Command and Control Vulnerabilities to Communications Jamming

By RONALD C. WILGENBUSCH *and* ALAN HEISIG

If the United States ever has to face a peer adversary in a no-holds-barred fight, we will encounter a serious operational obstacle. The way we command and control our forces is highly vulnerable to disastrous disruption. Modern operations have become dependent on high-capacity communications, and this vulnerability could cause our forces to sustain a serious mauling or, perhaps, not to prevail.

Why is this? The ability to provide the information required for successful high-impact/low-committed asset warfare has developed an overwhelming reliance on unprotected communications satellites. There is an increasing public awareness of these vulnerabilities and the relative ease by which jamming can foil our methods of highly effective warfare. In this article, *jamming* is defined as electronically rendering a circuit or network unusable by disrupting it so it cannot be effectively used as a means of communication for purposes of command and control. Such an attack could be directed against any portion of the communications system and be of extended duration or else just long enough to lose crypto synchronization. Jamming is at the discretion of the enemy. It does not have to be constant or dependent on large fixed sites. It is often difficult to immediately distinguish jamming from other information flow disruptions caused by systemic disturbances such as cryptographic resets, system management changes, and natural phenomena.

U.S. Air Force maintenance technicians conduct pre-flight checks on RQ-4 Global Hawk unmanned aerial vehicle

DOD (Andy M. Kim)

While we have placed an appropriate emphasis on cyber warfare, we have neglected the less sophisticated threat of jamming. At some point prior to or during combat, an adversary might decide spoofing, intrusion, and exploitation of our networks are insufficient. The adversary could try to shut our networks down.

Then what? If our networks are jammed, commanders in the field, at sea, and in the air would not be able to employ their forces adequately. Our warfighters are dependent on these links to coordinate joint information, make reports, request supplies, coordinate land, sea, and air operations, and evacuate wounded. Clever application of jamming might go undiagnosed for a long period. Most likely, initial attribution would be to equipment malfunction, crypto problems, or operator error. This dependency is a significant vulnerability—one that can only get worse unless action is taken soon to direct our communication paths toward more protected communications systems.

In 2010, Loren Thompson of the Lexington Institute published an article pointing out this gap in future warfighting capability.[1] He stated that 80 to 90 percent of all military transmission travels on vulnerable commercial satellite communications channels and that only 1 percent of defense communications is protected against even modest jamming. He asserts that the "only satellite constellation the military is currently building that can provide protection against the full array of potential communications threats is the Advanced Extremely High Frequency (AEHF) system. . . . The feasible, affordable answer is not to begin a new program, but to start incrementally evolving AEHF towards a more robust capability." His assessment recognizes the persistent historic demand for greater capacity through satellite communications links.

In January 2012, the Department of Defense (DOD) released its Strategic Defense Guidance entitled *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*. The guidance states, "we will continue to invest in the capabilities critical to future success, including intelligence, surveillance, and reconnaissance [ISR]; counterterrorism; countering weapons of mass destruction; operating in anti-access [and area-denial (A2/AD)[2]] environments; and prevailing in all domains, including cyber."[3] We have taken great strides along these lines, but are we fully prepared?

The space-enabled communications systems used by the U.S. military are the most omnipresent information infrastructure to deployed forces. The military depends largely on commercial broadcast satellite systems architectures. In some cases, it leases capacity from the same operators of satellite systems that commercial organizations use. These systems are virtually unprotected against jamming, which is probably the cheapest, most readily available, and most likely form of denying or degrading the reliability of information flow.

Communications networks are decisive in all aspects of U.S. global military responsibilities. Commander of U.S. Pacific Command, Admiral Samuel Locklear, highlighted this issue: "we still have to be able to operate the networks that allow us to produce combat power . . . so one of my priority jobs is to ensure those [command] networks will survive when they have to survive."[4]

Why So Critical?

Since the 1980s, the U.S. military's approach to conventional operations has become more dependent on access to space-based systems—particularly long-haul satellite communications and the precision navigation and timing information provided by the Global Positioning System (GPS) constellation. For this reason, the military has invested heavily in developing battle networks to detect, identify, and track targets with sufficient timely precision to enable them to be struck. Intelligence, surveillance, and reconnaissance systems reflect how dependent U.S. forces have become on access to the orbital and cyber dimensions of the global commons.[5]

In concert with the move toward precision munitions, U.S. warfighting doctrine has become inseparably joint at all levels of the Services. Joint coordination between widely dispersed forces is only possible by assured information flows. Moreover, all Services have an increasing realization of their dependencies on protected communications. The protection of information and ability to maintain freedom of maneuver in space is essential to Army success;[6] the highly mobile Army of the future requires communications on the move with networked operations. It depends on the availability of high-bandwidth, reliable, protected satellite communications to achieve this goal.[7] The Air Force is hotly debating the methodologies to ensure space capabilities, including protected communications, at a balanced cost and risk.[8] The Navy has reorganized its entire information apparatus to focus on information dominance as a key element of its future. The Joint Staff has reestablished its J6 Command, Control, Communications, and Computers/Cyber Directorate due to the increased importance of and dependence on assured information technology and networks.

The dependence on information flows (communications) of all kinds has produced superior combat efficiencies and effectiveness. Today's Army uses significantly smaller and dispersed units to operationally control battlespace areas than in prior warfighting constructs. The shift to strategic small units is possible, in part, because of the significantly increased lethality of smaller units enabled by the use of ISR and precision weapons. This precision, however, depends largely on reliable communications. This overall change in operational concepts has become a fundamental shift in military thinking. The Army is starting to build around the platoon level and the Marine Corps around the squad. Special operations forces build around the team. This shift exponentially expands the need for high bandwidth information, particularly ISR.

The ability to provide the required voluminous information has so far developed a strong reliance on unprotected satellites including the ability to use unmanned aerial vehicles (UAVs) and beyond-line-of-sight capabilities for over-the-horizon control and real-time communication. This has led to an increasingly widespread public discussion of the vulnerabilities of using unprotected satellite communications.[9] The ubiquitous use of unprotected commercial wideband satellite communications leads to a false sense of comfort and assurance of availability, which is deceptively dangerous. Jamming is the enemy's side of asymmetric information warfare.

Rear Admiral Ronald C. Wilgenbusch, USN (Ret.), is a Consultant in Command, Control, Communications, Computers, and Intelligence (C4I). During his career, he served as an Electronic Technician, Surface Warfare Officer, and Acquisition Professional. Captain Alan Heisig, USN (Ret.), is also a Consultant in C4I. He commanded several surface ships and amphibious squadrons.


U.S. Air Force (Raymond McKoy)

Air Force cadets defend their network during National Security Agency's Cyber Defense Exercise at U.S. Air Force Academy, Colorado Springs

Potential adversaries have a variety of options to accomplish disruption including physical destruction of satellites and ground stations, cyber, and jamming. Jamming is an important element of any communications-denial plan. It is cheap to obtain and simple to operate. It can effectively be used surgically or in broadly based attacks. The absence of planning and programmatic actions to protect against a jamming threat is worrisome given the likelihood of its use.

Jamming and Antiaccess/Area Denial

A principal priority of the Strategic Defense Guidance is to project power despite A2/AD challenges.[10] The recent conflicts in Iraq and Afghanistan do not provide experience against an adversary employing significant communications-denial methods. Information access was assured in those conflicts. Potential adversaries in other areas of the world have studied U.S. force enablers for two decades. They realize how dependent we are on assured communications. They understand that the best way to confront U.S. military power is to prevent it from deploying. China, for example, has sent clear signals of its intent through a variety of activities including a naval buildup, submarine deployments, ballistic missiles capable of targeting aircraft carriers, cyber activities, and an antisatellite demonstration. There can be no question that jamming capabilities would play a significant part in any A2/AD campaign.

The ability to counter area-denial activities depends in many ways on reliable satellite communications capabilities. Such capabilities exist today in China[11] and, by extension, any surrogate or client regimes with area-denial agendas. U.S. forces must be able to operate in this challenging environment. The obvious counter to jamming is to protect communications for operational forces. The necessity for protected communications is not limited to A2/AD scenarios. A striking example is the strong reliance by the Intelligence Community on UAVs for tactically relevant information supporting ground troops. These vehicles require wideband satellite communications systems for over-the-horizon control and real-time information dissemination. Future tactical forces will rely on robust and reliable information systems. They are at huge risk to jammers.

China and Russia have well-documented satellite jamming capabilities. Some versions of militarily effective jammers are even commercially available.[12] The proliferation of jamming technology has led to an increasing utilization of strategic and tactical jamming.[13] Satellite jamming, in particular, is proliferating. Military jamming equipment can be purchased on the Internet by anyone, including nonstate actors. The attraction of this economical, highly effective capability to disrupt vastly superior forces is an ominous reality. The omnipresent capability by widely divergent players almost guarantees that jamming source attribution will be a problem even after detection is accomplished.

In February 2012, the United Nations International Telecommunications Union hosted the World Radiocommunications Conference in Geneva. In recognition of the upswing of satellite jamming in 2011, the union issued a change to its regulations and a call to all nations to stop international interference with satellite telecommunications.[14] Moreover, recent incidents illustrating the need for action were the jamming of satellite operators EUTELSAT, NILESAT, and ARABSAT.[15] Jamming has occurred from a variety of locations recently across the globe. Interference with satellite television broadcasting has come from Indonesia,[16] Cuba,[17] Ethiopia,[18] Libya,[19] and Syria.[20] Additionally, in the case of Libya, the use of tactical jamming of satellite telephones was reported during the course of combat operations.[21]

The proliferation of jamming does not have to depend on land-based fixed or mobile facilities. China is not tied to castoff Soviet naval designs. The People's Liberation Army Navy (PLAN) has small, fast, and capable craft with good seakeeping capabilities such as the *Houbei* missile attack craft. Even a cursory look at the craft's superstructure shows that attention is paid to shipboard electronics. The superstructure could be equipped with powerful jammers and operated collaboratively far from U.S. forces. This could seriously complicate U.S. naval or air power projection. The PLAN continues to field these state-of-the-art, ocean-capable, wave-piercing aluminum hull SWATH craft. According to in-country open sources, by February of 2011, the PLAN had fielded over 80 type 22 *Houbei*-class fast attack craft, and the number is growing.[22] The question is no longer who has jamming capabilities but, rather, have we prepared to operate effectively when it happens. At present, the answer is a resounding no.

Causes and Actions

Historically, protected communications were viewed as the realm of strategic existential threats to the Nation. The underlying principle of U.S. protected communications continued to have its raison d'être linked to nuclear communications survivability and essential, highest-level command and control. The approach was heavily focused on getting

DOD

***Arleigh Burke*–class guided missile destroyer USS *Hopper* (DDG 70), equipped with Aegis integrated weapons system, launches RIM-161 Standard Missile**

through a small number of human-to-human messages on which dispersed forces could execute preplanned objectives. This focused view kept protected communications capability development geared toward the "Armageddon" context and did not significantly influence tactical requirements.

During Operation *Desert Storm* in 1991, laser-guided bombs, Tomahawk land-attack missiles (TLAMs), and the GPS-aided conventional air-launched cruise missiles demonstrated that U.S. forces had the capability to hit almost any target whose location could be pinpointed. For this reason, the U.S. military has invested heavily in developing battle networks to detect, identify, and track targets with sufficient timely precision to enable target strikes. ISR systems such as the RQ-4 Global Hawk, GPS constellation, and photoreconnaissance satellites reflect how dependent U.S. forces have become on access to the orbital and cyber dimensions of the global commons.[23] The preplanned targeting initially envisioned for these types of precision weapons incrementally has given way to a need for real-time responsiveness.

Desert Storm also highlighted the inadequacy of the existing satellite communications architecture. The starkest reality was the inability to transmit large data files to tactical forces. The air tasking order (a daily compilation of all joint and coalition aircraft planning and execution) was unable to reach the significant airpower resident on Navy carriers. The reprogramming of TLAMs, laser-guided bombs, joint direct attack munition, and other precision munitions took exceedingly long times to transmit and overwhelmed the beyond-line-of-sight systems of the day.

The vulnerability of unprotected broadband communications went unchallenged in the last two decades. Recent conflicts have not been fought against major adversaries with comparable capabilities.[24] The U.S. military was able to accomplish its ends cheaply by taking advantage of a commercial overbuilding of satellite communications capacity in the late part of the last century and the early years of this one. That convenient resource is no longer available. Market developments have made commercial leasing a much more expensive alternative. Moreover, commercial communications satellites retain their inherent jamming vulnerabilities.

Realization and Acceptance of the Requirement

The paucity of protected communications below the highest levels of requirements of nuclear command and control is starting to wend its way into the thinking of military leadership. A 2010 Defense Intelligence Agency (DIA)–sponsored wargame, with over 60 Active-duty troops and civilian representatives from each of the Services, tried to grapple specifically with the loss of assured satellite communications. The players made several key comments as they became aware of the impact of threats to existing warfighting doctrine. The consensus among participants was that "significant risk" to mission success occurred when protected beyond-line-of-sight communications were limited to existing capabilities. In the presence of even modest jamming capability, participant reaction was to revert to Cold War–era doctrine and tactics.

U.S. Soldiers set up tactical satellite communication system in Shekhabad Valley, Wardak Province, Afghanistan

U.S. Army (Russell Gilchrest)

Those reactions were immediately frustrated by a lack of available older systems; the infrastructure to accomplish those doctrines and tactics no longer exists. The combat functions of planning, command and control, movement and maneuver, intelligence, fires, force protection, logistics/personnel support, and special operations were all significantly or critically degraded. Additionally, there were issues with force structure, organization, training, and equipment. Essentially, the entire spectrum of warfighting capability beyond preplanned initial insertion and organic logistics was significantly adversely affected. These risks translated into longer engagement timelines, increased casualties, and the need for a larger force structure for each mission and reduced multimission capability.[25]

The wargame specifically focused on satellite jamming as the most mature and economically available means to deny satellite capability. The issue of physical destruction of orbital assets was not addressed as it had several military/political elements that were deemed too expensive or carried a significantly disproportionate geopolitical risk. The same denial effect is achieved by spot jamming without the protagonist having to develop physical methods of interfering with space-related infrastructure.

Pinpointing the source of jamming is not easy. Jammers can appear innocuous and can be quite mobile. They can be intermittent in operation. A jammer can physically appear as some sort of commercial system, such as a news uplink vehicle or normal receive antenna on a fixed site.

We have many lessons to draw on that point to a future where a large component of beyond-the-horizon communications must be protected. Given the huge advantages that space communications provide, it makes sense to protect the capability against the inexpensive and ubiquitous development of disruptive capability by potential adversaries. The risk of not protecting it is an exponential rise in force structure and cost coupled with the plummeting warfighting effectiveness of existing forces. Accordingly, DOD will continue to work with domestic partners and international allies and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space.[26] In the President's words, "Going forward, we will also remember the lessons of history and avoid repeating the mistakes of the past when our military was left ill-prepared for the future."

Are There Options?

Optimists would say that the picture is not so grim—that there *are* options. So what might these options be if or when we encounter an enemy who wishes to shut down our communications? How quickly can we turn options into operational capabilities? Are these really viable options that will keep our forces fighting as they have trained?

The most frequently discussed option is that we would "go old school." Participants in the previously mentioned DIA-sponsored wargame suggested that they could still accomplish their warfighting missions by using old-school techniques such as high-frequency (HF) radio links. But, on examination, they came to realize that this is not viable. The worldwide system of fixed HF transmitters and antennas that was once the mainstay of our HF communications systems is gone. Even if it was still in place, the skilled HF operators needed aboard ships and ashore have been cashing retirement checks for years.

There is a more basic issue. Our satellite links have enabled completely different types of operational communications and tactics and procedures that cannot be supported on HF. This includes high bandwidth machine-to-machine data exchanges, video teleconference, Web sites, chat, email, and other mechanisms that in a large context allow decisionmaking to be viable at low levels in the chain of command. That is the fundamental capability that enables quick, adaptive, and effective warfighting that exponentially multiplies smaller force capabilities. Yet going old school, reverting to HF, was exactly the alternative a senior Navy officer suggested as the course of action in trying to overcome a potential jamming threat at the 2012 Navy Information Technology Day briefing.

A second knee-jerk option is that we would "shoot the jammer." This is a nonstarter. Almost everyone has seen the massed army of television trucks/vans wherever and whenever some sensational news event occurs. Imagine downtown Baghdad or Kabul with the same number of trucks. Any one of them could be a jammer. Which one should be shot, and how long would it take to sort them out? Even if the jammer was working in the middle of an open desert in enemy-controlled territory, it would still be a tough target. The jammer could stand out in the open just long enough to disrupt the crypto set on the link/network. Then it could go silent, move to another location, or focus on another satellite link. As mentioned, operators frequently confuse jamming with equipment problems or a self-imposed mistake. At best, locating and shooting the jammer is a difficult targeting problem that would certainly tax the intelligence and strike assets assigned to other high-value targets.

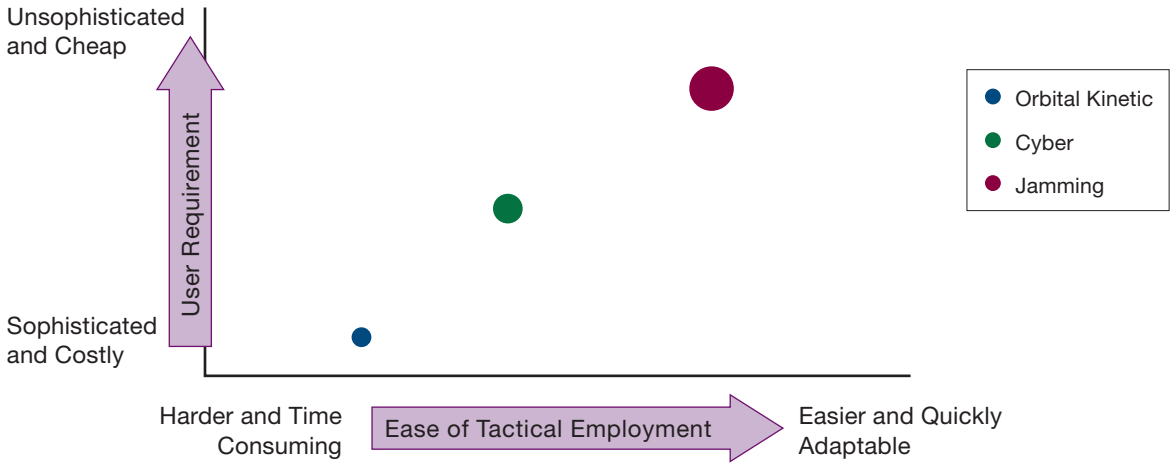
A third option is that we would attempt to reconstitute the satellite constellations by rapidly replacing capability on orbit. This usually implies a set of smaller satellites already in storage. It also means the availability of a nearly immediate launch period acceptable for military operations. However, replacing one disrupted satellite with another equally vulnerable to jamming hardly seems to solve the problem. Furthermore, none of the smaller satellites that have been proposed has the capability to replace the types of satellites used today. At present, there are simply not enough launch vehicles or launch sites available to support such an alternative.

A fourth option might be to design an entirely new satellite system with new features. This is theoretically feasible. However, it is hard to envision what this solution additionally offers in the sense of timeliness, cost reduction, and operational improvement over expanding the constellation of existing protected communications satellites such as advanced extremely high frequency (AEHF) ones. The current and evolving technology is understood and carries known programmatic risk. We can certainly improve and expand the AEHF constellation much faster than engage in multiple new technology program starts.

A fifth option is centered on redundancy. In this alternative, even though most communications links are not protected, there are many of them. It is hard to imagine an adversary who could take the entire infrastructure down simultaneously. High-level DOD officials have suggested that an enemy might be able to mount a jamming attack that would leave operational forces with only about 60 percent of our present capability. But when was the last time we were using only 60 percent of our satellite communications capacity?

We must further assume that an intelligent enemy would have at least determined

Likelihood of Occurrence for Types of Communications Attack



our most critical links to operations in progress. Those are likely to be the first to go. More concerning is the fact that a swept tone jammer could take out all our links, or certainly more than DOD officials estimate. The 60 percent figure appears unsupported by analysis.

In any event, forces experiencing jamming without prior training and a management plan would create operational chaos. Managing heavy jamming attacks in this environment becomes an effort to plan for gradual degradation of communications. Operational concepts must be modified on the fly as individual circuits are lost. Training must also be conducted both to recognize and counter jamming as it occurs. These actions should be pursued. It appears at present that little progress has been made in this direction. The reality is that many important circuits have no backup. For example, many UAVs have only one form of over-the-horizon communication available. It would not be difficult for an adversary to learn where to target his jamming efforts for the greatest effect against UAVs.

It has been suggested that the present military satellite communications system is composed of too many and too large satellites that are overly vulnerable, overly complex, and unnecessarily costly. The proposed solution is to develop and deploy disaggregated system architecture to replace present architectures.

There are two obvious problems with this suggestion. First, it presupposes that there is a disaggregated architecture that would offer the same capability at a reduced deployed cost. In order to make a disaggregated satellite constellation acceptable from a cost standpoint, it would have to be supported by math to show that it is less expensive than the evolving current highly effective and efficient systems. Second, it is suggested that disaggregation would reduce vulnerability, but in fact no amount of disaggregation could offer protection against effective jamming or ASAT attack. Furthermore, simple logic would tell us that, if it is known that an attack on our *strategic* antijam main asset, AEHF, is tantamount to an act of war, extending the use of that same asset to provide secure coverage for both tactical and strategic forces would make the tactical support more secure simply by being on the same strategic asset. On the other hand, disaggregating the two missions on different satellites would seem, from a logic standpoint, to make the disaggregated tactical asset more vulnerable to attack. After all, would jamming one of many tactical assets be considered an act of war? Additionally, a disaggregated architecture presents questions of technical risk and complexities not yet answered.

Of course, there are other alternatives, such as adding antijam capability to unprotected wideband systems. The properties of transmission physics dictate that an increase in antijam capability implies modifications to the waveform that would, of necessity, cause a reduction of the data rate. There are no halfway measures. There is no point in adding just a "little antijam." We either defeat the jamming capability or we do not. So we have to be prepared to defeat the most likely jamming threats.

One alternative put forth that seems to offer potential is to supplement the existing satellite system through the development of the Aerial Layer Network (ALN). However, like an entirely new satellite system, it is not fully defined and has yet to be built. ALN is a solution that might be able to take existing satellite technology, scaled down in size but not in capability, and have it ready for rapid deployment to enable our forces to operate in some scenarios in the face of jamming. This involves engineering developments that carry all the risks of any new start. By its nature, it is best used in a permissive environment or one with airspace dominance. This concept seems ripe for use as a pseudosatellite augmentation to support a land area of operations or a battlegroup maneuvering at sea.

Dr. Thompson's thesis of incrementally expanding the capability of AEHF is not sufficient; it should be matched with a realization that the EHF spectrum also contains the capability to accommodate a wide variety of high bandwidth requirements. This could provide ground, maritime, and atmospheric forces with the protected wideband capabilities that complement the mobile, highly integrated forces the U.S. military fields today and will field tomorrow.

Conclusion

Jamming is a highly effective technique that could cripple U.S. military operations, and our potential adversaries know it and

have the capability to employ it. We should not underestimate what they might do. Realizing our current operational dependency on reliable high data rate communications, and considering the attractiveness and availability of jamming to potential adversaries, we have only two choices. The first is to reduce our dependency on communications—an unlikely alternative for obvious reasons. Doing so would reduce operational effectiveness and require a correspondingly larger and more expensive force structure. It should be obvious that the way we have learned to fight over recent years simply will not allow a reduction in the amount of communications capacity we will need.

The second choice is to ensure that our communications infrastructure is sufficiently resilient to withstand the type of attack discussed herein. As one unnamed senior officer put it, in our present situation and failing to add more protected communications, we could be "out of Schlitz by noon on the first day of battle." This is clearly not where we ought to be. Increasing the capacity of protected communications is an essential part of this latter alternative.

Failure to address the predictable jamming threat could (*will*) lead to mission degradation or failure. The time to act is now. **JFQ**

NOTES

[1] Loren B. Thompson, "Lack of Protected Satellite Communications Could Mean Defeat for Joint Force in Future War," *Lexington Institute Early Warning Blog*, April 14, 2010, available at <www.lexingtoninstitute.org/lack-of-protected-satellite-communications-could-mean-defeat-for-joint-force-in-future-war>.

[2] *Antiaccess/area denial* is defined thusly: "anti-access capabilities [are] ones that slow deployment of friendly forces into a theater, prevent them from operating from certain locations within that theater or cause them to operate over longer distances than they would like. Area-denial efforts are those that reduce friendly forces' freedom of action in the more narrow confines of the area under the enemy's direct control." See Phillip Dupree and Jordan Thomas, "Air-Sea Battle: Clearing the Fog," *Armed Forces Journal* (June 2012), available at <www.armedforcesjournal.com/2012/05/10318204>.

[3] *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: Department of Defense, January 2012).

[4] Admiral Samuel J. Locklear, USN, U.S. Pacific Command change of command address, March 2012.

[5] Barry D. Watts, *The Maturing Revolution in Military Affairs* (Washington, DC: Center for Strategic and Budgetary Assessments, 2011).

[6] U.S. Army Training and Doctrine Command (USTRADOC), *The United States Army Operating Concept*, TRADOC Pamphlet 525-3-1 (Fort Monroe, VA: Headquarters Department of the Army, August 19, 2010), available at <www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf>.

[7] Warfighter Information Network–Tactical Commanders Handbook, Version 1.6.

[8] C. Robert Kehler, "Implementing the National Security Space Strategy," *Strategic Studies Quarterly* (Spring 2012), 18–26, available at <www.au.af.mil/au/ssq/2012/spring/kehler.pdf>.

[9] "Protecting [unmanned aerial vehicle] satellite communications links also will be an important challenge in the future," stated Stuart Linsky, vice president of communications systems at Northrop Grumman. "Where it once took an advanced nation state to jam U.S. military communications, new ubiquitous technologies now expose unmanned systems to jamming and cyber-attacks. 'The ease with which the bad guys can do bad things has gotten easier.'" See Henry Kenyon, "New satellite capabilities target UAV needs: Waveforms and spacecraft help support warfighter mission requirements," *DefenseSystems.com*, March 15, 2012, available at <http://defensesystems.com/articles/2012/03/15/satellite-2012-uav-satellite-needs.aspx>.

[10] *Sustaining U.S. Global Leadership.*

[11] Andrew Erickson, "China Testing Ballistic Missile 'Carrier-Killer,'" *Wired*, March 29, 2010, available at <www.wired.com/images_blogs/dangerroom/2010/03/asbm_graphic_admiralwillard-testimony_chinese-article.png>.

[12] Available at <http://jammerfactory.en.made-in-china.com/product/DMcQoSlPCNWE/China-100W-Military-Communications-Jammers-Backpack-Blockers.html>.

[13] Electronic and information warfare techniques including hacking into computer networks and electronic jamming of satellite communications links are negation capabilities that are becoming increasingly available to both state and nonstate actors. A number of incidents of electronically jammed media broadcasts have been reported in recent years, including interruptions to U.S. broadcasts to Iran, Kurdish news broadcasts, and Chinese television (allegedly by the Falun Gong). Iraq's acquisition of Global Positioning System (GPS)–jamming equipment for use against U.S. GPS-guided munitions during Operation *Iraqi Freedom* in 2003 suggests that jamming capabilities are proliferating; the equipment was reportedly acquired commercially from a Russian company. See *Space Security 2007* (Waterloo, ON: Project Ploughshares, August 2007), available at <www.spacesecurity.org/SSI2007.pdf>.

[14] "International Broadcasters Call for End of Satellite Jamming," Broadcasting Board of Governors, January 24, 2012, available at <www.bbg.gov/press-release/international-broadcasters-call-for-end-of-satellite-jamming/>.

[15] See David Klinger, "Satellite-jamming becoming a big problem in the Middle East and North Africa," March 28, 2012, *Arstechnica.com*, available at <http://arstechnica.com/science/news/2012/03/satellite-jamming-becoming-a-big-problem-in-the-middle-east.ars>.

[16] Recent examples of satellite jamming include Indonesia jamming a transponder on a Chinese-owned satellite and Iran and Turkey jamming satellite television broadcasts of dissidents. See "Space, today and the future," available at <www.dod.mil/pubs/spacechapter2.pdf>.

[17] Broadcasting Board of Governors, Washington, DC, July 15, 2003.

[18] "Ethiopia Jamming Eritrean Television, Knock out own Satellite channel," available at <www.topix.com/forum/world/eritrea/TKPS5MNR2DH67LOFM>.

[19] Peter B. de Selding, "Libya Accused of Jamming Satellite Signals," *Space.com*, March 1, 2011, available at <www.space.com/11000-libya-satellite-jamming-accusations.html>.

[20] The Obama administration asserts that the Syrian government, with Iran's help, is actively jamming private communications and satellite Arabic television networks in an aggressive campaign to cut off antigovernment organizers from the outside. See "Officials: Obama ramps up aid to Syrian opposition," Associated Press, April 13, 2012, available at <www.usatoday.com/news/world/story/2012-04-13/syria-un-annan/54258456/1>.

[21] "Thuraya Accuses Libya of Jamming Satellite Signals," *SpaceNews.com*, February 25, 2011, available at <www.spacenews.com/satellite_telecom/110225-thuraya-accuses-libya-jamming.html>.

[22] David Lague, "Insight: From a ferry, a Chinese fast-attack boat," Reuters, May 31, 2012, available at <www.reuters.com/article/2012/05/31/us-china-military-technology-idUSBRE84U1HG20120531?goback=.gde_104677_member_120627756>.

[23] Watts.

[24] Ibid.

[25] Verbal assessment comments from Protected Communications Wargame Outbrief, May 26–27, 2010.

[26] *Sustaining U.S. Global Leadership.*