SSI
STRATEGIC STUDIES INSTITUTE
Executive Summary
UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM
Strategic Studies Institute and U.S. Army War College Press

MAINTAINING INFORMATION DOMINANCE IN COMPLEX ENVIRONMENTS

John A. S. Ardis
Shima D. Keene

The U.S. Army is committed to a high state of resilience and readiness. The problem is that for complex environments, the U.S. Army cannot afford simply to be very effective in a known set of circumstances and unprepared for others, and neither can it afford to be no more than moderately capable in the broadest possible range of circumstances. The U.S. Army has to be effective across the board, and that places extraordinary demands on its Soldiers during all phases of preparation for and engagement in conflict.

Dominance in the information space is a critical capability that will enable the U.S. Army to determine if, how, and when it will engage in conflict. For the U.S. Army to achieve and maintain information dominance, it will have to advance its capabilities to the point where it can rapidly and effectively deploy capabilities that outmaneuver advanced, well-resourced, and unconstrained threats under very difficult circumstances. This will require innovation, planning, and resilience, allowing its information capabilities to survive complex, premeditated, and asymmetric attack. In addition to deploying advanced information related capabilities (IRCs), the U.S. Army has to protect its own capabilities (including those of joint forces and allies) while degrading the adversary's capabilities.

This monograph explores some example risks and suggests that, when combating an unconstrained adversary, training and preparing of a suite of novel and tested operations is a necessary complement to the U.S. Army's current warfighting capabilities.

The risks to information dominance are varied. Examples include the likelihood that potential adversaries are already committed to aggressive information activities ranging from elementary deception operations to the nuanced use of multiple channels to achieve information and physical sabotage. It is also likely that there will be a further proliferation of communications and cyber technologies allowing nations, terrorist groups, and even individuals to corrupt, jam, and spoof U.S. Army communications; interrupt the supply chain; and possibly degrade command and control systems.

The tempo of information warfare may increase to the point where the mean time between significant events is shorter than the time needed to generate rational decisions or resolve ambiguities. This will challenge even the most expert decision-maker. Some nations will field highly protected special capabilities, so the U.S. Army will have to account for advanced information warfare methods and systems in the Joint Plan, even when the adversary's capabilities are unknown. It may also be increasingly challenging for all participants to discriminate between real and decoy physical targets in congested and noisy environments—even with advanced sensors.

In order to achieve and maintain information dominance, the U.S. Army must exploit the complexity and uncertainty of the battlespace and not simply seek to overcome it. As part of this venture, the U.S. Army must be prepared to field robust and potentially complex deceptions in support of its strategic objectives—enough to overmatch the adversary's counter-deception capabilities.

The U.S. Army's prowess in conventional warfighting should be augmented by the exploitation of a variety of advanced special operations in the technological and informational domains, expertly and rapidly integrated, using multiple tested outcome strategies that will survive and succeed under uncertain and very aggressive circumstances. The proficient use of special information operations (SIO) will create cumulative effects, where each operation magnifies the effect of those already undertaken, and prepares the ground for subsequent operations. SIO are particularly useful when the commander wishes to put the adversary on the back foot, and, as such, they are one of the most cost-effective and low-risk means by which the U.S. Army can achieve and maintain information dominance.

The U.S. Army should field a strong tactical and operational level active counterintelligence capability that deliberately targets adversary intelligence functions and undertakes various activities to mislead and degrade them. In particular, we note that the U.S. Army's existing Integration Staff within the Army Capabilities Integration Center (ARCIC) are pivotal in the process of coordinating the significant conventional warfighting and information capabilities along with additional special capabilities. The integration process exists in the preparatory stages (led by ARCIC), and also during conflict (within the U.S. Army and at the joint level). We present recommendations that will support the U.S. Army's need to seize the initiative and deploy coordinated operations that protect its assets and Soldiers, and manipulate and penetrate the mind of the adversary commander, leaving him confused and ineffective.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *http://ssi.armywarcollege.edu/.*

*****

Organizations interested in reprinting this or other SSI and USAWC Press executive summaries should contact the Editor for Production via e-mail at *usarmy.carlisle.awc.mbx.ssi-editor-for-production@mail.mil.* All organizations granted this right must include the following statement: "Reprinted with permission of the Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College."

This Publication

SSI Website

USAWC Website