

Risky Business: Enabling Commander's Risk Mitigation in the Information Environment



By Daniel W. Clark

The enemies, adversaries, and competitors of the U.S. and her allies continue to grow and [improve their use of the information environment](#) (IE). With each uncontested effort, they hone their tactics and techniques and improve their ability to sow confusion and doubt amongst Western forces and populations. These developments have created a pressing need for military leaders — commanders at every echelon — who understand and operate within the information environment. It is, however, incumbent upon those leaders — on you — to understand the risks of all activities within the IE.

This is not a simple responsibility, given the [complexity of the environment](#). The IE is global, nebulous, and constantly changing. The sentiment of the IE can turn 180 degrees due to a single action of one individual who may or may not be within the commander's span of control.

The importance of the information environment is recognized by senior leaders. Gen. Mark Milley, recently confirmed Chairman of the Joint Chiefs of Staff, stated in his pre-confirmation [questionnaire](#) that a significant investment in information warfare capabilities is necessary. United States military services are already expanding their information warfare capabilities. The Air Force's [39th Information Operations Squadron](#) is [growing its training capacity](#). The [Marine Corps Information Operations Center](#) has begun dabbling with providing information operations (IO) support to the Joint Force. Even the U.S. Army Cyber Command is [considering changing](#) to something that better describes its more robust involvement in the information environment. the U.S. Army Information Warfare Command.

Partners and allies such as the [Australians](#), Candians, and Emiratis are also stepping up their information warfare capabilities. The United Kingdom has been the leader in this effort with the [77th UK Brigade](#) actively working to counter foreign malign influence activities that target Europe and NATO.

With all of these changes and the growing emphasis on the information environment, it can

be hard for Army commanders to know where to turn for expertise when managing and mitigating the risks associated with this newly emphasized form of competition. The U.S. Army's 1st Information Operations Command can help.

1st IO Command is itself in the midst of a transition. As the Army works to adjust its forces to account for the proliferation of information warfare, the 1st IO Command will serve to fill some of the identified gaps, providing information warfare expertise today. The command's force design update is meant to increase efficiency and expand its capacity to support Army and joint force commanders' ability to project power in and through the information environment. The linchpins of this expansion are the IO field support team (FST) and the Army Information Operations Center (AIOC). The AIOC is being designed to provide a reach-back information planning and intelligence fusion capability that is unmatched in its ability to help commanders understand, visualize, and describe the information environment and its associated risks. Their mission is to help you "see" the IE and identify ways to mitigate those risks.

The IO FST is a purpose-built, deployable unit of action designed to not only support the integration and synchronization of all of a commander's available information related capabilities (IRCs) as part of multi-domain operations, but also to serve as operations security (OPSEC) and military deception (MILDEC) experts. These experts are trained and experienced in both planning for operations in the IE and employing these IRCs. They are critical to mitigating both risk to force and risk to mission.

Far more than just programmatic, the synchronized application of operational MILDEC and OPSEC serve to both preserve and project combat power. When managed by these experts, employing their unique access to national level assets, MILDEC and OPSEC can effectively delay or disrupt adversary decision making. These capabilities enable commanders to maneuver in and through the IE, occupy key terrain, and maintain a position of relative advantage over adversaries and enemies, whether in combat or competition.

Already employed to great effect by the joint force, the demand for this capability will only continue to grow. As commanders and future commanders of army and joint forces, it is critical that you know how to employ these experts to achieve your desired outcomes. Your information operations officers within your formation can help you submit requests for forces to engage this growing critical capability to support your accomplishment of tactical through national strategic objectives.

For more information about how to gain access to this growing capability, visit the 1st Information Operations Command booth in the room immediately preceding the *Risky Business: Leadership in the Information Age* panel on Monday, October 14, 2019 from 1:30pm to 3:00pm at the 2019 AUSA National Meeting and Exposition.

Daniel W. Clark is an Army officer, communications strategist, and the director of communications for The Strategy Bridge (@Strategy_Bridge), a non-profit international journal focused on the development of leaders in strategy, national security, and military affairs. Follow him on Twitter at @Clark_IO. The views expressed in this work are the author's and do not represent the official positions of the U.S. Army, Department of Defense, the U.S. Government, or The Strategy Bridge.

Share this:

- [Email](#)
- [Twitter](#)
- [Facebook](#)
- [LinkedIn](#)
- [Pinterest](#)