

Multi-Domain Operations and Information Warfare in the European Theater



Maj. Jennifer L. Purser, U.S. Army

The U.S. military is undergoing a major doctrinal transition from a counterinsurgency-focused fight to large-scale combat operations (LSCO). In the European theater, this evolution arguably began in late 2014. The United States did not execute a palpable response to Russia's military incursion into Georgia (a U.S. partner) in 2008, and with a second bold Russian military move that was the 2014 Crimean annexation, the United States strategically needed to stage a military response of some kind. However, the Russian threat demanded a

U.S. doctrinal change in order to effectively counter the near-peer adversary. Likewise, Russia is one of America's most experienced adversaries in the realm of information warfare (IW). Therefore, in contemporary warfare (i.e., LSCO), the U.S. capability of setting a theater to both apply IW and defend against enemy IW is paramount. Because of the case's relevance to LSCO, multi-domain operations (MDO), and IW, I will describe successful strategies for setting the theater from an IW perspective using a case study from the European theater between 2015 and 2019.



Relevant Terms Defined

Before fully launching into the case study details, defining a few applicable terms is necessary. According to the Center for Army Lessons Learned, “setting the theater” (STT) is a “continuous shaping activity to establish favorable conditions for the rapid execution of military operations.”¹ Most Department of Defense publications provide a largely logistics-centric definition to STT; however, two key tasks annotated for STT in Field Manual 3-94, *Theater Army, Corps, and Division Operations*, include “providing force protection,” and “modernizing forward-stationed Army units.”² These tasks are critical to enabling successful MDO from an IW perspective in the European theater.

MDO are the ways and means for the joint force [Army, Navy, Air Force, and Marine Corps] [to] counter and defeat a near-peer adversary capable of contesting the U.S. in all domains [air, land, maritime, space, and cyberspace] in both competition and armed conflict [emphasis added by author]. ...

... MDO provides commanders numerous options for executing simultaneous and sequential operations using surprise and the rapid and continuous integration of capabilities across all domains to present multiple dilemmas to an adversary in order to gain physical and psychological advantages and influence and control over the operational environment.³

A critical element to MDO is the electromagnetic spectrum (EMS), especially as it relates to IW. Joint Publication (JP) 3-0, *Joint Operations*, posits, “The joint force is critically dependent on the EMS for operations across all joint functions and throughout the OE ... therefore, the joint force should strive for local EMS superiority prior to executing joint operations.”⁴

A Department of Defense primer on information operations (IO) maintains that IW and IO are linked in the context of military MDO.⁵ As such, JP 3-13, *Information Operations*, defines IO (and IW in this context) as 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.”⁶ IO relies upon cooperation with various related entities to include strategic communications, public affairs (PAO), interagency coordination, civil-military operations, cyberspace operations, information assurance, space operations, military information support to operations (MISO), intelligence, military deception, operations security, and joint electromagnetic spectrum operations (JEMSO), among others.⁷ Within this context, MISO focuses on “the cognitive dimension of the information environment” and as such, relates heavily to the effects of disinformation and cyber/electronic warfare on a society.⁸ JEMSO, also referred to as cyber/electronic warfare operations, “are the coordinated efforts of EW [electronic warfare] and joint electromagnetic spectrum management operations to exploit, attack, protect, and manage the electromagnetic operational environment.”⁹ Examples include jamming communications (a Russian favorite), electromagnetic interference/interception, and even utilizing bots and trolls in social media. Signals intelligence (SIGINT) “is intelligence produced by exploiting foreign communications systems and noncommunications emitters. SIGINT subcategories include COMINT [communications intelligence], ELINT [electronic intelligence], and FISINT [foreign instrumentation signals intelligence].”¹⁰ SIGINT plays a significant role in JEMSO because of its role in collection and exploitation of elements of the EMS. Planners must coordinate for all entities that affect IO in order to adequately set the theater for MDO.

Case Study: Combatting Russian IW during Atlantic Resolve Operations 2015-2019

As a response to Russia’s annexation of Crimea, Operation Dragoon Ride 2015 (ODR ’15) was a

Previous page: Completing the first leg of their tactical road march from Rose Barracks, Germany, to Tapa Military Training Area, Estonia, soldiers of the 2nd Cavalry Regiment drive their Strykers into Ruzyně, Czech Republic, 27 May 2016 during Operation Dragoon Ride. The soldiers were met by a crowd of Czech citizens who showed their support for the U.S. presence in the Czech Republic. On their journey, approximately 1,400 soldiers in four hundred vehicles traveled over 2,200 kilometers through six countries. Dragoon Ride is conducted to validate U.S. partnering allies’ abilities to assemble forces rapidly, deploy them on short notice, and improve the ability to shoot, move, and communicate as a multinational alliance. (Photo by Sgt. Caitlyn Byrne, U.S. Army)

high-profile and controversial U.S. Army Europe (USAREUR) tactical convoy. A squadron of 2nd Cavalry Regiment (2CR) Stryker vehicles with additional logistical and support elements traveled in a convoy almost two thousand kilometers from Estonia back to their home base in Vilseck, Germany, through the Baltics, Poland, and the Czech Republic. Largely because of the convoy's representation as a symbol against Russian adventurism, pro-Russian IW actors were prevalent during ODR '15. Associated disinformation contributed to the convoy's controversy and had a significant impact on society in the countries through which the convoy transited. As a result of ODR '15 and subsequent Atlantic Resolve convoys, combined with a changing IW landscape (an uptick in pro-Russian disinformation and IW attempts), tactics and techniques used in the European theater to counter IW have ebbed and flowed over the past five years. Two primary public relations models and counter-IW techniques have emerged, one advocating preempting

enemy IW through high-profile U.S. presence in the press and the other espousing a quieter public approach. Both strategies have proven effective at setting the theater to combat disinformation and IW.

Under the leadership of Lt. Gen. Ben Hodges, USAREUR employed the active-messaging technique, specifically during ODR '15. ODR '15's intent, as Hodges explained during an interview, was fourfold in the wake of Russia's annexation of Crimea: (1) to show NATO partners that the United States was willing to defend them; (2) to show Russia that the U.S. would come to the aid of a partner in the event of a Russian incursion

U.S. Army Staff Sgt. Marion Szwyck, weapons squad leader from Apache Troop, 1st Squadron, 2nd Cavalry Regiment, Battle Group Poland, briefs Polish army soldiers from the 15th Mechanized Brigade on range cards 7 June 2018 during Saber Strike 18 in Wyreby, Poland. (Photo by 1st Lt. Erica Mitchell, Michigan Army National Guard)





into a NATO state; (3) to conduct a logistical reconnaissance (in preparation to defend against possible Russian hostility); and (4) to send a message to policy makers in the United States that more troops, training, and military might was needed in the European theater to ensure NATO's integrity.¹¹ In the meantime, Hodges aspired to make the thirty thousand U.S. troops who were then stationed and operating in Europe look and feel like a three hundred thousand-troop-strong economy of force (a significant IO undertaking in its own right). Some of USAREUR's IO-related strategies during ODR '15 included employing intelligence, signal/communications, PAO, and IO reserve entities to augment U.S. European active forces, bolstering NATO allies to enable enduring strategic defense against Russia, and maintaining a dynamic presence—meaning a moving, visible, capable, professional force—in order to deter Russian adventurism in the Baltics and potentially elsewhere.¹² The U.S. European Command (EUCOM) employed PAO and IO elements in abundance to amplify the pro-U.S. message and counter the Russian narrative to foreign and domestic audiences alike.¹³ Accordingly, ODR '15 incorporated focused, preemptive PAO messaging to include press

On 23 March 2015, day three of Operation Dagon Ride, soldiers from Iron Troop, 3rd Squadron, 2nd Cavalry Regiment, visit the town of Panevezys, Lithuania. A large crowd of onlookers came out to interact with the soldiers and take pictures of themselves with the U.S. Stryker armored vehicles. (Photo by Sgt. 1st Class John Wollaston, U.S. Army)

releases before mission commencement and after mission completion to discuss the U.S. military objective in the convoy. ODR '15 also placed an emphasis on conducting numerous static displays, command meet-and-greets, public commemorations, and even a concert. All these events were covered by the press.

However, because of the high-profile public messaging from the U.S. side during ODR '15, large-scale pro-Russian IW activities were lodged against convoy operations with the goal of undermining the true mission objectives of said operations. Though U.S./NATO elements tracked and tried to counter IW attempts, they were not always successful in countering falsehoods. Russian IW success made some countries less willing to host large-scale U.S. convoy events. Disinformation surrounding ODR '15 caused both public protest as well

as positive responses to opposition protests. Public activism, whether positive or negative, can be troublesome for the political environment of a host country. Further, no matter how carefully planned a convoy operation, a host nation will experience some inconvenience (e.g., traffic delays, property damage, etc.). As such, host-nation appetites for large, public convoys waned somewhat in the European theater after ODR '15.

Thus, as annual Atlantic Resolve convoys became common, the propensity for missions to be high-profile became less common. In fact, troops noticed that higher-profile convoys attracted more IW attempts. According to recent tactical leaders serving under USAREUR, sometimes the best way to combat disinformation surrounding an operation is to reduce the attention on it altogether, thus negating the likelihood of IW.¹⁴ The “smaller footprint” approach to contemporary Atlantic Resolve convoys was exemplified during a more recent operation, 2CR's 2018 iteration of Saber Strike. At the suggestion of host-nation governments, the convoy maneuvered through neighboring countries overnight (as

opposed to during the day). U.S. military and host-nation political leaders recommended the low-profile approach as a result of societal reactions to previous convoys that had experienced various negative effects from Russian IW.

Strategies for Setting the Theater to Counter Enemy IW

This section will discuss several unclassified tactics, techniques, and procedures (TTPs) the joint force can apply to help counter adversarial IW actions while promoting friendly operations. Core values and national narratives

are important to setting the joint theater for IW success. EUCOM's former digital media chief said, “The Russian government is OK with spreading falsehoods. Conversely, U.S. culture is rooted in the belief of honesty and fact. And that is the best way to combat Russian IW—by spreading the truth.”¹⁵ A USAREUR IW expert echoed the same notion:

Combating disinformation is all about a cultural battle of values. The U.S. military must continue to display truth, humanity, and a fairness in how we treat people, and continue to provide evidence that the disinformation reports which suggest we are willing to lie, run over people, kill people, etc., are false. If the U.S. loses credibility, it's a slippery slope.¹⁶

To reinforce combating disinformation, the USAREUR disinformation expert advocated publishing “fact sheets” before operations as TTP. He said,

We publish fact sheets for Atlantic Resolve missions which contain the ground truth facts. Then we share them around social and mainstream media as much as possible. We control the narrative by publishing what is really happening before any IW or disinformation agents can put a spin on anything. When Russia Today (RT—a state-backed Russian media company) says something like “the US is deploying 400 tanks in Europe,” and the previously published Fact Sheet says something completely different, it is pretty easy to see RT is spreading a falsehood.¹⁷

He continued,

The Russians paid attention. They exploited what we did when we kept operations a secret, now we preclude them from that ability to exploit our secrecy because we don't keep anything a secret anymore. They cannot take advantage of that any longer.¹⁸

Promoting fact-checking within the journalism community can assist in setting the theater for U.S. success in the IW realm. The USAREUR IW/disinformation expert also said,

Since Crimea, professional media outlets like AP, Reuters, and other Western media, have changed how they report things. In fact, outlets are going back to so-called “old-school” journalism and have started cracking down

Maj. Jennifer L. Purser, U.S. Army, is a military intelligence officer serving as the 101st Airborne (Air Assault) Division Analysis and Control Element (ACE) chief. Purser has served with the 201st Expeditionary Military Intelligence Brigade, U.S. Army Special Operations Command, and the U.S. Army Information and Security Command. Most recently, she was an Olmsted Scholar assigned to Brno, Czech Republic, at Masaryk University. Her studies focused on disinformation, hybrid warfare, and European security threats. She holds a BA from the College of William and Mary, an MA from American Military University, and an MA from Masaryk University.



After returning from supporting Battle Group Poland and NATO's Enhanced Forward Presence initiative, the 3rd Squadron, 2nd Cavalry Regiment, conducts a maneuver rehearsal of concept 27 May 2018 to prepare for its departure to Saber Strike 18. The day after the image was tweeted, *Voennoe Obozrenie* (Military Review), a Russian media outlet that covers military affairs, published an article titled "NATO servicemen are carrying out the seizure of Kaliningrad during 'Saber Strike-18' exercise." The article also stated, "We remind that in NATO countries, as well as in Russia, servicemen put on the map the symbols of likely enemies in red. You can see well that on the map the red color indicates the Russian Kaliningrad." (Photo courtesy of 2nd Cavalry Regiment Twitter. Supporting information courtesy of Atlantic Council's Digital Forensic Research Lab [DFRLab] via Medium.com)

on fact-checking. We don't see nearly as many examples of disinformation ending up in Western mainstream media.¹⁹

He added that an array of policy changes across Europe have advocated tightening good journalism rules within many countries and contributed to better reception toward U.S. operations than in the past.²⁰

EUCOM's former digital media chief suggested that an effective strategy at promoting facts and winning the narrative during operations is aligning on a tagline. She endorsed this method during ODR '15, and it helped to reverse the negative social media narrative about the operation. Troops painted #DragoonRide on Strykers and other trucks.²¹ The #DragoonRide tagline allowed anyone with a smartphone to tie their experience with the convoy in real time, which crippled IW attacks on

social media. In fact, according to a 2015 Atlantic Resolve report about social media, using hashtags aligned with the tactical mission (e.g., #DragoonRide) in conjunction with taglines of the operational or strategic mission (e.g., #AtlanticResolve or #StrongEurope) increased visibility by up to 10 percent or more and also helped nest ODR '15's mission within the overarching framework.²² Visibility amplified public knowledge of the operation's objectives and helped combat adversary IW.

Recent 2CR public affairs and civil affairs leaders shared some techniques for preventing the opportunity for disinformation agents to manipulate a story from the beginning. They mentioned a "no maps rule" for 2CR social media, which the unit adopted during a Saber Strike exercise in 2018. According to the team, 2CR posted a picture with various regimental leaders huddled around

	Жилин: от учений НАТО в Прибалтике выигрывают только проститутки	Zhilin: only prostitutes win from NATO action in the Baltic
	От учений НАТО в Прибалтике страдает народ, считает военный обозреватель	Local population is suffering because of NATO exercises, a military observer thinks
	Учения НАТО – угроза для местных жителей. Рассказы очевидцев	NATO exercises - threat for local inhabitants. Stories of witnesses

(Screenshot and quote below courtesy of Atlantic Council's Digital Forensic Research Lab [DFRLab] via Medium.com)

Headlines of Articles Published on Russian Propaganda Social Media Outlets in Response to Saber Strike 2018

“

Unfortunately, few people realize that Anglo-Saxons deploy a military contingent there, this contingent in particular, because the exercise and other exercises are just

a cover for military equipment transfer. In fact, it is a direct confrontation with the Russian Federation. This loss is most immediate for the civilian population, as the level of security of the countries is close to zero. We cannot but react to this situation, therefore, prostitutes are happy, political prostitutes receive money from the Anglo-Saxons to trade their national interests. Wherever you look—prostitutes win.

”

—Alexander Zhilin, reputed Russian military expert, as said to Sputnik, 9 June 2018

a map, planning transportation routes for the exercise. The photo was intended to reflect effective communication and team camaraderie. Kaliningrad, a small Russian territory in the Baltics, was colored in red on the map to ensure no convoy movements traversed through the territory.²³ However, Pravda.ru (another state-backed Russian media company, similar to RT) used the map to spread disinformation claiming, “Saber Strike 2018 is a provocation against the Russian Federation and NATO/USA will train how to isolate and occupy Kaliningrad.”²⁴ 2CR leaders also indicated that they collaborate with host-nation military and IW teams as much as possible, as NATO partners often have more experience with Russian IW than their U.S. counterparts.²⁵

In response to other changes in U.S./NATO TTPs for setting the theater to facilitate success in the IW realm, the USAREUR IW expert suggested coordination and deconfliction as tools to combat enemy IW.²⁶ He said,

U.S. leaders must understand the impact of our actions. The fewer opportunities we give platforms like RT to find a “kernel

of truth,” the more we can neutralize IW before it even begins. After ODR ’15 we started anticipating more in our planning, making deliberate attempts to publish pre-coordinated information with ample lead time before the operations. We didn’t want local communities to be surprised by a U.S./NATO convoy. Causing unexpected traffic backups could affect public sentiment negatively, which is opposite of the message we want to convey.²⁷

Conclusion

The U.S. military doctrine shift toward LSCO with an IW-savvy Russia representing one of America’s most capable adversaries makes the European theater a prime example of the importance of setting the theater for MDO from the IW perspective. IO and IW are linked to a wide array of contributing fields including JEMSO, MISO, SIGINT, cyber, PAO, and signal/communications, to name a few. This work analyzed unclassified measures U.S. military leaders have employed

within the European theater after 2014 that have set the conditions for favorable friendly IW and have been successful at countering enemy IW. Examples include two broad PAO strategies, one espousing elevated operational presence in the media and among host nations, the other advocating the opposite—remaining as low profile as possible. Each represents a strategy toward enabling successful offensive and defensive IW operations. Similarly, TTPs that facilitate U.S. dominance in the IW landscape include publishing fact sheets, advertising linked operational taglines, promoting fact-checking among the journalism community, coordinating release of relevant operational plans in a timely manner, and reducing public opportunities for exploitation. Finally, relentlessly maintaining U.S. operational transparency to both foreign and domestic audiences sets the firmest foundation for enabling MDO from an IW perspective. ■

The views expressed are those of the author and do not reflect the official policy or position of the U.S. Army, Department of Defense, or the U.S. government.

Notes

1. Center for Army Lessons Learned (CALL), *Set the Theater*, Catalog No. 19-10 (Fort Leavenworth, KS: CALL, March 2019), 1, accessed 12 August 2020, <https://usacac.army.mil/sites/default/files/publications/19-10.pdf>.

2. Field Manual 3-94, *Theater Army, Corps, and Division Operations* (Washington, DC: U.S. Government Printing Office, 21 April 2014), 2-9.

3. Andrew Feickert, *Defense Primer: Army Multi-Domain Operations (MDO)*, No. IF11409 (Washington, DC: Congressional Research Service [CRS], 16 January 2020), 1.

4. Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: U.S. Government Publishing Office, 17 January 2017), VIII-6.

5. Catherine A. Theohary, *Defense Primer: Information Operations*, No. IF10771 (Washington, DC: CRS, 18 December 2018), 1.

6. JP 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 20 November 2014), ix.

7. Ibid., II-5–II-13.

8. Ibid., II-9–II-10.

9. JP 3-13.1, *Electronic Warfare* (Washington, DC: U.S. Government Printing Office, 8 February 2012), vii.

10. JP 2-0, *Intelligence* (Washington, DC: U.S. Government Printing Office, 22 October 2013), B-5–B-6.

11. Ben Hodges (former commanding general, U.S. Army Europe [USAREUR]), interview by the author, 7 November 2018, Prague, Czech Republic. Record and transcription in author’s archive.

12. Ibid.

13. Ibid.

14. X. X. (three members of 2nd Cavalry Regiment), interviews by the author, 13 February 2019, Vilseck, Rose Barracks, Germany (2019 a, b, and c). Record and transcription in author’s archive.

15. J. W. (former digital communications chief, U.S. European Command), telephone interview by the author, 20 November 2018; follow-up interviews via email between 21 November 2018 and 30 November 2018. Record and transcription in author’s archive.

16. R. P. (USAREUR information warfare/disinformation expert), telephone and email interviews by the author, 21 November 2018. Record and transcription in author’s archive.

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid.

21. J. W., interview.

22. Richard Takacs, *Atlantic Resolve Social Media Environment Baseline Assessment* (Grafenwoehr, Germany: 4th Infantry Division Mission Command Element, 2015), 10.

23. X. X., interview.

24. Lithuanian Armed Forces (LAF), *Strategic Communication Department: Disinformation Hostile Information Activity* (Vilnius, Lithuania: LAF, June 2018), 1.

25. X. X., interview.

26. R. P., interview.

27. Ibid.