratic institutions and values that the joint force exists to preserve.

Russian IO actions that de-emphasize or ignore aspects of legitimacy and credibility inevitably gain degrees of speed and agility that U.S. joint doctrine and policy cannot hope to match. Confusing and disrupting adversary decision cycles (which often represent the core aim of Russian IO actions) merely requires that the volume of produced messages outpace an opponent's ability to interpret and deci-

and planning representatives to fully synchronize IO actions.¹⁷ Furthermore, IO policy directives are teeming with mandates to coordinate actions through oversight bodies such as the Executive Steering Group that consists of joint staff members from multiple directorates.¹⁸ While this architecture may emphasize and achieve IO coordination aimed at preserving whole-of-government legitimacy and credibility in the information space, in the meantime, Russian IO actions can swiftly and decisively outmaneuver such cumbersome regulations to achieve effects.

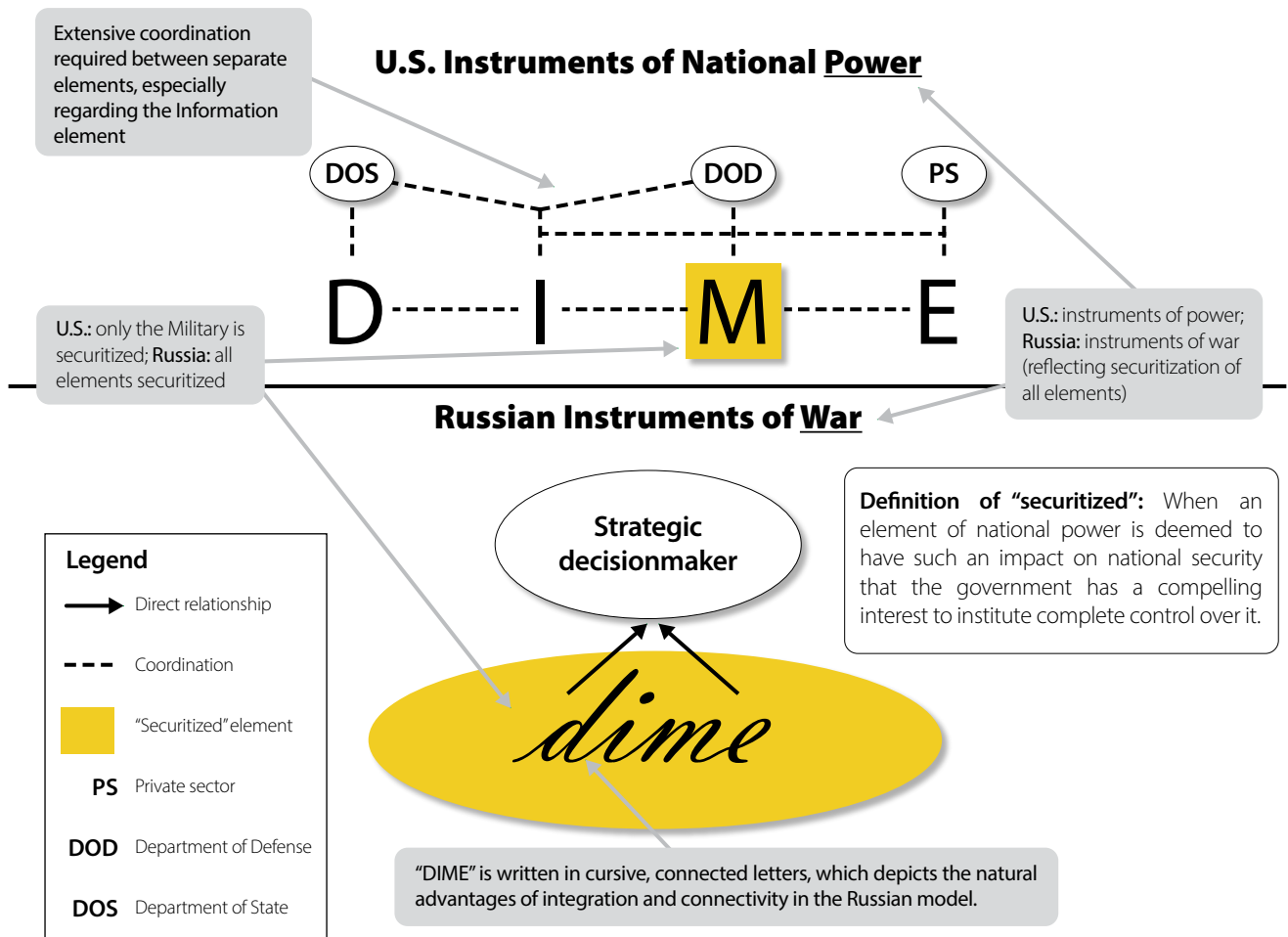


pher the true strategic intent of the message to take meaningful action. Analysts denote this characteristic of Russian IO as a doctrine of “reflexive control” and highlight how Russia has successfully used the tactic to shroud its actions in Ukraine and the Crimea, creating a paralyzing confusion that has largely prevented U.S. action.¹⁶ In contrast to the free-wheeling tactics of reflexive control, U.S. joint doctrine and policy demand extensive coordination for IO actions that must account for all interagency stakeholders. Figure 4 (page 46) highlights the doctrinally recommended composition of an IO joint planning cell taken from JP 3-13. The construct calls for the coordination of no less than *twenty-three* separate operational

Russian “propaganda” poster, 25 July 2010. Translation: “To find and not let go! Together against Terrorism.” (Photo by Vitaly Kuzmin, <http://www.vitalykuzmin.net>)

The Doctrine of Contested Acknowledgment for the Joint Force

Given the areas of overmatch outlined above based on both political and institutional constraints that are unlikely to change, and given Russia's steadfast commitment to investing in and fighting according to the so-called Gerasimov Doctrine, Russia will likely maintain critical advantages in the information space



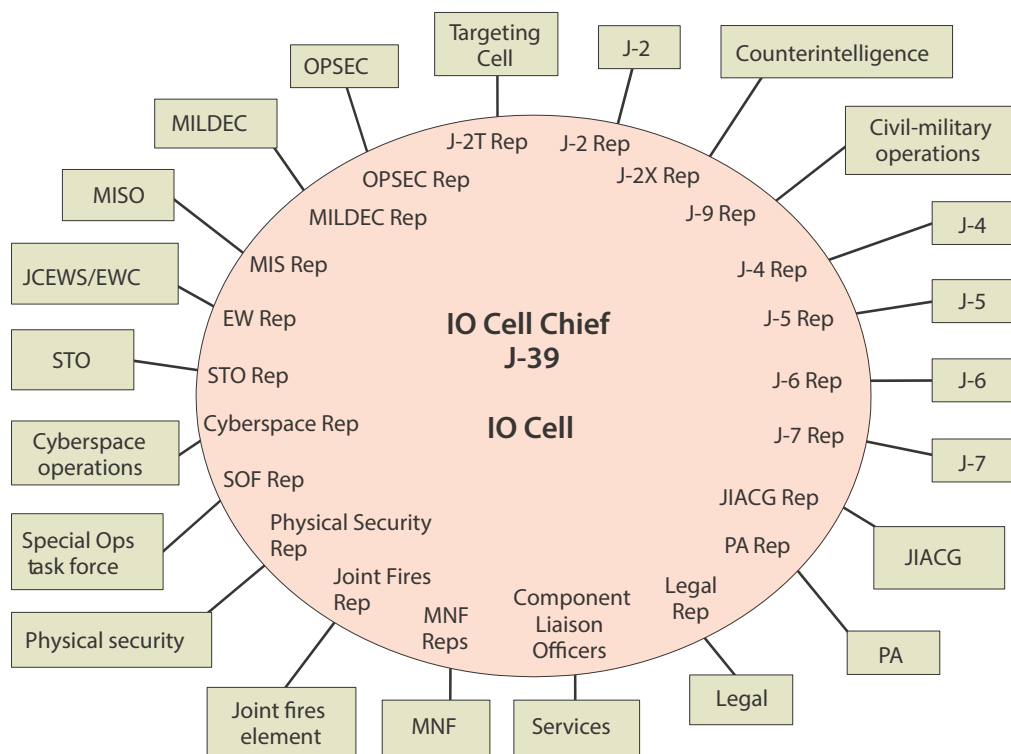
(Graphic by author)

Figure 3. Comparing DIME (Diplomacy, Information, Military, and Economic) in the Russian Securitized Context

into the foreseeable future. This admission of Russian overmatch by no means suggests that the United States should concede this domain to a powerful near-peer adversary. Rather, a doctrine of contested acknowledgment should be adopted by the joint force to counter and meet Russian IO actions that threaten or undermine strategic interests. Under this doctrine, the joint force pragmatically acknowledges Russian advantages in this domain while simultaneously contesting them to the utmost without sacrificing combined arms or joint lethal capabilities—which, despite what the Gerasimov Doctrine calls to the contrary, will remain the most decisive capabilities in exerting national power during conflicts. Implementing this doctrine against Russian actions in Europe relies on U.S. State Department

(DOS) efforts to bolster and project narratives of U.S. prosperity and freedom abroad as well as increased and sustained Department of Defense (DOD) efforts to train, advise, and assist partner nations within Russia's sphere of influence in IO techniques and principles.

It is important to clarify here that U.S. efforts in this regard need only focus on sovereign states that are either NATO partners or have undergone steps to initiate NATO membership. U.S. assistance, then, would be invited and welcomed by states that have, in essence, declared their intentions to emulate Western-style governments and economies (a certain level of these intentions is required for NATO membership, as per its charter).¹⁹ While NATO expansion, as rightly noted by Dr. John Mearsheimer, has been a key



Legend

EW—Electronic warfare
EWC—Electronic warfare cell
IO—Information operations
J-2—Intelligence directorate of a joint staff
J-2T—Deputy directorate for targeting
J-2X—Joint force counterintelligence and human intelligence staff element
J-39—Information operations staff
J-4—Logistics directorate of a joint staff
J-5—Plans directorate of a joint staff
J-6—Communications system directorate of a joint staff
J-7—Force development directorate of a joint staff
J-9—Civil-military operations directorate of a joint staff

JCEWS—Joint force commander's electronic warfare staff
JIACG—Joint interagency coordination group
MILDEC—Military deception
MIS—Military information support
MISO—Military information support operations
MNF—Multinational force
Ops—Operations
OPSEC—Operations security
PA—Public affairs
Rep(s)—Representative(s)
SOF—Special operations forces
STO—Special technical operations

(Graphic from Joint Publication 3-13, *Information Operations* [Washington, DC: U.S. Government Publishing Office, 2012], II-6)

Figure 4. Recommended Information Operations Planning Cell

agitor promoting friction in U.S.-Russian relations since 2008, it is also important to recognize that many of the eastern European nations, as free sovereign states, have chosen Western methods of government and commerce despite Russian influence and pressure to “rejoin” the Soviet Union. To concede these states to a so-called Russian sphere of influence (losers of the Cold War and purveyors of an ideology far short of the liberty and democracy valued in the West) for fear of antagonizing Russia would sacrifice American ideals for the sake of Russian appeasement.

short term, if Americans truly believe in the viability of their values, this approach is better in the long term at holding Russia accountable for its actions and preventing the dangerous spread of ideologies detrimental to the human condition.

As noted earlier, the propaganda advantages that Russia creates by securitizing its informational instrument of war for domestic support represents a double-edged sword that suggests a powerful U.S. counteraction in the IO domain. As the leading tool of diplomacy and foreign policy and part of an

Put bluntly, if Russia sees American efforts in eastern Europe as a threat, then there is a simple way to diffuse the tension: Russia can democratize its government or undertake other reforms to make their ideology more attractive to its former Soviet states. Clearly, no one should promote a strategy that threatens to return U.S.-Russian relations to the Cold War era. However, because states have (or should have) the right to pursue their own national interests, then those that beckon America's assistance should be heeded. While the augmented train, advise, and assist role of the United States under the doctrine of contested acknowledgment may risk more tension with Russia in the

interagency “manning” response, DOS experts should augment their embedment with current DOD personnel in U.S. European Command to lead a coordinated effort to saturate contested IO realms with images and messages of American prosperity and freedom. These messages will undermine the authoritarian mechanisms within the Russian political system that allow for total population control and manipulation. Fundamentally, if Russians begin to perceive that the “grass is greener” in America through IO campaigns ruthlessly waged by whole-of-government U.S. entities, they may push back on their government and, ideally, deny it the sustained advantages shaping public opinion that have allowed Russia to succeed in recent international conflicts at the expense of U.S. strategic interests. In this effort, the DOD plays a supporting role by assisting in the delivery of IO messages and by conducting shows of military force that propagate narratives of American confidence and invincibility.

It is also important to clarify how American messages of prosperity and liberty, propagated in Russia and eastern Europe, differ from the alleged and infuriating Russian efforts to meddle in and influence U.S. politics. Firstly, while the alleged Russian efforts to influence American politics centered on Russia providing *negative* information about the United States and candidates through cyber hacking, American efforts in the doctrine of contested acknowledgment would rely on simply advertising the *positive* benefits of a free society. So, while not directly poking holes in the Russian government, messages would simply inform the Russian population that perhaps a better, freer way of life exists. Secondly, Russian IO, due to their dubious nature, frequently rely on deniability and the impossibility of attributing such actions to the Russian government. U.S. messages as part of the contested acknowledgment doctrine, on the other hand, would welcome attribution because it would simply highlight the virtues of civil society in a democracy. So, for example, if Russia accused the United States of planting a message showing peaceful protests in the United States, the United States could simply take credit and essentially say “yes, those are peaceful protests against the government because that’s the level of freedom we enjoy in the United States.” Finally, this type of democracy promotion by the United States offers a way to spread American ideals and values without the “regime

change” model that experts like Mearsheimer have identified as both the primary Russian perception of American democracy promotion methods and a huge agitator of U.S.-Russian relations.²⁰

The DOD assumes the lead role in the doctrine of contested acknowledgment by undertaking augmented “train, advise, assist” missions in the contested space within the European Command area of responsibility. Military information support operations (MISO) forces represent the best, if limited, manning solution for these actions. The launching of the European Reassurance MISO Program and the expansion of authorities and IO training proposed in 2016 represent prudent actions that should be approved, replicated, and expanded.²¹ Training partner forces with expertly trained and equipped MISO soldiers yields the two-fold benefit of developing durable capabilities within partner forces while also giving countries with differing political constraints the means to (potentially) leverage IO in ways that the United States cannot organically accomplish. If the joint force expects to be adequately manned, trained, and equipped to contest the IO domain, augmenting and incentivizing MISO recruitment may be a key starting point.

Conclusion

In April 2003, as American tanks thundered into Baghdad, Mohammed Saeed al-Sahhaf, Iraq’s information minister (derisively known as “Baghdad Bob”), vehemently broadcasted denials of an American presence in Iraq while simultaneously forecasting wild predictions of American defeat and destruction.²² Obviously discredited by the reality of events on the ground, Baghdad Bob viscerally illustrates the limits of IO in the face of overwhelming combat power. While many such as Gerasimov have boldly predicted that modern forms of war will supplant decisive combat, nothing in the history of humanity and war validates this prediction. Even in the face of Russian IO overmatch, the U.S. joint force should not sacrifice lethal combat capabilities or, worse, notions of liberal democratic ideals to match Russian actions stride for stride in the information space. Rather, by steadfastly adopting a doctrine of contested acknowledgment, the joint force can pragmatically face the realities of Russian IO applications in the operational environment while simultaneously degrading them and, in this way, preserving American ideals while defending American interests. ■

CALL FOR PAPERS

Journal of Military Learning

The *Journal of Military Learning (JML)* is a peer-reviewed semiannual publication that seeks to support the military's effort to improve education and training for the U.S. Army and the overall profession of arms. The *JML* invites practitioners, researchers, academics, and military professionals to submit manuscripts that address the issues and challenges of adult education and training, such as education technology, adult learning models and theory, distance learning, training development, and other subjects relevant to the field. Book reviews of published relevant works are also encouraged.

To view the inaugural edition of the *JML* now available online, visit Army University Press at <http://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/>.

We are now accepting manuscripts for future editions of *JML*. Manuscripts should be submitted to usarmy.leavenworth.tradoc.mbx.army-press@mail.mil. Submissions should be between 3,500 and 5,000 words and supported by research, evident through the citation of sources. For detailed author submission guidelines, visit the *JML* page on the Army University Press website at <http://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/>.

For additional information call 913-684-9339 or send an e-mail to the above address.

Notes

1. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* 96, no. 1 (January-February 2016): 24, accessed 18 July 2017, http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf.
2. Charles Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (January-February 2016): 30, accessed 18 July 2017, http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf.
3. Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *The Journal of Slavic Military Studies* 29, no. 4 (2016): 554-75.
4. Ibid.
5. Joint Publication (JP) 5-0, *Joint Operation Planning* (Washington, DC: U.S. Government Publishing Office [GPO], 2011), III-21, accessed 2 May 2017, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.
6. Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, no. 1 (January-February 2013): 35.
7. Ioana-Nelia Bercean, "Ukraine: Russia's New Art of War," *Online Journal Modelling the New Europe* 21 (December 2016): 164.
8. Dumitru Parfeni, "Russian Federation's Propaganda Versus the Republic of Moldova's Strategic Security Policy" (thesis, Command and General Staff College, 2017), 53.
9. Ibid., 56.
10. Nathalie Maréchal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communication* 5, no. 1 (2017), accessed 18 July 2017, <https://search.proquest.com/docview/1907348349?accountid=28992>.
11. JP 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 2017), A-3.
12. Jessikka Aro, "The Cyberspace War: Propaganda and Trolling as Warfare Tools," *European View* 15, no. 1 (June 2016): 121, [doi:10.1007/s12290-016-0395-5](https://doi.org/10.1007/s12290-016-0395-5).
13. Oliver Fitton, "Cyber Operations and Gray Zones: Challenges for NATO," *Connections: The Quarterly Journal* 15, no. 2 (Spring 2016): 114, accessed 18 July 2017, http://connections-qj.org/system/files/15.2.08_fitton_cyber_gray_zones.pdf.
14. Department of Defense Directive Number 3600.01, *Information Operations* (Washington, DC: U.S. GPO, 2 May 2013), 2; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01C, *Joint Information Operations Proponent* (Washington, DC: U.S. GPO, 14 February 2014).
15. JP 3-13, *Information Operations* (Washington, DC: U.S. GPO, 2012), I-1.
16. Bercean, "Ukraine: Russia's New Art of War."
17. JP 3-13, *Information Operations*. The suggested information operations (IO) cell requires extensive coordination between interagency entities. While JP 3-13 repeatedly states and emphasizes that, with IO, "it is not the ownership of the capabilities and techniques that is important, but rather their integrated application in order to achieve a JFC's [joint force commander's] end state," for practical purposes, the IO cell construct nullifies the usefulness of coordination by ensuring IO actions are not responsive enough to the environment relative to adversaries' (e.g., Russia's) capabilities.
18. CJCSI 3210.01C, *Joint Information Operations Proponent*, A-1.
19. NATO Charter and foundational documents can be found at http://www.nato.int/cps/en/natolive/topics_49212.htm.
20. John Mearsheimer, "Defining a New Security Architecture for Europe that Brings Russia in from the Cold," *Military Review* 96, no. 3 (May-June 2016): 27-31, accessed 18 July 2017, http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160630_art008.pdf.
21. Charles Moore, "Countering Adversary Propaganda through Special Information Operations," *Hampton Roads International Security Quarterly* 65 (2016).
22. William Pierce and Robert Coon, "Understanding the Link between Center of Gravity and Mission Accomplishment," *Military Review* 87, no. 3 (May-June 2007): 80, accessed 18 July 2017, http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20070630_art013.pdf.