

facebook



U.S. Army graphic by Carrie David Campbell, SMDC

Federal civilian employees and Service members must be cautious of information-related activity on social media.

The Threat of Social Media: Operations in the Information Environment

by Mr. Joshua Jackson and Mr. Rick Rodriguez

Introduction

The U.S. Army's brigade combat team had not yet concluded its final rehearsal for an attack against enemy forces that were dug in just across the international boundary, when amateur bloggers released video footage of rocket strikes in a suburb near the unit's support area. Local news and social media posts quickly confirmed that the attack claimed 32 civilian lives and wounded more than 83 others, many of them women and children. No group claimed responsibility, but social media sites presented altered pictures and false narratives of U.S. Soldiers who were actually attempting to render aid, placing blame on U.S. forces. This rapid and unpredictable development quickly led to unrest and

insecurities in the brigade's rear area, which the unit had to stabilize before committing its combat forces to the attack—the attack was delayed.

While this incident is one of many replicated at Army combat training centers, it is a representation of the significant reality "information" has on military operations. In the real world, just last year, eastern adversaries disrupted United States training in Poland with alarming social media posts stating that a member of 1st Armored Division had allegedly killed a Polish soldier, had stolen a car, and was on the run. The posts even referenced the Soldier's unit, which was in the country at the time, and used his real photos.¹

Information Environment

For information operations to be effective, commanders' and their staffs' visualization of the area of operations must be expanded to include the information environment.² JP 3-13, *Information Operations*, defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."³ Numerous military information-related efforts/capabilities contribute to the information environment, including command, control, communications, computers, intelligence, surveillance, and reconnaissance systems; electromagnetic warfare; cyberspace operations; military deception; military information support operations; operations security; special technical operations; public affairs of- fice; and psychological operations, to name just a few.

The end state for most information engagements is to affect the decision making and behavior of adversaries and

designated others to gain an advantage across the range of military operations.⁴ Many of these engagements occur not directly with red (threat) on blue (friendly) but in the gray (civil) space, especially at the division and above echelons, which encompass social media platforms such as Facebook and Twitter. The collection, manipulation, and dissemination of publicly available information captured across social media and digital domains can accomplish adversarial objectives of influencing the operational environment; it can also diminish civilian and political support for current and future military operations. Future threats contend aggressively in the information environment throughout the entire competition continuum, seeking to deny support from civilian, political, and military audiences.⁵

Training for Information Engagements

To train for such engagements, the opposing forces (OPFOR) at all combat training centers have permissions to

The composite image consists of several parts:

- Top Left:** A news article snippet titled "A 24 Hour ceasefire between [redacted] collapse after a spat [redacted]".
- Top Right:** Two social media posts from a user named "Watcher_Unknown". The first post, dated July 17, 2020 at 3:23am, says "Many deaths reported. Destroyed homes and roads in the Kaaawa area. Take cover and stay safe!!! #FreeInformation". The second post, dated July 17, 2020 at 3:30am, says "Reports are coming in from Kaaawa that state that US artillery rounds aimed at DPRT forces have missed and are hitting civilians!".
- Middle Left:** A news article snippet titled "IN ANTICIPATION OF A BROKEN CEASEFIRE IN THE REPUBLIC OF TORBIA, IDPS COLLECT BELONGINGS". It includes a photo of a makeshift IDP camp and text describing the situation in Torbia.
- Middle Right:** A graphic with the "CRIP" logo and the text "Innocent People Whipped Out in the Republic of Torbia by the American Invaders". Below the text is a photo of hands holding small, metallic objects.
- Bottom Left:** A graphic titled "EXPLOSIVE WEAPONS" with the text "The use of explosive weapons in populated areas - it is time to act". It includes the "Advocacy" logo and a "STOP BOMBING CIVILIANS" logo.
- Bottom Right:** A graphic titled "KEY FACTS²¹" with the text "Between 2011 and 2015, nearly 108,325 persons were reported dead or injured globally due to the use of explosive weapons." and a bulleted list:
 - 77% of those casualties were civilians
 - When explosive weapons were used in populated areas, more than 90% of the identified victims were children.

These images are fictitious training scenario examples developed for and contained within the Information Operations Network for training purposes only.

access, obtain, and use publicly available information about rotational units to help them plan and execute their OPFOR mission. With some caveats, OPFOR Soldiers may view publicly available information posted to the internet, including social networking sites, installation newspaper websites, blogs, and any form of social media not requiring a login or the creation of a username and password. This information may then be analyzed to collect order of battle and other critical unit metrics to determine and assess the rotational unit's level of training, morale, strength, and deployment timeline,⁶ while also providing the training unit commander with feedback about their operations security vulnerability within the information environment.

At a recent home-station training exercise, a brigade combat team conducted decisive action operations in a live, virtual, and constructive environment against a multitude of threats. One of the commander's training objectives was to dominate the information environment, at echelon. To replicate the competitive information environment on the internet, the unit used the Information Operations Network, which is a U.S. Army Training and Doctrine Command (TRADOC)-developed government off-the-shelf system for replicating immersive aspects of the worldwide web, especially social media. Information Operations Network content is housed on closed intranets and accessed via the web. Content is unique to each exercise or event and allows the training audience to search web material and social media content that matches the scenario and meets training needs.

During the brigade's exercise, scenario developers, OPFOR elements, and intelligence subject matter experts used the Information Operations Network to replicate the effects that would naturally occur in the operational environment. The Information Operations Network reinforced intelligence message traffic while correlating network linkages developed through human intelligence reporting and patterns of life observed on social media. The Information Operations Network was also used to identify friendly and adversary



A TRADOC G-2 Information Operations Network training scenario with the 25th Infantry Division.

Screenshot provided by author.

locations, provide real-time indicators and warnings, and confirm target locations and battle damage assessments via social networking sites and microblogging services.

Additionally, the Information Operations Network allowed analysts (not just intelligence analysts) to monitor sentiments and actions of the local populace and potential OPFOR elements based on tweets and social media posts. Conversely, the OPFOR capitalized on information about the training unit to conduct hasty attacks and long-range fire missions. The OPFOR also developed a robust anti-U.S. campaign focused on disrupting military movements and operations by creating chaos while blaming attacks and events on the brigade. Deliberate deception stories inundated the internet, showing U.S. forces breaking the rules of engagement by shooting into buildings falsely identified as schools or community centers. As misinformation increased throughout the exercise without appropriate training-unit responses, their area of operation further destabilized, undermining their ability to maintain stability operations as the third pillar to decisive actions (simultaneous offense, defense, and stability operations).

At the combat training centers, exercise developers take the Information Operations Network to even more complex

levels by introducing specialized training units to the surface (or white) web and deep web. This includes replicating dark web/net domains, which consists of underground café chat rooms (for criminal and adversarial irregular forces networks), as well as a black-market interface, from which adversarial networks can buy, sell, and trade nefarious items based on the scenario.

During exercise execution, Operations Group planners develop daily scenario “normal” internet content (news stories, videos, and social media posts) and place heavy emphasis on dynamic scripting that is based on exercise-driven outcomes and robust adversarial social media attacks/rhetoric, all delivered through microblogging services, social networking sites, and adversarial news outlets.


To better prepare, some training-unit best practices include having designated personnel monitor the information environment continuously, proactively posting information ahead of an exercise to establish context of the operational environment, and anticipating and rapidly countering misinformation that may affect the unit’s mission. Additionally, Soldiers must take personal responsibility to keep their information safe and assist in detecting and countering misinformation. U.S. forces must be prepared to operate effectively in the complex, dynamic operational environment created by the ubiquitous nature of the information environment in which local incidents can have global effects.

Learn More about the TRADOC G-2 Operational Environment Center

The Operational Environment Center (OEC) supports the creation of a complex, tailorable operational environment for training, education, and leader development, using global data and innovative technologies to enable readiness. The OEC’s Support Division collaborates closely with the operational units, mission training complexes, Global Simulation Center, and combat training centers to help provide focused and scalable exercise design and expertise, share operational environment-derived lessons, and present OPFOR training and support to develop tough, realistic, and complex multi-echelon training.

In addition to the Information Operations Network and exercise design support, the OEC captures supported ex-

ercise data into comprehensive exercise support packages and posts them to the Exercise Support Application, a web-based repository where users can download exercise material for reuse or request additional OEC support. The TRADOC G-2 OEC Application and Service Hub, which houses the Information Operations Network, Exercise Support Application, and Operational Environment Data Integration Network, the authoritative source for all decisive action training environment operational environments, is located at <https://oedata.army.mil>.

To learn more about the TRADOC G-2 training tools and capabilities, contact the authors or the OEC at usarmy.jble.tradoc.list.tboc-operations@mail.mil or call (757) 878-9564/9503/9696. The TRADOC G-2 hosts in-person tools training sessions at Fort Eustis, Virginia, can travel to meet your organization’s needs, or can conduct virtual or telephonic training. Training includes more than the tools listed in this article. More information is available at <https://oe.tradoc.army.mil/operational-environment-center/>. “Victory Starts Here!” 

Endnotes

1. Gina Harkins, “Fake News Is Wreaking Havoc on the Battlefield. Here’s What the Military’s Doing About It,” *Military.com*, 16 August 2020, <https://www.military.com/daily-news/2020/08/16/fake-news-wreaking-havoc-battlefield-heres-what-militarys-doing-about-it.html>.
2. Robert Cordray III and Marc J. Romanych, “Mapping the Information Environment,” *Joint Information Operations Center* (Summer 2005): 7–10, <https://www.quantico.marines.mil/Portals/147/Docs/MCIIOC/IORecruiting/MappingtheInformationEnvironmentIOSPHERESummer2005.pdf>.
3. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations* (Washington, DC: The Joint Staff, 27 November 2012, incorporating change 1, 20 November 2014), I-1.
4. Department of Defense, *Strategy for Operations in the Information Environment* (June 2016).
5. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-8, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* (Fort Eustis, VA: TRADOC, 6 December 2018).
6. U.S. Army Forces Command memorandum, 10 April 2018; and 7th Army Training Command memorandum, 25 June 2018.

Mr. Joshua Jackson is a U.S. Army Veteran who continues to serve the Army as a civil servant within the U.S. Army Training and Doctrine Command (TRADOC) G-2. In his current capacity, he supports the Army’s program for replicating the dynamic complexities of the operational environment within training, education, and leader development.

Mr. Rick Rodriguez is a training specialist assigned to the U.S. Army TRADOC G-2 Operational Environment Support Division. He is a retired U.S. Army intelligence officer with 22 years of service, multiple deployments, and experience in a variety of government contractor positions at the U.S. Army Intelligence Center of Excellence.