A Ukrainian service member takes a selfie in a front of a destroyed Russian T-72 tank 1 April 2022 in the village of Dmytrivka in Kyiv region, Ukraine. (Photo by Oleksandr Klymenko, Reuters/Alamy Stock Photo)

Tactical TikTok for Great Power Competition

Applying the Lessons of Ukraine's IO Campaign to Future Large-Scale Conventional Operations

Col. Theodore W. Kleisner, U.S. Army

Trevor T. Garmey

As the first large-scale conventional conflict between near-peer adversaries since the 1973 Yom Kippur War, the Russian invasion of Ukraine has provided warfighters a unique opportunity to assess prevailing assumptions about large-scale combat operations (LSCO) in real time. The conflict offers lessons spanning the full spectrum of U.S. arms, and its campaigns must be carefully studied as the U.S. Army focuses on great-power competition.

As we write, the conflict is barely four weeks old. Yet the impressive results of Ukraine military operations have already galvanized wholesale revisions to Army tactical and strategic doctrine, ranging from the lethality of antitank guided missiles to the efficacy of loitering munitions against lines of communication.

But of all the lessons available to Army warfighters, the most significant is the role of information operations (IO) in modern LSCO. By empowering soldiers to rapidly distribute tactical information and shape a focused narrative that seamlessly integrates battlefield imagery, heroic exploits, and evidence of potential Russian war crimes, the Ukrainian military and its civilian leadership have mobilized the globe against Russia and contributed substantially to degrading enemy will. Meanwhile, the Russian military—purported experts at disinformation and cyberwarfare—has been utterly incapable of rebutting Ukrainian messaging or communicating a coherent explanation of Russian war aims.

Ukraine has achieved these results by merging commercial applications, including mobile devices, messaging services, and social media, into its IO strategy and delegating distribution authority—by design or by default—to the tip of the spear.[1] Ukraine has also merged strategic communications into its IO programming, empowering Ukraine warfighters to reinforce themes articulated by their political leadership. The result is a stand-alone combat capability that has rallied international support, allowed rapid dissemination of battlefield success, humiliated the adversary, and produced an authentic narrative that resonates with target markets.

For the U.S. Army, the Ukraine conflict offers a timely opportunity to review existing doctrine and consider whether current Army IO and public affairs (PA) methodologies adequately leverage IO as a combat capability. More specifically, the Army must examine whether its existing IO and PA strategies address winning the information war at the point of contact.

In this article, we first trace the evolution of IO; summarize Army and joint doctrine on IO, PA, and strategic communications; and assess whether the present Army approach fully leverages the potential of IO at the tactical level. We pay particular attention to the failure of present IO doctrine to embrace winning the IO fight at the point of contact. We then examine the use of IO in Ukraine and argue that the experience of the Ukraine army (UA) demonstrates that with appropriate training, guidance, and oversight, the tactical deployment of IO improves combat performance and is a necessary component of great power competition. Finally, we offer recommendations and considerations for the Army and the joint force to ensure that in the battlefield of the future, warfighters can apply IO to neutralize adversaries and improve combat outcomes.

Importantly, we do not purport to have all the answers on the integration of IO into Army doctrine. We do not, for example, address the implications of the Ukraine conflict for traditional information warfare—the use of sensors, software, and data to disrupt or destroy the information systems of the adversary. Access to the information required for that analysis is not available at this time. Nor do we provide solutions to the inherent tension between IO, information security, and information assurance. Instead, we mean for this article to be the catalyst for important conversations on the future of IO and how to best position the Army for dominance in future LSCO.

Historical Summary of Army IO Initiatives

While this article is not a comprehensive history of IO, a summary of recent Army efforts to explore and implement IO helps explain current Army IO doctrine and its application on future battlefields.

Col. Theodore W. Kleisner, U.S. Army, commands 1st Brigade, 82nd Airborne Division. A graduate of West Point, the National War College, and the School of Advanced International Studies at Johns Hopkins University, he has led units in peacekeeping and combat operations in Europe, Afghanistan, and Iraq.

Trevor T. Garmey is an attorney in private practice in Los Angeles and a graduate of the University of Virginia School of Law and the College of William and Mary.

The Army's IO and PA record during the Second World War, Korea, Vietnam, and Operation Desert Storm has been the subject of detailed analysis and does not require further explication here.[2] The most helpful starting point is instead the post-Cold War focus on future conflict, generally referred to as the revolution in military affairs (RMA).

"The RMA also witnessed the first attempt by the Army to define IO. In a pattern that remains true, the Army framed IO as an ancillary attribute of combat operations, rather than a stand-alone combat capability."

The revolution in military affairs. Widely attributed to Andrew Marshall and the Office of Net Assessment, RMA theory coalesced after the fall of the Soviet Union.[3] RMA advocates focused on the potential for technology—including information technology—to drive rapid change in warfare.

The RAND Corporation's 1996 treatise, *Strategic Information Warfare: A New Face of War*, is a useful exemplar of RMA theory because it identifies "information" as a core domain of future conflict. The authors repeatedly emphasize the low entry costs of information warfare, the security risks of growing network dependence, and above all, the potential for new technology to enhance deception techniques and allow the manipulation of public perception.[4]

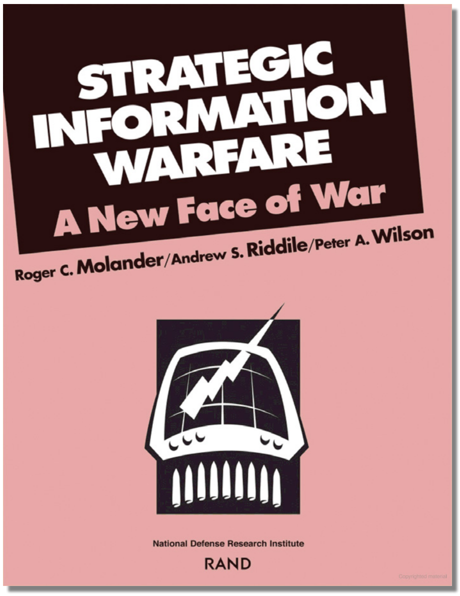
For the Army, RMA theories found their first expression in "Force XXI," a catchall for efforts preparing the force for operations in a unipolar world.[5] As stated by Lt. Gen. Paul E. Menoher Jr. in "Force XXI: Redesigning the Army through Warfighting Experiments," the Army sought to "push[] the envelope and transform[] … into an even better information age, knowledge- and capabilities-based Army, capable of land force dominance across the continuum of 21st century military operations."[6]

The RMA also witnessed the first attempt by the Army to define IO. In a pattern that remains true, the Army framed IO as an ancillary attribute of combat operations rather than a stand-alone combat capability. U.S. Army Training and Doctrine Command Pamphlet 525-5, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Twenty-First Century*, defined IO as

> continuous combined arms operations that enable, enhance, and protect the commander's decision cycle and execution while influencing an opponent's operations are accomplished through effective intelligence, command and control, and command and control warfare operations, supported by all available friendly information systems; battle command information operations are conducted across the full range of military operations.[7]

Two years later, Field Manual (FM) 100-6, *Information Operations*, modified the definition to

> continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the


STRATEGIC INFORMATION WARFARE
A New Face of War
Roger C. Molander/Andrew S. Riddile/Peter A. Wilson
National Defense Research Institute
RAND

To view *Strategic Information Warfare: A New Face of War*, visit https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf.

> full range of military operations; IO include interacting with the GIE (Global Information Environment) and exploiting or denying an adversary's information and decision capabilities.[8]

Thus, even early RMA advocates classified IO by technical features rather than war-making potential. This dynamic was highlighted by Robert J. Bunker in 1998. Bunker questioned whether IO was properly classified as a force multiplier serving existing combat functions or as a stand-alone capability for the warfighter to exploit in the combat environment.[9] Bunker stated that the "actual value" of IO was disputed because

> One school of thought posits that [IO] represent an adjunct to current operations—the end result of which is to enhance current Army capabilities by making what it has traditionally done better by means of a force multiplier effect. Another school of thought suggests that information operations will provide the Army with new capabilities. Instead of being a simple adjunct to current operations, according to this school, the influence of the "information revolution" on warfare will result in the redefinition of operations themselves.[10]

Those who saw IO as a force multiplier focused on the ability of IO to identify, geolocate, and neutralize an adversary using sensors, high-speed data transmission, and imagery. Warfighters who saw IO as a stand-alone capability, by contrast, tended to focus more on the potential for information itself to impose substantial costs on an adversary, whether through the elimination of electronic systems or the dissemination of adverse content.

There were also debates about what precisely *information* meant in the context of IO and the RMA. None of the Army publications cited above offered a clear definition for "information." The Joint Chiefs of Staff offered a concise definition in 1997, describing information as "data collected from the environment and processed into usable form."[11] Data, meanwhile, was defined as "representations of facts, concepts, or instructions in a formalized manner suitable for communications, interpretation, or processing by humans or automated means."[12]

Gen. Gordon Sullivan, by contrast, offered a more nuanced and functional definition of information that focused on the character of the data involved. Writing in *War in the Information Age*, Sullivan identified four distinct types of information: content information, "the simple inventory of information about the quantity, location and types of items"; form information, "the descriptions of the shape and composition of objects"; behavior information, "three dimensional simulation that will predict behavior of at least physical objects, ultimately being able to 'wargame' courses of action"; and action information, "information that allows operations to take the appropriate action quickly."[13]

Regardless of these semantic debates—which continue to this day—by 2001, IO was a featured aspect of the Bush administration's revisions to national defense policy. IO was identified as a "key military capability" for the future joint force in the 2001 *Quadrennial Defense Review*.[14] Two years later, the Department of Defense issued its *Information Operations Roadmap*, intended to serve as a blueprint for the development of IO capabilities.[15] The roadmap recommended the creation of a "well-trained" IO workforce, and identified IO as a "core competency" for warfighters, stating "the importance of dominating the information spectrum explains the objective of transforming IO into a core military competency on par with air, ground, maritime, and special operations."[16]

The Global War on Terrorism. Despite these aggressive mandates, the intervening years—and the Global War on Terrorism (GWOT)—did not result in widespread deployment of Army IO capabilities. Said another way, while the GWOT demonstrated the potential benefits of IO, the application of IO in a static counterinsurgency environment arguably institutionalized many habits that may not readily translate to LSCO. As an example, the staffing, centralization, and withholding of IO authority at echelons above brigade (EAB)—a central attribute of current Army IO doctrine—may limit the Army's ability to deploy IO in a fast-paced LSCO environment.

In fact, third-party experts noted deficiencies in Army IO from the outset of the GWOT.[17] And while Army IO arguably improved during the GWOT, it is difficult to assess the overall impact of IO on adversaries because the targets often lacked meaningful access to digital devices and were arguably less susceptible to American influence than potential near-peer opponents.

To the Army's credit, many senior commanders granted IO deployment authority to battalion- and company-grade officers during the GWOT.[18] This was particularly true for key leader engagements. Junior and field-grade officers were empowered to engage directly with tribal elders, religious figures, and political leaders.[19]

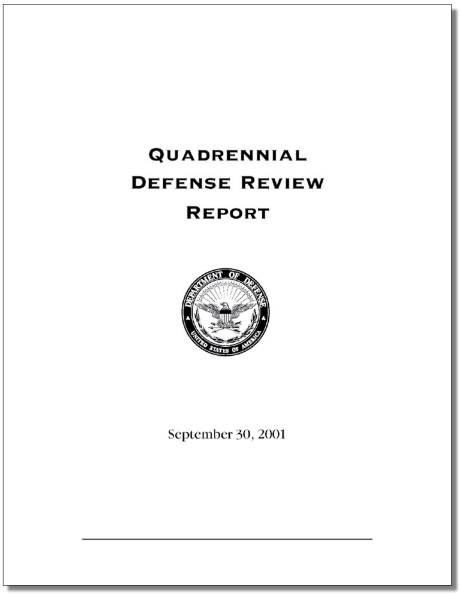
However, according to the Center for Army Lessons Learned, formal IO battle rhythm events that required extensive IO planning and outputs were concentrated at the division and joint task force levels, and largely orchestrated by dedicated IO professionals and IO working groups at EAB.[20] Meanwhile, officers at the point of contact who sought to deploy IO as an alternative to lethal force often faced cumbersome procedures, onerous questioning from targeting boards, and excruciating approval timelines.[21] In evaluating Army IO efforts during the GWOT, it is fair to question why junior and field-grade officers were often encouraged to build interpersonal relationships with centers of influence in Iraq and Afghanistan but excluded from other IO initiatives.

> "In evaluating Army IO efforts during the GWOT, it is fair to question why junior and field-grade officers were often encouraged to build interpersonal relationships with centers of influence in Iraq and Afghanistan but excluded from other IO initiatives."

Critics pointed to these and other deficiencies as the GWOT progressed. Writing in 2007, Dr. Daniel Kuehl, professor of information warfare at the National Defense University, commented that the Army suffered from a deficit of "information strategists" with the ability to "coordinate and exploit the contribution of the information component of power and the synergies it offers."[22] Several years later, Corey D. Schou, J. Ryan, and Leigh Armistead wrote in the *Journal of Information Warfare* that many of the same commands conducting IO "over 15 years ago … are still the key agencies conducting IO, just renamed and slightly expanded, but with no true increase in scope and capability."[23] The authors concluded "it is not surprising that in many ways, the Department of Defense [and by default, the Army] are moving backwards with regard to [IO] strategy, capabilities, and scope."[24]

The failure of the Army (and other service branches) to embrace IO across all combat functions was implicitly acknowledged by the Joint Chiefs of Staff in 2018. The *Joint Concept for Operating in the Information Environment* identified "information" as the seventh joint function for the Armed Forces of the United States.[25] Noting that "every joint force action, written or spoken word, and displayed or related image has informational aspects," the document demanded that the service branches "shift how [they] think about information *from an afterthought* … to a foundational consideration for all military activities."[26]

For the Joint Chiefs to admit that IO was still an operational afterthought—nearly twenty years after the publication of the 2001 *Quadrennial Defense Review*—speaks volumes about the failure of the joint force to recognize the importance of IO and develop IO expertise and capabilities across all combat commands.



QUADRENNIAL DEFENSE REVIEW REPORT

September 30, 2001

To view the 2001 *Quadrennial Defense Review* report, visit https://history.defense.gov/Portals/70/Documents/quadrennial/QDR2001.pdf?ver=AFts7axkH2zWUHncRd8yUg%3d%3d.

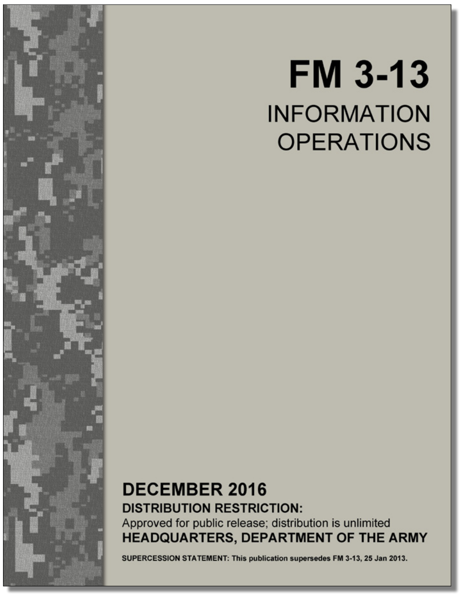
The Present State of Army IO Doctrine

The transition in Army focus from the GWOT to near-peer competition—a policy shift that began in earnest in 2014 with the Russian invasion of Crimea and the U.S. military's shift in focus to the Indo-Pacific theater in response to increasing threats from China—gave the Army an opportunity to rethink its IO strategy.

Near-peer competition also arguably requires a different structural approach to Army IO. As noted above, senior commanders generally oversaw IO campaigns in Iraq and Afghanistan, and delegated campaign execution to subject-matter experts (SME) who did not always possess tactical experience at the point of contact. With the transition from low-intensity conflicts to LSCO, Army leadership reemphasized the need for combat arms to "win at the point of contact" in "all warfighting functions."[27] That principle now echoes throughout Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces*. For example, paragraph 1-26 instructs commanders in LSCO to prepare mission orders that "focus on the purpose of an operation and essential coordination measures rather than on the details of how to perform assigned tasks, giving subordinates the latitude to accomplish those tasks in a manner that best fits the situation."[28]

Field Manual 3-13. Considering the growing need for tactical IO capability, the demonstrated success of IO efforts by near-peer competitors in Syria, and the Army's renewed emphasis on dominating LSCO at the point of contact, it is surprising that the Army's primary IO doctrines continue to reflect a centralized, hierarchical approach to IO deployment. FM 3-13, *Information Operations*, published on 6 December 2016, does not contain a single instruction for the tactical deployment of IO by junior officers or noncommissioned officers (NCOs) in the field. Instead, the manual institutionalizes IO as a function executed primarily at EAB levels.

As an initial matter, we note that much content in FM 3-13 is quite relevant and useful for Army professionals, regardless of rank. The manual offers a concise definition of IO: "the integrated employment, during military operations, of information-related capabilities in concern with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries while protecting our own."[29] The manual identifies IO as an essential feature of all combat operations.[30] And the manual properly identifies the purpose of IO: to "create effects in and through the information environment that provide commanders decisive advantage over enemies and adversaries."[31] Overall, FM 3-13 provides the Army with an outstanding conceptual foundation for IO.



FM 3-13
INFORMATION OPERATIONS

DECEMBER 2016
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited
HEADQUARTERS, DEPARTMENT OF THE ARMY
SUPERCESSION STATEMENT: This publication supersedes FM 3-13, 25 Jan 2013.

To view Field Manual 3-13, *Information Operations*, visit https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf.

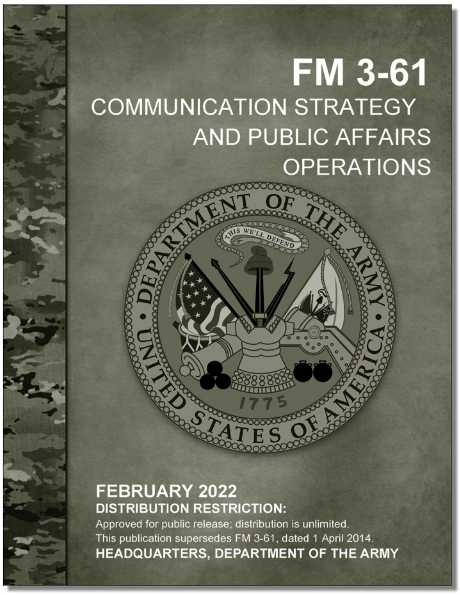
The critical area where we believe FM 3-13 (and Army IO doctrine as a whole) requires revision, considering recent events in Ukraine, is the absence of any specific guidance for or discussion of tactical IO application.[32] The current manual focuses on IO deployment at the EAB level. The manual positions brigade and division staffs as the centerpiece of the IO infrastructure but provides very limited guidance for field-grade officers, junior officers, and NCOs to apply in conducting IO at the point of contact.

Further, FM 3-13 does not encourage brigade and battalion commanders to develop internal IO expertise. Instead, the manual briefly discusses the potential for division commanders to employ an IO specialist and provides an extensive overview of the SMEs available to senior commanders upon request. In other words, the manual seems to conceive of IO as a specialized capability with identical application across the spectrum of Army combat units, regardless of the function a unit serves or the theater where the unit deploys.

Future LSCO will arguably feature a battle rhythm requiring maneuver officers and their support staff—rather than EAB SMEs—to plan and execute IO within the relevant commander's intent. It is therefore critical that the IO field manuals not only discuss IO in accessible language but also offer junior and field-grade officers a practical framework for deploying IO in the field.[33]

Field Manual 3-61. Review of Field Manual 3-61, *Communication Strategy and Public Affairs Operations*, produces a similar result.[34] The manual devotes extensive attention to the Army's public affairs infrastructure, the training of public affairs officers, and the importance of unified messaging across combat commands. The manual also provides detailed descriptions of messaging protocols and the translation of commanders' intent into effective communications by the public affairs officer and subordinates. But the manual devotes almost no attention to how combatants at the tip of the spear—the junior officers and NCOs leading soldiers in combat—can effectively communicate the strategic objectives of the Army and the joint force, or reinforce messaging developed by commanders in the EAB.

> "Future LSCO will arguably feature a battle rhythm requiring maneuver officers and their support staff—rather than EAB SMEs—to plan and execute IO within the relevant commander's intent."


FM 3-61

COMMUNICATION STRATEGY AND PUBLIC AFFAIRS OPERATIONS

FEBRUARY 2022

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes FM 3-61, dated 1 April 2014.

HEADQUARTERS, DEPARTMENT OF THE ARMY

To view Field Manual 3-61, *Communication Strategy and Public Affairs Operations*, visit https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34864-FM_3-61-000-WEB-1.pdf.

There is a fundamental difference, in our view, between instructing public affairs officers in providing rudimentary training to soldiers and empowering the most educated military force in history to make good decisions about content creation and distribution. In an environment where every noncombatant will have a mobile device and the ability to immediately stream footage of Army operations to the world, the failure of the Army to develop doctrine that empowers every soldier to advance favorable narratives and reinforce U.S. war aims leaves a glaring hole in Army LSCO capabilities.

Convergence. Turning from doctrine to planning, the Army's most significant future force initiative, Project Convergence, also relegates IO to a subordinate discipline. Convergence, at its core, focuses on the integration of capabilities from a multitude of domains, including information, and the synchronized deployment of those capabilities against an adversary at greater speed and range to achieve decision dominance. Yet review of the Army Futures Command materials on Convergence—at least those within the public domain—show the same focus on command-level IO deployment and the same preference for the more machine-driven aspects of IO.[35] Theoretically, the concept of convergence compels the Army to match its IO doctrine and techniques to an increasingly flat and interconnected network of battlefield nodes from the point of contact to strategic headquarters.

Present Army training programs for company- and field-grade officers. The absence of IO doctrine focused on tactical deployment would be less noteworthy if Army training programs for new officers, NCOs, and recruits rectified the gap. That is unfortunately not the case. The U.S. Army's Maneuver Center of Excellence curriculum for the Maneuver Captain's Career Course (MCCC) does not contain an instructional block for

IO, and the Command and Tactics Directorate does not employ IO professionals. Of the eight orders produced by students in the MCCC, only one includes a psychological operations team, and effective deployment of that team is immaterial to the student's overall grade.[36]

The Command and General Staff College (CGSC) includes a single two-hour block of instruction in its months-long curriculum to prepare majors to serve at EAB. To be fair, the IO lesson plan thoroughly reviews doctrine and concepts and offers techniques for integration IO planning into the military decision-making and targeting processes. To our point, however, the lesson concentrates on actions at EAB with little focus on integrating or enabling leaders at the point of contact. The CGSC also offers an elective with approximately thirty students attending each class.[37]

> "The IO campaigns waged by Ukraine against Russia are a perfect example of the efficacy of IO when stripped of intellectual pretense and unleashed at the tactical level."

Why is this significant? Because the MCCC and the CGSC produce the majority of maneuver commanders at the company and battalion levels and develop most officers assigned to battalion, brigade, and division staff positions. MCCC and CGSC graduates will therefore play a disproportionate role in the planning and execution of future LSCO. There is no question that future LSCO will feature a contested information environment and cognitive domain. Absent independent study, few of these officers will have any exposure to or training for IO.

In light of the July 2018 mandate from the Joint Chiefs of Staff, instructing the joint force to prioritize IO and identifying information as the seventh joint function, the failure to incorporate IO as a foundational aspect of recruit and officer training curricula is quite striking.

Analysis of the Ukraine IO Campaign

The IO campaigns waged by Ukraine against Russia are a perfect example of the efficacy of IO when stripped of intellectual pretense and unleashed at the tactical level. In many ways, the use of IO by the UA represents the most comprehensive expression to date of the RMA. RMA advocates envisioned a fully networked battlefield with each soldier as a node, capable of receiving and distributing information in real time about enemy movements, fires, capabilities, and morale.

A few caveats are necessary here. First, we acknowledge that we write without the benefit of a full record of UA operations and largely rely on facts drawn from third-party reporting, social media, and public statements from the UA and the government of Ukraine. Second, we acknowledge that we do not currently have access to UA war plans, IO doctrine, training manuals, or policies and procedures governing the use of mobile devices and social media by UA personnel. Third, the record that we do have is biased in favor of content-based IO readily discernible from the public domain. We do not currently have visibility into electronic warfare or psychological operations by the UA or efforts by the UA to disrupt Russian command, control, communications, computers, intelligence, surveillance, and reconnaissance. Therefore, the findings below and our recommendations may require revision as more facts come to light.

Features of Ukraine IO strategy. As we write, the Ukraine army has not only weathered the initial storm of the Russian invasion, but after four weeks of continuous combat, it has also begun to retake territory previously occupied by Russian units. Before the conflict began, these results were inconceivable. The overwhelming majority of pundits, military experts, and public officials in the United States and across the European Union anticipated a rapid Russian victory. That did not happen.

Instead, the UA has inflicted tremendous damage on Russian forces, and in the process, radically altered global perceptions of Russian military competence. While numerous authors have commented on the unanticipated weakness of Russian combat arms, perhaps the most concise summary of this remarkable transformation in perception came from CNA's Michael Kofman. Speaking to War on the Rocks on 7 March 2022, Kofman

A group of Ukrainian men cheer as they take a Russian tank on a joyride on 2 March 2022. (Screenshot from Twitter/@666_mancer)

remarked that he had spent much of the past decade attempting to "convince the world that the Russian Army was not twelve feet tall," but now expected to spend the next decade attempting to convince policy makers that the Russian army was "not two feet tall."[38] Meanwhile, global support for Ukraine has reached heights that were unimaginable when the war began.

Obviously, much of the credit for these titanic opinion shifts in global opinion goes to the competence of the UA and the leadership of Ukraine President Volodymyr Zelensky. But Ukraine is not the first underdog to achieve surprising results against a purportedly superior adversary. In fact, the Soviet Union endured a similar experience in the "Winter War" of 1939–1940, when its invasion of Finland resulted in horrendous casualties.

But the Winter War did not generate the same rapid revision in global perception; while observers at the time noted the poor tactics employed by the Soviet army, few commentators saw in the conflict evidence that Soviet forces were completely inept.[39] Only when the Wehrmacht swept aside Red Army divisions early in Operation Barbarossa did most observers recognize that the Winter War was an accurate reflection of then-existing Soviet capabilities, training, and doctrine. Compare that to the present mood among policy makers in Washington. On 28 March 2022, for example, the *Washington Post* reported that senior Department of Defense officials were convinced that Russia was effectively finished as a global power and ebullient about the prospects for the United States and its allies in future competition with China.[40]

So what has made the difference? The answer is simple. Ukraine, whether by prewar design or by postinvasion necessity, has taken the war viral—unleashing IO at the tactical level and weaving every heroic deed, every Russian misstep, and every successful combat operation into a persuasive multimedia narrative that, when aggregated with ongoing success on the battlefield, has proven largely invulnerable to Russian influence.

We now attempt to isolate—from the thousands of UA videos, social media postings, "tactical TikTok," and pronouncements—the doctrinal foundation and critical features of Ukraine's IO campaign. Because the relevant content is published across diverse platforms, including TikTok, Facebook, Telegram, Twitter, and too many others to name, we focus less on specific examples (and the resulting citations), and more on the general strategies and narrative themes that the UA has used to successfully conduct IO.

Risk acceptance in the use of mobile devices. By far, the most striking characteristic of Ukraine IO has been the prevalence of mobile devices among UA forces. From the opening moments of the Russian invasion, UA personnel were uploading carefully curated imagery, videos, and messages to multiple social media platforms.

A Ukrainian serviceman talks on a smartphone in front of a damaged residential building, allegedly hit by a Russian shell, on 25 February 2022 on Koshytsa Street in a suburb of the Ukrainian capital Kyiv. Russian forces reached the outskirts of Kyiv as Ukrainian President Volodymyr Zelensky said the invading troops were targeting civilians and explosions could be heard in the besieged capital. Russia's full-scale ground invasion and air assault in January claimed dozens of lives and displaced at least one hundred thousand people. (Photo by Daniel Leal, Agence France-Presse)

While we do not, as noted above, have access to current UA policies on mobile devices, it is obvious that the Ukraine army has made a calculated decision to (a) permit some soldiers to retain their devices—whether privately owned or issued—and (b) to use those devices to selectively document combat activities.[41]

What does that tell us? That in confronting an unprovoked invasion by a hostile power, the UA has likely decided to accept the risks that accompany the use of mobile devices in a tactical environment. Put another way, the UA has apparently decided that, since its soldiers are defending their homeland against a hostile invasion, it makes no sense to impose onerous restrictions on devices that have shown meaningful combat potential.

Implementation of best practices for recording and publication. Four weeks into the conflict, it is also apparent that while the UA has decided to accept the risks of allowing soldiers to carry mobile devices at the forward line of troops, it has not given carte blanche to transmit every unscripted moment. Instead, it appears that UA field commanders have included IO in their statements of intent, and company and field-grade officers have given maneuver units guidance on what is and is not appropriate for documentation and transmission.[42]

In some ways, this is more discernable by what is absent from the current landscape than what is present. In surveying the universe of UA messaging, we have seen little to no evidence of the following: (1) Russian soldiers in flex cuffs or otherwise restrained after combat, (2) documentation of Russian fatalities that permits identification, (3) severely wounded Russian soldiers, (4) punishment or torture inflicted on Russian combatants, (5) videos of UA tactics that resemble tactics employed by insurgents in Iraq or Afghanistan and that might therefore inspire conflicted emotions from viewers in NATO units—such as IEDs, (6) documentation of vindictive actions taken by UA personnel or Ukraine civilians on Russian prisoners, or (7) overt taunting or mockery of Russian personnel or Russian capabilities.[43]

Now contrast that to the most common tactical scenarios on social media platforms: (1) the aftermath of antitank guided missile (ATGM) strikes on Russian convoys, (2) the poor supply situation affecting Russian soldiers, (3) the high state of morale among UA squads and platoons, (4) the compassion of UA soldiers for civilians and noncombatants, (5) the heroic exploits of individual UA personnel, and (6) the use of excessive force by Russia against civilian targets.

Some might argue that the above merely reflects the exercise of common sense by UA personnel or aggressive filtering by combat commanders. We believe that explanation is too simplistic. The type of images and videos missing from the narrative represent the "worst nightmare" of every combat commander, and senior Army leaders have invoked the same to deny mobile devices to soldiers in active combat. And lest we forget, UA personnel are operating under conditions of immense stress, facing an enemy that has shown no qualms in the indiscriminate use of unguided munitions against a civilian population. Yet at least in terms of publication, UA personnel have shown tremendous discipline in their use of mobile devices and social media.

While we have no direct evidence, we believe that the best explanation for the above is that the UA has provided practical guidance to its personnel on the appropriate uses of mobile devices and content that is suited for distribution. We further believe that UA personnel have embraced this trust and discretion and demonstrated tremendous buy-in to achieve their strategic and tactical objectives.

Leveraging civilian expertise to build an IO infrastructure. While much of the footage of UA operations appears to come from the mobile devices held by UA personnel, the vast volume of publication across numerous social media platforms, and the postproduction processing (such as time stamps, text, and other after-the-fact edits) show that Ukraine has also implemented a substantial IO support infrastructure.

Given that the UA is relatively small, it is not surprising that rather than assign soldiers fit for combat to IO support, Ukraine relied on its substantial civilian expertise in information technology. On 26 March 2022, *The Economist* highlighted how the UA mustered substantial portions of Ukraine's private sector to support its IO campaigns.[44] Noting how the Ukraine government mobilized the private sector shortly after the invasion, *The Economist* noted that "across Ukraine, public-relations specialists, designers and other media types have banded together through bottom-up networks that emerged within hours of the invasion."[45] The result has allowed Ukraine to focus its limited military manpower on combatants, but also provided expertise that the UA arguably lacked before the war began. These ad hoc, public-private partnerships have likely facilitated the widespread distribution of what otherwise might have been limited and isolated publications by tactical combatants.

The absence of embedded reporters. One of the most compelling contrasts between Ukraine IO and the IO/PA efforts of the Army in the GWOT is authenticity. Ukraine has forsaken the U.S. Army approach of permitting approved reporters to embed with tactical units and report their observations. Regardless of the underlying intent, the resulting coverage never, in our opinion, produced an authentic interpretation of events as they unfolded. Not only were the reports often delayed due to the use of traditional media outlets and long-form journalism, but readers on the home front understood that the footage and articles were subject to curation and careful review, if not by the Army, then by network executives.

Ukraine, by contrast, has seemingly made little effort to arrange for embedded media or scripted coverage, at least for international correspondents. Instead, whether by design or necessity, Ukraine has frequently distributed live-action footage alongside announcements from its military about operations and outcomes. While some of the footage released by the UA shows signs of editorial review, rarely do the clips contain narrative overlays, expert analysis, or overt propaganda. By letting its soldiers and the power of imagery tell the story, Ukraine has ensured a more authentic record of its resistance. In our opinion, the absence of embedded reporters and staged interviews has contributed to the massive outpouring of international support for the UA and for Ukraine's political leadership.

Use of military IO to reinforce political messaging. Ukraine has also leveraged military imagery and narratives to validate and reinforce the decisions and messaging of its political leadership. Zelensky and his key ministers have shown remarkable discipline in articulating a unified message to Russia (Ukraine will resist to the end), to Ukraine citizens (your leadership is here, will stay here, and will suffer with you), and to NATO leadership (we require your help and are grateful for your assistance). These themes are communicated across social media platforms and echoed in every speech, press conference, and meeting with foreign dignitaries.

The UA shows how effectively the battlefield imagery published by the UA and its organic support infrastructure reinforce Ukraine's political messaging. When NATO forces began to supply Ukraine with antitank guided missiles, for example, the UA distributed videos from combat units gratefully unpacking British Next-Generation Light Antitank Weapons and using Javelin missiles to disable Russian armored vehicles. Taken together with stunning images of the devastation caused by Russian artillery and missile strikes, and selectively published photographs of wounded civilians, this coordinated IO campaign made it very difficult for NATO governments to refuse additional aid.

Similarly, Ukraine has opted for complete transparency in the publication of Russian military efforts to disrupt or eliminate its political leadership. For example, as Zelensky and his military and civilian advisors publicize their activities on a daily basis, meet with combat units, and emphasize their commitment to staying the course, the UA has selectively released evidence that Russian units have sought to kill Zelensky and seize control of Ukraine's political institutions.[46] The concurrent narrative of a political leader refusing to abandon his people while repeatedly surviving military decapitation attacks that flout international law has helped propel Zelensky to global prominence while further degrading the reputation of President Vladimir Putin.

Thematic Narratives

It is also important to highlight the thematic focus of Ukraine's IO campaign, as these narratives have resonated with a global audience that, before hostilities broke out, seemed remarkably uninterested in Ukrainian affairs.

UA battlefield performance. Perhaps the most frequent subject of Ukraine IO is highlighting the success of its forces in engaging Russian units. The videos of Ukraine ATGM teams ambushing Russian armor or devastating Russian supply columns contain far more narrative power than the most beautifully written piece of favorable journalism. Similarly, videos of Ukraine antiaircraft units successfully engaging Russian helicopters and attack aircraft have rallied the population centers subject to attack.

Zelensky condemns Putin's 'genocide' after seeing sickening aftermath
HORRORS OF WAR SHOCK HERO OF UKRAINE
INSIDE: TRIBUTE TO THE LEGENDARY JUNE BROWN
A message to the Russian people...
Вам нужно знать
YOU NEED TO KNOW
The Guardian
Horror in Bucha: Russia accused of torture and massacre of civilians
by AMANDA PLAT
Moscow accused of genocide and war cri
executions, rapes and mass graves revea
Russian retreat echo horror of Second Wor
PUTIN'S STA
ON HUMANIT
EXCLUSI
THE TIMES
The no-fault divorce
How to end it (amicably)
I nearly fell for a Kremlin honeytrap by Bill Browder
Civilians 'shot in the streets'
METRO
PUTIN'S WAR CRIME SHAM
EVIDENCE OF THE MASS KILLINGS OF CIVILIANS GROWS AS RUSSIANS RETREAT
UK VOWS THAT KREMLIN LEADERS WILL FACE JUSTICE FOR MASSACRES
'WORSE THAN ISIS'

Recent headlines reflect the social media content posted by Ukrainian soldiers on the battlefield. (Composite graphic by Beth Warrington, Army University Press)

Russian war crimes. The UA has also made a point of highlighting Russian tactics that potentially violate international law. In particular, the UA and the Ukraine government have circulated a large volume of video demonstrating the indiscriminate use of heavy artillery, rocket artillery, and thermobaric weapons against population centers. More recently, the UA has focused on showcasing conditions in the eastern theater of operations, where Russian forces have laid siege to Mariupol. The images and videos, again often shared on social media with little to no narrative overlays, have eliminated any opportunities for Russia to plausibly defend its war aims and further rallied international support for UA resistance.

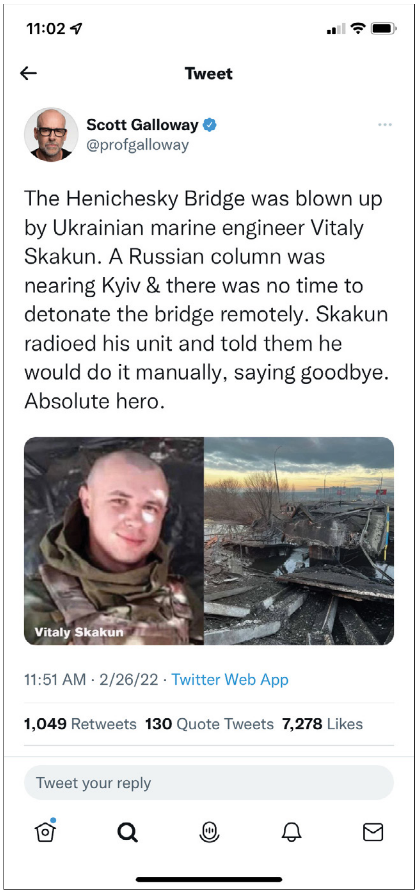
> "The images and videos, again often shared on social media with little to no narrative overlays, have eliminated any opportunities for Russia to plausibly defend its war aims and further rallied international support for UA resistance."

Russian logistical difficulties. While many UA IO efforts focus on documenting combat efficacy, the UA has also layered IO onto its lethal targeting priorities by documenting the consistent failure of Russian forces to protect supply columns and the poor logistical performance of the Russian army. Social media is replete with video documentation of UA strikes on Russian trucks and transports, and similar footage of captured Russian equipment revealing shoddy maintenance, insufficient food and water, and the absence of adequate medical supplies. While some of the documentation is clearly after the fact and may originate from civilian sources, there is also abundant footage shot by UA infantry during or shortly after engagements. Importantly, Russian soldiers captured or killed by Ukraine forces have often been in possession of mobile devices, and there are reports that Ukraine has focused its IO targeting efforts on ensuring that Russians are able to access and view combat footage. Thus, Russian soldiers intimately aware of shortages are subject to further demoralization in the form of daily announcements about the destruction of additional supplies.

Statements from Russian prisoners. One of the most powerful moments in the Ukraine IO offensive came on 9 March when Ukraine officials released interviews taken with Russian prisoners captured during combat operations.[47] Each of the prisoners affirmed that they were speaking to media outlets voluntarily and provided stunning revelations about the conduct of senior Russian officers in advance of the invasion. Specifically, the Russian soldiers testified that enlisted personnel received no prior notice of the invasion and received no briefings on operational plans. The soldiers further testified to shortages of food, medical supplies, and adequate clothing. Finally, the soldiers claimed to have been misinformed about both the purpose of the operation and the reception to expect from the UA and from Ukraine civilians. And because Ukraine permitted the soldiers to speak rather than layering their words with narratives and/or arranging media interviews, the messaging resonated with the target market—civilians in the NATO countries supplying the UA with critical munitions.

Heroic deeds. The UA has also prioritized distribution of narratives surrounding heroic deeds by Ukrainian personnel. Very early in the conflict, the focus of these narratives was the potentially mythic "ghost of Kyiv," a Mig-29 pilot allegedly responsible for numerous air-to-air kills.[48] Later, Ukraine media and the UA lauded the heroic sacrifice of combat engineer Vitaliy Skakun, who sacrificed himself to complete the demolition of the Genichesky Bridge on the Crimean isthmus.[49] Finally, there was the widely publicized engagement between a Russian frigate and a small detachment of Ukraine personnel on Snake Island.[50] Initially, reports suggested that when the frigate demanded that Ukrainians surrender, Ukrainian personnel responded with obscenities, and were killed to the last man. It was later acknowledged that the Russians had captured Snake Island and merely taken Ukrainian soldiers as prisoners, but by that point, the image of Ukrainian resolve was firmly fixed in the global conscience.

The tendency of UA IO practitioners to stretch the truth highlights an important lesson for future LSCO.



11:02

Tweet

Scott Galloway
@profgalloway

The Henichesky Bridge was blown up by Ukrainian marine engineer Vitaly Skakun. A Russian column was nearing Kyiv & there was no time to detonate the bridge remotely. Skakun radioed his unit and told them he would do it manually, saying goodbye. Absolute hero.

Vitaly Skakun

11:51 AM · 2/26/22 · Twitter Web App

1,049 Retweets 130 Quote Tweets 7,278 Likes

Tweet your reply

(Screenshot from Twitter/@profgalloway)

The Army cannot expect domestic media outlets to provide the same leeway to public statements or narratives, as the international media has afforded Ukraine. In many ways, the international media have afforded Ukraine a measure of forgiveness for factual errors. The Army must expect the opposite. Every Army factual error or exaggeration, no matter the source, will be magnified and cited as evidence of dishonesty. It is therefore imperative that all commanders that implement IO insist facts drive the narrative and train their subordinates that it is better to omit a publication altogether than to push out content that may not withstand scrutiny.

Presidential appearances. We would be remiss if we did not discuss the appeals and statements issued by Zelensky. From the tactical garb that the president donned after the invasion began to his epic video on the streets of Kyiv early in the invasion, when Zelensky personally refuted Russian reports that he had fled the capital, the Ukrainian president has become a critical component of the UA IO offensive.[51] Arguably, Zelensky's aggressive use of social media, in the form of Twitter statements and live appeals for military assistance, were the critical factor in persuading NATO governments to increase their military support. Zelensky also gained legendary status when he refused U.S. offers to evacuate from Kyiv, allegedly telling State Department officials that he "needed ammunition, not a ride." Through these and other direct statements, and appeals to NATO governments, the president has reinforced the IO effects of the UA while generating massive support for Ukraine across the globe. And Zelensky's widely publicized and repeated visits to the front lines have corroborated the emerging narrative of his personal heroism.

Comic relief and adversary humiliation. The final theme of the IO offensive that we wish to highlight is the use of comic relief to humiliate the adversary in the international court of public opinion. Of all the UA narratives to heap scorn on the Russian military, none have had more impact than the repeated videos of Ukraine farmers using John Deere tractors to tow away abandoned or disabled Russian military vehicles. The sight of multiple T-90 tanks and advanced air defense systems dragged behind Ukrainian tractors after either running out of gasoline or suffering mechanical breakdowns is now a global meme for Russian military incompetence. Making these narratives more compelling is, once again, the relative absence of commentary or heavy edits. While UA IO teams may identify or take these videos and increase their circulation, the UA has largely allowed the images to speak for themselves—adding authenticity to an already compelling storyline.

Ukrainian President Volodomyr Zelensky addresses his country 3 April 2022 following the massacre of Ukrainian civilians by Russian military forces in Bucha. (Screenshot from YouTube/President of Ukraine)

Recommendations and Caveats

If the war in Ukraine offers a preview of future Army engagements—and we believe it does—then LSCO will offer a target-rich IO environment. Three characteristics of near-peer LSCO make these engagements particularly suitable for IO deployment.

First, because future LSCO would be likely be waged against state militaries, LSCO offer an unprecedented opportunity to target the nexus of an adversary's military leadership, political leadership, and popular support—a radical departure from recent counterinsurgency campaigns.

> "Digital devices will blanket the battlefield in any future near-peer engagement. Even if the Army retains its current restrictions on personal devices, future adversaries may not."

Second, digital devices will blanket the battlefield in any future near-peer engagement. Even if the Army retains its current restrictions on personal devices, future adversaries may not. We also anticipate that every noncombatant will have access to multiple digital platforms. In Ukraine, for example, the latest figures show that at least 70 percent of the population have internet access, while 87 percent have access to a 4G/LTE network.[52] Therefore, IO practitioners will have a broad array of options for generating influence.

Third, the pace and scale of LSCO will require a faster IO decision cycle involving more decision-makers. In Ukraine, the UA is currently engaged in LSCO on three fronts, each featuring multiple commanders at the EAB, and all in direct proximity to a civilian population. To prevail in this ultimate test of wills, the UA must rapidly identify IO targets that align with tactical objectives, push out information, assess the impact, and prepare for the next cycle—while simultaneously ensuring appropriate coordination with civilian authorities. Such a rapid operational tempo—that almost certainly will characterize future Army engagements—is fundamentally incompatible with the concentration of IO at the EAB. As noted above, Ukraine has deployed its entire civilian IT infrastructure alongside its IO experts and combatants to expedite the targeting and distribution cycle. Present Army IO strategies do not in any way account for the pace and scale of LSCO.

Policy Recommendations

In the hopes of helping the Army capitalize on the success of the UA and implement prudent modifications to current IO doctrine suitable for near-peer LSCO, we humbly offer the following recommendations for consideration.

First, we recommend revisions to Army doctrine to require the incorporation of IO in all statements of commander's intent, at least at the brigade combat team-level and above. A commander's IO intent should be articulated in the statement describing the purpose of the operation (often addressing the operational framework) or the end state the operation seeks to achieve. The incorporation of IO into the commander's intent will ensure that company-grade commanders incorporate IO into their own procedures for briefing and deploying tactical units. At the present, IO is generally absent from commander's intent. Instead, most EAB staffs prepare a separate statement of intent specifically focused on IO and relegate the statement to the base order's IO annex. It is therefore unsurprising that IO remains an ancillary consideration in the planning and execution of LSCO. By requiring combat commanders to address IO before operational planning begins, the Army will ensure that IO figures prominently in every commander's approach to future engagements.

Second, the Army and the joint force must debate the appropriate amount of IO and PA control that is appropriate for LSCO. Under the policy mandates of ADP 6-0, that debate should center on the degree of empowerment and execution appropriate to the situation. In our view, achieving significant IO outcomes will require less control by the EAB. The more senior commanders consolidate IO and PA at the division and brigade levels, the less likely the Army is to achieve the results seen by Ukraine. This is hardly a revolutionary idea; the core of the Army's approach to mission command is to empower subordinates wherever possible and appropriate. This could see leaders at the point of contact not waging their own discrete IO but rather rapidly feeding relevant facts, truths, and narratives only available at the forward line of troops up through the chain of command using Integrated Tactical Network end-user devices—Samsung phones with cameras—to drive the tempo of IO targeting while pushing their own facts, truths, and narratives through engagement and psychological operations.

This comes with some risk acceptance by EAB leaders, which private sector research indicates may be reasonable. In recent years, domestic corporations have increasingly empowered employees to use social media and other digital tools to advance corporate aims and market products and ideas while also tracking the statements of competitors to identify opportunities for capturing market share. Generally, corporations that vest junior and mid-career employees in public-facing positions (such as sales, marketing, diversity and inclusion, and vendor management) with publication discretion rely on training, best practices, and oversight to ensure compliance with federal law and the mission and goals of the organization—the civilian equivalent of commander's intent. Corporations that take this leap nearly universally find that employees embrace the trust and responsibility conferred and use the discretion provided to bolster customer relationships and improve productivity and profitability.[53] By contrast, there are relatively few instances where *employees* (as opposed to activists, hackers, or competitors) have used social media to reveal trade secrets, disclose confidential information, or otherwise compromise corporate interests. Summarized succinctly, corporations that trust and educate their people in the information domain achieve better results. We believe the same will be true for the Army maneuver units in future LSCO.

Third, the Army and the joint force must enable echelons at the tactical level to create IO and PA effects. This is not merely a matter of doctrine and mission command. Producing tactical IO results will require examination of technology infrastructure and staffing, and review of the equipment provided to soldiers on the front lines. The Army must also review policies governing military hardware, including the Samsung end-user devices currently fielded as part of the Integrated Tactical Network, and the potential viability of personally owned devices for official use.

Fourth, as we noted earlier, the Army as an institution should emphasize IO education, starting with entry-level officer training and the education of NCOs. Presently, IO education for tactical warfighters is cursory at best. As a result, junior officers and NCOs lack the professional foundation for conducting offensive IO. More importantly, without a doctrinal grasp of IO, the soldiers most vulnerable to enemy IO on the battlefield may struggle to recognize and mitigate adverse effects. They certainly will lack the intellectual agility to know how their feel for the battlefield can contribute tangibly to their battalion commander's IO line of effort. The current generation of platoon and company leaders had access to smartphone technology from the age that they could reasonably gain digital literacy. Their generation possesses an unprecedented familiarity with technology and the skills to influence. It is now up to the Army to educate tactical leaders on how that skill contributes to the broader operational framework.

Fifth, Army and joint targeting methodologies provide a readily available medium for the deployment of IO in multi-domain operations. Targeting boards should not allow IO to be eclipsed by lethal effects. This may require staffing targeting boards with an IO professional, as the Army brigade combat team PA officer cannot reasonably conduct public affairs activities and remain an active member of the targeting team.[54] Further, the Army should scrutinize LSCO assumptions about the pace of IO. In doing so, the Army and the joint force may determine that IO targeting cycles move faster than lethal targeting cycles. Brigade targeting boards routinely convene based on the air tasking cycle. The tasking cycle generally occurs every twenty-four hours and projects assets for seventy-two hours. Arguably, a social media influence cycle will repeat multiple times within a single tasking cycle, rendering targeting boards reactive rather than offensive. In either case, those findings should be incorporated into the targeting process and unit standard operating procedures, even if the outcome is the creation of a separate IO targeting board.

Sixth, the U.S. Army Training and Doctrine Command must double down on its investment in the Information Operations Network (ION), the series of closed internets that contribute to the realistic training environment at the combat training centers (CTCs). ION currently hosts applications that mimic the most popular social media applications, and it allows a limited number of devices to interact, both friend and foe. To date, the ION and applications on it are largely used for open-source intelligence and less so for IO.[55] Improvements to the ION should include an increase in the number of phones issued for use commensurate with the inundation of phones on the LSCO battlefield, a full upgrade of the network's 4G/LTE capability, and the continued evolution of applications in use on the ION to better replicate the quality and plethora of social media applications available worldwide. Further, units training at the CTCs should be incentivized to increase their use of ION to support IO influence in the cognitive domain. With improvements to IO education, manning, doctrine, and techniques, the ION-enabled CTCs will become the proving grounds for the future of IO at the point of contact.

> "IO doctrine must provide maneuver and planning officers with a functional understanding of IO that readily translates to future LSCO, and a practical and flexible menu of techniques and options for using IO to achieve effects on the battlefield."

Seventh, the Army should incorporate tactical application in future revisions to FM 3-13 and FM 3-61 and incorporate IO into the MCCC and CGSC curricula.

We believe that IO doctrine must provide maneuver and planning officers with a functional understanding of IO that readily translates to future LSCO, and a practical and flexible menu of techniques and options for using IO to achieve effects on the battlefield. IO is a relatively straightforward capability. It is no more difficult to comprehend intellectually than the lethal force doctrine that junior officers must master before earning the right to lead troops in combat. Yet the combat potential of IO is, in our view, too often obscured by the highly abstract and technical language used to convey Army IO doctrine.

The demands on maneuver officers and their field-grade counterparts on battalion and brigade staffs are considerable. In the high-pressure and fast-paced planning environment that will characterize future LSCO, it is simply unrealistic to expect staff and maneuver officers and NCOs to deploy effective IO campaigns when Army IO doctrines remain abstract and conceptual rather than practical.

The Army excels at translating complex lethal-force concepts into accessible materials for rapid absorption and application to a tactical environment. The same should be true for IO. Given the absence of IO from nearly all officer training, we support the development of concrete and highly accessible IO doctrine that permits rapid assimilation of IO principles and ready translation of those principles into practice.

Eighth, the Army need not reinvent the wheel. The IO campaigns executed by Ukraine have roots in and borrow heavily from the social media and information strategies of domestic corporations. *The Economist*, among others, has repeatedly highlighted the contributions of Ukraine's private sector. The private sector in the United States leads the world in the use of information to persuade, inform, compete, and influence behavior. The Army would be foolish not to leverage such expertise.

The appalling behavior by Russian forces in Ukraine also offers the Army a convenient basis to open conversations with the companies largely driving the IO revolution. Any arguments about the relative values of the United States and its near-peer competitors have vanished over the past three years, with the indiscriminate use of Russian artillery in Ukraine and the absence of Chinese condemnation serving as the final nail in the coffin. The Army should seize this moment to on-board expertise from the private sector to bolster IO capabilities. For lessons in outreach, the Army can look to the efforts of former Air Force Assistant Secretary of Acquisition William Roper, who made tremendous progress in expanding the defense industrial base to include cutting-edge, privately held companies focused on sensors, software development, and materials science.

Caveats

We make these recommendations while remaining cognizant of several underlying realities. First, Army and joint force leadership can raise legitimate questions about the relationship between tactical IO and increased risks to information and network security. We are not experts on cybersecurity or network infrastructure, and we do not purport to offer solutions to this tension. However, we do believe it is possible to strike an appropriate balance between deployable IO capabilities at the tactical level and information security.

Emissions control is also a legitimate concern, as is the potential geotracking of units in the field. It is important to note, however, that unless future Army deployments occur in an unpopulated area, noncombatants will likely observe and report on all movements and actions by Army units operating on foreign soil via mobile devices or other means. Note that in Ukraine, even when Ukrainian citizens refrain from publishing information on UA units operating in their vicinity, journalists and expatriates from other countries have published real-time video and photographs of UA soldiers that permit the identification of units, assessments of size and scale, and armaments. Further, Army units engaged in LSCO produce a massive electromagnetic footprint that will scarcely be affected by the use of mobile devices by individual soldiers. Again, we believe that the potential power of IO as a tactical capability supports exploring the appropriate balance with emissions control.

Finally, we acknowledge the delicate balance between effective IO and compliance with the Uniform Code of Military Justice (UCMJ) and the Geneva Conventions. Some Ukrainian IO, while arguably compliant with the Geneva Conventions, would likely run afoul of the UCMJ or existing Army best practices on the treatment of enemy combatants and the publication of enemy casualties. And if history is any guide, Army forces in the next war will be subject to far greater scrutiny from U.S. media outlets—which has generally refrained from criticizing Ukraine IO. The importance of Geneva Conventions and UCMJ compliance further reinforces the need for the Army to develop highly effective training modules for junior officers and NCOs to ensure that adequate instruction is provided to all soldiers at the tip of the spear.

Conclusion

In writing this article, we were guided by one fundamental conviction: that by successfully deploying IO as a tactical combat capability, the UA has erased any doubts about the significance of IO as a core component of modern warfare, and it is a domain the Army must master to achieve battlefield dominance in future LSCO.

To its credit, over the last eight years, the Army has embraced the shift to great-power competition and undertaken a systematic effort to modernize and streamline its lethal force capabilities, doctrine, and training for near-peer engagement. As part of that modernization, the Army has boldly embraced recent changes in munitions, C4/ISR, and unmanned aircraft systems. Army warfighters and doctrine writers, in our view, deserve tremendous credit for these efforts, particularly given the nearly overnight shift in Army focus from counterinsurgency to great-power competition.

IO is the one domain where the Army and the joint force must make significant and meaningful improvements. At a minimum, the Ukraine experience demonstrates the need for the Army to develop a practical approach to IO that emphasizes the ability of information, in all its modern facets, to diminish enemy will.

Ultimately, all UA IO—from the celebration of heroic deeds and the photographs of burned-out supply columns to the videos of UA soldiers opening ATGM shipments—has one objective: reducing Russian morale and will to fight. TikTok videos and Telegram taunts are not bullets, but in our view, the tactical deployment of IO has contributed significantly to UA lethality. The numerous reports of low Russian morale, elite Russian units fleeing at the first sign of contact, and fratricide among Russian enlisted personnel and officers testify to the efficacy of UA IO and the integration of IO into all aspects of UA combat operations.

Our review of existing Army IO capabilities and infrastructure suggests that, were the Army to face a near-peer opponent in LSCO soon, the Army could not reasonably expect to match the UA standard. That must change, and we hope this article will facilitate the difficult conversations necessary to rectify the prevailing gaps in Army IO capabilities. ■

Notes

1. Currently, public domain primary source material on Ukraine's current information operations (IO) strategy, policies, procedures, and training is extremely limited. The conclusions on Ukrainian military strategy we offer are therefore preliminary, drawn primarily from open-source intelligence and may require supplementation or revision based on the future dissemination of primary source material.

2. For scholarship on IO and public affairs efforts in the Second World War, see Anthony Rhodes, *Propaganda: The Art of Persuasion: World War II* (New York: Chelsea, 1988); John W. Dower, *War Without Mercy: Race & Power in the Pacific War* (New York: Pantheon, 1987); and Allen Winkler, *The Politics of Propaganda: Office of War Information, 1942-1945* (New Haven, CT: Yale University Press, 1978). On Vietnam, see Caroline Page, *U.S. Official Propaganda During the Vietnam War, 1965-1973: The Limits of Persuasion* (New York: Bloomsburg Academic, 1981); and Robert W. Chandler, *War of Ideas: the U.S. Propaganda Campaign in Vietnam* (Boulder, CO: Westview Press, 1978). For Operation Desert Storm, we recommend Michael R. Gordon and Bernard R. Trainer, *The General's War: The Inside Story of the Conflict in the Gulf* (New York: Little, Brown, 1995).

3. For examples of revolution in military affairs (RMA) scholarship, see Elinor C. Sloan, *The Revolution in Military Affairs* (Montreal: McGill-Queen's University Press, 2002); Ashton B. Carter and William J. Perry, *Preventative Defense: A New Security Strategy for America* (Washington, DC: Brookings Institution Press, 1999); John Arquila and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997); Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND Corporation, 1996); and Earl H. Tilford Jr., *The Revolution in Military Affairs: Prospects and Cautions* (Carlisle, PA: U.S. Army War College Press, 1995).

4. Molander, Riddile, and Wilson, *Strategic Information Warfare*, 15–19.

5. With the benefit of hindsight, it is tempting to classify the RMA as a misguided attempt to endorse wholesale revisions to Army doctrine, based on the speculative combat potential of immature technology and "netcentric" warfare. Critics of the RMA often invoke costly, problematic experiments such as LandWarrior to discredit an entire generation of professional military scholarship. We believe that approach is simplistic and fails to account for the austere budgets and global obligations the Army faced following the collapse of the Soviet Union, and the difficulties of adapting to a unipolar world order while simultaneously implementing massive conventional force reductions. Viewed in that context, it is readily apparent why the RMA had such appeal to senior warfighters instructed to do more with less.

6. Paul E. Menoher Jr., "Force XXI: Redesigning the Army through Warfighting Experiments," *Military Intelligence Professional Bulletin* (April-June 1996): 6–8, accessed 11 April 2022, https://www.ikn.army.mil/apps/MIPBW/MIPB_Issues/MIPB%20Apr%201996.pdf.

7. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-5, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Twenty-First Century* (Fort Monroe, VA: TRADOC, 1 August 1994 [obsolete]), Glossary-4.

8. Field Manual (FM) 100-6, *Information Operations* (Washington, DC: U.S. Government Printing Office, 27 August 1996 [obsolete]), Glossary-7.

9. Robert J. Bunker, *Information Operations and the Conduct of Land Warfare*, Land Warfare Paper 31 (Arlington, VA: Association of the United States Army, 1998), accessed 11 April 2022, https://www.ausa.org/sites/default/files/LWP-31-Information-Operations-and-the-Conduct-of-Land-Warfare.pdf.

10. Ibid., 2.

11. Joint Chiefs of Staff, *Concept for Future Joint Operations: Expanding Joint Vision 2010* (Fort Monroe, VA: Joint Warfighting Center, 1997), 85.

12. Ibid.

13. Gordon R. Sullivan and James M. Dubik, *War in the Information Age* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 6 June 1994).

14. Department of Defense (DOD), *Quadrennial Defense Review Report* (Washington, DC: DOD, 30 September 2001), 43.

15. DOD, *Information Operations Roadmap* (Washington, DC: DOD, 30 October 2003).

16. Ibid., 4.

17. Peter W. Singer, "Winning the War of Words: Information Warfare in Afghanistan," Brookings Institution, 23 October 2001, accessed 11 April 2022, https://www.brookings.edu/research/winning-the-war-of-words-information-warfare-in-afghanistan/ (highlighting poor outcomes of Army IO during initial Afghanistan campaigns).

18. U.S. Army Combined Arms Center (USACAC) Center for Army Lessons Learned (CALL) Report No. 08-31, *Gap Analysis: Information Operations Tactics, Techniques, and Procedures* (Fort Leavenworth, KS: USACAC CALL, May 2008); CALL Initial Impressions Report, *III Corps as Multinational Corps Iraq, December 2006-February 2008* (Fort Leavenworth, KS: USACAC CALL, n.d.); USACAC CALL, *Tactical Commander's Handbook: Information Operations* (Fort Leavenworth, KS: USACAC CALL, May 2005).

19. This dynamic conforms to the personal experience of author Theodore Kleisner as a company commander in the 82nd Airborne Division, where he served as a member of the Shullah District Council in Baghdad and received significant discretion to operate and meet with local leaders, within the defined intent of his superior officers.

20. Ibid.

21. Kleisner served as a Combined Joint Special Operations Task Force J-3 and commander during four deployments from 2010 to 2013 in Afghanistan. This statement reflects his professional experience in those assignments.

22. Dan Kuehl, "Introduction: 'Brother, Can You Spare Me a DIME?,'" in *Information Warfare: Separating Hype from Reality*, ed. Leigh Augustine (Dulles, VA: Potomac Books, 2007), 1.

23. Corey D. Schou, J. Ryan, and Leigh Armistead, "Developing an Academic Curriculum in Information Operations: The First Steps," *Journal of Information Warfare* 8, no. 3 (2009): 50.

24. Ibid.

25. Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)* (Washington, DC: DOD, 25 July 2018), iii.

26. Ibid., viii (emphasis added).

27. Michael X. Garrett, "Winning at the Point of Contact," Army.mil, 13 August 2020, accessed 11 April 2022, https://www.army.mil/article/238107/winning_at_the_point_of_contact.

28. Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. Army Government Publishing Office [GPO], July 2019), 1-6.

29. FM 3-13, *Information Operations* (Washington, DC: U.S. GPO, 6 December 2016), 1-2.

30. Ibid., 1-3.

31. Ibid., 1-4.

32. Ibid., 9-1–9-2. FM 3-13 as presently construed devotes two pages to IO below the brigade level.

33. The authors cannot emphasize strongly enough that their desire to see future IO doctrine expressed in concise and practical language does not in any way imply that junior- and field-grade officers are incapable of understanding and processing complex and abstract ideas or technical explanations. Rather, the authors believe that in future large-scale combat operations, the maneuver and staff officers charged with planning and deploying IO at the point of contact will operate under incredible stress. Many officers may be required to learn IO "on the fly," in addition to numerous other responsibilities. Therefore, the authors believe that IO field manuals should provide tactical warfighters with concrete and readily applicable explanations and techniques for exploiting IO at brigade level and below.

34. FM 3-61, *Communication Strategy and Public Affairs Operations* (Washington, DC: U.S. GPO, February 2022).

35. See "Project Convergence," Army Futures Command, 2022, accessed 12 April 2022, https://armyfuturescommand.com/convergence/ (discussing features of Project Convergence and describing methodology and areas of focus); Stew Magnuson, "Army's Project Convergence Continues on 10-Year Learning Curve," *National Defense* (website), 17 December 2021, accessed 12 April 2022, https://www.nationaldefensemagazine.org/articles/2021/12/17/armys-project-convergence-continues-on-10-year-learning-curve.

36. Author interview with small-group instructor, U.S. Army Maneuver Center of Excellence, Maneuver Captain's Career Course, 27 March 2022.

37. Author review of Command and General Staff College (CGSC) lesson plan for IO and an interview with an Army doctrine writer and former CGSC instructor, U.S. Army Combined Arms Center, Fort Leavenworth, Kansas, 28 March 2022.

38. Michael Kofman and Ryan Evans, *11 Days In: Russia's Invasion Stumbles Forward* (podcast), War on the Rocks, 7 March 2022, accessed 14 April 2022, https://warontherocks.com/2022/03/11-days-in-russias-invasion-stumbles-forward/.

39. See William R. Trotter, *The Winter War: The Russo-Finish War of 1939-1940* (London: Aurum Press, 1991).

40. Greg Jaffe and Dan Lamothe, "Russia's Failures in Ukraine Imbue Pentagon with Newfound Confidence," *Washington Post* (website), 26 March 2022, accessed 13 April 2022, https://www.washingtonpost.com/national-security/2022/03/26/russia-ukraine-pentagon-american-power/.

41. We purposefully do not cite specific examples from Twitter, Telegram, TikTok, or other platforms to corroborate this point and others that follow, for several reasons. First, the sheer volume of IO, the ephemeral nature of many postings, and the difficulty of pinpointing the original source for an image or video (as opposed to a retweet, share, or copy). Second, much of the IO playing out between Ukraine and Russia is first distributed on an encrypted messaging platform (Telegram) that we are not professionally authorized to use. Nor do we possess the necessary expertise to find and cite to original Telegram content.

42. Michael Kofman and Ryan Evans, *A New Phase of the Russo-Ukrainian War Begins* (podcast), War on the Rocks, 27 March 2022 accessed 12 April 2022, https://warontherocks.com/2022/03/a-new-phase-of-the-russo-ukrainian-war-begins/. One factor that may also contribute to the decentralized and organic nature of Ukraine IO is the high degree of operational independence exercised by the military district commanders in the Ukraine army and the relative autonomy exercised by local elected officials in Ukraine's constitutional system.

43. Sinead Baker, "Video Appearing to Show Ukraine Forces Shooting Russian Prisoners Seems Plausible but Remains Unverified, Experts Say," Business Insider, 29 March 2022, accessed 12 April 2022, https://www.businessinsider.com/video-ukrainians-apparently-shooting-russian-prisoners-plausible-not-verified-experts-2022-3. There is one exception. On 28 March 2022, a video of questionable legitimacy emerged on Telegram, purporting to show Ukrainian soldiers wounding Russian prisoners. The Ukrainian government has questioned the authenticity of the video but has stated that it will conduct a full investigation and takes the matter "extremely seriously." In the view of the authors, even if the video is authentic, the absence of others, after more than four weeks of brutal urban warfare, and considering the diverse mix of professional soldiers, militia, and international volunteers defending Ukraine, remains powerful evidence of the efficacy of Ukrainian policy.

44. "The Invasion of Ukraine Is Not the First Social Media War, but It Is the Most Viral," *The Economist* (website), 26 March 2022, accessed 12 April 2022, https://www.economist.com/international/the-invasion-of-ukraine-is-not-the-first-social-media-war-but-it-is-the-most-viral/21808456; Missy Ryan et al., "Outmatched in Military Might, Ukraine Has Excelled in the Information War," *Washington Post* (website), 16 March 2022, accessed 12 April 2022, https://www.washingtonpost.com/national-security/2022/03/16/ukraine-zelensky-information-war/ (discussing key features of Ukraine IO campaign).

45. Ibid.

46. See, for example, Gerrard Kaonga, "Zelensky Has Survived Over a Dozen Assassination Attempts, Ukraine Claims," *Newsweek* (website), 9 March 2022, accessed 12 April 2022, https://www.newsweek.com/volodymyr-zelenskyy-assassination-attempt-killing-ukraine-president-russia-1686329.

47. *Russian Prisoners of War in Ukraine Deliver a Message to Vladimir Putin*, YouTube video, posted by "7News Australia," 9 March 2022, accessed 12 April 2022, https://www.youtube.com/watch?v=tQDFmRJddWo.

48. Thomas Novelly, "Ukraine's Fighter Ace 'Ghost of Kyiv' May Be a Myth, but It's Lethal as War Morale," Military.com, 2 March 2022, accessed 12 April 2022, https://www.military.com/daily-news/2022/03/02/ukraines-fighter-ace-ghost-of-kyiv-may-be-myth-its-lethal-war-morale.html.

49. Chloe Fulmer, "Ukraine Military Says Soldier Blew Himself Up on Bridge to Halt Russian Advance," The Hill, 25 February 2022, accessed 12 April 2022, https://thehill.com/policy/international/russia/595914-ukraine-military-says-soldier-blew-himself-up-on-bridge-to-halt.

50. Bill Chappell, "Snake Island Sailors Are Freed as Ukraine and Russia Conduct Prisoner Exchange," NPR, 24 March 2022, accessed 12 April 2022, https://www.npr.org/2022/03/24/1088593653/snake-island-sailors-freed-prisoner-swap.

51. *Ukrainian President Volodymyr Zelenskyy Shares a Message from Kyiv*, YouTube video, posted by "USA Today," 25 February 2022, accessed 12 April 2022, https://www.youtube.com/watch?v=tLv9IqcoNe8.

52. International Telecommunications Union Office for Europe, *Ukraine: Digital Development Country Profile* (Geneva: International Telecommunications Union, February 2022), 6, accessed 12 April 2022, https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Publications/Publications.aspx.

53. As part of his legal practice, author Trevor Garmey frequently advises multinational corporations on mitigating reputational risk and provides training and best practices for social media use by employees. The conclusions in this paragraph reflect lessons learned from his professional experience.

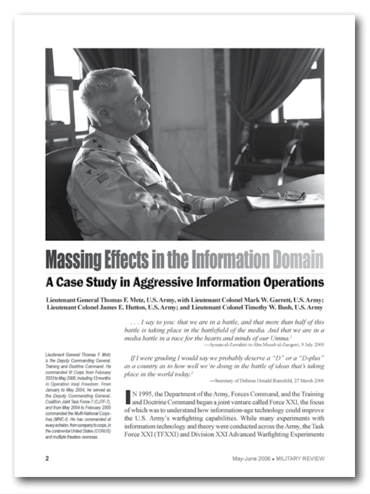
54. This recommendation will become increasingly prudent after the fiscal year 2023 modified table of organization and equipment adjustment removes public affairs officers from brigade-level headquarters. This ostensibly leaves brigades with no professionals who identify with IO as their primary tradecraft.

55. Author interviews with a former military intelligence observer/coach/trainer and a current senior leader at the Joint Readiness Training Center, 27 March 2022.

MilitaryReview

WE RECOMMEND

For those interested in learning more about information operations, we invite your attention to a selection of articles previously published in *Military Review*:



Massing Effects in the Information Domain

A Case Study in Aggressive Information Operations

Lieutenant General Thomas F. Metz, U.S. Army, with Lieutenant Colonel Mark W. Garrett, U.S. Army; Lieutenant Colonel James E. Hutton, U.S. Army; and Lieutenant Colonel Timothy W. Bush, U.S. Army

. . . I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our Umma.[1]

—Ayman al-Zawahiri to Abu Musab al-Zarqawi, 9 July 2005

If I were grading I would say we probably deserve a "D" or a "D-plus" as a country as to how well we're doing in the battle of ideas that's taking place in the world today.[2]

—Secretary of Defense Donald Rumsfeld, 27 March 2006

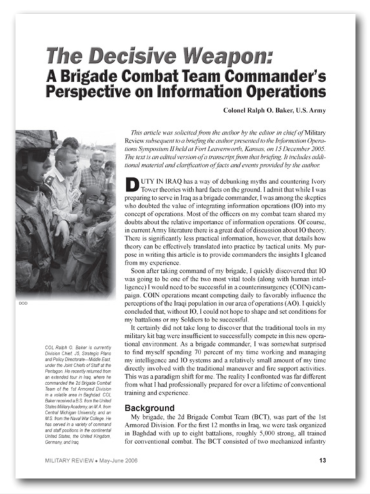
Lieutenant General Thomas F. Metz is the Deputy Commanding General, Training and Doctrine Command. He commanded III Corps from February 2003 to May 2006, including 13 months in Operation Iraqi Freedom. From January to May 2004, he served as the Deputy Commanding General, Coalition Joint Task Force-7 (CJTF-7), and from May 2004 to February 2005 commanded the Multi-National Corps-Iraq (MNC-I). He has commanded at every echelon, from company to corps, in the continental United States (CONUS) and multiple theaters overseas.

IN 1995, the Department of the Army, Forces Command, and the Training and Doctrine Command began a joint venture called Force XXI, the focus of which was to understand how information-age technology could improve the U.S. Army's warfighting capabilities. While many experiments with information technology and theory were conducted across the Army, the Task Force XXI (TFXXI) and Division XXI Advanced Warfighting Experiments

2 May-June 2006 • MILITARY REVIEW

"Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," by Lt. Gen. Thomas F. Metz, U.S. Army; Lt. Col. Mark W. Garrett, U.S. Army; Lt. Col. James E. Hutton, U.S. Army; and Lt. Col. Timothy W. Bush, U.S. Army

https://apps.dtic.mil/sti/pdfs/ADA489043.pdf



The Decisive Weapon:

A Brigade Combat Team Commander's Perspective on Information Operations

Colonel Ralph O. Baker, U.S. Army

This article was solicited from the author by the editor in chief of Military Review *subsequent to a briefing the author presented to the Information Operations Symposium II held at Fort Leavenworth, Kansas, on 15 December 2005. The text is an edited version of a transcript from that briefing. It includes additional material and clarification of facts and events provided by the author.*

DUTY IN IRAQ has a way of debunking myths and countering Ivory Tower theories with hard facts on the ground. I admit that while I was preparing to serve in Iraq as a brigade commander, I was among the skeptics who doubted the value of integrating information operations (IO) into my concept of operations. Most of the officers on my combat team shared my doubts about the relative importance of information operations. Of course, in current Army literature there is a great deal of discussion about IO theory. There is significantly less practical information, however, that details how theory can be effectively translated into practice by tactical units. My purpose in writing this article is to provide commanders the insights I gleaned from my experience.

Soon after taking command of my brigade, I quickly discovered that IO was going to be one of the two most vital tools (along with human intelligence) I would need to be successful in a counterinsurgency (COIN) campaign. COIN operations meant competing daily to favorably influence the perceptions of the Iraqi population in our area of operations (AO). I quickly concluded that, without IO, I could not hope to shape and set conditions for my battalions or my Soldiers to be successful.

It certainly did not take long to discover that the traditional tools in my military kit bag were insufficient to successfully compete in this new operational environment. As a brigade commander, I was somewhat surprised to find myself spending 70 percent of my time working and managing my intelligence and IO systems and a relatively small amount of my time directly involved with the traditional maneuver and fire support activities. This was a paradigm shift for me. The reality I confronted was far different from what I had professionally prepared for over a lifetime of conventional training and experience.

Background

My brigade, the 2d Brigade Combat Team (BCT), was part of the 1st Armored Division. For the first 12 months in Iraq, we were task organized in Baghdad with up to eight battalions, roughly 5,000 strong, all trained for conventional combat. The BCT consisted of two mechanized infantry

DOD

COL Ralph O. Baker is currently Division Chief, J5, Strategic Plans and Policy Directorate—Middle East, under the Joint Chiefs of Staff at the Pentagon. He recently returned from an extended tour in Iraq, where he commanded the 2d Brigade Combat Team of the 1st Armored Division in a volatile area in Baghdad. COL Baker received a B.S. from the United States Military Academy, an M.A. from Central Michigan University, and an M.S. from the Naval War College. He has served in a variety of command and staff positions in the continental United States, the United Kingdom, Germany, and Iraq.

MILITARY REVIEW • May-June 2006 13

"The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," by Col. Ralph O. Baker, U.S. Army

https://apps.dtic.mil/sti/pdfs/ADA489185.pdf

Iraqi President Fuad Masum (*right*) and Rakan Said al-Juburi, governor of Kirkuk, speak to the press 27 November 2017 following a meeting during a surprise visit to the multiethnic northern Iraqi city of Kirkuk. Influencers often leverage the media to engage target audiences and shape domestic and international opinions, though the number of media is increasingly numerous and diverse. (Photo by Marwan Ibrahim, Agence France-Presse)

How We Win the Competition for Influence

Lt. Col. Wilson C. Blythe Jr., U.S. Army
Lt. Col. Luke T. Calhoun, U.S. Army

The days of securing campaign success solely through traditional combat operations are over. Victories on the twenty-first century's physical battlefields will be fleeting unless tied to an integrated information operations campaign.[1] The achievement of campaign and strategic objectives requires a sustained competitive advantage over other actors in the ability to influence outcomes. Otherwise, hard-won victories

MILITARY REVIEW May-June 2019 37

"How We Win the Competition for Influence," Lt. Col. Wilson C. Blythe Jr., U.S. Army; and Lt. Col. Luke T. Calhoun, U.S. Army

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Blythe-the-Calhoun-Influence/

US ISSN 0026-4148