

Information Operations and the Joint Force

By Mark Goracke

Space surveillance, negation, prevention, protection, computer network operations, deception, operation security, influence operations — how does it all fit?

These activities are just some of the pieces of the Space ops and Information Operations (IO) puzzle. It has been 11 years since work began to develop joint doctrine for Space Joint Publication 3-14, (Joint Doctrine for Space Operations). When JP 3-14 is formally approved, you will discover it still won't have all the answers, but it does illuminate the operational framework and describe mission areas in language even I can understand. My purpose here is to focus on the Space control mission area articulated in JP 3-14. I'll outline its missions and discuss how it will likely relate to emerging DoD views on IO and joint operations.

In accordance with joint doctrine, Space operations consist of four primary mission areas: Space control, force enhancement, Space support, and force application. Space control operations include surveillance of Space, protection, prevention and negation missions. For our purposes here, I will peel the onion a little and discuss the four Space control missions that are conducted across the range of military operations (peace-time to war).

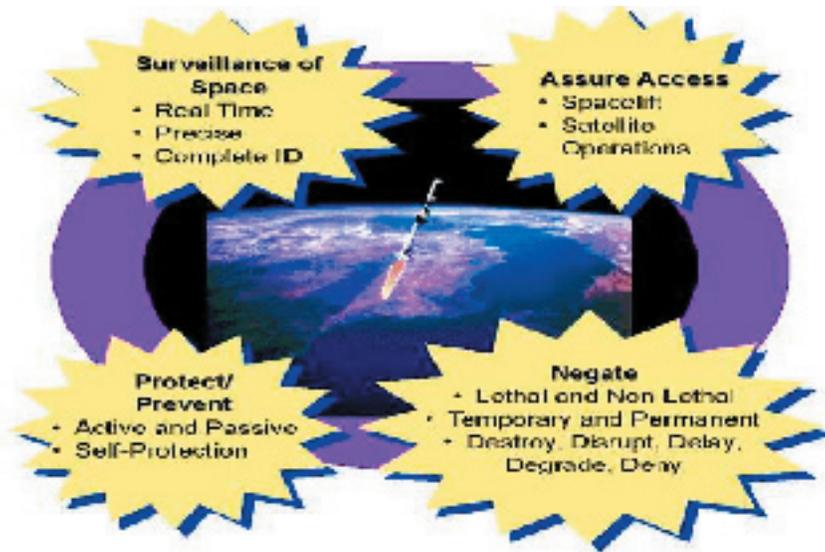
Surveillance of Space is conducted to detect, identify, assess, and track Space objects and events. Effective Space surveillance is essential for our ability to conduct Space control and achieve situational awareness within a given theater/Joint Operational Area. The information or data produced through surveillance of Space can be used to support terrestrial-based operations, such as missile defense, and avoidance of enemy reconnaissance assets. **BOTTOM LINE:** Space surveillance products should be available to a tactical user (Patriot battery in the field) as well as the intelligence analyst stationed in Washington, D.C.

Negation measures are designed to deceive, disrupt, deny, degrade or destroy enemy Space systems and capabilities. They are offensive actions that often target a ground link or Space segment of an enemy Space system. Deception measures are designed to mislead an adversary through manipulation, distortion or falsification. Disruption temporarily impairs enemy systems; denial temporarily removes or eliminates them.

Degradation efforts permanently or partially impair an enemy Space system, usually through physical damage, and include attacking both ground and Space segments of the targeted system. Destruction is the permanent elimination of a given Space system's capability. Examples include attacks on key ground nodes, uplink or downlink and power sources, command and control facilities and even assets in orbit. Destruction can be achieved employing kinetic or non-kinetic means — it could even involve dispatching a person armed with a hammer or a laptop, although that *might* be an over-simplification.

Prevention activities preclude an enemy's use of U.S. or third party Space systems and services. Prevention measures include military as well as political or economic actions. An example of prevention could be our effort to purchase all the available commercial imagery in a given theater of operations. In simple terms, we may not be able to prevent commercial sources from taking pictures but we can buy all the pictures they take and thus prevent the information from falling into the wrong hands.

Protection measures consist of active and passive measures to ensure U.S. and friendly Space systems continue to operate in a hostile environment. In essence, these measures counter an enemy's Space negation efforts or minimize their effects. Space protection measures may also be employed to counter or marginalize the effects of Space environmental factors. Active and



passive protection measures must be prioritized and consistent with overall mission priorities. Examples of protection measures include ground facility defenses, satellite radiation hardening, mobility, concealment, and link encryption.

Now that I have briefly described the doctrinal framework for Space control, I will cover some of the emerging IO policy changes and how they tie into the Space control mission area. On the Office of the Secretary of Defense's initiative, DoD Directive 3600.1, Information Operations policy, is obtaining a face-lift and will trigger a revision of JP 3-13, IO Joint Doctrine. Hopefully, that effort won't require as many restarts as JP 3-14 and there will be something for us to use in 21 months or less. The sixth version of the draft 3600.1 is currently being staffed with the military services and redefines IO as actions taken to influence, affect or defend information, information systems and decision-making. On the surface, the differences between this definition and the old one in JP 3-13 are rather subtle, but in essence it narrows the IO focus. For starters, the new definition indicates that we should look at influencing all foreign perceptions and decision-making. It implies that in peacetime, IO influence ops could mean not only targeting an enemy or adversary, but also neutral foreign parties or potential allies. In crisis short of hostilities, the draft directive states that IO may also be used as a flexible deterrent option to communicate national interests or demonstrate resolve. In conflict it may still be applied in its traditional role to achieve physical and psychological results in support of strategic or operational objectives.

The IO framework outlined in the new 3600.1 revolves around core, supporting and related capabilities. Core capabilities are divided into two parts: psychological operations, military deception, and operations security oriented on influencing adversary decision makers

or groups while protecting friendly decision-making; and Computer Network Operations and electronic warfare which are employed to affect and defend the electromagnetic spectrum, IO systems, information weapons and command and control. Supporting capabilities include Counter Intelligence, physical attacks, physical security, information assurance and intelligence. Related capabilities consist of public affairs and civil-military operations.

Now that I have outlined the Space Control and emerging IO frameworks, let's briefly discuss how these missions and capabilities complement one another. To begin, Space surveillance, also categorized as an intelligence activity, is an IO supporting capability. It's not implied here that all Space-based surveillance only supports IO. The point is, Space surveillance is critical to achieving information superiority — the IO objective. Negation activities in Space closely align with the IO core capabilities of deception, operations security, electronic warfare, and Computer Network Operations. An example of mission lash-up would be electronic spoofing measures to deceive an enemy on the true location of our Space surveillance assets.

The take-away point is negation deception measures should be fully coordinated and integrated with overall IO deception planning and execution. U.S. Space Command is the DoD lead for Computer Network Attack and Defenses and therefore, joint Space support teams and other Space experts deployed to a given theater must be involved in theater Computer Network Operations planning and operations. Space Control prevention activities support the IO core capability of operations security and supporting capabilities of counter intelligence, physical security, and information assurance. Examples of merging Space control prevention and

(See Joint Force page 40)

Security Challenge ... from Page 35

Space access to operations.

Space control is too important to this nation to be relegated to whispers. We must plan for it, train to conduct operations, and learn how to debate the finer points while maintaining security. Professional discussions enhance the deterrence value by putting a potential adversary on notice that what seems to be vulnerability may in fact be strength. Remember, Space control does not equal Space negation. It also includes those measures designed for surveillance, prevention, and protection. A system's capability to support Space control in a general context is usually unclassified. When you begin to make further association with specific mission areas and technical

capabilities and the technical capabilities tend to lead to classified system specific discussions, then you cross into the gray area where conclusions may be drawn or facts derived that reveal secrets.

Candid open discussions about Space Control should prove healthy and enlightening for all. The military is charged with protecting national security interests. The nation's reliance on Space is too important to be left unprotected. As former Army Chief of Staff General Gordon Sullivan stated once, "Hope is not a method." With people and countries still seeking and finding vulnerabilities to attack, the military must plan for when disaster strikes and all Space assets are vulnerable. We must continue frank

professional discussions and take the initiative. Using a security classification guide as a Rosetta Stone, we can proceed without revealing secrets.

LTC Robert Bruce serves as Chief, Space Division, U.S. Army Space and Missile Defense Command for the office of the Deputy Chief of Staff for Operations in Arlington, VA. He served as the Commander of Task Force 1-40th AR and on the Joint Staff and Strategic Command. He graduated from the first Space Operations Officer Qualifications course in Aug 01.

End Notes:

1. "Normalizing the Army's Use of Space with Seamless Integration", Vol 1, September 2001, Lieutenant General Joseph M. Cosumano, Jr., commander, USASMDC
2. "Military Information Technology", Vol 6, Issue 2, February 2002 Interview with General Ralph E. Eberhart, combatant commander NORAD, combatant commander U.S. Space Command, and commander Air Force Space Command by Executive Editor, JoAnn Sperber.
3. Derived from Space and Electronic Warfare Detachment (SEWD) Security Classification Guide, 30 April 2001.

JOINT FORCE ... from Page 9

IO efforts are: denying enemy access to high-resolution commercial imagery, and the electronic protection element of electronic warfare — disrupting their satellite communications networks by electronic attack. Space protection measures, both active and passive, touch many of the IO core and supporting capabilities. An example of a passive protection measure as it relates to IO operations security is satellite communications link encryption.

From the very basics mentioned, one can understand why it makes good sense to create a joint entity to plan, coordinate, and synchronize IO and Space operations in tandem, or in other words, employ a Space and IO Element (SIOE). The vote is still out as to how well the SIOE functions, but it's pretty clear to me that the SIOE, coupled with reach-back assets at U.S. Space Command, works.

I am also certain we will continue to debate how Space and IO should be coordinated, integrated and synchronized into the joint warfight. In accordance with

joint doctrine, the IO function remains embedded in the joint force J-3's range of activities. In addition, Joint Space doctrine will outline that a Joint Force commander has options. The language in JP 3-14 will stipulate that the commander should designate an authority to coordinate, integrate and synchronize Space operations for the theater/joint area of operations. It also states that the Joint Force Commander can retain this authority. In other words, he can use his staff to do the work and designate an officer (Space authority) to direct the effort. The second option is for the commander to delegate the task to a component. Based on lessons learned in Operation Enduring Freedom and the linkages between Space and IO joint doctrine and policy, I would conclude that the joint force is best served by performing both IO and Space coordination/ integration functions at the joint force level. In other words, the J-3 should be the center of activity for both, with the "Space authority" working for the J-3.

Certainly joint force components should be authorized to plan and execute their own Space operations and IO, but they should be coordinated, synchronized and integrated with joint activities.

So how do all the pieces and parts fit together? There may not be a clear answer yet, but the current trends are, and future policy and doctrine may direct, that IO and Space operations continue to merge. Given the current direction, joint force IO and Space experts should get used to working together.

Mark Goracke supports the U.S. Army Space and Missile Defense Command and Office of the Deputy Chief of Staff, G-3, HQDA, and the Strategy, Concepts, and Doctrine Division, in the Pentagon. He is the Army joint and multinational doctrine integrator for Information Operations, Space, and air and missile defense and also is the co-author of JP 3-26, Joint Doctrine for Homeland Security. He retired from the Army in 1998 after serving on the Army Staff as a strategist and policy analyst.