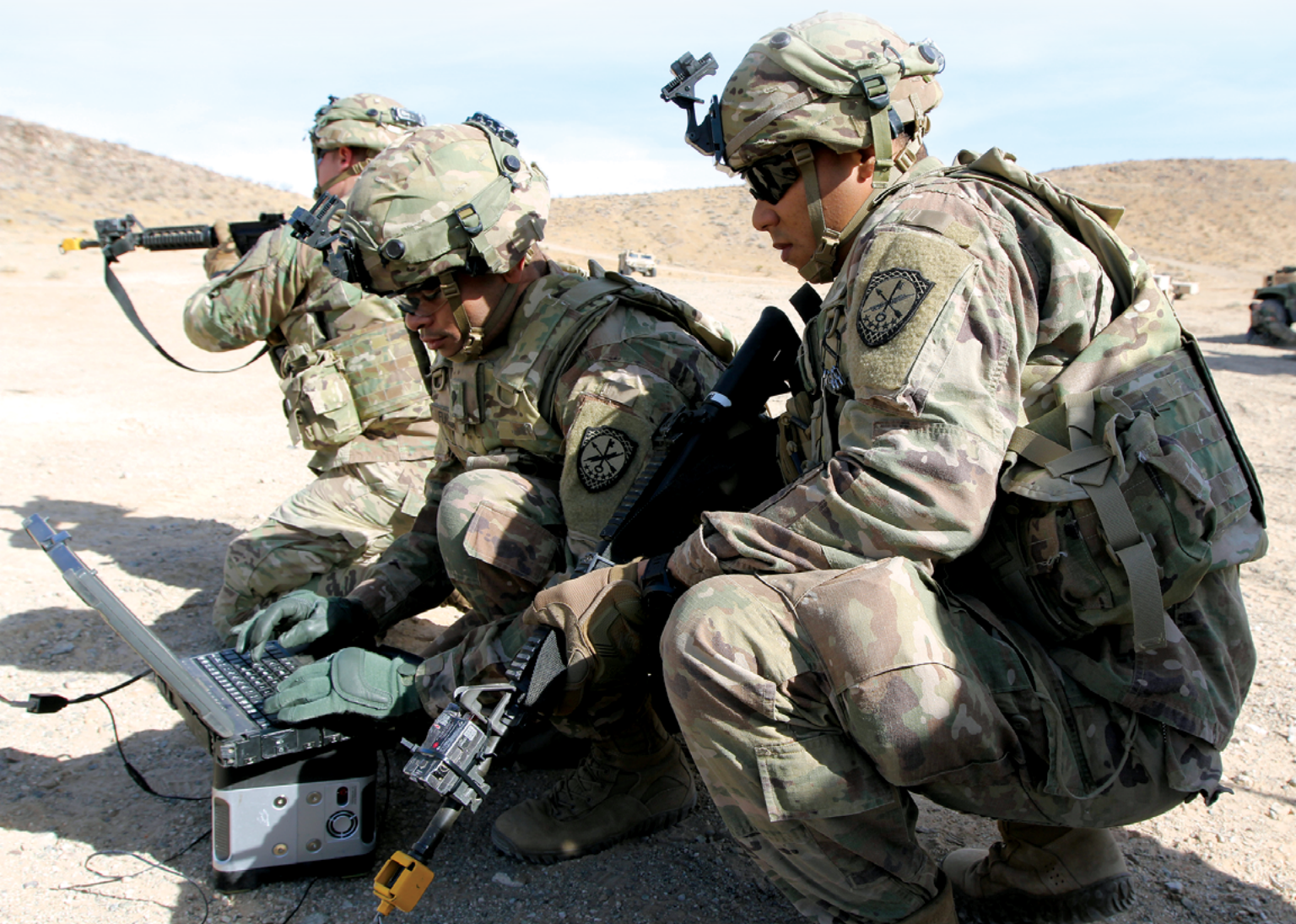
The Case for an Information Warfighting Function

Lt. Col. Gregory M. Tomlin, PhD, U.S. Army

In September 2017, then Defense Secretary James Mattis established "information" as the seventh joint function, recognizing this capability as unique from those already codified in doctrine: command and control, intelligence, fires, movement and maneuver, protection, and sustainment. As a distinct function, he charged the department with considering the implications of this addition across doctrine, organizations, education, and personnel.[1] A year later, the Joint Staff revised its capstone document for operations, Joint Publication 3-0,



Joint Operations, to include a ten-page explanation of the information function and a description of the multifaceted information environment.[2] The Joint Staff deputy director for global operations (J-39) charged information operations (IO) officers within his directorate to facilitate discussions between the services and combatant commands about how to enhance cross-command information planning as a part of globally integrated plans. Within the joint professional military education curriculum, the Joint Forces Staff College expanded its introduction to and application of the information function.

While the Joint Staff and National Defense University found ways to integrate the new function into its doctrine, organization, and education of its personnel, the U.S. Army did not establish information as a seventh warfighting function. Previously, the Army adopted each joint function as one of its warfighting functions, making information the conspicuous outlier. Since the information domain is integral to all existing warfighting functions, some senior Army leaders contend that a separate distinction would be superfluous. This viewpoint gives short shrift to the information capabilities that are either forced into other warfighting functions, namely intelligence and fires, or worse, applied as an afterthought to the planning process. Designation as a warfighting function would benefit the Army by elevating the importance of thinking more critically about and better resourcing the deliberate integration of strategic communications, public affairs, IO, electronic warfare (EW), and cyber operations into all unified land operations.

The dynamism of today's information environment threatens to impede the Army's ability to gain a competitive advantage over potential adversaries of the United States and its allies, regardless of the accuracy of its long-range artillery or deployment speed of a global response force. The sophistication of China, Russia, and nonstate actors' disinformation efforts continues to erode the confidence that foreign leaders and populations used to place in security partnerships with the United States. For example, suppose President Rodrigo Duterte succeeds in convincing the majority of the Philippine populace that military cooperation with the United States threatens their "extinction" because it will lead to a cataclysmic war with China. In that case, it will not matter whether the U.S. Army Pacific wants to deploy Stryker brigades to the archipelago for an exercise.[3] Public opinion swayed in the information domain could deny U.S. and Philippine militaries the ability to continue with longstanding combined defensive maneuvers that serve as a visible deterrence against Chinese expansion in the region.

To win the competitive advantage in multi-domain operations, the Army must invest as heavily in developing future information capabilities as it does in creating artificial intelligence collection assets and extended-range fires delivery platforms. The establishment of an information warfighting function would require the U.S. Army to fund and integrate information efforts more deliberately into the tactical, operational, and strategic levels of war. There are limitations to competing in today's information environment when the U.S. government underresources the agencies and departments responsible for conducting strategic communications, IO, EW, and cyber operations. Specific to enabling the Army to shape the information domain as part of the joint force, the service would gain doctrinal and organizational benefits by codifying a seventh warfighting function.

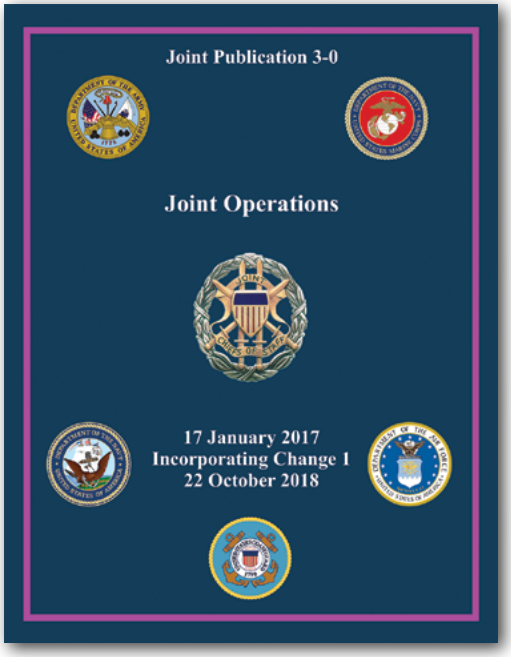
The Information Environment

For decades, strategists have identified information as a significant instrument of national power, the "I" in DIME (diplomacy, information, military, and economic). Yet, the disparity between how the U.S. government and the military invest in information capabilities is bracing, evidenced by the Army's current challenges with competing in the information domain.[4] From the brigade combat team to the theater army, the sheer volume of information available today presents a challenge to staff officers responsible with providing sound analysis, courses of action, and strategic options to commanders who want to leverage public affairs, IO, EW, and cyber operations as shaping efforts to enable mission success. While the speed of information dissemination continues to accelerate exponentially—with the ability to post an evocative statement or image and then share it

Previous page: Spc. Victorious Fuqua (*with laptop*) and Staff Sgt. Isaias Laureano (*front*), both cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), provide offensive cyber operations while Spc. Mark Osterholt provides security 18 January 2018 during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center rotation at Fort Irwin, California. (Photo by Steven Stover)

through a global network of social media platforms in a matter of minutes—the time frame for providing recommendations to decision-makers has not expanded. This can cause well-intentioned action officers to provide unsound assessments because they do not vet sources carefully enough or they fail to corroborate the accuracy of a report in their rush to meet a briefing deadline.

For U.S. adversaries, the contemporary information environment makes the exploitation of disinformation a favorable tool to advance their foreign policies. At the end of the Cold War, Russian leaders recognized their inability to maintain a superpower's military and elected to downsize their pricey field armies, naval fleets, and air wings. Shaped by his own KGB career, a newly inaugurated President Vladimir Putin chose to invest heavily in the information domain. This much smaller financial burden provided him with a way to leverage his country's diminished power through disinformation and propaganda. In recent years, Putin has reaped the benefits of this investment, particularly in Eastern Europe where the public increasingly identifies with Russia over their European Union neighbors and questions the relevance of the NATO, causing U.S. Army Europe to deploy brigades deeper into the former Warsaw Pact to help sustain the NATO alliance.[5]



To view Joint Publication 3-0, *Joint Operations*, visit https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf.

In contrast to the Russians, as the world entered the information age, the United States closed its own information agency (USIA) that had synchronized the federal government's public diplomacy and strategic communications efforts from 1953 until 1999. With an air of Cold War triumphalism, leaders in both political parties assumed that by retaining a superpower military and remaining the leading global economy, presidential administrations could maintain the same grand strategy for achieving foreign policy goals through the twenty-first century. Vestiges of the USIA still exist, including the Voice of America and Radio Free Europe, but these are only forms of international broadcasting. When the USIA closed, the Clinton administration established the Broadcasting Board of Governors (BBG) to manage federally funded international broadcasts and introduce online content for foreign audiences as the internet became more accessible globally.[6]

Unfortunately, the BBG did not synchronize the other elements of public diplomacy or national-level strategic communications as the USIA had, particularly in spearheading interagency efforts to keep the State and Defense Departments on the same message during times of international crisis. When the USIA closed its headquarters, the State Department consolidated the agency's three overseas print plants that published pamphlets and magazines but shuttered its television and documentary divisions that had produced short films watched by millions of people in overseas theaters the same way we watch previews before movies today. Perhaps the most significant flaw of the public diplomacy restructuring plan concerned the decision to not incorporate USIA's Research and Analysis Division into the BBG. By focusing on broadcast media exclusively, the BBG lacked a robust capacity to listen to feedback and assess whether messages built credibility with an international audience. During the Cold War, USIA analysis revealed that the U.S. government could not adopt the same broadcast format for listeners in Eastern Europe as in Latin America. Surveys conducted by the agency's public diplomacy officers in the Soviet bloc found listeners receptive to long, detailed monologues about the news of the day, while feedback on attention spans in Latin American countries led Voice of America broadcasters to modify the format to short news updates between Bossa Nova and jazz music.[7]

In 2016 the Obama administration established the State Department's Global Engagement Center (GEC) to counter foreign disinformation and propaganda through

four threat teams: China/North Korea, Russia, Iran, and counterterrorism. Ideally, the GEC serves as the coordination nexus for liaisons from various agencies and departments to respond to disinformation, yet today it remains undermanned and underresourced.[8] Four years since the GEC's inception, information "silos of excellence," scattered across the National Capital Region, project various messages from the Pentagon to Foggy Bottom to the Voice of America headquarters at the base of Capitol Hill. The absence of a national integrator for strategic communications—one like the director of national intelligence established in the wake of the attacks on 11 September 2001—has weakened the United States' security.

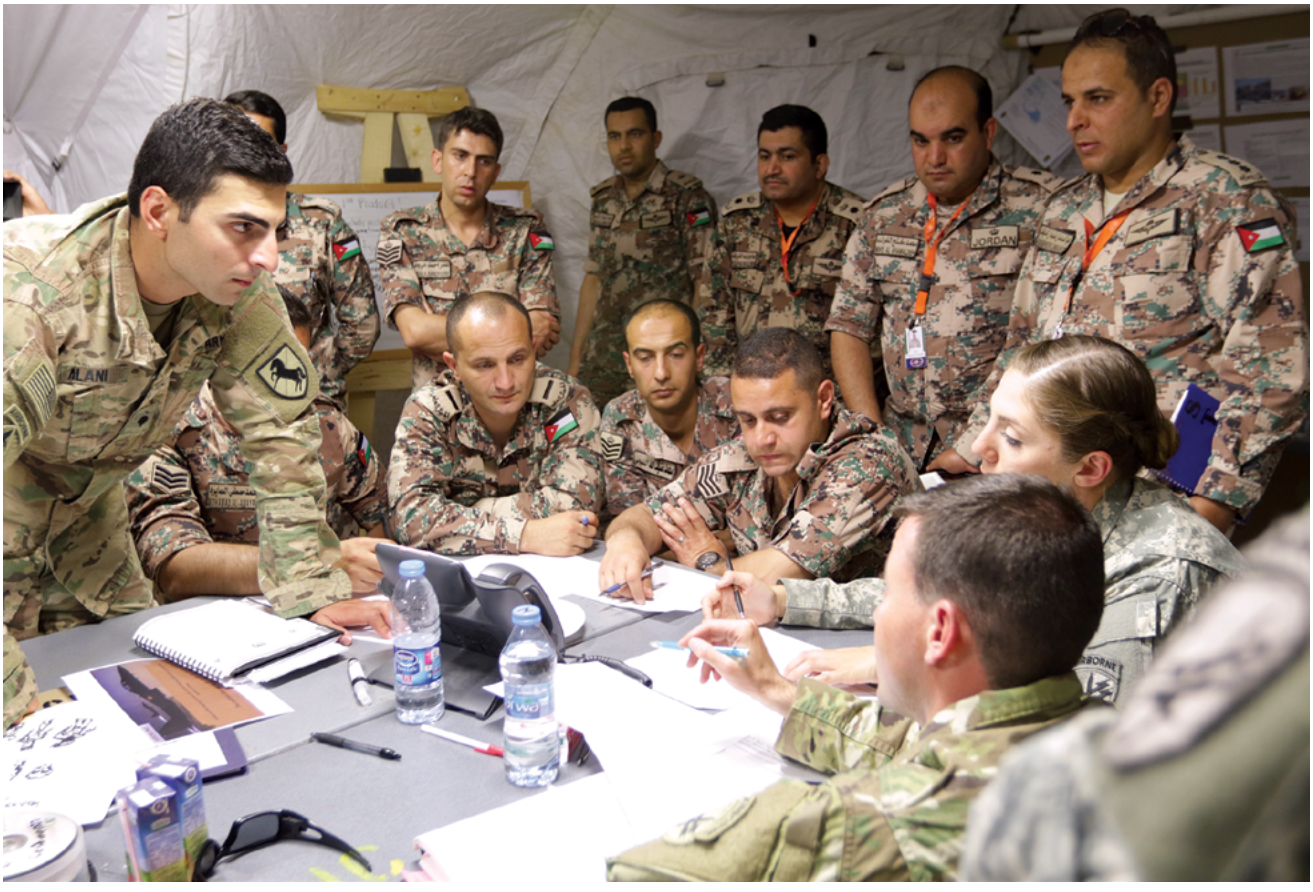
Through their skillful and sustained disinformation campaigns, the Russians have discredited American international leadership, eroded U.S. soft power, and undermined confidence in democracy, freedom of the press, and social norms. Since the collapse of the Soviet Union, the Putin administration has created proxy news sites of questionable journalistic integrity. The international news channel RT (formerly Russia Today) uses the tagline "Question More," while its radio counterpart, Sputnik, pledges to "Tell the Untold." What should we question? From Putin's geostrategic perspective, begin with the reporting of mainstream journalists and government authorities' official statements.

During their daily newscast, RT anchors casually sandwich a conspiracy theory or unchallenged statement between legitimate news stories that would appear on the BBC or CNN. In January 2017, while coalition forces worked aggressively in Syria to liberate cities from Islamic State control, RT displayed images of human bodies wrapped in bedding laying on the side of a street. The news anchor reported that according to "one eyewitness" U.S. pilots killed "women and children" indiscriminately before he transitioned to a recap of the day's market performance.[9] Wait! Who was the eyewitness? An anonymous bystander interviewed by a RT journalist or a Syrian official? The anchor did not explain. Alarmingly, few in RT's international audience understood the extensive precautions taken by U.S. pilots to minimize collateral damage. Yet, the matter-of-fact presentation of this dubious report in the daily newscast led many undoubtedly to believe that the United States drops bombs with little regard for protecting civilians in the combat zone.

During the COVID pandemic, the Chinese government picked up Putin's playbook to create international doubt in the American government. The Chinese Foreign Ministry spokesman tweeted two conspiracies: an American soldier participating in the October 2019 Military World Games brought COVID-19 to China and the virus originated in a U.S. Army laboratory at Fort Detrick, Maryland.[10] As bizarre as these accusations may sound, they were not innovative. They echoed Soviet-favored propaganda techniques from the Cold War that accused the United States of committing germ warfare against North Korean soldiers and noncombatants during the Korean War. In the early 1980s, the Kremlin blamed the U.S. Army for inventing AIDS at that same laboratory at Fort Detrick where others would like to believe COVID originated in 2019.[11] Regardless of the outlandish Chinese official spokesman's tweets, the fact that Secretary of State Michael Pompeo chose to rebuff the comments via Twitter brought the conspiracy theories into broader circulation through a whole new online network of people following the State Department's account or the media outlets that highlighted the secretary's comments.[12]

Marine Corps University professor Donald M. Bishop explained in a *Foreign Service Journal* article that official Chinese messages during the pandemic reveal three themes: the Chinese Communist Party brought a swift end to the crisis in China, the Chinese government "bought enough time" for other nations to respond, and generous Chinese medical aid to other nations reaffirms the Chinese Communist Party's position as the global leader during the pandemic.[13] These messages did not enter the information domain solely through an official Chinese spokesmen. Investigative journalists at

Lt. Col. Gregory M. Tomlin, PhD, commands the 1st Battalion, 37th Field Artillery, 7th Infantry Division, at Joint Base Lewis-McChord, Washington. In addition to fire support billets in the 1st Infantry, 2nd Infantry, and 1st Armored divisions, he has served as chief of the Targeting Doctrine and Policy Branch on the Joint Staff at the Pentagon, an Eighth Army strategic planner in Seoul, and assistant professor of history at West Point. He holds a doctorate in history from the George Washington University and authored *Murrow's Cold War: Public Diplomacy for the Kennedy Administration.*



Spc. Yasir Alani (*left*), an interpreter with the 11th Armor Cavalry Regiment, helps translate military information operations training products created by Jordanian soldiers from the Department of Moral Guidance with the help of Sgt. Lin Wiebalk (*right front*) and Spc. Annabela Stigliano (*second from right*), both psychological operations specialists with the 360th Psychological Operations Company, 14 May 2017 during exercise Eager Lion 2017 at the Joint Training Center in Zarqa, Jordan. (Photo by Sgt. Marco Gutierrez, U.S. Army)

ProPublica found ten thousand fake Twitter accounts advancing the Chinese COVID message campaign, and the U.S. intelligence community attributed 70 percent of U.S. social media stories related to COVID to Russian and Chinese bots, trolls, and fake accounts.[14]

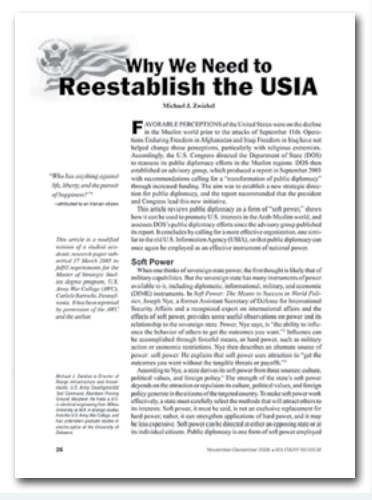
Bret Schafer of the German Marshall Fund favors the term "information laundering" for describing the subtle impact of fake stories planted in social media. Someone posts a tweet amplified by hundreds if not thousands of fake accounts, often accounts created with artificial intelligence that modifies the message each time with different adjectives or colloquialisms to make it sound authentic.[15] Eventually the viral tweet makes its way into a newsroom or an intelligence agency where either a journalist or open-source analyst includes it in their report. Finally, the disinformation makes its way to decision-makers, including the hands of Army commanders leading multi-domain operations.

Shaping the Information Domain

The U.S. Army would benefit from approaching the dynamic information environment with the same level of discipline as it does the air and ground dimensions of any area of operations. Similarly, to the BBG's international broadcasting efforts, the Army must build an audience through credible and compelling messages before and during deployments. Akin to the former USIA Research and Analysis Division, the Army must also create a permanent means at echelon to assess the effectiveness of the information enablers they leverage. Many combat arms officers who assume high command are simply not familiar with the unique information capabilities available at the strategic and operational levels, much less how to synchronize them with better-known warfighting functions to affect an audience or target. Throughout the planning and execution phases, commanders and their staffs must

refine enduring messages, discern which disinformation to counter and which outrageous reports to ignore, and develop metrics for *listening* before assessing their information campaign as a critical shaping operation to any mission.

Military Review
WE RECOMMEND


Why We Need to Reestablish the USIA

Michael J. Zwiebel

FAVORABLE PERCEPTIONS of the United States were on the decline in the Muslim world prior to the attacks of September 11th. Operations Enduring Freedom in Afghanistan and Iraqi Freedom in Iraq have not helped change those perceptions, particularly with religious extremists. Accordingly, the U.S. Congress directed the Department of State (DOS) to reassess its public diplomacy efforts in the Muslim regions. DOS then established an advisory group, which produced a report in September 2003 with recommendations calling for a "transformation of public diplomacy" through increased funding. The aim was to establish a new strategic direction for public diplomacy, and the report recommended that the president and Congress lead this new initiative.

This article reviews public diplomacy as a form of "soft power," shows how it can be used to promote U.S. interests in the Arab-Muslim world, and assesses DOS's public diplomacy efforts since the advisory group published its report. It concludes by calling for a more effective organization, one similar to the old U.S. Information Agency (USIA), so that public diplomacy can once again be employed as an effective instrument of national power.

Soft Power

When one thinks of sovereign state power, the first thought is likely that of military capabilities. But the sovereign state has many instruments of power available to it, including diplomatic, informational, military, and economic (DIME) instruments. In *Soft Power: The Means to Success in World Politics*, Joseph Nye, a former Assistant Secretary of Defense for International Security Affairs and a recognized expert on international affairs and the effects of soft power, provides some useful observations on power and its relationship to the sovereign state. Power, Nye says, is "the ability to influence the behavior of others to get the outcomes you want." Influence can be accomplished through forceful means, or hard power, such as military action or economic restrictions. Nye then describes an alternate source of power: soft power. He explains that soft power uses attraction to "get the outcomes you want without the tangible threats or payoffs."

According to Nye, a state derives its soft power from three sources: culture, political values, and foreign policy.[1] The strength of the state's soft power depends on the attraction or rejection its culture, political values, and foreign policy generate in the eyes of the targeted enemy. To make soft power work effectively, a state must carefully select the methods that will attract others to its interests. Soft power, it must be said, is not an exclusive replacement for hard power; rather, it can strengthen applications of hard power, and it may be less expensive. Soft power can be directed at either an opposing state or at its individual citizens. Public diplomacy is one form of soft power employed

The article "Why We Need to Reestablish the USIA" is based on a student's academic research paper submitted 17 March 2005 to fulfill requirements for the Master of Strategic Studies degree program at the U.S. Army War College in Carlisle, Pennsylvania. It provides a salient tutorial on the essential role the United States Information Agency (USIA) played in the public relations dimension of the global competition that existed between the United States and the Soviet Union during the Cold War. With the 1999 disestablishment of the USIA, the United States has never since had a suitably robust and centrally managed replacement agency capable of "all of government" formulation and synchronization of national strategic messaging and has suffered the consequences of uneven, uncoordinated, and even contradictory information conveyed to the world from multiple competing agencies inside the U.S. government. To view the article originally published in the November-December 2006 edition of *Military Review*, visit https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20061231_art006.pdf.

Army planners would be aided greatly by the introduction of information warfighting function doctrine delineating how a command should coordinate with the U.S. embassy, other U.S. agencies and components of the joint force, host-nation officials, and nongovernmental organizations sharing the area of operations, lest they commit "information fratricide." This form of unintentional harm to friendly elements occurs when one trusted spokesman's message contradicts another reliable information source. Suppose a U.S. Agency for International Development official promises a provincial governor that the U.S. Army will rebuild a bridge without first verifying that the deployed engineer battalion has the equipment and skillset on hand to complete the project. In that case, the entire country team loses credibility. The governor may take to the airways or social media to criticize the sincerity of the Americans in his or her province, fomenting wider public distrust. From humanitarian relief to postconflict stability operations, populations desperately seeking assistance can turn against American soldiers quickly when their deeds do not match their words. A setback requiring the command to concentrate on regaining its credibility with the local populace will frustrate the Army's ability to focus influence operations on higher priority objectives such as improving trust in the host-nation government or support for the rule of law.

Earning the host-nation populace's trust and deterring an adversary through the information domain requires deftness at the tactical, operational, and strategic levels. Existing investments in 1st IO Command and the Army component of U.S. Cyber Command provide more capacity at the strategic level than to operational and tactical echelons. These organizations also seem as inaccessible to most commanders as space-based capabilities. However, given the sheer numbers of soldiers participating in deployments, the Army misses an opportunity to advance national security objectives through the information domain by not developing the doctrine or organizational structures to empower those with boots on the ground to engage in influence operations confidently. Tactical units should not develop themes and messages independently, which is why a corps or field army serving as a combined-joint task force needs leaders armed with a doctrinal compendium for designing an information campaign, just as they have for laying out their intelligence collection plan. Intelligence warfighting function doctrine provides insight into how the G-2 (intelligence)

should collaborate with the higher echelon's J-2 (intelligence) and intelligence community partners, especially to protect covert assets and vet sources, but when it comes to shaping the information domain, the approach is often ad hoc from one operational deployment to the next.

detonate on the desired object. For this reason, in the absence of better doctrine, IO planners often force their nonlethal efforts into a targeting cycle designed to build air tasking orders and fire support plans. This problem is not unique to the Army, and the joint force

> Strategic communications, information operations, and cyber operations demand the use of a wide range of online platforms. A corps or field Army general staff must consider which ones are the most effective for establishing an audience, building credibility, and countering an adversary's disinformation.

As after action reports from division and corps Warfighters and brigade-level combat training center (CTC) rotations consistently amplify, Army units cannot compete in the information domain if they limit themselves to command messages posted by public affairs officers on official online accounts. Unfortunately, outside of these semiannual exercises, units do not devote considerable time at home station to integrating IO, EW, or cyber operations, often because these capabilities are not organic to their organization. Information enablers join a brigade combat team or division temporarily, arriving just in time for an exercise and departing immediately upon its conclusion. Equally as problematic, rarely do IO, psychological operations, civil affairs, or cyber elements pair with the same tactical unit from one exercise to the next in order to develop a rapport or standard operating procedures. Without permanent representation inside their formations, units naturally focus their postexercise retraining on the present warfighting functions. A division chief of staff can order the G-2 Analysis and Control Element to practice its all-source intelligence and targeting requirements in garrison by scheduling a tabletop exercise with other directorates from the general staff. Similarly, the division artillery commander remains accountable for the annual live-fire qualification requirements of the direct support artillery battalions to ensure the delivery of timely and accurate fires during their brigades' next fire support coordination exercise.

Fires warfighting function doctrine requires planners to refine the exact location of targets developed by a higher headquarters to ensure that munitions

continues to grapple with a similar doctrinal debate about whether to align information enablers with the joint targeting cycle.[16] Since a target is an object or entity that provides a function for an adversary, the Army's simplified targeting cycle—decide, detect, deliver, and assess—does not provide guidance for how to influence those audiences that are not associated with the threat. Neither the Polish nor Philippine citizenry is a "target" of the United States, but both U.S. Army Europe and U.S. Army Pacific need to be able to amplify Defense and State Department messages to convince them of the security benefits that come from participating in combined exercises.

Not only must the Army build credibility with audiences before and during deployments, but it must also apply information enablers according to a battle rhythm divorced from the rapid, seventy-two hour targeting cycle because influence operations take considerably more time to achieve desired effects. An overhead surveillance system or observer on the ground can confirm the destructive effects of an Air Force bomber's precision munition against a target immediately after the debris cloud dissipates. Yet this targeting example is not a helpful comparison for understanding how to assess an information campaign's ability to deter Afghan youth from joining the Taliban—a twenty-year-old ongoing effort. Influence operations often require months or years to change opinions or behavior, although a staff must assess the approach more frequently and refine how to employ public affairs, IO, and cyber enablers. Too frequently, however, when information efforts are

subsumed into the lethal targeting cycle, commanders lose patience with the lack of immediate changes in attitudes supporting U.S. foreign policies because they begin to equate the information domain with the fires warfighting function.

Strategic communications, IO, and cyber operations demand the use of a wide range of online platforms. A corps or field Army general staff must consider which ones are the most effective for establishing an audience, building credibility, and countering an adversary's disinformation. IO and intelligence planners must assess whether their official and covert presence on a platform is influencing foreign audiences to support U.S. national security objectives. The staff needs guidance on how to tap into interagency resources that can provide intelligence into which platforms an adversary leverages as well as ongoing efforts external to the Army to respond to them. As any adroit public affairs officer will advise a commander, some salacious accusations must be countered immediately, while a cyber expert may advise that a better approach could be to bury the story in social media through an offensive cyber action.

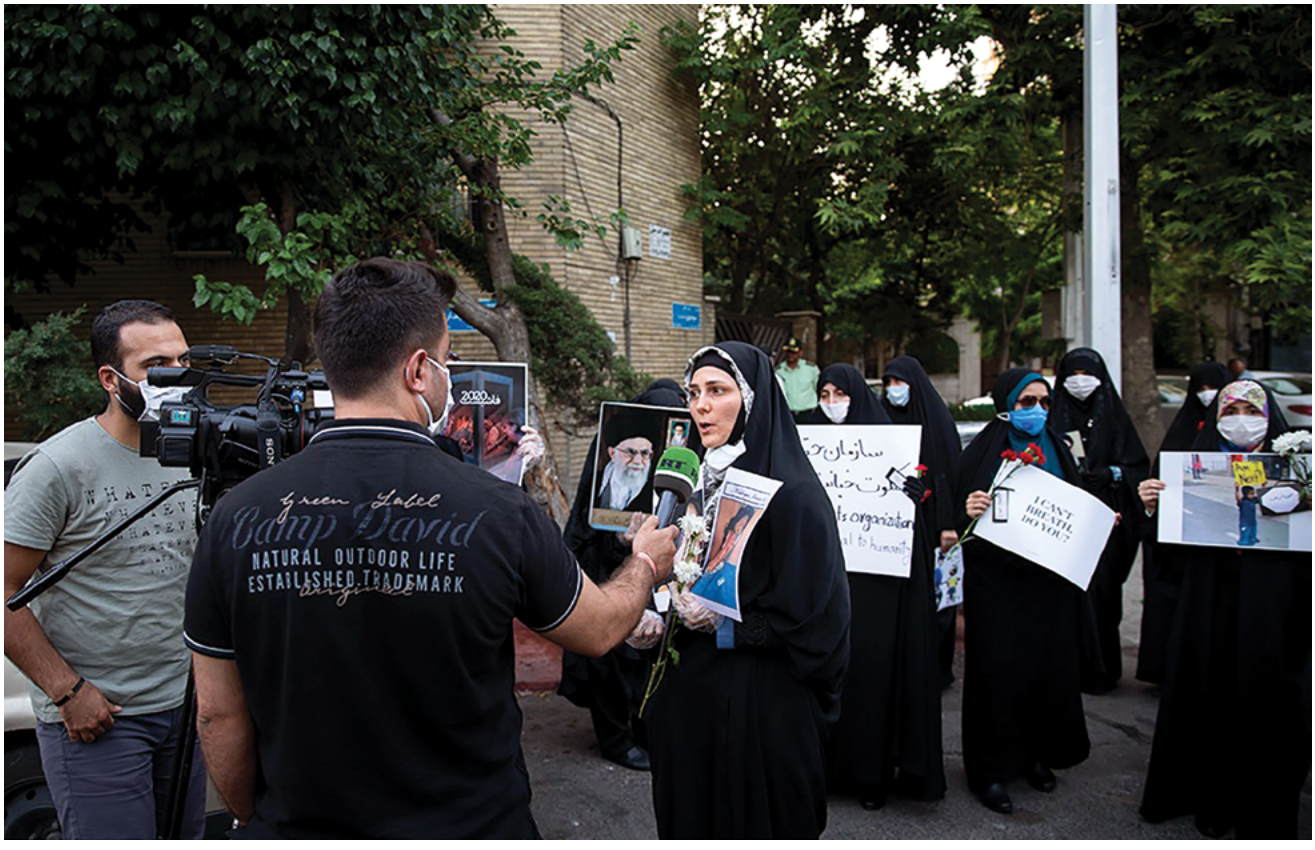
Adding to today's complexity is the demography of a foreign audience, as Jian Wang, the director of the Center on Public Diplomacy at the University of Southern California, observed. Regardless of the continent, the audience is more urban with a "youth bulge" of disenfranchised individuals susceptible to exploitation by political extremists and conspiracy theorists. The ethnic remapping caused by migration patterns affects the languages needed for broadcasting or online written material directed toward specific regions of Europe and the Middle East.[17] Nonstate actors like the Islamic State effectively manipulated social media over the past decade to gain recruits from Europe and East Asia to build a caliphate in the Levant. Multinational businesses have interests and often the technological means to outreach official government influence. Civic organizations, including nongovernmental organizations focused on human rights and the environment, should be considered in the public-private partnership needed to expand the Army's appeal and messages. This complex environment reaffirms that at the operational and strategic levels, the Army must consider the information domain as a critical shaping effort for any decisive operation requiring the deployment of soldiers.

The Tactical Advantage

Since the Russian incursion into Ukraine in 2014, CTCs enjoy showcasing to rotational units the electronic signature of brigade and battalion tactical operations centers (TOCs). Observer-controllers present rainbow-colored graphics differentiating the electromagnetic-spectrum indicators of maneuver, field artillery, and sustainment command posts across the battlefield. If an adversary can identify these high-value targets, they will most assuredly seek to destroy them through fires, EW, or offensive cyber operations. Inevitably this after-action comment leads commanders to reduce their electronic signature by turning off communication systems or dividing their headquarters between the TOC and a leaner tactical command post (TAC).

This training scenario creates two problems for a brigade combat team. First, while the observer-controllers present rotational units with their electronic signature, they do not offer any meaningful solution for masking it. Instead, they simply discourage units from leveraging the advanced communication systems that they need to validate over extended distances during the exercise. Second, when a commander divides his or her limited resources between a TOC and a TAC, the nonlethal working group responsible for synchronizing information capabilities atrophies, since public affairs, IO, and EW personnel rarely make the cut to join the forward command post. Intelligence and fire support personnel accompany the operations officer to the TAC, since these are warfighting functions. However, current doctrine does not elevate information enablers to the same level of importance during the current fight, nor does the brigade's modified table of organization and equipment provide the redundancy in public affairs, IO, and EW manpower or systems to allow them to work from dual locations. When the TAC manages the fight for twenty-four hours or longer (a more frequent occurrence than most commanders anticipate), information enablers lose connectivity with the intelligence, fire support, and operations officers who continue to drive the lethal targeting cycle from the TAC. Without a clear understanding of the current fight, enemy disposition, or attitudes of the host-nation populace, the information enablers struggle to contribute to brigade operations until the TOC and TAC reunite.

If a brigade stopped its lethal targeting cycle for a day or more to concentrate on the current fight, the commander and staff would fail to master the transition



An RT media operative interviews a reputed student 3 June 2020 during an Iranian government orchestrated protest alleging "racist actions of the U.S. regime" held in front of the Swiss Embassy in Tehran, Iran. The placards carried by the students were written in both Farsi and English to illustrate that international audiences were the intended targets of the protest. RT is considered a major component of the Russian propaganda system that poses as a legitimate news agency. Its principal aim is to repeatedly promote perceptions of the United States in the worst possible light to undermine U.S. prestige and influence globally. (Photo by Zoheir Seidanloo, Fars News)

to the next battle period. The Air Force and brigade's division headquarters require the submission of aviation and general-support artillery requests seventy-two hours in advance, based on the air tasking cycle. The brigade sustainment battalion depends on the same amount of time to order and to distribute the ammunition required by organic mortar and artillery systems to engage the new high-payoff targets associated with the next phase. These fires and sustainment warfighting functions requirements ensure that intelligence, fire support, and airspace management systems appear in the TAC. Yet in the absence of clarity in command-and-control doctrine for public affairs, IO, and EW integration, there is no requirement to provide them with workstations in the TAC.

Although the long duration of information campaigns may make a commander comfortable with suspending the brigade's nonlethal targeting process for a couple of days, this disadvantages the brigade for two reasons. First is related to the lethal fight, since the absence of the EW officer in the TAC prevents this technical staff officer from requesting jamming efforts as part of the suppression of enemy air defense planning. The target working group convened at the TAC may coordinate for close air support or Army attack aviation to be on station, but their request may be denied if it does not include a coordinated suppression of enemy air defense plan. Although a nonlethal enabler, EW contributes to the fires warfighting function just as much as it does to shaping the information domain through broadcasting, jamming communications, or sending a mass text message to all the residents of one town.

Second, while the nonlethal working group pauses for a day or two, an armor or Stryker brigade combat team may clear multiple objectives across dozens of miles and

through several populated areas. As the tactical fight shifts the boundaries of the close fight and the security area expands behind the maneuver units, the brigade has immediate information requirements to inform the local populace about whether to shelter in place, direct internally displaced persons where to go, assess damage to public works, and hold key leader engagements with local leaders. The trauma of street fighting, destruction of utilities, and the citizenry's humanitarian needs require immediate attention. For every day that the brigade does not synchronize information enablers with the scheme of maneuver, it loses the opportunity to task subordinate units through the orders process to escort and protect IO, civil affairs, psychological operations, and human intelligence teams into the overlooked parts of the security zone where discontent will most likely brew. Given enough time to fester, as the U.S. Army witnessed in Iraq between the springs of 2003 and 2004, an insurgency will not only risk the lives of the deployed soldiers but also undermine coalition or national-level strategic communications efforts to laud the success of a military operation.

Yet even if elevated to a warfighting function and brought forward to the TAC in doctrine, information enablers cannot shape a brigade's operations when the billets are not filled. A brigade combat team staff includes two positions for field artillery majors, one to coordinate lethal targeting and the other for nonlethal efforts, but the latter billet is almost never filled because it is widely seen as less of a key developmental experience than coordinating the fires warfighting function. Where IO and cyber functional area billets exist in tactical units, they often remain vacant because of priority fills at the strategic and operational levels where generous funding supports offensive and defensive cyber operations. The Army IO proponent office did not help the situation by removing the position for an IO officer in the grade of major on the brigade combat team staff for several years. However, since the return of the position to the brigade staff, it is still not considered a career-enhancing opportunity. With the inception of the joint information function, it is not coincidental that the combatant commands and the Joint Staff appear more appealing for Army IO and cyber officers than positions within their service. Those concerned with their promotion potential are wary of trying to compete with combat arms officers on staff for a "most qualified" evaluation. To attract the most capable IO and cyber officers to tactical-level units would require a cultural change across the Army that recognizes their contributions to mission success.

Credence to the Information Domain

The Army continues to struggle to operationalize emerging technologies that shape the information domain because its doctrine and culture do not value information enablers as highly as those capabilities associated with the six warfighting functions. From basic training to the Senior Service College, every Army schoolhouse reminds students that if there are too many priorities then no one has articulated what is genuinely essential for the unit to accomplish its mission. To assist in discerning those priorities, commanders refer to doctrine before providing guidance to their staffs planning for unified land operations: the principles of operational design, the military decision-making process, and Field Manual 3-0's (*Operations*) explanation on how to integrate the warfighting functions. Rarely does dominance in the information domain top the list of key tasks or critical shaping efforts because influence operations do not merit the same level of concern as reconnaissance, fires planning, protection posture, and maneuver tasks. As a consequence, in a postdeployment or postexercise evaluation, a unit that realizes it struggled with leveraging strategic communications, IO, EW, and cyber operations can summarily dismiss these deficiencies, since the information domain remains an ambiguous concept in comparison to synchronizing collection, fires, and direct-fire systems.

Establishment of an information warfighting function would lead to a deeper development of doctrine to shape future Army requirements at all three levels of war. At the strategic level, a theater army must coordinate with interagency and coalition elements responsible for developing enduring messages for peacetime and in war. At the operational level, a corps or field army serving as a combined-joint task force requires access to and an understanding of the technologies possessed by 1st IO Command and the Army component of U.S. Cyber Command, in addition to a partnership with a U.S. embassy. At the tactical level, commanders who lack skilled staff members to lead the nonlethal efforts will instead concentrate on the warfighting functions represented in the headquarters. Fomenting requirements for collective and individual information tasks would justify the creation of permanent billets at all echelons. The expansion

of influence operations in Army doctrine would allow instructors to introduce leaders at each stage of their professional military education to existing and emerging capabilities to synchronize into their planning effort. Fidelity in career-enhancing positions and planning guidance would enable observer-controllers in Warfighters and CTCs to point out where a unit struggles to leverage information capabilities and coach them into applying doctrinal solutions to shape the area of operations.

The National Endowment for Democracy has warned against the nefarious "sharp power" applied by authoritarian regimes that "pierces, penetrates, or perforates the political and information environments in the targeted countries."[18] As one of those targeted countries, the United States cannot ignore this threat any more than it could the extended range rockets of North Korea or Russian missiles capable of shooting down a satellite. As part of the joint force, the Army must leverage experts knowledgeable in the culture, language, and social norms of each designated audience and target to improve the likelihood that messages will build trust and influence attitudes and behavior. The Army cannot do this in a vacuum; it must align its efforts with the other agencies and foreign partners participating in the information domain to minimize the risk of "information fratricide." The Army's more deliberate approach for adapting the joint information function through the creation of an information warfighting function would limit the need to deploy soldiers into combat once again to advance our national security objectives. ■

Notes

1. James Mattis, memorandum to the Department of Defense, "Information as a Joint Function," 15 September 2017.

2. Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. Government Publishing Office, 17 January 2017, incorporating Change 1, 22 October 2018).

3. Ritchel Mendiola, "Duterte Rejects Reported U.S. Plan to Return to Subic," *Asian Journal* (website), 29 July 2020, accessed 12 March 2021, https://www.asianjournal.com/philippines/metro-manila/duterte-rejects-reported-us-plan-to-return-to-subic/.

4. Robert M. Gates, "The Overmilitarization of American Foreign Policy: The United States Must Recover the Full Range of Its Power," *Foreign Affairs* 99, no. 4 (July-August 2020): 121–32.

5. Jennifer H. Svan, "Troops Living Deployment-Style in Poland as U.S. Military Ramps up Presence in Region," *Stars and Stripes* (website), 29 August 2019, accessed 12 March 2021, https://www.stripes.com/news/europe/troops-living-deployment-style-in-poland-as-us-military-ramps-up-presence-in-region-1.596399.

6. In 2018, the Trump administration rebranded the Broadcasting Board of Governors as the U.S. Agency for Global Media.

7. Alan L. Heil Jr., oral history conducted by author, 6 November 2008.

8. *Audit of Global Engagement Center Federal Assistance Award Management and Monitoring* (Washington, DC: Office of the Inspector General, U.S. Department of State, April 2020), accessed 12 March 2021, https://www.stateoig.gov/system/files/aud-mero-20-26-.pdf.

9. RT America News broadcast, viewed live by author, 17 January 2017.

10. Ryan Pickrell, "Chinese Foreign Ministry Spokesman Pushes Coronavirus Conspiracy Theory that the U.S. Army 'Brought the Epidemic to Wuhan,'" *Business Insider* (website), 14 March 2020, accessed 23 March 2021, https://www.businessinsider.com/chinese-official-says-us-army-maybe-brought-coronavirus-to-wuhan-2020-3.

11. Nicholas J. Cull, *The Decline and Fall of the United States Information Agency: American Public Diplomacy, 1989-2001* (New York: Palgrave MacMillan, 2012), 11.

12. "Mike Pompeo doubles down on unproven theory that COVID-19 originated from a Chinese lab," Twitter, 4 May 2020, accessed 12 March 2021, https://twitter.com/i/events/1257047441292922880?lang=en.

13. Donald M. Bishop, "Disinformation Challenges in a Pandemic," *The Foreign Service Journal* 97, no. 6 (July-August 2020): 39, accessed 12 March 2021, https://www.afsa.org/sites/default/files/fsj-2020-07-08-july-august.pdf.

14. Jeff Kao and Mia Shuang Li, "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus," ProPublica, 26 March 2020, accessed 23 March 2021, https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus.

15. Bret Schafer, "Disinformation and Election 2020," Council on Foreign Relations Local Journalists Initiative, 6 August 2020, accessed 12 March 2021, https://www.cfr.org/conference-calls/disinformation-and-election-2020.

16. Gregory M. Tomlin, "The Joint Force Needs a Global Engagement Cycle," *Joint Force Quarterly* 97 (2nd Quarter, April 2020), accessed 12 March 2021, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106514/the-joint-force-needs-a-global-engagement-cycle/.

17. Jian Wang, "Rethinking Public Diplomacy for a Post-Pandemic World," *The Foreign Service Journal* 97, no. 6 (July-August 2020): 42–43.

18. Juan Pablo Cardenal et al., *Sharp Power: Rising Authoritarian Influence* (Washington, DC: National Endowment for Democracy, 2017), 6, accessed 12 March 2021, https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.