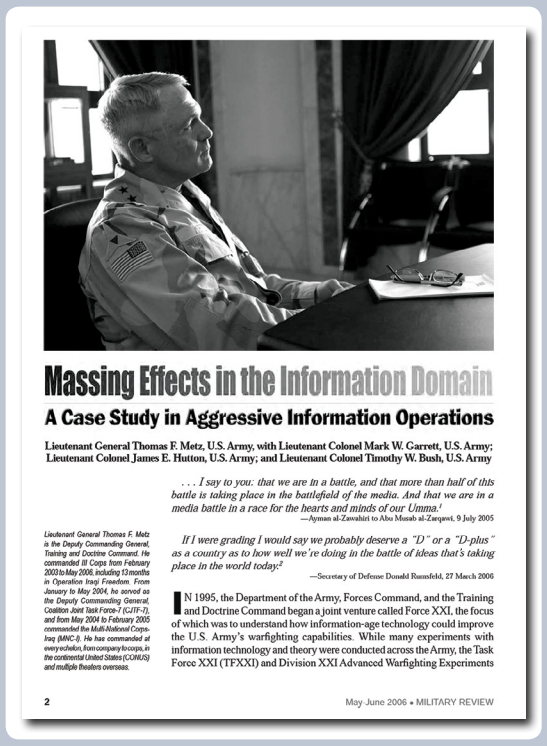
Military Review

WE RECOMMEND



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]

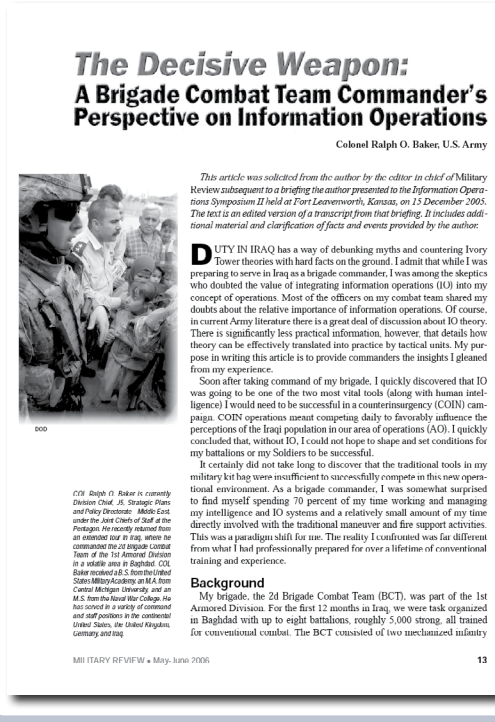
—Ayman al-Zawahiri to Abu Musab al-Zarqawi, 9 July 2005

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



The Decisive Weapon:

A Brigade Combat Team Commander's Perspective on Information Operations

Colonel Ralph O. Baker, U.S. Army

DOD

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.

COL Ralph O. Baker is currently Division Chief, JA, 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.

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

For those interested in studying the evolution of information operations concepts and practices, the May-June 2006 edition of *Military Review* features two seminal articles by commanders who pioneered tactical information operations at the corps and brigade levels: "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations" by Lt. Gen. Thomas F. Metz, U.S. Army, and "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations" by Col. Ralph O. Baker, U.S. Army.

To view the digital version of this edition of *Military Review*, please visit http://cgsc.contentdm.oclc.org/cdm/singleitem/collection/p124201coll1/id/165/rec/4. The articles are found on page 2 and page 13, respectively.

The above propaganda leaflet depicting Islamic State executioners slaughtering innocent civilians in a meat grinder was dropped over Raqqa, Syria, in March 2015 by coalition forces to help prepare the way for follow-on maneuver operations against that city. Information warfare creates operational advantages by the synergy of physical attacks that deny, disrupt, and destroy key enemy command, control, communications, computers, and intelligence (C4I) systems at the same time psychological and sociological measures are used to undermine the moral and cognitive commitment of adversaries to their cause by actions that foster confusion, intimidation, or persuasion. During I Corps' Warfighter Exercise 18-2, simulated leaflet drops similar to those conducted in Raqqa in conjunction with simulated physical attacks created the desired synergistic effects of information warfare in support of overall corps' exercise objectives. (Image courtesy of the U.S. Army)

Integrating Information Warfare

Lessons Learned from Warfighter Exercise 18-2

Lt. Col. Jonathan Rittenberg, U.S. Army

Maj. Mike Barry, U.S. Army

Maj. Daniel Hickey, U.S. Army

Maj. Bryan Rhee, U.S. Army

Capt. Holly Cross, U.S. Army

Conducting information warfare against nation-state near-peer competitors and various substate actors requires different approaches. Over the past sixteen years, U.S. Army information operations (IO) have focused on population-centric counterinsurgency operations with a strong emphasis on counternarratives, influence, and perception management. As the Army develops and inculcates new doctrine such as multi-domain operations and refocuses on near-peer adversaries, it must reinvigorate the use of information warfare.

Currently, U.S. joint doctrine does not provide an official definition for information warfare. The term last appeared in Joint Publication 3-13, *Joint Doctrine for Information Operations*, dated 9 October 1998, which stated, "Information warfare is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries."[1] Outdated and too broad in scope, we found this definition inadequate for our use. For the purposes of this paper, information warfare is defined as actions directed at affecting an adversary's "information detection sources, information channels, information processing, and decision-making systems."[2]

G39 is the information warfare enterprise staff section of I Corps. It is responsible for integration of information operations, psychological operations, space operations, and cyberelectromagnetic activities into operational planning.

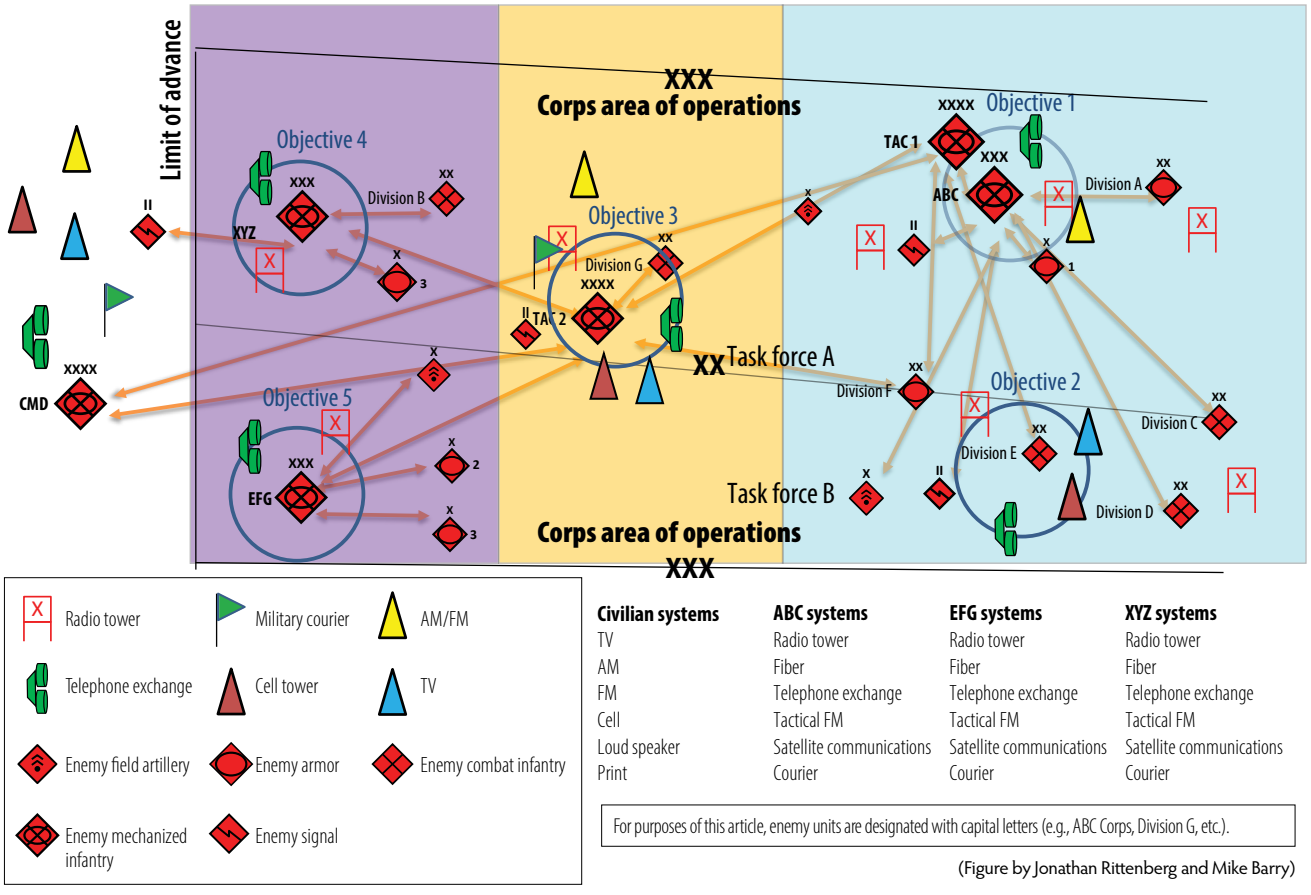
To gain an advantage, information warfare effects must focus on denying, disrupting, and destroying key enemy command, control, communications, computers, and intelligence (C4I) systems. The I Corps' organizational structure and its implementation of information warfare, integrated through an enhanced G39 (information operations) staff section, provides a model for the U.S. Army to integrate information-related capabilities (IRCs) for use against near-peer adversaries in future conflicts.

Lessons from Warfighter Exercise 18-2

During November 2017, I Corps, "America's First Corps," participated in Warfighter Exercise (WfX) 18-2, a Forces Command validation exercise for a tactical corps headquarters. The twelve-day command post exercise was set in a notional complex environment against a determined near-peer enemy force. WfX 18-2 tested the corps on all aspects of unified land operations and warfighting functions, and in all phases of the operations process.

One observation from the exercise was the need for rigor in the mission analysis process to understand the information environment.[3] The most critical output for the G39 enterprise during mission analysis was the combined information overlay (CIO). The CIO is a part of joint and Army doctrine, but it is not commonly used by corps- and division-level headquarters, according to observations by the Mission Command Training Program observers and the J7 of the Joint Staff.[4] The CIO developed during WfX 18-2 depicted enemy communications systems from strategic to tactical levels (see figure 1, page 102). Additionally, the CIO illustrated the information flow within the enemy organizational structure, which, when combined with intelligence assessments, clearly displayed the adversary's decision-making and command-and-control nodes. The CIO encompassed physical communication infrastructure such as satellite communication stations, cell phone towers, fiber-optic lines, radio communication towers, AM and FM radio stations, and television stations, as well as communication support units and military couriers. This allowed the corps G39 to understand the adversary's primary, alternate, contingency, and emergency plans and then prioritize physical destruction targets to disrupt enemy communication capability as well as prevent them from restoring communication paths.

Additionally, the CIO provided the staff with a general understanding of the communications processes and means the adversary government used to communicate with the population. This allowed the G39 to target these means (e.g., radio, TV, and cell phone text messaging) at the most advantageous time and place to create an information gap between the central government and the



(Figure by Jonathan Rittenberg and Mike Barry)

Figure 1. Cognitive Combined Information Overlay on Adversary Command, Control, Communications, Computers, and Intelligence Systems and Information Flow

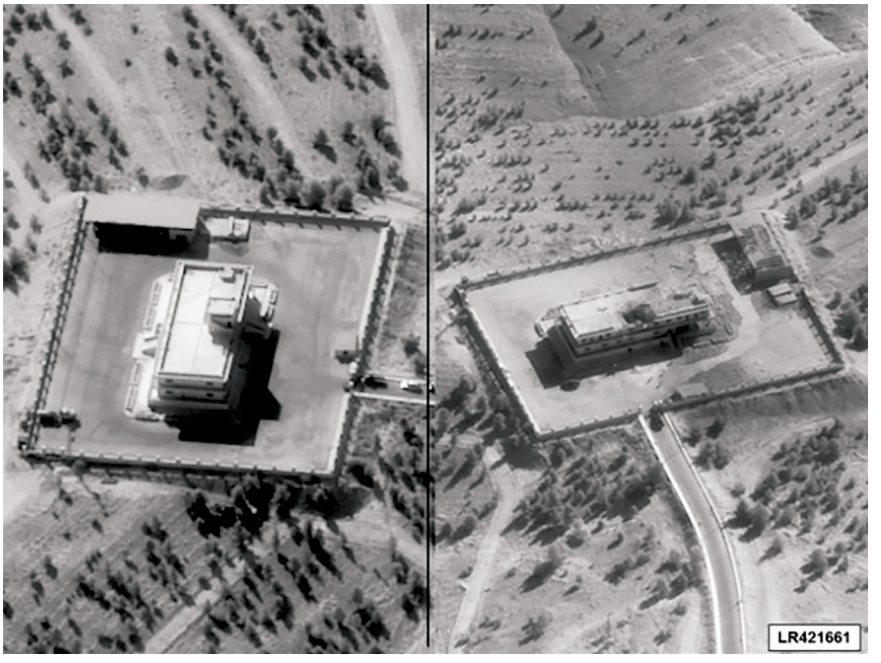
people, and it provided an opportunity for friendly psychological operations (PSYOP) messages that promoted civilian noninterference to reach the target audience.

The lethal and nonlethal targeting teams' analysis of the CIO provided refined targets to the corps high payoff target list. This analysis fed the targeting process by creating layered, synchronized, and coordinated lethal and nonlethal effects that disrupted, destroyed, and degraded enemy C4I systems. By delaying enemy decision-making and disrupting the enemy's ability to conduct coordinated operations, it created tactical advantages for the U.S. divisions in the corps area of operations. As enemy decision-makers grew more isolated and enemy units were destroyed, their maneuver forces began to reposition to consolidate combat power. These concentrations provided maneuver space for the divisions to target and exploit the remaining enemy. Additionally, the divisions were able to shape enemy tactical-level C4I by targeting brigade-and-below communications retransmission sites identified through the corps collection plan.

Lt. Col. Jonathan Rittenberg, U.S. Army, is the G39 deputy information operations chief for I Corps at Joint Base Lewis-McChord, Washington. He holds a BA from the University of Iowa and is currently working on an MA in strategic communications from the University of Iowa. As an IO officer, he has served at the brigade and corps levels.

Maj. Mike Barry, U.S. Army, is an information operations planner for I Corps, G39, at Joint Base Lewis-McChord, Washington. He holds a BA from the University of Wisconsin-Whitewater and an MS in information strategy and political warfare from the Naval Postgraduate School in Monterey, California.

During exercise execution, the systematic destruction of enemy information systems, command-and-control elements, signal units, and information maintenance units, from the strategic to tactical levels, isolated operational- and tactical-level decision-makers from the national-level command. The isolation effect allowed for friendly PSYOP influence efforts to decrease enemy units' will to fight. These effects, as depicted in figure 2 (on page 104), were timed and coordinated as part of the corps shaping operations to set conditions for the corps' and divisions' fights. As the fight progressed, the combination of lethal fires with PSYOP "will to fight" messages resulted in noticeable and measurable enemy surrenders as verified through the collection efforts of the corps intelligence (G2) section. While this is tough to replicate in simulation, the integrated planning, collection, and targeting processes are the critical lessons learned, and these results would likely be sustainable during actual combat operations.



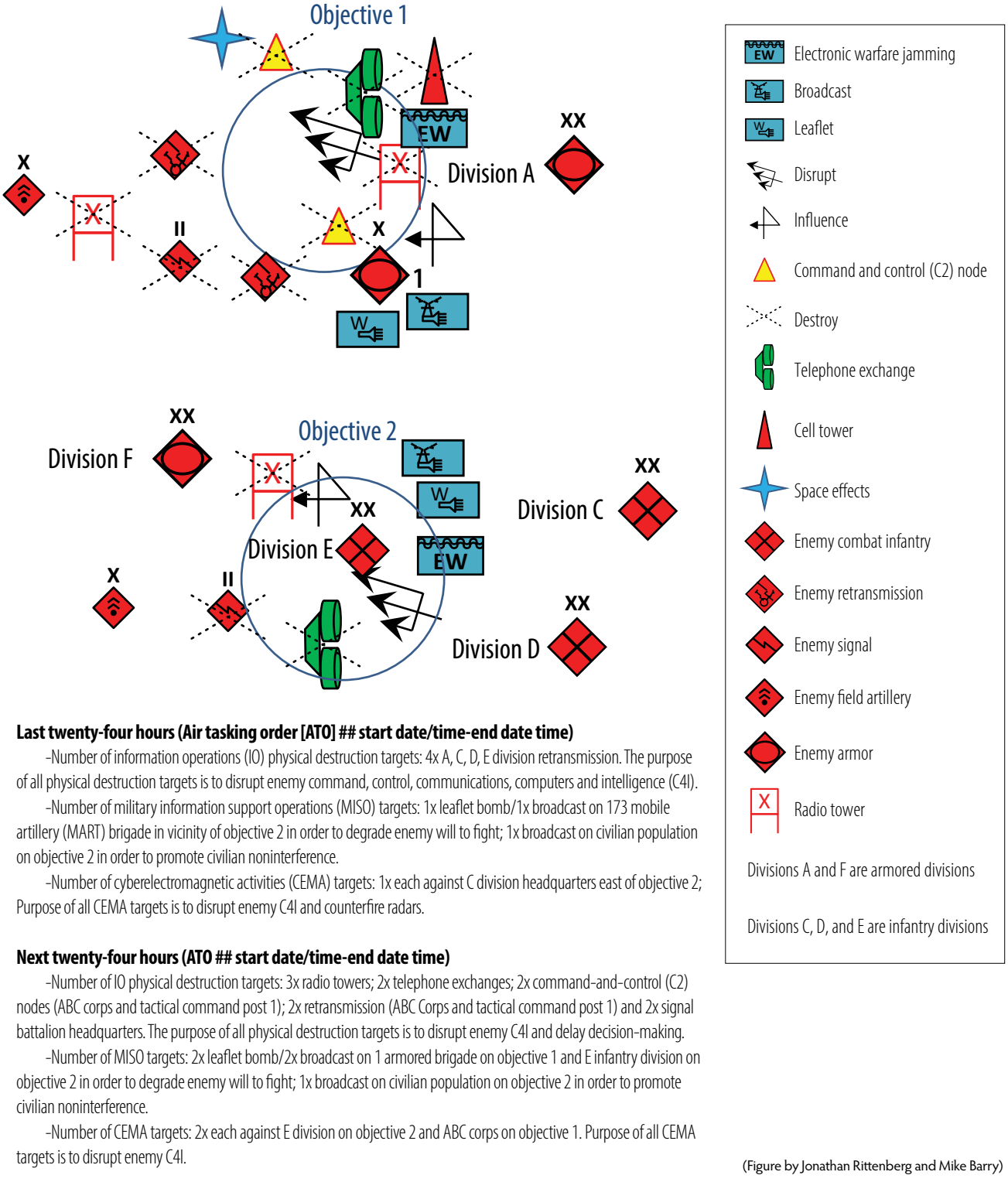
Battle-damage assessment overhead imagery shows the effects of a September 2014 attack against an Islamic State command and control center in Raqqa, Syria. During I Corps' Warfighter Exercise 18-2, similar simulated attacks were conducted against key command-and-control nodes at the same time other information operations measures were simulated to create the desired synergistic effects of information warfare in support of overall Corps' exercise objectives. (Photo compilation courtesy of the Department of Defense)

An example of the combination of information warfare and fires against an enemy capability occurred during the corps shaping efforts against the enemy long-range artillery brigades. Through the targeting process, fires focused on the destruction of key capabilities and equipment such as the artillery pieces and their sustainment support. Concurrently, the information warfare focus was on disrupting enemy communications through electronic warfare (EW) activities against radars and tactical communications systems. PSYOP focused on conveying the message that the enemy was doomed to inevitable defeat through leaflet drops and aerial broadcasts, as well as on nominating key enemy

Maj. Daniel Hickey, U.S. Army, is the cyber and electronic warfare planner for I Corps at Joint Base Lewis-McChord, Washington. He holds a BS and an MA from Western Kentucky University. His career includes two deployments in support of Operation Iraqi Freedom and assignments at the Joint Readiness Training Center, 4th Infantry Division, U.S. Army Cyber Command, and I Corps.

Maj. Bryan Rhee, U.S. Army, is a psychological operations planner for I Corps at Joint Base Lewis-McChord, Washington. He holds a BS in information technology from Rensselaer Polytechnic Institute and an MS in joint information operations from the Naval Postgraduate School. His previous assignments include tours of duty in Afghanistan, Indonesia, Korea, and Qatar.

Capt. Holly Cross, U.S. Army, is a space operations officer at Joint Base Lewis-McChord, Washington. She holds a BS from Texas A&M University-Kingsville and is currently working toward an MS from Johns Hopkins University. Her previous assignments include Fort Carson and Fort Myer.



Last twenty-four hours (Air tasking order [ATO] ## start date/time-end date time)

-Number of information operations (IO) physical destruction targets: 4x A, C, D, E division retransmission. The purpose of all physical destruction targets is to disrupt enemy command, control, communications, computers and intelligence (C4I).

-Number of military information support operations (MISO) targets: 1x leaflet bomb/1x broadcast on 173 mobile artillery (MART) brigade in vicinity of objective 2 in order to degrade enemy will to fight; 1x broadcast on civilian population on objective 2 in order to promote civilian noninterference.

-Number of cyberelectromagnetic activities (CEMA) targets: 1x each against C division headquarters east of objective 2; Purpose of all CEMA targets is to disrupt enemy C4I and counterfire radars.

Next twenty-four hours (ATO ## start date/time-end date time)

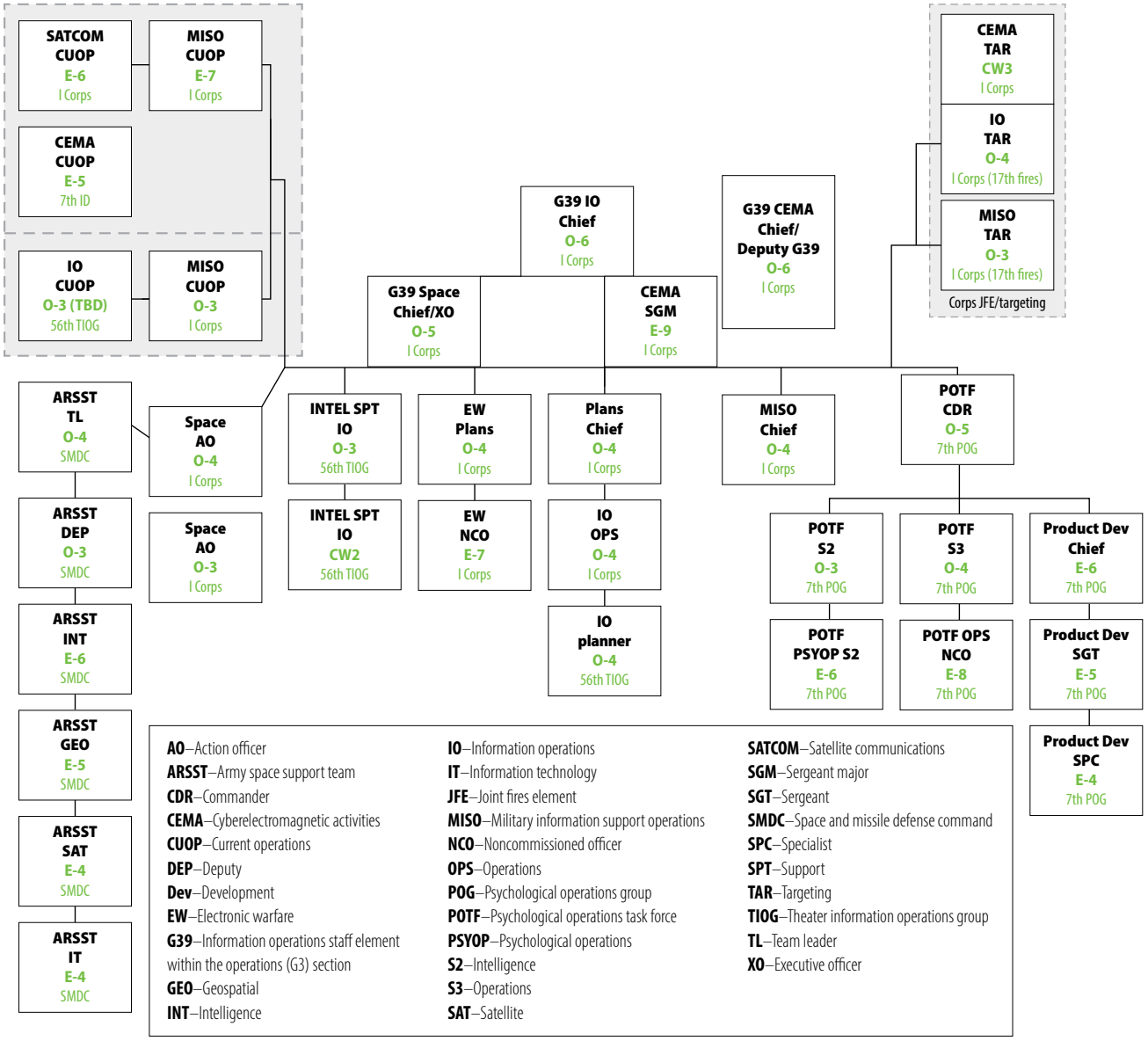
-Number of IO physical destruction targets: 3x radio towers; 2x telephone exchanges; 2x command-and-control (C2) nodes (ABC corps and tactical command post 1); 2x retransmission (ABC Corps and tactical command post 1) and 2x signal battalion headquarters. The purpose of all physical destruction targets is to disrupt enemy C4I and delay decision-making.

-Number of MISO targets: 2x leaflet bomb/2x broadcast on 1 armored brigade on objective 1 and E infantry division on objective 2 in order to degrade enemy will to fight; 1x broadcast on civilian population on objective 2 in order to promote civilian noninterference.

-Number of CEMA targets: 2x each against E division on objective 2 and ABC corps on objective 1. Purpose of all CEMA targets is to disrupt enemy C4I.

(Figure by Jonathan Rittenberg and Mike Barry)

Figure 2. Commanders Stand-Up Brief—Information Warfare Effects Applied during the Targeting Process



(Figure by Jonathan Rittenberg and Mike Barry)

Figure 3. G39 Staff Organization for Warfighter Exercise 18-2

garrisons for physical destruction. The PSYOP planners timed the release of the broadcasts and leaflet drops to occur just after destruction of enemy units, focusing on subordinate and adjacent enemy units. As discussed earlier, the resulting effect was an increase in enemy surrenders and desertions. Information warfare, specifically, physical destruction, was used to destroy the long-range artillery headquarters radio towers, telephone exchanges, and retransmission sites, which impacted the adversary's communications paths and overall ability to coordinate operations.

Corps G39 Organizational Structure

In discussion with other IO sections at both the corps and division levels, and with the Mission Command Training Program observer coach/trainers, it is clear that not every G39 section in the U.S. Army is organized the same. The I Corps G39 organization for WfX 18-2 is an optimal organizational structure to maximize effectiveness against a near-peer threat. The I Corps G39 is an integrated section made up of IO, EW, PSYOP, and space operations. For WfX 18-2, the G39 was augmented with a six-soldier PSYOP task force (POTF), a six-soldier

Army space support team (ARSST), and a six-soldier forward support team from the 56th Theater Information Operations Group. The intent for the augmentation while deployed is to increase the capabilities and work capacity of the G39 section to meet mission requirements and to provide the corps commander with more assets to use against the enemy. Figure 3 (on page 105) shows the organization structure of the I Corps G39 section during WfX 18-2. The increased capacity and staff integration provided through the intelligence support to information operations (ISTIO) team, the POTF, and the ARSST personnel were critical to I Corps success at WfX 18-2.

To sustain the understanding of the information environment during the exercise, it was critical to have an ISTIO team within the G39. This team consisted of two intelligence captains, a signal warrant officer, and an intelligence noncommissioned officer. The ISTIO team created an IO-specific intelligence collection plan that ensured information requirements were observed by corps organic and higher-level collection assets. This enhanced the G39's ability to assess the effectiveness against previous target nominations and to inform the G39 targeting officer for future information warfare nominations. More importantly, the ISTIO team's ability to assess the corps' information warfare effectiveness provided the corps commander with increased situational awareness through a clear operational picture of the adversary's degraded and destroyed C4I networks. Without the ISTIO team, the corps information warfare effects would not have been as timely, responsive, or successful.

The G39 also embedded an IO targeting team with the G3 (operations) fires section consisting of an IO major, a PSYOP captain, and a cyberelectromagnetic activities chief warrant officer. This team took the section's targeting priorities and ensured that they were nested with the corps high payoff target list and were integrated with the corps concept of fires.

The I Corps space support element (SSE) is a member of the G39 section at home station and forward. The SSE is typically augmented by an ARSST to provide continuous coverage for space events and to provide increased space capability to the corps. The ARSST and SSE focused on integration to provide space force enhancement to the corps staff for continued mission analysis and battlefield characterization as the operation progressed. The ARSST assisted with current operations by focusing on overhead persistent infrared data. By plotting this data and monitoring trends, the ARSST was able to work with the G2's current operations section in the combined operations intelligence center and recommend shifting assets. This action allowed I Corps to confirm enemy locations and expand its targeting based on intelligence, surveillance, and reconnaissance overflights. The ARSST also provided analysis to depict the effects of enemy jammers, while also monitoring jammer activity trends across the battlefield to provide targetable data for lethal fires. Additionally, the ARSST provided daily GPS accuracy data for maneuver and fires planning, and space weather and environmental data for the G6 section to maintain communication with higher, adjacent, and subordinate units. The ARSST provided imagery to the combat aviation brigade, the corps engineer section, and the G39 to assist in branch planning. Using the ARSST allowed the SSE to focus on layering special technical effects with other nonlethal fires from the G39 and lethal fires to support maneuver operations.

Recommendations

We recommend that corps and division formations consider replicating the organizational structure discussed in figure 3. This structure effectively facilitated the integration of the IRCs, intelligence, and targeting support to the G39 and enhanced planning and targeting effectiveness. It was a catalyst that enabled shared understanding among the G39, G2, G3, and G3 fires sections and the corps commander about the information environment and the information warfare capabilities available to the corps.

Our experience leads us to recommend the addition of one 35-series (intelligence) warrant officer and one 131-series (targeting) warrant officer as permanent members of the G39 staff section. This will allow the section to increase its contributions to and understanding of both the collection and targeting processes. The alternative is to rely on an intelligence analyst and targeting officer from the G2 and G3 fires sections. When faced with a high operational tempo and as competing priorities increase, the ad hoc ability of another staff section to provide dedicated specialty support to the G39 information warfare fight is suspect.

These organizational structure recommendations increase the manning within the G39 section and may be viewed as "empire building"; however, we see it as necessary. For too long, leaders within the Department

of Defense have discussed the importance of IO and how, strategically, the U.S. Army has routinely lost in the information environment.[5] Still, little has been done to organizationally increase unit IO and information warfare capabilities structures at the corps and division levels. The above recommendations may help improve how the Army fights and wins in the information environment.

Our final recommendation is to utilize all available authorities and IRCs to gain information superiority both against enemy C4I structures and in the narrative space. Information operations, and more specifically information warfare, is not restricted to nonlethal fires. It is our opinion that the title of "nonlethal fires" is a result of the years of focusing on counterinsurgency-centric concepts such as the battle of narratives, the war of ideas, or perception management. Additionally, nonlethal fires is often used to explain what IO does because for years, the results have been more often qualitative and hard to measure. As demonstrated in WfX 18-2, the I Corps G39 section's focus was not limited to nonlethal fires, as it used physical destruction against the enemies C4I systems in concert with EW, PSYOP, and other IRCs.

When it comes to fighting a near-peer threat, IO practitioners and Army leadership need to think beyond how IO has been used since the onset of the Global War on Terrorism. Leaders must allow planners to widen the aperture of how IO and information warfare is planned and executed. This requires commanders to promote creativity, staff integration, and planning that expands our options of what is possible.

Finally, G39 planners, regardless of whether they are IO, PSYOP, EW, cyber, space, or any other warfighting function, must aggressively execute and take advantage of created opportunities. G39 planners have to proactively integrate across the staff and break down any internal and external barriers to success. The bottom line is, if a G39 section is going to be successful in maximizing effects in the information environment against a near-peer adversary, the members of that section must increase the demand signal for information warfare, meet or exceed this demand, and tirelessly advocate for G39 capabilities and effects at every available opportunity.

Conclusion

I Corps put strong emphasis on the information warfare aspect of IO. This emphasis was decisive to setting conditions for the G39 to effectively isolate enemy formations through the destruction, disruption, and degradation of their C4I systems. These actions also enhanced the PSYOP effect on isolated enemy formations, increasing enemy surrenders and desertions, as well as increasing civilian compliance with I Corps instructions. The G39 focus on ensuring nonlethal targets were prioritized for collection ensured flexibility in subsequent targeting cycles to reinforce success or modify its nominations. A broad understanding of the information environment allowed the corps G39 to systematically dismantle the adversary's C4I systems, which degraded the adversary's ability to conduct operations. All of this was achieved due to the hard work of the corps staff and the optimized organizational structure of the G39. It is our hope that the recommendations in the paper will inspire other organizations to take a hard look at how they are conducting IO, to not settle for the status quo of the past sixteen years of counterinsurgency-centric logic, to challenge themselves and their staff to be agile and adaptive, and for the G39 section to truly integrate information warfare into every operation. ■

Notes

1. Joint Publication 3-13, *Joint Doctrine for Information Operations* (Washington, DC: U.S. Government Printing Office, 9 October 1998 [obsolete]), I-1.

2. Zhang Yuliang, *The Science of Military Campaigns*, ed. Zhanyi Xue (Beijing: National Defense University Press, 2006), 155.

3. Lt. Col. Daniel Billquist, Mission Command Training Program senior information operations observer coach/trainer, interview with Jonathan Rittenberg, November 2017.

4. Ibid.

5. Ralph O. Baker, "Information Operations: From Good to Great," *Military Review* 91, no. 4 (July-August 2011): 2–7. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20110831_art004.pdf.