# Going Viral: Preparing Ground Forces for Combat in the Information Age

## Description

*This Irregular Warfare Initiative article was originally posted through our partner organization, the Modern War Institute at West Point.*

Of all the lessons of the ongoing Russia-Ukraine conflict, one stands out: the importance of achieving dominance in the information domain. From the first days of the war, Ukraine has used information to shape the course of the conflict to its advantage. But American policymakers should not be too quick to mock Russiaâ??s failures in the information environment: the US military itself is underprepared for war in the information age, where the actions of military units and individual soldiers may go viral in an instant. As the US Army continues to reconceptualize the role of information as both a weapon *and* a battlespace, it should learn some lessons from Ukraineâ??s success.

**Failing to Train for Warfare in the Information Domain**

Despite impressive strides by the US military to elevate the importance of information in modern warfare, gaps remain that threaten to hinder its efforts in future conflicts. Senior leaders still tend to have a shortsighted view of information operations: at best, they view it as something that can help support or shape the decisive operation; at worst, itâ??s an afterthought. Maneuver commanders instinctively prioritize their efforts to dominate air, ground, and other domains, rather than focusing on the information space. They ignore Major General Robert Scalesâ??s advice that armies should prioritize â??capturing the psycho-cultural rather than the geographical high ground.â?•

In addition, the centralization of information operations authorities at echelons above the brigade level inhibits tactical commanders. Over the past two decades of counterterrorism and counterinsurgency operations, junior officers who attempted to leverage information confronted numerous protocols and grueling approval timelines as division and joint task force commands retained oversight in most cases. If this restrictive authority structure severely limited the effectiveness of information in counterinsurgency, then it will be crippling in large-scale combat operations, where the rapid pace of operations demands immediate exploitation of informationâ??a reality that has been demonstrated daily in the current Russia-Ukraine conflict.

Moreover, training and doctrine fail to adequately prepare tactical leaders for operating in an information-dense environment. Army doctrine, for example, does not explain how junior officers and

noncommissioned officers can successfully deploy information on the battlefield. Instead, the doctrine views brigade and division staffâ??who are often far from the point of contactâ??as the epicenter for information application. And there are gaps in training tactical leaders on how to effectively publicize US strategic goals and echo messages from echelons above brigade. A soldier being live streamed while on patrol will not be able to confer with a public affairs officer. The failure to develop military doctrine and training that empower tactical leaders represents a dangerous liability for future large-scale conflicts.

**The Primacy of the Information Domain**

The military should expect noncombatants to broadcast the actions of military units on the internet. Ukraine demonstrated the value of this by empowering each soldier as a network node able to accept and disseminate information instantaneously about Russian locations, fires, capabilities, and morale. The ability to exploit information at the tactical level allowed Ukraine to publicize every heroic act, every Russian failure, and every successful military engagement, creating an inspiring multilayered media narrative. While the origins of the mythical â??Ghost of Kyivâ?• remain uncertain, Ukraine profited from its popularity and promulgation, which has inspired a spirit of resistance captured in the phrase â??we are all ghosts of Kyiv.â?• Additionally, Ukrainian information operations demonstrate the primacy of emotional content. An example includes a display of 109 empty baby strollers representing the children who died at the start of the Russian invasion. These stories have effectively influenced international public sentiment and shaped the responses of political leaders. Information warfare makes war viral.

Adversaries also employ information warfare to shape the environment according to their interests. The proliferation of individually identifiable, commercially accessible data allows adversaries to microtarget American soldiers and commanders to disrupt and influence military operations. These techniques have already been employed in combat, pairing classic psychological operations with new technology to deliver pinpoint messages direct to soldiersâ?? phones. While the methods are new, the concepts are not. Many of these operations appear to be rudimentary and simple forms of harassment, but future efforts will likely employ more sophisticated technology, including deepfakes and machine learning to deliver powerful effects. The demonstrated willingness of adversaries to employ these techniques should inform future training and doctrine.

**Next Steps for the United States Army**

Instead of fixating on geographical key terrain, tactical commanders must acknowledge that winning in the information environment should be a priority. As Ukraine has proven, war is a contest of wills and the US military must recognize that to gain advantage in modern warfare, it must elevate the primacy of the information domain.

First, tactical operations and kinetic engagements need to serve a narrative strategy. The commanderâ??s intentâ??arguably the most important portion of a military orderâ??often fails to include how the mission supports the overall information campaign. As Lieutenant General Dennis Crall, the Joint Staffâ??s former director of command, control, communications and computers/cyber and chief information officer, J6 has warned, commanders currently have an attitude of â??sprinkle some IO on that.â?• That is a mistake. Information warfare should not be an ancillary thought in preparing for large-scale conflict but rather a primary means to achieving victory. Operational orders should therefore include an insertion on how the mission supports other information activities.

Second, the Army should consider options for decentralizing information operations and build a shared understanding of release authority across its formations. Dr. Raphael Cohen, a political scientist at Rand, highlights this organizational problem: â??I know what the release authority is for a JDAM [Joint Direct Attack Munition], but I donâ??t know the release authority for a tweet.â?• This centralized authority inhibits the potential of influence activities in a large-scale conflict. Ukraine has attained success in the information domain because of its ability to rapidly leverage information at the point of contact. Recognizing the potential benefits of decentralization, the US military should consider planning now for situations in which junior and noncommissioned officers might be the key to achieving information dominance in a future war. To do this effectively, however, the Army must educate the force on the appropriate use of information.

Third, commanders should prioritize enhanced media training and prepare for digital communication vulnerabilities. Increasing media awareness, integrating advanced media activities into field training scenarios, and strengthening relationships with journalists can better prepare American forces for modern combat. In Afghanistan, for example, commanders who fostered a relationship with journalists found that their initial concerns about operational security leaks were overblown. Instead, they found that through their media relationships, they were able to accurately convey the story of their unitsâ?? operations.

The Russia-Ukraine conflict should serve as a wake-up call for the Pentagon. The information domain is critical to modern warfare. The US military must reevaluate how conventional forces train and operate in this increasingly complex environment. Otherwise, it will cede the initiative to US adversaries, who are no doubt learning from Russiaâ??s experience in Ukraine and doing what they can to improve their influence capabilities. The US military must do the same.

*Captain Don Gomez is a psychological operations officer and student of information strategy and political warfare at the Naval Postgraduate School. Don is the deputy communications director at the Irregular Warfare Initiative.*

*Second Lieutenant Tucker Chase is an Army field artillery officer who holds a bachelorâ??s degree in defense and strategic studies from the United States Military Academy. He also serves as a research assistant for the Irregular Warfare Initiative.*

*The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.*

*Main Image: Ruined city center in Kharkiv, Ukraine. (PavelDorogoy, via depositphotos.com)*

*If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.*

**Date Created**
2022/09/01