Navstar global positioning system.

Boeing

Globalizing **Space Security**

By SIMON P. WORDEN *and* JOAN JOHNSON-FREESE

The Nation is losing the information war against global terrorism. Many audiences abroad regard the United States as the aggressor despite the unprovoked attacks visited on New York and Washington in September 2001. Moreover, most of the Islamic world is growing increasingly hostile to Washington and its agenda. Even traditional allies and friends have responded negatively to the perceived American intent of going it alone. One key factor is the widening gap between U.S. and foreign military capabilities, which is largely attributable to superior and more integrated use of global information, in particular space-derived information.

The United States has shown little inclination to work with allies to integrate the military uses of space in multilateral planning and operations. The well-financed European effort to build an independent space-based global

Brigadier General Simon P. Worden, USAF, is director of development and transformation in the Space and Missile Systems Center at Air Force Space Command and Joan Johnson-Freese chairs the National Security Decision Making Department at the Naval War College.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2002 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Globalizing Space Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 Fifth Avenue SW Bg 64 Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

Network system supervisors, Lions Wrath.

U.S. Air Force (Karen F. Silcott)

navigation system (Galileo) is a clear reaction to U.S. intentions regarding the global positioning system (GPS). Space and information can be forces of integration rather than the causes of fragmentation in global security. They can present security opportunities. Internationally, this debate is especially important given the U.S. commitment to missile defense and military space programs and resulting perceptions abroad that the Pentagon is working to acquire sword and shield capabilities in space.

Globalization

If globalization is not the dominant trend of the 21st century, it will only be neglected at great peril. As an integrative force it creates networks that draw individuals, organizations, and nations closer together while simultaneously driving them toward diminishing units of identification. The major difference between globalization today and in the past is the role of information technology, which increases both the influence of networks and speed of change. Moreover, technology democratizes information, providing access to previously sequestered material. Transparency becomes another dual-edged sword demanding the attention of security planning.

Few factors dominate the security environment like globalization. But the term has become a buzzword that ultimately adds little value to discussions. Immediately following the collapse of the Soviet Union and renaissance in Eastern Europe, globalism—or globalization—had essentially an economic connotation, signifying a rush to create an integrated market-oriented system. While the network had developed earlier, between 1989 and 1991 the last major holdouts not only became true believers in market economies but devout capitalists. Before long, however, the downside of economic integration began to appear.

the need to include security in the globalization equation has become evident

Though initially regarded as a positive force that would level the economic playing field and dissolve national barriers, globalization sometimes actually widened the gap. Moreover, posturing for success in a globalized world required obeisance to international institutions and norms, which were often viewed as U.S.-sponsored and even neocolonialist, especially when anticipated benefits went unrealized. And when successful, costs to national culture and sovereignty were often high. Globalization intensified a fragmenting nationalist counterreaction.

The need to include security in the globalization equation has become evident. Nations are no longer the only actors involved in security. In the global war on terrorism, the United States is focused on al Qaeda, a group of individuals. Globalization gives rise to economic, cultural, political, and security considerations, both positive and negative. The most useful definition of globalization may be the simplest: the impact of events beyond national borders and often regions.[1] With the primary difference in globalization today being information technology, rapid change becomes critical.

Many terrorists do not fight for recognition or political goals. They are instead apocalyptic or nihilistic, negating the premises of deterrence. In addition, rogue states often seek to perpetuate regimes rather than serve national interests, ignoring the balance of power premise. Such actors are technologically astute and have been empowered by previously unavailable information through the Internet and other advanced communications capabilities, particularly those relying on space assets. Democratization of information provides unimaginable opportunities for linkages, but not without becoming a transnational threat. An unprecedented electronic attack in October 2002 temporarily crippled nine of thirteen worldwide servers critical to the Internet, serving notice that cyberterrorism is real and that cooperation to thwart it is both necessary and possible. The attack was halted in an hour through cooperation among root server operators and authorities.

Globalization can become a complementary factor in security planning. Shared interests in maintaining the Internet, for example, have created a large unofficial and official coalition of parties for which uninterrupted access is vital. The United States serves as the link among all cyberspace-vested interests and other technically based domains, including space.

Satellite operations center, Schriever Air Force Base.

U.S. Air Force (Lono Collars)

Protecting space assets can become an international rather than an exclusively U.S. interest. With its overwhelming capabilities and advantages for force enhancement, America is viewed with mixed feelings by many countries. Potential enemies are keenly aware that reliance on space assets makes the Nation vulnerable to interruption. Global positioning provides an interesting example in this regard. With airlines dependent on space capabilities for navigation, and diversified civilian utilization expanding exponentially, the system serves as a global utility that warrants international protection. Few countries besides the United States, however, have the capabilities to defend it.

Integration

Nations must cooperate more actively to thwart the dark side of globalization, and they must work not only with each other but also with the private sector. Multilateralism is the only option, but network-centric concepts and plug-and-play assets are more elusive.

The gap in space-based assets among nations presents special problems: interoperability, vulnerability, and disparities in military capabilities. The Japanese investment of some $2 billion in an information gathering satellite system, which provides one-meter resolution images (the same as commercial sources), demonstrates independent decisionmaking. Distrust among allies has reached such a level that Europeans are working to initiate at least one Galileo signal that could overlay and interfere with U.S. military signals. Finally, vulnerability also means that America has the greatest interest in protecting space assets, leading to further resentment abroad over the implied movement toward weaponizing space.

A new approach to protecting space assets seems warranted. Ideally it would contribute to multilateralism and increased interoperability. Two critical factors in exacerbating the gap between the United States and other nations have been technology transfer concerns and economics. With advances in microsat technology and resulting reduced costs, there may be opportunities to work together in space, a win-win formula for both America and its partners.

Emerging Capabilities

The Internet became the most significant global utility in the last decade. It gave rise to two issues: the unclassified (versus classified defense only) system, which is an indispensable part of national security operations, and the increasing potential of wireless accesses.

While U.S.-only secure Internet remains essential to military operations, its very classified nature and nonaccessibility to allies have meant increasing military use of the unclassified Internet. Critical functions such as logistics are conducted via this link, which is used for virtually all allied coordination. DOD Internet concerns have grown. A joint task force was organized in 1999 for computer network defense under U.S. Space Command. In 2002 this organization was redesignated Computer Network Operations (JTF/CNO), given added responsibility for network attack functions, and transferred to U.S. Strategic Command.

The primary function of JTF/CNO is protecting Internet use within DOD. As threats such as computer worms and viruses increase, it has instituted increasingly vigorous defenses. But the organization has two drawbacks. First, though it interacts directly with the National Infrastructure Protection Center, it is not charged with protecting non-DOD channels and systems. Moreover, many of its methods would be considered intrusive or totalitarian to commercial or public Internet systems. Second, JTF/CNO is not involved with coalition-wide use of or defense of the Internet. Meanwhile, global terrorists have increasingly turned to the Internet as the command and control and recruiting tool of choice. Organizations such as al Qaeda have used it to circumvent efforts to crush them. Moreover, Web sites that recruit terrorists have remained online by hopping from nation to nation and provider to provider.

One major development in expanded Internet access that promises both great opportunities for information operations and potential pitfalls is the growth of systems linking to the Internet via wireless connections such as cellular telephones or other broadcast signals. Many of these access links run through or totally rely on space-provided communications.

Global time standards. Most experts regard global positioning as a central global utility. However, its value as a global time standard rather than as a navigation aid is more important. It is virtually the only global source for accurate timing. An error broadcast over one satellite in 1996 for a few seconds caused massive cell phone outages across the eastern United States. Multiplexed systems such as telephones require accurate timing to calculate exactly when to send signals in a given direction and on which channel. The precision of the timing signals at send-and-receive locations contributes to the efficient use of communications channels. Timing errors at one site can disrupt an entire well-oiled communications system.

employing space assets to gather information in denied areas was an important feature of the Cold War

With increasing bandwidth demand on existing channels, improvements in efficiency have great economic payoffs. Future global positioning systems with prospective improvements in timing accuracy can add one to two orders of magnitude and can significantly increase economic returns. Not just cellular communications systems but the Internet itself relies on accurate timing. If accuracy increases two orders of magnitude to a tenth of a nanosecond (one ten billionth of a second), a radically different and more efficient Internet becomes possible, with the entire world linked to a single massive computational web.

The increased dependence on accurate timing also means a greater economic vulnerability to outages—accidental or deliberate. For example, the Leonid meteor storm that occurs every 33 years last peaked in 1999. It had the potential to knock out much of the global positioning constellation, which would have caused a massive disruption of life on Earth.

Dependence on global positioning for precision guided munitions is a decisive advantage. Consequently, special new military-only signals are being deployed on satellites that are relatively resistant to conventional interference. However, because the Armed Forces rely heavily on global positioning signals, the United States has resisted involving foreign actors—even its most trusted allies.

Global communications. The original global utility was satellite-based communications. While much high bandwidth international communication travels via land and undersea optical fiber cables, satellite communications systems are significant for two applications. The first is bandwidth on demand for short-term needs and the second is free-space communications where little or no infrastructure exists. Such communications are particularly important operationally.

It is significant that new global communications systems are direct broadcast radio systems. The Asian and African service of Worldspace has great potential as an influential tool in the global war on terrorism. Beyond the control of local authorities and also difficult to jam, the distribution of Worldspace direct broadcast receivers to provide balanced news and globally-oriented distance learning programs has utility in combating terrorism in remote areas.

But these commercial space systems are vulnerable. The accidental loss in 1998 of a single pager satellite halted much of North American electronic commerce for a few days because not only were pagers inoperable, but also services such as credit card payment systems at service stations. Moreover, the Armed Forces rely on commercial systems for long-distance communications, which could encourage an enemy to attempt denial.

Situational awareness. Employing space assets to gather information in denied areas was an important feature of the Cold War. With technological advancements, a growing commercial

Tactical communications shelter.

U.S. Army (Claude Stallings)

constellation of optical imaging satellites has been developed. These systems can now obtain sub-meter resolution imagery comparable to aircraft and overhead imagery formally monopolized by the superpowers. DOD is the biggest consumer of these capabilities. Conversely, the government is worried about enemy access to such data and has utilized multiple approaches to avoid unwanted dispersion, from legal restrictions and shutter control to buying up all available imagery. However, as foreign suppliers proliferate, particularly in the all-weather, day/night synthetic aperture radar regime, these maneuvers will likely be ineffective in denying information to an enemy.

Air Force space surveillance network and contributing sensors monitor and obtain virtually all Earth orbit event data. This information is vital in protecting assets and determining the status of foreign space systems in distress. Other nations, notably Canada, France, and the United Kingdom, are developing space tracking systems. Space-based sensors are needed to acquire optimal space situation awareness. Some users, such as Canada, are planning surveillance systems.

Situational awareness includes detecting and tracking hazardous near-Earth natural objects such as asteroids. Currently, the most productive resource is a refitted military space surveillance sensor. Systems capable of searching for and detecting asteroids can also be used to locate Earth-orbiting satellites.

Some thirty objects approximately a few meters in diameter strike the Earth's atmosphere annually and release energy comparable to nuclear blasts of several kilotons. As nuclear weapons spread there is concern that nations such as India and Pakistan, both nuclear armed and lacking sophisticated sensors to distinguish between nuclear blasts and asteroid impacts, might mistake a natural explosion for an attack, triggering a nuclear exchange. The United States is the only nation that possesses sophisticated space-based sensors able to rapidly distinguish natural from man-made explosions in the upper atmosphere. There are no provisions for sharing such data.

Access to space. Getting capable systems into space has been expensive until recently. Only well-funded government efforts could field launch systems because each launch costs tens of millions of dollars. Corresponding satellite costs for deployed systems ran to hundreds of millions of dollars. With such large investments there has been little incentive to enter into cooperative ventures.

Access to space is growing with the emergence of so-called microsatellites. These systems weigh only tens to several hundred kilograms and usually cost under $10 million to develop and build. Most can ride as auxiliary payloads on large primary launches, adding as little as $1 million per launch. The most impressive development of this technology has been achieved by the Space Centre at the University of Surrey. This facility has built and launched over 25 microsats performing a range of scientific missions, including Earth surveillance, and it markets affordable capabilities to nations such as Algeria, Chile, Egypt, Malaysia, Nigeria, and Taiwan.

One growing concern about microsat technology is its potential to interfere with the use of space by other nations. China has worked closely with the University of Surrey and has also developed its own capability. Beijing has suggested that it might use this technology to deny the United States from using space in a conflict. Other nations could develop similar capabilities. And microsats are difficult to detect and track because of their size. Any enemy which possesses them could mount an effective surprise denial of essential commercial and military space resources.

Space Threats

The political dimension is a significant concern to space professionals. National security space efforts were highly classified throughout the Cold War. Near the end of the Soviet Union, the Strategic Defense Initiative, including the proposed use of space-based missile defenses, caused controversy over the military use of space, particularly on weapons. Many members of the national security space community

it may be time to use space cooperation as a key element in future influence activities

realize the advantages of space for security purposes yet are fearful of public outcry. Extensive exchanges with foreign partners about routine use of space to support security operations would be inherently less classified and thus relatively open to public discussion. Foreign cooperation with the Armed Forces is likely to generate even more opposition since people abroad are more antimilitary on space issues than those at home.

The United States enjoys a virtual monopoly in the use of space for military operations and almost total dominance over Internet use. This offers an easy means to reconfigure space and information systems. Since capabilities such as global positioning have a large economic impact, international discussion of what is actually an American military system would only slow decisions and constrain flexibility, another reason the military has avoided cooperative space efforts.

Preventing hostile use of U.S. space systems is one of the four pillars in the emerging field of space control, along with space situational awareness, protection of friendly assets, and denial of enemy use of their own space systems. It is generally thought to be unwise to assist other nations or groups in this effort. With experience in the use of space systems proliferating, the difficulty of preventing hostile exploitation grows—an added incentive to eschew international cooperation on use of space data for security purposes.

Another reason to avoid space and cyber systems cooperation is the economic argument. The United States has seen its competitiveness erode across the aerospace industry. International cooperation invariably leads to foreign technology development that in turn can lead to commercial competition.

Finally, there is the issue of secrecy. The military seeks to preserve its advantage in space through strict classification procedures and sharing information on a need-to-know basis. Because space information is critical in denied areas, it is among the most secret of U.S. capabilities. The National Reconnaissance Office, which safeguards space intelligence data, remains among the most powerful agencies for maintaining classification on space capabilities. Similarly, the organization with responsibility for much information intelligence, the National Security Agency, strictly controls emerging cyber capabilities.

Opportunities

Whereas much of the attention in the past on the military use of space has been placed on supporting military operations, the situation is changing rapidly. With the advent of U.S. Strategic Command and its focus on global missions, perspectives on space and information systems must also change. Influence in military affairs was often gained through high-technology cooperation, which involved high-performance aircraft. Space cooperation was generally not considered within most partnerships because of both high costs and security sensitivities. That could change with the proliferation of low-cost microsatellites. Recent thinking suggests that it may be time to use space cooperation as a key element in future U.S. Government influence activities.[2]

One area of potential cooperation is protecting global utilities because they are critical to the international economy. The Internet is a good place to start. Threats to it abound and global calls for action grow with each new worm or virus. As noted before, DOD has developed a reasonable regime for protecting its cyber systems. But to safeguard the American economy, the measures needed are neither available nor generally accepted because of their intrusiveness. Almost no regimes exist to protect the Internet, though there has been consideration of such arrangements. The use of cyberspace by terrorists conjures up wider concerns. It may be feasible to consider cooperation in Internet security as a bilateral and multilateral issue rather than a law enforcement matter. That could circumvent subsequent difficulties by establishing a genuinely global regime at the outset and serve as a template for space cooperation.

Global communications circuits have already come under attack. America must cautiously protect them in order to deny use of global and regional communications to an enemy. One limited option is reaching agreements on defensive schemes, perhaps including on-orbit arrangements such as mandating that commercial payloads carry routine attack and interference sensors.

The most critical capabilities to protect may be global positioning, navigation, and timing networks. Only the United States and Russia maintain them, with Galileo to follow within the next decade. Defending these signals—including when and to whom service should be denied—could be a crucial bilateral concern.

Combating Terrorism

The nature of the global war on terrorism demands worldwide capabilities to respond. It requires the close

Tethered picosatellites.

Aerospace Corporation

integration of global surveillance systems, including the Internet, with local and regional information systems. Local governments that may be reluctant to cooperate often control the latter systems. Global surveillance systems, especially space-based, can be effective in detecting terrorist activities. Moreover, the availability of such systems to local governments can be a strong incentive for cooperation. It would be sensible to consider new low-cost space-based surveillance systems that are less capable but have more comprehensive coverage. A network of antiterrorist sensors would be bilaterally negotiated. The current U.S. early warning regime involving shared missile launch warning data has been an effective pathfinder which has gained influence with minimal threat to national security.

New systems that survey large terrestrial areas and provide unfettered information access from space also have economic benefits. Direct access and interaction with the global information grid opens opportunities for economic development. Collaborative efforts in space have been seen in the past as dangerous to American interests. However, as the successful marketing of microsat capabilities demonstrates, far from migrating capabilities overseas, joint ventures result in greater product use and growing markets for all concerned.

Of particular importance to long-term global stability is the need to integrate isolated areas into the global economy, particularly those of the Islamic world. While mere access to the Internet and modern education may not cure this problem, it will help. Sharing and even providing access to the global information grid could also contribute to a long-term solution to terrorism by promoting economic development and opportunities for many regions around the globe.

Force Multiplier

The military use of space primarily provides a force multiplier for other systems. Direct communications, surveillance, intelligence and targeting, weather, and position, navigation, and timing are key advantages for the Armed Forces. But global issues demand global responses. It is in the national interest to seek means to provide space and information force multipliers to allies. Developing low-cost space systems and access through microsatellites and leveraging commercial capabilities can provide others most of the advantages enjoyed by the United States.

Some caution that encouraging even close allies to strengthen their use of high-technology force multipliers such as space could backfire. Transferring systems could threaten American lives. But it is important to note that the Nation is likely to expand its control over space and cyberspace in a crisis. Thus it is improbable that any ally will have access to sophisticated information if the United States deems it a threat to national security.

Planetary Defense

Some consider the ultimate danger to mankind to be near-Earth asteroids. The impact of a 10-kilometer diameter asteriod 65 million years ago wiped out the dinosaurs and 90 percent of the other species on the planet. Global concern over this threat, fueled by blockbuster movies, has increased the call for action. The possibility that one of the numerous small annual impacts on the upper atmosphere may be mistaken for a nuclear attack adds to the anxiety.

The United States is unique in the world in being able to address the threat of asteroids. It operates the Air Force space surveillance system, the only comprehensive system of its type. DOD space-based early warning sensors already gather data that distinguish near-earth asteroid impacts on the atmosphere from nuclear detonations. Finally, the capability to deflect objects on a collision course with Earth is under development for other military missions.

The foremost need is surveying the skies for threatening objects. Systems to track satellites can also detect and track objects. If the United States assumed the lead in a project to increase these capabilities, it could not only leverage foreign efforts—which are growing because of public fear of asteroids—but also maintain a lead in space situational awareness.

Space and information are the first authentic global capabilities. Security is a global as well as regional or national concern. The establishment of U.S. Strategic Command with oversight for these capabilities, along with other worldwide military assets, recognizes this reality. Global space and information capabilities are essential to solving these problems. A cooperative approach on the part of the United States to their development and employment is essential to building a coalition to meet common threats all nations face. **JFQ**

NOTES

[1] Franklin Kramer, "Is Security Possible in a Globalized World?" *U.S. Naval Institute Proceedings,* vol. 27, no. 10 (October 2001), pp. 50–52.

[2] Stephen N. Whiting, "Policy, Influence, and Diplomacy: Space as a National Power Element," masters thesis (Maxwell Air Force Base, Ala.: School of Advanced Airpower Studies, June 2002).