

# The Five OIE Truths

What it takes to be successful in the information environment

by Col Brian Russell

In the summer of 2020, LCpl Drinkwater was almost charged for disobeying orders when he criticized his battalion commander on social media in the midst of a force-on-force training exercise in Camp Lejeune, NC.<sup>1</sup> His actions were in clear violation of LtCol Beltfed's policy restricting cellular phone use in the field,<sup>2</sup> and Drinkwater's demeaning language about the proficiency of his commander (he sucks) and the overall conduct of the exercise (it sucked too) were not endearing any in his chain of command to his side. The only problem here is that LCpl Drinkwater's social media posts were all "fake news." Instead, the crafting and delivery of these messages, referred to as deliberately planted disinformation, to LtCol Beltfed were all orchestrated by the task organized II MEF Information Group detachment supporting the exercise's adversary force. For a period of several hours, this operation in the information environment (OIE) threw LtCol Beltfed and his subordinate commanders off their game plan. Instead of fighting the adversary force, they were dealing with internal friction caused by this and other sustained adversary force actions that exploited this vulnerability.

As a current MEF Information Group commander, fellow commanders often ask me "what it takes" to be successful in OIE. They deserve succinct and easily understood answers as all of us exist in an information environment that is very real and very now. In that light, I am sharing what originally started as assumptions of mine upon taking command as to "what it takes" to produce successful outcomes in the information environment. To do so, I am borrowing an approach from the special operations community by framing my former assumptions as the Five Truths of OIE.<sup>3</sup> I am convinced that having

**>Col Russell is the Commanding Officer of II MEF Information Group in Camp Lejeune, NC.**

the right mindset for this mission is the most important thing commanders and their staff can bring to the fight. After describing each truth using the LCpl Drinkwater example, I offer some recommendations for commanders to implement the right mindset in their own formations.

## #1 Humans Are in Fact More Important Than Hardware

This OIE truth is very similar to the first special operations forces (SOF) truth that recognizes a focus on training, educating, and caring for the special operator is more important than

the weapons and equipment that operator employs. OIE professionals are no different, as the success demonstrated in confusing LCpl Drinkwater's commander was born from the creativity of the combined intelligence, psychological operations (PSYOP), and communications strategy and operations (COMSTRAT) Marines of the MAGTF Information Group (MIG) Detachment embedded with the equally creative members of the adversary force. But I want to flip this truth on its head and emphatically state that the people in the adversary systems we are competing with are also more important than the weapon systems we seem to prioritize in our targeting processes. In the case of our example adversary force, the target was the exercise force commander, and they knew him well enough to know what would cause him cognitive friction.

To be successful in OIE, commanders need to be tasking their staff, par-



**Commanders and their staff must bring the right mindset to the fight in OIE. (Photo by SSgt. Stephany Richards.)**

ticularly the intelligence officer, to develop a comprehensive understanding of the entire adversary system—and this includes the thoughts, relationships, and behaviors of adversary decision makers. Only with that knowledge will we ever be able to influence, deceive, or attack and exploit networks of humans and their machines. In terms of naval integration, we should be prepared to exercise leadership here as the Navy also tends to focus on the adversary platforms rather than the people manning those platforms. When the Commandant recently challenged us to think about how our Corps could contribute to the anti-submarine warfare mission,<sup>4</sup> I hope I was not the only one thinking about how we could target the crews.

## #2 OIE Requires A Campaigning, Competition, and Collaboration Mindset

In this age of competing with powers who wield global tools of influence, commanders must realize we are in this fight for the long haul, we are always in contact with elements of the adversary's system, and we can leverage partners well beyond our chain of command to disrupt that system. Exploiting LtCol Beltfed in the singular action already described was born from repeated engagements, both physical and informational, over the course of the exercise. In this case, the adversary force had a slight white card advantage by being members of the same unit and local environment here at Camp Lejeune. But that only reinforces the need to be engaged in the environment as much as possible; the operational advantage is worth it. The adversary force was also not encumbered by established command and control (C2) relationships and the exercise "box" to complete their mission. Much of the information derived to build the targeting package against the commander came from infiltrations in the exercise force "garrison" headquarters by sympathetic elements not aligned to the exercise and forces outside the training area (or area of operations in a deployed scenario).

*MCDP 1-4, Competition*, (a must read) describes quite well the benefit of these three "Cs" of OIE: persistent

engagement with allies and partners against the adversary system, something akin to a wrestling match, lets us truly understand the systems behavior and shape it to our advantage. Unit planners should be developing operational, adversary-focused campaigns for their units instead of just waiting for deployment orders before thinking about the adversary system. The work invested in understanding adversary influence

and image. This disinformation was then delivered to LtCol Beltfed by the PSYOP Marines using a system under electronic warfare (depending on use case could also be cyberspace) authorities. What "sold" the news was the fact LtCol Beltfed received this message immediately after the adversary force delivered him pictures of LCpl Drinkwater's capture. The capture was real. The message saying "here's what we

---

***In terms of naval integration, we should be prepared to exercise leadership here as the Navy also tends to focus on the adversary platforms rather than the people manning those platforms.***

---

from an operational security and counterintelligence perspective is time well spent on that alone. For those in the weapon engagement zone or about to deploy into one, commanders should cultivate relationships with expected ally and interagency partners now. Not only will you be surprised at the level of support you can provide to one another's understanding and efforts, but you will be that more effective higher up along the competition continuum. Bottom line: if you wait until you get called into the blunt layer, it is too late to implement OIE.

## #3 OIE Requires Agility Across Authorities

The hacking of LtCol Beltfed's head resulted from the creative weaponizing of multiple OIE capabilities, each with a unique authority or permission, that were closely integrated into the scheme of maneuver by the adversary force commander and his staff. In this case, intelligence was used to acquire the names of the exercise force participants (including Drinkwater) and the MIG Detachment Marines used their presence in social media to find his social media profiles. The COMSTRAT graphics section then modified the social media screenshots with the endearing language (this sucks) under the Drinkwater's real social media name

found on his phone" was not. Here we had the tight integration of physical and informational actions to achieve the outcome.

OIE like this is only possible when commanders break down the silos across their staff and supporting forces to recognize and capitalize on all the authorities those entities bring to bear. This is how we accomplish OIE in the Information Command Center of the MIG. OIE capability specialists sitting together with all source intelligence teams to solve problems together. MAGTF and subordinate commanders need to create their own version of this convergence and enhance that with supporting MIG detachments when the mission requires it. We should be well beyond the days of commanders asking for a specific information related capability. Instead, describe what you want to achieve (or effects), break down the silos between intelligence, communications, and the OIE planners in operations shops, and you will be amazed by what you can do with the authorities you already have.

## #4 Quantity Is a Quality All Its Own

Unlike the SOF truth that posits quality forces are much more important than the amount of SOF produced, conducting OIE at scale with our adversaries can be the decisive factor in terms of legitimacy and relevancy with key pub-

lics and target audiences. The adversary force in our example was able to create real cognitive dissonance in LtCol Beltfed's decision making through steady and repeated engagement. Following the Drinkwater incident, the adversary force initiated a weather disinformation campaign against the commander. With a hurricane bearing down on the exercise force several days away and inclinations to end the exercise early, the PSYOPS team engaged the commander with reports of tornado warnings in the local area (this was disinformation too) and calls for the much-anticipated ENDEX (again, disinformation). The key to influence is pushing your target toward a behavior or decision they are already inclined to make, and let us refer back to OIE Truth #1. Do we really know our adversaries well enough to do this? All these actions accumulated to slow down the exercise forces actions against the adversary force. Adherents of John Boyd will recognize the approach:

shatter the enemy's cohesion through a series of rapid, violent, and unexpected actions which create a turbulent and rapidly deteriorating situation with which he cannot cope.<sup>5</sup>

We must do better here. Commanders need to direct their COMSTRAT officers and forces to embrace not only the bias for action in *MCDP 1* but also the strategy portion of their names by implementing sustained inform campaigns that are synchronized with maneuver. While it will stretch capacity, every training and exercise event should have a COMSTRAT CONOP that demonstrates our competence and professionalism. You should encourage your Marines and families on social media to take those messages and spread them with the influence they have within their spheres. Commanders should be on social media, conduct media engagements, and write as often as possible. Every bit of truth we put out is something our adversaries must contend with. This is competing.

### #5 Everybody Fights

I stole this truth from a good friend, mentor, and *Gazette* contributor, Lt-Col Mike Grice (ret). When he commanded 1st Air Naval Gunfire Liaison

Company, he inculcated an "everybody fights" mentality across the command. Everyone, from the personnel clerk to the motor transport mechanic, knew how to pick up a radio handset and guide fires onto a target. Learning how to do that after the observer was killed by enemy fire was too late. All Marines are part of the information environment whether they realize it (or like it) or not. For LtCol Beltfed and LCpl Drinkwater, it was too late when they finally realized they were part of this information fight that is all too real today.<sup>6</sup>

---

## **Fundamentally, there is nothing preventing us from successfully conducting OIE ...**

---

For commanders, that means we have an obligation to train and educate our Marines and families for the modern-day reality that there is no sanctuary. The Netflix documentary, *The Social Dilemma*,<sup>7</sup> became mandatory viewing not only at II MIG but the whole Russell family. Social media platforms are designed to addict and manipulate, and our adversaries are leveraging them to push us in a direction we are already inclined that supports their strategic to tactical objectives. Per my previous point, social media can be used responsibly, but we must all know the risks. As I write this, we are all thinking through the Secretary of Defense's guidance to conduct a stand down on extremism in our ranks.<sup>8</sup> Four years of fighting ISIS extremism in cyberspace at US-CYBERCOM tells me we have a lot of work here to keep our force protected from multiple forms of influence. Fortunately, proven Marine Corps education (critical thinking) and training (Combat Hunter) can go a long way to help our Marines spot, investigate, and report anomalous behavior in the information environment.

### Conclusion

Fundamentally, there is nothing preventing us from successfully conducting OIE than perhaps our own mental models that keep us from approaching and organizing for this fight. Integrated campaigning that brings to bear all available authorities to persistently engage our adversaries at home station and abroad represents our bid for success within our own formations and as a service. Perhaps it is too early to label these approaches as truths, but I feel in the depths of my professional being this is the best advice I can give to fellow commanders at any echelon on how to embrace and exploit our emerging OIE doctrine and capabilities. I welcome anybody's feedback on what they have found to be true about OIE so we can expand the body of knowledge and practice.

---

#### Notes

1. Name has been changed.
2. Name has been changed.
3. Staff, "SOF Truths," USSOCOM, (n.d.), available <https://www.socom.mil>.
4. Gen David H. Berger, "Marines Will Help Fight Submarines," *Proceedings*, (November 2020), available at <https://www.usni.org>.
5. Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: 1997).
6. Just the latest in a series of reports detailing the broad and enduring influence campaign Russia has been waging against citizens of the United States. Maria Snegovaya, "The Kremlin's Social Media Influence inside the United States: A Moving Target," *Free Russia*, (February 2021), available at <https://www.4freerussia.org>.
7. *The Social Dilemma*, directed by Jeff Orlowski, (Boulder, CO: Exposure Labs, 2020).
8. Staff, "DOD Stand-Down to Address Extremism in the Ranks," *Defense*, (February 2021), available at <https://www.defense.gov>.

