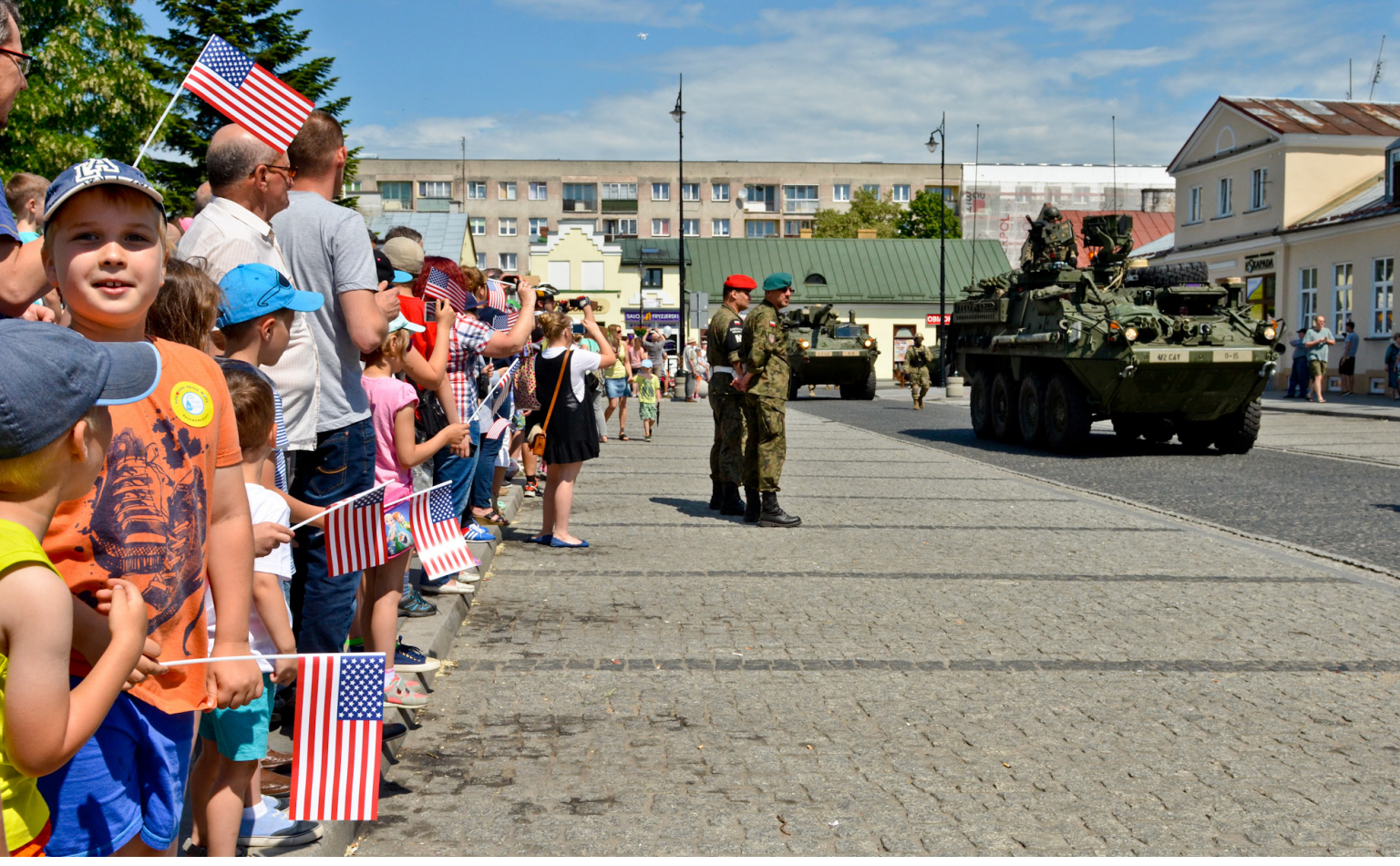


Soldiers of 4th Squadron, 2nd Calvary Regiment drive Stryker combat vehicles through the main square of Suwalki, Poland, 4 June 2016 during Exercise Dragoon Ride. Polish citizens were able to meet soldiers and see military equipment as well as witness the exchange of thanks between U.S. and Polish leaders during this civil-military engagement. (Photo by Sgt. Caitlyn Byrne, 10th Press Camp Headquarters, U.S. Army)

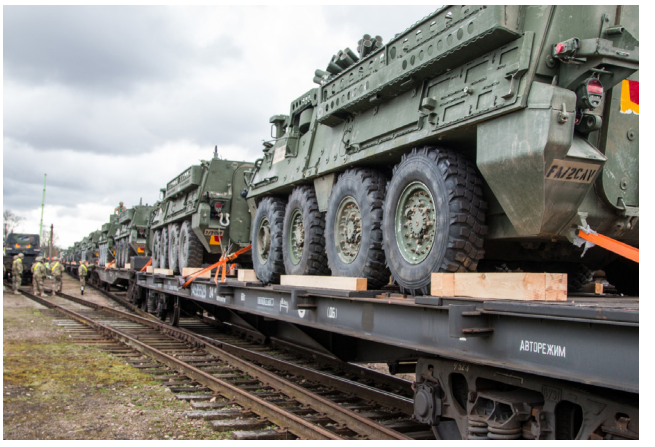
U.S. Army Information Operations and Cyber-Electromagnetic Activities

Lessons from Atlantic Resolve

Lt. Col. Matthew J. Sheiffer, U.S. Army

America's competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information. … U.S. efforts to counter the exploitation of information by rivals have been tepid and fragmented. U.S. efforts have lacked a sustained focus and have been hampered by the lack of properly trained professionals.

—*National Security Strategy of the United States of America,* December 2017



Stryker combat vehicles belonging to Ghost Troop, 2nd Squadron, 2nd Cavalry Regiment wait to unload during a rail operation 21 April 2016 at Gaiziunai, Lithuania. Ghost Troop received more than seventy pieces of equipment during the rail operation, which included containers, Humvees, and Stryker combat vehicles. (Photo by Staff Sgt. Michael Behlin, U.S. Army)

Following the 2014 Russian actions in Ukraine, the U.S. Army expanded its presence in Europe in support of Atlantic Resolve—a series of actions designed to reassure NATO allies and deter potential aggression. U.S. Army support to Atlantic Resolve illuminated a number of challenges that weaken the ability of tactical units to fight and win in the information environment. Barriers between the Army's information-related capabilities and the effective synchronization of those capabilities contributed to those challenges. With the recognition of how America's competitors use information found in the December 2017 *National Security Strategy*, the Army should consider whether lessons learned from Atlantic Resolve might inform larger discussions on the future of how the Army fights and wins in the information environment.

Operating in the Information Environment

Since February 2015, the 4th Infantry Division has deployed a mission command element to U.S. Army Europe (USAREUR) in a rotational capacity to support Atlantic Resolve.[1] For the U.S. Army, Atlantic Resolve includes a combination of persistent U.S. presence along the eastern flank of NATO, expanded participation in joint and combined exercises, and activities to demonstrate U.S. and NATO capability and capacity to move freely and conduct decisive action. Under the control of the forward-deployed mission command element, USAREUR-assigned and rotational forces executed synchronized activities to demonstrate U.S. commitment to upholding its collective security obligations, sending clear and visible signals about the credible and capable combat power of the United States and NATO.

Support to Atlantic Resolve resulted in identification of a number of lessons learned and best practices regarding the synchronization of information-related capabilities in a contested information environment involving a peer competitor.[2] Barriers between the Army's information-related capabilities and the effective synchronization of those capabilities weakened the ability of tactical units to fight and win in the information environment. These barriers arose from a combination of doctrinal changes, force design, and the emphasis on regaining decisive action proficiency after more than a decade of counterinsurgency efforts.

Lt. Col. Matthew J. Sheiffer, U.S. Army, is the commander of 1st Information Operations (IO) Battalion, 1st IO Command (Land). He served as the chief of IO for the 4th Infantry Division from June 2015 to May 2016 and the chief of staff of the mission command element in Germany from January to May 2016. He holds a BA from The College of William and Mary, and an MA from the University of Virginia. Sheiffer has served as the IO Branch chief in Army G-3/5/7 and the deputy IO chief with the 10th Mountain Division. From 2006 to 2009, he taught international relations and comparative politics in the Department of Social Science at the United States Military Academy, West Point, New York.

Doctrinal changes. In 2014, the thirty-eighth chief of staff of the Army, Gen. Raymond Odierno, discontinued use of the inform and influence activities (IIA) doctrine promulgated by Army Field Manual (FM) 3-13, *Inform and Influence Activities*, which had been released in January 2013.[3] This doctrine emphasized the important role of information-related capabilities during the wars in Iraq and Afghanistan. IIA emphasized the importance of interacting with foreign and domestic audiences to achieve military objectives. Although based on information operations (IO) doctrine, it only emphasized the more human-centric capabilities such as key leader engagement, public affairs, and military information support operations (MISO).

Polish tank crews assigned to the 11th Lubuska Armoured Cavalry Division roll into position to provide supporting fire to soldiers of the 3rd Combined Arms Battalion, 69th Armor Regiment, 3rd Infantry Division, 19 July 2016 during a live-fire training exercise in Trzebien, Poland. The exercise fostered interoperability between U.S. and Polish forces as part of Operation Atlantic Resolve, a U.S.-led effort in eastern Europe to demonstrate U.S. commitment to the collective security of NATO and to enduring peace and stability in the region. (Photo by Sgt. Lauren Harrah, U.S. Army)

With the end of IIA, Army doctrine returned to the joint definition of IO, "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[4] Yet, when the Army ended IIA, it retained the mission command task for commanders to inform and influence key audiences inside and outside the organization in Army Doctrine Publication 6-0, *Mission Command*.[5] It also retained the staff task to conduct cyber-electromagnetic activities (CEMA) and added a staff task to synchronize the employment of information-related capabilities. The Army also created separate doctrine for CEMA in recognition of the importance of cyberspace operations and electronic warfare.[6]

These doctrinal changes have contributed to gaps in understanding about the relationship between IO and CEMA. The Army has made CEMA an integrating function similar to IO and has focused on the importance of growing cyberspace operations and electronic warfare capabilities. However, doing so has unintentionally marginalized the IO synchronizing function due to the lack of a common understanding of the relationship between IO and CEMA.

While training guidance emphasizing the importance of CEMA has become common, there is less evidence that units prioritize how IO and CEMA work together to achieve effects in the information environment. While development of individual information-related capabilities like cyberspace operations and electronic warfare is essential, the Army should also retain an emphasis on the synchronized employment of these capabilities. That synchronization is critical to translating technical capabilities into effects on the battlefield that further the accomplishment of military objectives.

Force design. The challenges created by gaps in understanding about IO and CEMA have been exacerbated by Army force design. Army organizations disperse information-related capabilities throughout the staff. For example, at the division level, the Army has aligned MISO, civil affairs, and security cooperation in an engagement section under the operations staff (G-3)

while IO is a separate section under the G-3. Electronic warfare and cyberspace operations are in a CEMA section reporting directly to the chief of staff, and public affairs remains a personal staff section directly supporting the commander. Other information-related capabilities such as information assurance/cybersecurity are part of the signal staff (G-6) and counterintelligence is a part of the intelligence staff (G-2).

> The emphasis on CEMA as a discrete function separate from IO reinforced challenges in building teams that routinely utilized all of the functions at their disposal to create the conditions they desired in the information environment.

Although there are many good reasons to disperse information-related capabilities throughout the staff, it creates challenges to the synchronized employment of those capabilities. The decision to disperse information-related capabilities into separate staff elements has reinforced the misconception that these activities are separate and unrelated to IO. This deemphasizes the importance of the synchronized employment of information-related capabilities in creating the conditions in the information environment that support the achievement of the commander's desired end state.

Decisive action proficiency. The final factor that created challenges for Army units operating in a contested information environment is the unintended consequences of the emphasis on regaining decisive action proficiency after more than a decade of counterinsurgency. As units returned to full decisive action competency, they had to make hard choices and prioritize their training resources. This led to a tendency to reduce emphasis on synchronizing information-related capabilities since a return to decisive action meant less emphasis on the importance of the information environment than during counterinsurgency operations.

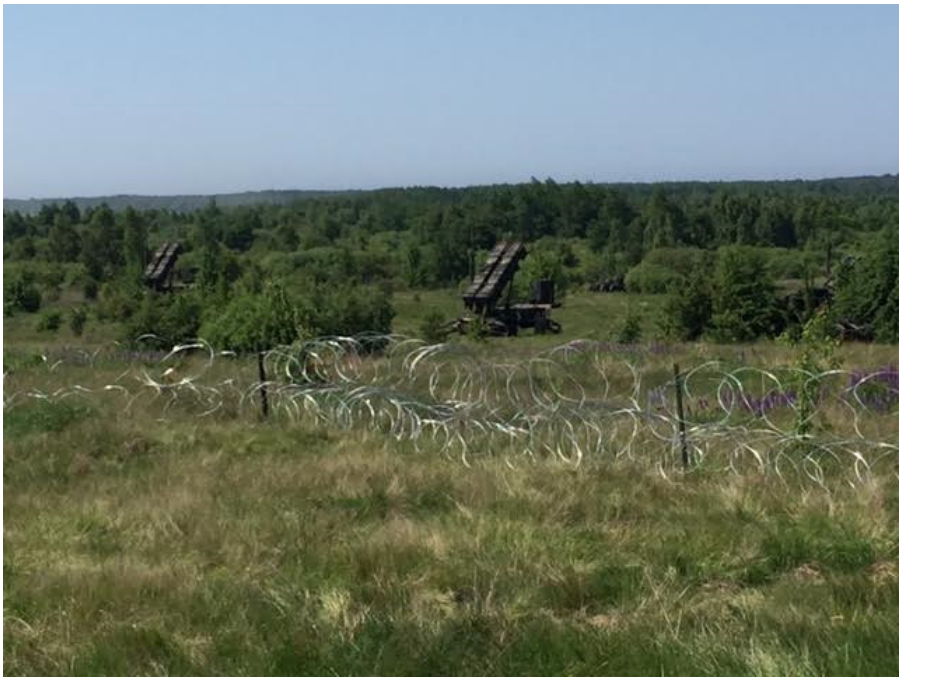
The challenge created by that mindset is that unless a unit is completely isolated from a population, it will always have a requirement to shape the information environment to accomplish its operational objectives. Trends in globalization and urbanization mean that the battlefields of the future will be in and among the population. Potential adversaries use cyberspace operations and electronic warfare in combination with IO to disrupt friendly decision-making and corrupt friendly mission command systems. Units that train for decisive action while ignoring the synchronization of information-related capabilities put themselves at a disadvantage.

Units that deemphasized the synchronization of information-related capabilities also tended to assign their IO officers to other duties within the headquarters. Although the IO officer positions on the brigade staff were key development assignments for those officers, many staffs assigned their IO officers to branch immaterial duties. While such personnel decisions benefited the unit, they did so at the cost of deemphasizing synchronizing information-related capabilities and the potential impact on the accomplishment of decisive action objectives due to lack of synchronization. It also came at a cost to the professional development of those IO officers. Officers pulled from their key and developmental assignments as captains and majors often experience challenges serving in related positions at higher echelons.

Many units did emphasize CEMA during their return to decisive action proficiency. However, the emphasis on CEMA as a discrete function separate from IO reinforced challenges in building teams that routinely utilized all of the functions at their disposal to create the conditions they desired in the information environment. While many units have grown and increased their capability and capacity to conduct information assurance/cybersecurity, defensive cyberspace operations, and electronic warfare, fewer have routinely synchronized those information-related capabilities with capabilities such as operations security, counterintelligence, and military deception to develop holistic and multidimensional approaches to protecting friendly mission command.

The Convergence: Information Operations and Cyber-Electromagnetic Activities

Too often, the convergence that receives the most attention is between cyberspace and the human domain. This emphasis ignores the broader problem set: that potential adversaries conduct activities throughout the entire information environment—not just in cyberspace—to achieve their objectives. Potential adversaries have not created the same barriers between capabilities such as public affairs, counterintelligence, military deception, cyberspace operations, electronic warfare, and operations security. They aggressively use foreign agents to exploit operations security weaknesses. They use what they learn from these collection efforts to create targeted phishing products designed to gain access to friendly information networks. They exploit information by disseminating misinformation and propaganda as conventional media activities. They mislead and deceive to create confusion and collective action challenges that prevent cohesive responses to their actions.



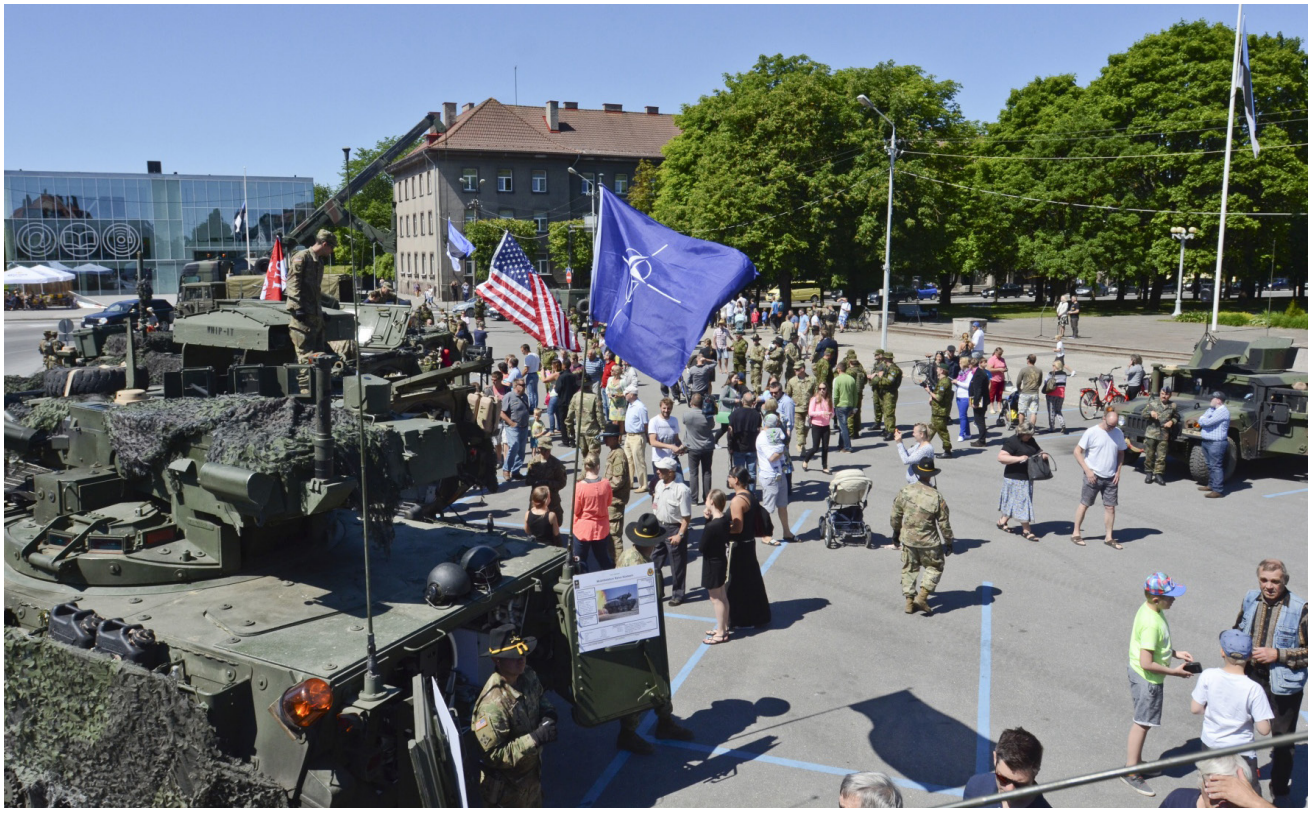
Soldiers from the 10th Army Air and Missile Defense Command along with joint partners from the U.S. Navy and Poland's 3rd Surface to Air Missile Brigade conducted electronic warfare testing on both Polish and American air defense systems in Turun, Poland 14–16 June 2016. (Photo by 2nd Lt. Brandt Ange, U.S. Army)

To overcome the challenges faced in affecting the information environment for operational advantage, the tactical formations supporting Atlantic Resolve had to change the culture within their organizations. This required a combination of command emphasis and creation of effective staff organizations capable of both executing the activities of individual information-related activities and synchronizing multiple information-related activities to affect the information environment for operational advantage.

Command emphasis. To effectively assure U.S. allies and deter aggression, Atlantic Resolve commanders had to relentlessly execute their mission command responsibility to inform and influence audiences inside and outside their organizations. Commanders, staff officers, and leaders at all levels routinely conducted face-to-face meetings, media engagement, and community relations, and they utilized websites and social media to engage key audiences. Every action a unit takes sends a message, and Atlantic Resolve challenged units to plan, prepare, and execute tactical tasks that sent the desired message.

The expectation for U.S. Army forces supporting Operation Atlantic Resolve was that leaders at all levels would maximize the use of activities to shape the information environment in ways that help the unit accomplish its objectives. To be successful, commanders, staff officers, and leaders at all levels had to take personal responsibility for requesting enabler support for information-related capabilities and for synchronizing those capabilities to ensure activities and exercises receive the visibility required to assure allies and deter potential aggression.

Units supporting Atlantic Resolve also had to protect critical information and mission command systems by synchronizing information-related capabilities such as information assurance/cybersecurity, defensive cyberspace operations, operations security, and counterintelligence. Potential adversaries manipulated the Atlantic Resolve information environment using the integrated employment of activities such as cyberspace operations, propaganda, and intelligence collection.



Hundreds of adults and children gather around the town center to look at Estonian, German, and U.S. military vehicles 14 June 2016 during a community engagement event in Parnu, Estonia. Events like this demonstrate U.S. commitment to the region and support Atlantic Resolve objectives. (Photo by Staff Sgt. Steven M. Colvin, U.S. Army)

Atlantic Resolve reinforced the importance of commanders ensuring their formations were capable of operating in a contested information environment.

The most successful units maximized opportunities to break down stovepipes during training and taught their soldiers how these functions worked together to better enable protection of friendly mission command. When leaders demonstrated they were serious about synchronizing information-related capabilities, units tended to emphasize these activities. At the brigade-level, emphasis by the commander and operations officer were critical to making synchronization work in the absence of a dedicated IO officer on the staff. The division, the first echelon with a dedicated IO staff, also played a critical role in resourcing brigade commanders and their staffs with enablers to synchronize.

Effective staff organizations. The 4th Infantry Division and its mission command element in Europe experimented with alignment of IO with the majority of the information-related capabilities on the staff to create a staff organization that maximized resources to both conduct individual information-related capabilities and to synchronize those capabilities. This involved an approach to operating in the information environment that took advantage of Army efforts to build cyber capabilities to keep up with the rapidly growing field of threats.

At the division level, an organizational approach that increased command emphasis, helped to break down stovepipes, and enabled a number of small sections to share resources was to create a collaboration group that included the following staff elements and functions: IO, operations security, military deception, CEMA, space, special technical operations, MISO, civil affairs, security cooperation, and public affairs. Although not a part of the core collaboration group, information-related capabilities such as information assurance/cybersecurity and counterintelligence collaborated as necessary.

The staff structure used by the 4th Infantry Division's mission command element in Europe organized its information-related capabilities into a consolidated, hierarchical element and designated an officer-in-charge. That position rotated between the

public affairs and IO elements, depending on which element was providing the more senior officer for the cell. When a public affairs officer led the organization, an IO officer served as the deputy to provide synchronization support. When an IO officer led the organization, there was no deputy, and public affairs retained its direct link to the commander.

The mission command element resourced a key leader engagement cell using borrowed military manpower from across the division. The mission command element also employed a civil affairs company from the 80th Civil Affairs Battalion and a public affairs detachment from the 10th Press Camp Headquarters to assist Atlantic Resolve forces with maximizing the reach of their messages. The civil affairs company commander served as the mission command element civil affairs officer while the public affairs detachment commander augmented the division public affairs element in the mission command element. All echelons also incorporated assessment into all activities by developing measures of effectiveness and reporting to their higher headquarters the impact of their activities on key audiences.

At the brigade level, most information-related capabilities on the staff were already located in the same staff element on the modified table of organization and equipment. However, with the loss of IO officers at the brigade level, commanders have had to shift staff responsibility for synchronizing information-related capabilities to reinforce the message the unit sends through its execution of tactical tasks.

In the absence of a dedicated IO position, the operations officer (S-3) has the doctrinal responsibility for executing the IO synchronizing function. Atlantic Resolve has required operations officers to use the operations process and targeting to incorporate enablers such as public affairs, civil affairs, and key leader engagement. By synchronizing these enablers with the unit's operations, commanders and their staffs ensured mutual support and reinforcing messaging to help key audiences understand the unit's actions.

Since the Army created the IO functional area in part to address challenges with ensuring adequate focus on information-related capabilities, it should come as no surprise that expecting a brigade S-3 to execute the IO synchronizing function without staff support was unrealistic. The proposed organization to maximize resource sharing and collaboration between brigade information-related capabilities was to consolidate public affairs, civil affairs, MISO, and CEMA into a single element at brigade level. The brigade could then utilize the intelligence officer in the electronic warfare cell and the psychological operations (PSYOP) noncommissioned officer to create a key leader engagement cell.

> "All units must train as they will fight and include training that tests their ability to synchronize information-related capabilities."

Brigades must choose how to designate a chief and noncommissioned officer-in-charge of the consolidated element. Only a brigade public affairs element is authorized a major. The other officer positions authorized are captains. Since most primary staff officers on the brigade staff are majors, there are benefits to designating a chief with the seniority and experience to interact effectively with their peers on the staff. Brigades can either fill this position by dual-hatting one of the organic positions or by using borrowed military manpower from another part of the brigade.

Conclusion

The execution of Atlantic Resolve demonstrated that a combination of command emphasis and effective staff organization could maximize the potential for Army units to compete and win in a contested information environment. Yet, the need for those solutions points to a larger challenge with how the Army is organizing and preparing its forces to conduct IO and CEMA.

The Army should consider whether the lessons learned from Atlantic Resolve offer observations that might contribute to larger discussions on how the Army should align its capabilities to fight and win in the information environment. Creating Army doctrine and staff organizations that explain and capitalize on the convergence of IO and CEMA are resource-neutral

options that could translate into immediate operational benefits. Such solutions could enable the Army to continue to grow individual information-related capabilities—such as cyberspace operations and electronic warfare—while retaining an emphasis on the synchronized employment of those capabilities.

In addition, IO elements must refocus their activities at home station and ensure a relentless focus on the preparation of their subordinate units to operate in a contested information environment. All home-station training should create opportunities to train units without IO officers to synchronize information-related capabilities. This can include resourcing unit-level training with external enablers and helping units to break down stovepipes between IO, CEMA, and other available information-related capabilities.

IO elements must develop scenarios during home station training to put pressure on their subordinate units so they cannot ignore the contributions that information-related capabilities can make to the achievement of military objectives. All units must train as they will fight and include training that tests their ability to synchronize information-related capabilities.

In addition to actions by IO elements, the Army should strongly consider further leveraging Army National Guard and U.S. Army Reserve IO capacity. The Army civil affairs and PSYOP communities have recognized that active-duty forces lack the capacity to support every brigade combat team. As a result, they habitually align Army National Guard and Army Reserve civil affairs and PSYOP units with brigade combat teams when they go through the combat training centers. The Army IO community should do the same. Theater IO groups should send teams to every combat training center rotation so that Army brigades habitually receive external augmentation by IO, civil affairs, and PSYOP units. In addition, the Army should consider conducting a holistic capability-based assessment of its IO and information-related capability forces to ensure they have sufficient resources to meet requirements.

If the Army intends to fight and win in a contested information environment, it will need to develop the capabilities and capacity to employ the full range of information-related capabilities. CEMA capabilities alone create necessary but not sufficient conditions for success. The IO synchronizing function is essential to translating technical capabilities into effects on the battlefield that create an operational advantage for the commander. ■

The opinions and conclusions expressed herein are those of the author and do not necessarily represent the views of the U.S. Army or any other government agency.

Notes

Epigraph. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017).

1. It has recently been announced that the mission to support Atlantic Resolve will transfer to 1st Infantry Division in May 2018. U.S. Army Europe Public Affairs, "'Big Red One' To Deploy as Atlantic Resolve Division-Level Headquarters," Army.mil, 17 January 2018, accessed 14 March 2018, https://www.army.mil/article/199163/big_red_one_to_deploy_as_atlantic_resolve_division_level_headquarters.

2. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 27 November 2012), GL-3. An information-related capability is "a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions."

3. Field Manual (FM) 3-13, *Inform and Influence Activities* (Washington, DC: U.S. GPO, January 2013 [now obsolete]).

4. JP 3-13, *Information Operations*, GL-3.

5. Army Doctrine Publication 6-0, *Mission Command* (Washington, DC: U.S. GPO, 10 September 2012), 10.

6. FM 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. GPO, 11 April 2017).

US ISSN 0026-4148