4-2006

Managing the Integration of Space and Information Operations

Daniel F. Gottrich

Michael R. Grimaila
Air Force Institute of Technology

Managing the Integration of Space and Information Operations

Maj Daniel F. Gottrich, USAF
Michael R. Grimaila, PhD, AFIT

We should not go to space unless it's the only way we can do a job, or can do it better, or it's cheaper. The global movement of information seems to be the one thing we can use space for that we have not learned how to do on earth.[1]

- Lt Gen Richard Henry, 1982

Because over twenty years has passed since the establishment of Space Command in 1982, most members of the military are now comfortable with the axiom that space is the fourth realm of warfare in addition to the traditional spheres of land, air, and sea. However, this transition was slow in coming. Even though the Cold War had seen operations brewing in space since the late 1950s, it took the establishment of a separate unified military command, the United States Space Command, or USSPACECOM (and, in 2001, a scathing Congressional report threatening to establish a separate space service), as well as years of joint space operations and wrangling over the creation of space doctrine, before space was accepted as a separate and distinct sphere of combat.

It is ironic, then, that a fifth dimension of conflict, the realm of information operations (IO), has been less universally accepted as a theater of offensive and defensive warfare, despite the fact that armed forces have sought, defended, attacked, and exploited information in battle for centuries. Information warfare is unfortunately tied to modern technology and computers, forgetting that the concept can be as simple as a wooden horse left as a gift outside a great fortified city.

However, military tacticians now understand and appreciate that the concept of information operations has been gradually getting more attention focused on it in doctrine and contemporary military operations. Inevitably in the 21st century the technological aspect of conducting information operations is going to be linked to two things: space and cyberspace. In this article, we will concentrate on the former, with the understanding that computers and the associated links, networks and nodes play a vital role in the command and control of operations in space. We will discuss the historical ties between space and information operations, the difficulty that we in the space community have had in grasping information operations as a viable separate construct, and we will review some of the Air Force's education efforts being applied to change that paradigm. Finally, we will propose solutions to ensure information operations continue to be an effective weapon in our military's arsenal.

History

> We've spent thirty-five or forty billion dollars on the space program. And if nothing else had come out of it except the knowledge we've gained from space photography it would be worth ten times what the whole program cost. Because tonight we know how many missiles the enemy has and, it turned out, our guesses were way off. We were doing things we didn't need to do. We were building things we didn't need to build. We were harboring fears we didn't need to harbor.[2]
>
> - President Lyndon Johnson, 1967

Similar to the first military uses of airplanes and balloons, the initial utility of satellites came from its surveillance capabilities. Space was the ultimate "high ground"—as every general from Patton to Napoleon to Caesar would tell you, knowing what is happening on the other side of that hill is paramount for situation awareness. The National Reconnaissance Office's recently declassified CORONA program was established in 1960 as the nation's first operational satellite photo reconnaissance project. Imagery intelligence is still a vital asset provided by optical satellite sensors today, though it is telling to see how far the technology has advanced in forty years.

Figure 1. NRO Figure 2. GeoEye

Figure 1. (left) First imagery taken by CORONA, Mys Shmidta Air Field, USSR, 1960. Figure 2. (right) Nellis AFB, Nevada, 2002.

Ever since the 1957 launch of Sputnik, when the United States realized that the Soviet Union could now launch a rocket capable of landing an object (a nuclear warhead?) anywhere on the globe, our military posture became based on information gathering and deterrence based on flexible response. As Lt Col James Lee wrote in *Counterspace Operations for Information Dominance,* "US military space systems were initially developed in a Cold War context and viewed as primarily strategic systems—supporting the Strategic Air Command, the intelligence community, and the National Command Authorities. Timely, accurate, and unambiguous strategic and tactical warning information from reconnaissance, surveillance, and communication satellites provided situation awareness of our perceived enemy and became integral to the deterrent power of the triad."[3]

In essence, Lee asserts that our military systems became almost a hidden fourth leg of the strategic nuclear triad. The strength of Soviet and American nuclear deterrence relied on the ability of satellites and their ground networks to collect, process, and disseminate information. The balance of information provided by these systems resulted in each of the belligerents having a

sufficient amount of timely warning of the other side's capabilities and actions. Lee continues, "Maintaining the balance in warning information prevented one side from achieving surprise and rendering the other side incapable of a nuclear retaliatory strike. In fact, the value of the information from space systems was viewed as essential for cold war stability, and many argued that space must remain a sanctuary to preserve stability."[4]

Ultimately, space's role in "standing toe to toe with the Ruskies" has been played out, with, some argue, President Reagan's threats to provide an anti-nuclear blanket of protection with his Strategic Defense Initiative bankrupting the Soviet coffers when they attempted to counter it. Space has more recently moved from this strategic role to the tactical missions of day-to-day combat support.

Operation DESERT STORM is mistakenly referred to as the "first space war," though no battles were fought from or through space. But the Gulf War saw the first combat use of Global Positioning System (GPS) satellites, used both by supporting General Norman Schwarzkopf's "left hook" through the featureless desert and through Joint Direct Attack Munitions, or "smart bombs." This war also highlighted the multiple uses of satellites in providing imagery, weather data, theater ballistic missile launch warning, and, especially, communications in remote areas with not a lot of land lines. More than 90 percent of communications intheater was provided via the Defense Satellite Communications System, an array of satellites orbiting 28,000 miles overhead.

The conflict also pointed out our asymmetric advantage in the space arena, however, and some of the benefits we enjoyed then, we could not realize today. For example, because of the multitude of commercial imaging satellites on the market, there is no way General Schwarzkopf's maneuver to the west and north around Kuwait would go undetected today. Our use of GPS technology compelled Saddam Hussein to purchase several GPS jamming devices prior to Operation IRAQI FREEDOM (though, fortunately, he and his military did not know how to employ them very effectively). Also, because of our reliance on satellites for communication, bandwidth was used to full capacity, sometimes forcing large files like imagery or Air Tasking Orders to be shipped by airplane rather than satellite links. Further, Operation DESERT STORM forced us to understand that our enemies do not rely on technology like we do, and we were still ineffective in shutting down all aspects of the Iraqi's ability to wage war. Several analysts suspect that after our forces destroyed Saddam Hussein's more advanced telecommunications systems (satellite, microwave, and cable systems), he continued to relay launch orders to Scud missile batteries via courier.[5]

As the last century closed, the cost of launching satellites started to decrease and the number of civil and foreign entities getting into the space business exploded. We had entered what many labeled "the Information Age." But in this case, the availability of information is a double-edged sword that is effectively whittling away at the advantage enjoyed by the United States as one of the historical few that has in the past controlled space system information.[6] The commercial application and exploitation of space information is another threat that must be a part of any military space professional education.

Organization and Education

> We need space professionals in all services and agencies…to exploit space effectively in the interests of national security. Development of a space cadre is one of our top agenda items for national security space programs in 2004.
>
> - Under Secretary of the Air Force Peter Teets
> Report to Congress, 12 March 2003

In 2001, Maj Daniel F. Gottrich was assigned to the USAF Space Operations School (SOPSC), a division in the Space Warfare Center on Schriever AFB, Colorado. Its mission was twofold: to develop space tactics, techniques, and procedures for warfighting doctrine and to educate space personnel (and members from other specialties who had signed up) about operational space systems. A career space officer who had just returned from an overseas tour in Turkey, he was tasked to develop a lesson for space doctrine, which he knew very little about, satellite communications, which he would have to brush up on, and something called IO. Major Gottrich had never heard of the term, so he was surprised to be assigned responsibility to teach a course on the topic to a room full of joint professionals.

To prepare, Major Gottrich attended an IO conference in February of 2002 in Las Cruces, New Mexico called "Phoenix Challenge" which brought together military, industry, and academic leaders to highlight the latest in IO technology, best practices, and literature. The over-arching message was how prevalent IO was in our society, and Major Gottrich was shocked that he had never heard of it during his military training. Too often we as a military equate IO with computers and consider it the bailiwick of communications experts. Indeed, Major Gottrich would often ask his class members why they thought he was teaching IO in a space operations class, and would inevitably receive the response: "because our satellites are controlled by computers."

The past few years have seen new strides in education, sparked by the creation of the Air Force Doctrine Center at Maxwell AFB, Alabama in 1997 (compare this date with Army's Training and Doctrine Command established in 1968). New space and IO doctrine has been created and updated several times in those eight years, and the lessons are trickling down to the units. "Air, space and information functions work best in an integrated and synergistic way," states a recent Doctrine Watch lecture emailed to every Operations Support Squadron for further dissemination. "Integrating effects-based information operations functions with the other air and space power functions is a crucial part of the Air Force's operational art."[7]

Doctrine became a very important part of SOPSC lectures, particularly tying space and information operations together. The course had already covered space doctrine, and the four core space mission areas:

- Space Control – ensures freedom of action in space for the US and its allies and may deny an adversary freedom of action
- Space Force Support – consists of operations that deploy, augment, sustain, and replenish space forces, including the configuration of command and control structures for space operations and all launch operations
- Space Force Application – would consist of attacks against terrestrial-based targets carried out by military weapons

operating in or through space

- Space Force Enhancement – provides navigation, communications, intelligence, surveillance, reconnaissance (ISR), ballistic missile warning, and environmental sensing (weather)

The SOPSC lesson would demonstrate that the Space Force Enhancement mission had the greatest impact on IO by providing the Information-In-Warfare (IIW) capabilities that enable the commanders to have a full picture of the battlespace in order to make the best decisions. It would also stress how space systems would enable these elements, specifically the IIW capabilities, through satellite support. ISR functions are supported by satellite imaging capabilities, weather services rely on the Defense Meteorological Support Program satellites and the precision, navigation and positioning is provided by GPS.[8]

Furthermore, Air Force Doctrine Document (AFDD) 2-2: Space Operations, states: Space, air, and information platforms are mutually supporting and supported throughout the spectrum of conflict:

- Space assets are unable to contribute if their uplinks and downlinks are interrupted or their ground control and receiving stations are disabled
- Information superiority helps ensure the freedom from attack for control and mission links that tie space providers to ground, air, or sea-based users
- Space, air, and information superiority are mutually supporting objectives. It is extremely difficult to maintain one without the others and the value of one is greatly enhanced when accompanied by the others[9]

Space and IO capabilities are intertwined and almost have a symbiotic relationship. Information is the lifeblood of IO and space plays a major role in providing the platforms for this info to flow. But space operations also enable some offensive and defensive IO tactics as well. Space assets can be used for public affairs, psychological operations, and operational security (OPSEC). Maj Robert Newberry wrote in *Space Doctrine for the Twenty-first Century* that OPSEC has been a prominent feature of our space forces, and the trick is to balance usability with classification issues. He writes, "A comprehensive OPSEC plan can help prevent attacks on US space forces by making it more difficult for an adversary to launch an attack." Newberry also asserts, "OPSEC can create uncertainty as to the true nature of US space operations and deny the adversary needed targeting data. Although the benefit to some space systems may be negligible, OPSEC can be particularly effective in protecting high-value assets."[10] Major Newberry offers the following table comparing different levels of OPSEC available within space operations and their effects on the enemy's ability to wage war.

Operational Art Element	Adversary's Uncertainty
1. Encryption	I don't know what they are doing.
2. Observation Management	Can I believe what I see?
3. Training	They seem to anticipate my moves.
4. Interoperability	What are the connections?
5. Data Fusion	Can I have a meaningful effect?
6. Launch on Demand	Should I expect more?

Robert D. Newberry

Table 1. Operational Art Element vs. Adversary's Uncertainty.

We can also use space assets to defend our actions or counter enemy propaganda. For instance, in 1998, Saddam Hussein decided to allow the United Nations weapons inspectors back into his country, but informed them that they would not be able to inspect "palace grounds." We were able to use satellites as part of a counter-information campaign to show the world how cooperative the Iraqi leader was really being.

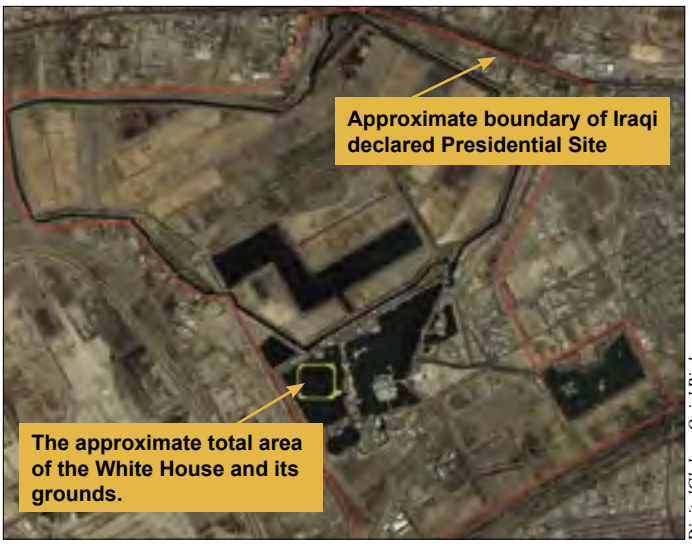

Figure 3. Radwaniyah Presidential Site.

However, satellite technology is not perfect. During Operation ALLIED FORCE, the Serbs were still able to fool some of our most skilled observers with rubber or wooden mock-ups of cannons or aircraft. In one instance, they even hung lanterns in the "exhaust" to make it appear on infra-red sensors to have a heat signature.

About the same time as Major Gottrich's arrival to the SOPSC, Air Force Space Command (AFSPC) was also reeling from a scathing Congressional report released in January of 2001. The *Report of the Commission to Assess United States National Security Space Management and Organization,*[11] also known as the "Rumsfeld Report" since Donald Rumsfeld was the Chairman of the Commission (before recusing himself to become Secretary of Defense) had given the services a failing grade in developing space professionals, in particular decrying the Air Force practice of bringing in pilots to command space units for short periods in a vain attempt to show breadth in leadership. Assignments were poorly managed, and continuing education after entry level (as a young airman or second lieutenant) was non-existent. The report recommended that the Air Force be given one last shot to transform itself before being forced to carve off its space operations into a separate service or a subordinate but separate entity like the Navy/Marine Corps relationship.

Early in 2003, the SOPSC took the lead for developing and executing the first four-week "Space 200" course, geared towards mid-career officers, noncommissioned officers, and civilians at the 8- to 10-year point. The course, using material taken from some existing SOPSC courses and augmented with additional material in the fields of acquisition, engineering, and nuclear operations, had a stronger emphasis on warfighter integration of space power in the joint fight. The course also consisted of increased technical

content, to include a design exercise in which student groups designed a satellite program to fulfill a Department of Defense (DoD) requirement, then considered its application in a capstone wargame exercise at the end of the course.

SOPSC also initiated the development of Advanced Space Training (AST) courses in order to produce system experts that will return to unit or wing tactics shops to be instructors. Currently, space officers are sent to the Weapons School at Nellis AFB, Nevada where they become generalists in all space systems and learn integration of air, space, and information operations. These graduates are sent to Major Commands (MAJCOMs), Unified Commands, and theater Air and Space Operations Centers (AOCs). The vision for AST is to mirror the air side of Weapons School, wherein pilots are immersed in their particular weapons system and graduate as experts on that platform. The SOPSC's first AST course, Navigation Operations, took ten officers and NCOs through an intensive, 12-week curriculum where they became experts in GPS, navigation tactics, the command and control structure, concepts of operation, acquisition, and weapon system applications.

In the spring of 2005, the Air Warfare Center and Space Warfare Center were administratively merged into the US Air Force Warfare Center in order to "better manage air, space, and information operations combat capabilities to support missions worldwide."[12] There is talk of including the Information Warfare Center (another potential assignment for space operations personnel), currently located at Lackland AFB, Texas, in future reorganization plans. In addition, more and more space professionals are deploying overseas, and many of them are being attached to Information Warfare (IW) Flights within an AOC.

Organizationally, space command has been tied to IO since the late 1990s. In response to a number of attacks on government computer networks, the Office of the Secretary of Defense ordered the Defense Information Systems Agency to establish the Joint Task Force-Computer Network Defense (JTF-CND), which was transferred to Colorado Springs' then Space Command (USSPACECOM) in 1999. As the senior computer emergency response team in the DoD, the JTF-CND was the responsible cell for all CND issues, including recommending changes to the information condition status when the situation required.[13] In 2001, it was renamed the Joint Task Force-Computer Network Operations to reflect its growth and mission, and continued to operate under the IO portion of the USSPACECOM mission until 2003, when US Northern Command was set up to coordinate military homeland security efforts and USSPACECOM was absorbed into US Strategic Command (USSTRATCOM), with the IO tasking going to USSTRATCOM at Offutt AFB in Omaha, Nebraska.[14]

Securing Information In Space

> The [DoD] must enhance the capability and survivability of its space systems. Activities conducted in space are critical to national security and the economic well-being of the nation. Both friends and potential adversaries will become more dependent on space systems for communications, situational awareness, positioning, navigation, and timing. In addition to exploiting space for their own purposes, future adversaries will likely also seek to deny US forces unimpeded access to and the ability to operate through and from space. US forces must ensure space control and thereby guarantee US freedom of action in space in time of conflict.[15]
>
> - Director, Force Transformation Office, 2003

Our dependence on space makes satellites not only a valuable tool, but prime targets. Ideally, all satellites should be hardened from attack; commercial investors, however, are reluctant to spend the money to protect their satellites.[16] High-altitude nuclear bursts and the resultant electromagnetic pulse (EMP) might render most allied space assets inert. EMP could burn out the circuitry of most allied radio systems, computers, transistors, and power grids in the region of combat, rendering many of the allies' high-tech assets harmless.[17]

On the flip side, because of cost and the physics involved, it is unlikely that many countries are attempting to develop anti-satellite weapons.[18] It is more likely that an adversary will try to exploit the information-gathering apparatus on the ground, either by physical destruction, jamming, or other means of denial. Jamming is very similar to a computer hacker's denial-of-service attack, essentially transmitting a high-power, bogus electronic signal that causes the bit error rate in the satellite's uplink or downlink signals to increase, resulting in the satellite or ground station receiver losing lock.[19] GPS receivers, for example, are notoriously vulnerable to jamming because of the low power in the navigation message. Power of just a few watts can jam the access code at a distance of 10-20 kilometers.[20] Indeed, the signal coming off a GPS satellite, orbiting at 12,500 miles, is the equivalent of a 25 watt light bulb.

Attacking the link segment by spoofing involves taking over the space system by appearing as an authorized user, such as establishing a command link with an enemy satellite and sending anomalous commands to degrade its performance. Spoofing is one of the most discrete and deniable non-lethal methods available for offensive counterspace operations.[21] These ground attacks will appear like a series of nuisance events, or computer vandalism. But how do we distinguish a computer "glitch" from an information attack that has disrupted our satellite command and control network, such as the May 1998 failure of PanAmSat's Galaxy 4 communications satellite? The satellite's computer crashed unexpectedly, and the spacecraft temporarily went out of control. Somewhere between 80 and 90 percent of America's 45 million pagers went dead, and National Public Radio lost its feed to local stations.[22]

Offensively, information dominance can be attained "by collapsing an adversary's command and control infrastructure through offensive operations, such as the disruption of critical communication links; or by denying access to reconnaissance and surveillance information, such as blinding optical sensors with ground-based lasers. Defensively, measures such as hardening, frequency hopping, and encryption further ensure information dominance by helping to ensure friendly forces have uninhibited access to communications, surveillance and reconnaissance information provided by space systems."[23] It is these offensive and defensive IO measures that the US needs to focus training and funding toward in the coming decades in order to thwart the up-and-coming challenges of a technologically savvy adversary such as China.

The US military traditionally uses spacepower assets for two primary purposes: (1) to improve the situation awareness of its

forces; and (2) as a means of command, control, and communications. Lieutenant Colonel Lee writes, "We essentially exploit space power assets as a permanent informational infrastructure that is globally available to friendly forces. This allows friendly forces to operate on interior lines of information around the globe."[24] But it also allows our enemies access to this same information. Indian President A.P.J. Abdul Kalam recently expressed concern over Google Earth's free satellite imagery software, which provides clear pictures of some of India's military and government facilities, claiming the information could be used by terrorists to plan attacks.[25]

"No claim is made that US military forces are neutered without space support. Terrestrial forces can still fight without space support," writes Maj M.V. Smith. "However, the absence of space support will inarguably increase the fog, friction, and overall costs of military operations."[26]

Recommendations for the Future

> The Air Force must begin to think and bring forward the technologies necessary for space control. Capabilities to defend our own space based resources and to disrupt, degrade, deny, or destroy that of the enemy will be needed sooner or later in the 21st century. The technologies needed to protect our space resources from enemies include high thrust, high specific impulse electric propulsion, large constellations of low cost satellites with distributed functionality or networking across the system, and autonomous guidance and navigation.[27] - USAF Scientific Advisory Board, 1995

Trying to predict our technological future is futile. In 1982, the contemporary feeling from senior Defense Department leaders was that space-based lasers, capable of global ballistic missile defense from ICBM launches from the Soviet Union, would be in orbit in "ten or eleven years."[28] It is fair to conclude that we are easily the world's best military force, though our dominance may not last forever, given the declining costs and spread of technology.[29] But speculation on our specific offensive and defensive capabilities is something for the scientific journals, though the research labs, battle labs, and warfare centers are doing remarkable research.

> The United States has fielded laser illuminators that use semiconductor laser arrays to aid night vision devices. Projecting a laser beam over a large area on the earth's surface would help low-light imaging systems to find targets. A space-based battlefield illuminator would generate beams from satellites in low-earth orbit and direct them to the target. This technology would allow military forces to acquire targets with low-light imaging systems, insert and remove special operations teams under low light conditions, and increase the security of high-value facilities at night. Because the beam is eye-safe, the illuminator could be used for psychological operations in which US observers search covertly for enemy units.[30]

Fascinating reading, but it doesn't help us prepare the troops for the type of combat we will start to see in the next thirty years, in whatever form it appears. Author Jeffrey Barnett says it best, "Information will dominate future war. Wars will be won by the side that enjoys and can exploit:

- cheap information while making information expensive for its opponent
- accurate information within its own organization while providing or inserting inaccurate data in its opponent's system
- near-real-time information while delaying its opponent's information loop
- massive amounts of data while restricting data available to its opponent; and
- pertinent information while filtering out unnecessary data."[31]

It does not matter who has the most toys, Barnett implies. "Tactical effectiveness … depends on the control systems over the war theater and efficiency in utilizing information from the theater."[32]

Information operations is a skill that must be taught early and properly managed throughout a career, just as AFSPC has tried to turn around the management of space professional education. To that end, it could use a senior-level champion, as proposed in the Space Commission report, which stated that an Under Secretary of Defense for Space, Intelligence and Information should be established to, among other things, "oversee the Department's research and development, acquisition, launch and operation of its space, intelligence and information assets."[33] Unfortunately, in May of 2001, Secretary of Defense Rumsfeld reported that he had instead recommended that the staff "review the responsibilities and functions of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence…" to this end.[34] This is the wrong focus; a cop-out. This again comfortably equates information with technology and allows the management of information operations to be swallowed up by a technocrat.

A second recommendation is to revamp information operations doctrine. As of December 2005, Joint Publication 3-13: *Information Operations,* has not been updated in over seven years.[35] (This is still better than the twelve years it took for JP 3-14, Space Doctrine, to get published initially.) We believe that this is woefully inadequate. AFDD 2-5, *Information Operations,* has been updated twice since 2002. If the military is going to continue to use doctrine as a repository for officially sanctioned beliefs, warfighting principles, and terminology that describes and guides the proper use of air and space forces in military operations, it must remain current, fluid, and substantive. It is appalling that Joint IO doctrine has been allowed to languish for nearly a decade.[36]

Third, the concept of *Information Control* should be adopted within IO doctrine. This would emphasize the importance of capabilities to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. In space doctrine, space control is the overall realm of responsibility in which space superiority is gained and maintained to assure friendly forces can use the space environment while denying its use to the enemy. To accomplish this, space forces must survey space, protect the ability to use space, prevent adversaries from exploiting US or allied space services, and negate the ability of adversaries to exploit their space forces. In the 21st century, air and space superiority is unfortunately almost immediately assumed before the first shot is fired. Implementing the overall situation awareness of the IO battlespace, and comprehending the offensive and defensive requirements necessary to sustain an "information control" mission would help solidify information as the fifth realm of warfare.

Finally, IO has become so important a concept in our military that we should start to train IO specialists, that is, create a separate

Air Force Specialty Code for information operations officers and enlisted troops, so that they can become IO experts. Currently, we train experts in air operations and space operations, in weather, in intelligence, in public affairs, in communications. We then assume that each of them knows enough about information operations that any one of them could fill a slot requiring IO experience. Until we begin to groom a cadre of IO professionals, and start to build a twenty-year arsenal of individuals performing the IO mission day in and day out, we will be forced to re-invent the wheel at every level each time a new person rotates into an IO assignment.

Conclusion

There is nothing we do in space that is not information operations.[36] - Maj Gen Thomas Goslin, 2001

In 2003, the Director of Force Transformation, Office of the Secretary of Defense, wrote that the DoD "will treat information operations, intelligence, and space assets not simply as enablers of current US forces but rather as core capabilities of future forces."[37] Therefore, information operations doctrine, training, and career specialization must continue to evolve in the 21st century, while simultaneiously strengthening its integration with space operations. As commander of the Space Warfare Center, Maj Gen Goslin once said, "Today, more than anything, space provides information. And information today is a show-stopper."[38]

Notes:

[1] Colin S. Gray, *American Military Space Policy: Information Systems, Weapon Systems and Arms Control* (Cambridge, MA: Abt Books, 1982), 37.

[2] William E. Burrows, *Deep Black: Space Espionage and National Security* (New York: Random House, 1986), vii.

[3] Lt Col James G. Lee, *Counterspace Operations for Information Dominance* (Maxwell Air Force Base, AL: Air University Press, 1994), 1-2.

[4] Ibid.

[5] Maj YuLin G. Whitehead, *Information as a Weapon: Reality versus Promises* (Maxwell Air Force Base, AL: Air University Press, 1999), 30.

[6] Leigh Armistead, ed., *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington: Brassey's, Inc., 2004), 119.

[7] Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, Air Force Doctrine Center, 11 January 2005.

[8] *Information Operations,* USAF Space Operations School, Space 200 Lesson Plan (March 2004).

[9] AFDD 2-2, *Space Operations*, AFD Center, 27 November 2001.

[10] Robert D. Newberry, *Space Doctrine for the Twenty-first Century,* (Maxwell Air Force Base, AL: Air University Press, 1998), 32-33.

[11] *Report of the Commission to Assess United States National Security Space Management and Organization,* Space Commission, Pursuant to Public Law 106-65, 11 January 2001.

[12] Lt Gen W.M. Fraser, "Space, Air Warfare Centers Integrate Capabilities," *Defense AT&L*, September-October 2005, 44.

[13] Armistead, *Information Operations,* 33.

[14] Ibid., 33-34.

[15] Director, Force Transformation, Office of the Secretary of Defense. *Military Transformation: A Strategic Approach* (Washington, 2003), 19.

[16] M.V. Smith, *Ten Propositions Regarding Spacepower* (Maxwell Air Force Base, AL: Air University Press, 2002), 100.

[17] Lawrence E. Grinter and Barry R. Schneider, eds., "On Twenty-first Century Warfare," in *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell Air Force Base, AL: Air University, 1998), 269.

[18] Scientific Advisory Board, US Air Force, "New World Vistas: Air & Space Powers for the 21st century," in *The DTIC Review Future Directions: Preparing for the 21st Century* 2, no. 2 (1996), ed., Christian M. Cupp, 46.

[19] Lee, *Counterspace Operations,* 32.

[20] Scientific Advisory Board, "New World Vistas," 46.

[21] Lee, *Counterspace Operations,* 32.

[22] Bruce Berkowitz, *The New Face of War: How War will be Fought in the 21st Century* (New York: The Free Press, 2003), 164-165.

[23] Lee, *Counterspace Operations,* 4.

[24] Smith, *Ten Propositions Regarding Spacepower,* 68.

[25] Associated Press. "India: Google Maps Too Graphic." *Wired News*, 3 December 2005, http://www.wired.com/news/technology/0,1282,6923,00.html?tw=wn_story_related.

[26] Smith, *Ten Propositions Regarding Spacepower,* 68-69.

[27] Scientific Advisory Board, "New World Vistas," 61.

[28] Gray, *American Military Space Policy,* 2.

[29] Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington: Brookings Institution Press, 2000), 17.

[30] William C. Martel ed., *The Technological Arsenal: Emerging Defense Capabilities* (Washington: Smithsonian Institution Press, 2001), 10.

[31] Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, AL: Air University Press, 1996), 2.

[32] Ibid.

[33] Smith, *Ten Propositions Regarding Spacepower,* 122.

[34] Department of Defense, "DOD Press Release on Rumsfeld Space Initiative," news release, 8 May 2001, http://www.space.gov/Articles/Rumsfeld1.asp (accessed 22 February 2006).

[35] Joint Publication 3-13, *Information Operations,* Department of Defense, Washington: GPO, 9 October 1998.

[36] Maj Gen Thomas Goslin, USSPACECOM/J3, Warfighter's Space Conference, 31 January 2001.

[37] Director, Force Transformation, "Military Transformation: A Strategic Approach" (Office of the Secretary of Defense, 2003): 19.

[38] Maj Gen Thomas Goslin, Commander's Call, Schriever AFB, Colorado, February 2002.

Maj Daniel F. Gottrich (BGS, Indiana University; MA, University of Colorado at Colorado Springs), is currently completing Intermediate Developmental Education in-residence at the AF Institute of Technology, Wright-Patterson AFB, Ohio. In previous assignments, he served on operational tours in the 4th Space Operations Squadron (50th Space Wing), 740th Missile Squadron (91st Space Wing), and 39th Wing (Incirlik AB, Turkey). He was also an instructor and Vice Dean of the USAF Space Operations School (Space Warfare Center). He has staff experience as Chief of Defense Integration for the QDR Joint Actions Directorate, Deputy Chief of Staff for Plans and Programs, HQ USAF. Major Gottrich is a distinguished graduate of Squadron Officer School.

Dr. Michael R. Grimaila (BS, MS, PhD, Texas A&M University; CISSP, CISM, GSEC) is currently an Assistant Professor in the Systems and Engineering Management department and a member of the Center for Information Security Education and Research at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. Dr. Grimaila serves as Editor of the Journal of Information Assurance, Security, and Protection (JIASP), Editorial Advisory Board member of the Information System Security Association (ISSA), and is a member of the International Systems Security Engineering Association (ISSEA) Metrics Working Group. He also holds memberships in the ACM, IEEE, IRMA, ISACA, ISC2, ISSA, ISSEA, and the SANS Institute.