Defending Our Satellites

The Need for Electronic Warfare Education and Training

Lt Col E. Lincoln Bonner, USAF

The US military enjoys tremendous advantages over any potential adversary because of its exploitation of space capabilities. It is of paramount importance that Air Force Space Command (AFSPC) position its Airmen to defend and protect America's space advantage in the contested space environment of the present and future. AFSPC can best develop space Airmen to win tomorrow's fight in this contested environment by significantly improving and expanding education and training in the use of electronic warfare to defend US satellites and improve their survivability.

The following discussion first describes why improving space system survivability is critical to US war fighting. It then explores and compares the role of electronic warfare in aircraft survivability to the space domain to demonstrate how prowess in electronic warfare is essential for successful defensive space control. The article next describes the current state of electronic warfare education and training for space operators. Finally, it explores suggestions for improving space leaders' readiness to win in electronic warfare in order to defend America's space advantage.

Space System Survivability and US War Fighting

The US military gains a disproportionate advantage over potential adversaries by exploiting space capabilities. Satellites provide an advantage similar to that of reconnaissance aircraft in World War I—(1) warning of enemy attack to help ensure that these attacks fail and (2) the enabling of precision strikes.[1] Additionally, satellites provide over-the-horizon communication at a combination of speed, volume, and mobility that terrestrial communications cannot match.

US military initiative—the ability to observe, orient, decide, and act more quickly and more effectively than an opponent—heavily depends upon space capabilities. US intelligence, surveillance, and reconnaissance satellites can observe far over the horizon, providing ample warning time to react to enemy moves and countermoves and help to ensure that adversary attacks fail—similar to the contributions of airborne reconnaissance in World War I. Space-based intelligence, surveillance, and reconnaissance extend that World War I airborne reconnaissance advantage,

though, by providing not only time to react but also enough warning to seize the initiative and choose the time, place, and conditions of battle.

In addition to reconnaissance, satellites enable precision strikes. US advantages in massing and concentrating effective firepower from fewer units and strike platforms stem largely from the use of precision-guided munitions, which are, in turn, heavily dependent upon data provided by Global Positioning System (GPS) satellites. For example, in the 1991 Operation Desert Storm against Iraq to liberate Kuwait, 1,207 strike aircraft participated in the air campaign, approximately 4 percent of which were precision guided by laser—GPS-guided munitions were not yet available.[2] In Operation Iraqi Freedom in 2003, 772 strike aircraft participated in the air campaign—36 percent fewer than in 1991—and 68 percent of the bombs released were precision guided, principally by the GPS.[3] Newer weapons like the Small Diameter Bomb have a relatively small blast radius to limit collateral damage and become combat ineffective in many scenarios without precision guidance data from the GPS or an alternate source. US air, land, and naval forces heavily depend upon GPS information for navigating and conducting precision strikes. Even modern-day airborne reconnaissance, which provides advantages similar to those of satellite reconnaissance, heavily depends upon space capabilities.

Remotely piloted aircraft like the MQ-9 Reaper and RQ-4 Global Hawk have assumed a significant portion of the airborne reconnaissance workload. These remotely piloted aircraft leverage GPS data for navigation and guidance as well as employ secure satellite communications. These communications provide for command and control and mission-data relay to processing, exploitation, and dissemination on the ground half a world away.

No potential adversary can yet match US war-fighting advantages to seize the initiative and conduct precision strike; neither can such an enemy equal the scope and scale of US global reach. These war-fighting advantages stem from exploitation of space-based reconnaissance, precision navigation and timing, and communication. Hence, the first priority for Air Force space leaders in a contested environment is to conduct effective defensive space control operations and improve space system survivability to ensure the endurance of US war-fighting advantages flowing from exploitation of the ultimate high ground.

Electronic Warfare and Aircraft Survivability

As the Air Force quickly learned in the realm of air combat, survivability in a contested environment largely depends upon the capability to dominate in the realm of electronic warfare. Initially, prior to the invention of radar, the dominant strategy to improve bomber survivability was to use multiple engines to increase bombers' flight speed and altitude so they could not be threatened by antiaircraft guns or slower, lower-flying, single-engine fighters. However, the attrition rate that Luftwaffe Me-109 single-engine fighters inflicted on Allied bomber forces in World War II horribly demonstrated that speed and altitude alone did not provide sufficient protection.

Prior to World War II, radar did not exist; as a result, there was insufficient warning time for fighters to be launched and intercept attacking bombers before they could strike and escape. This situation changed with the development of radar, which provided the warning time and information (e.g., raid count, altitude, speed, and direction) that underpin integrated air defense. Bolstered by the warning provided by the Chain Home radar system and the speed and altitude provided by the Spitfire fighter and its Merlin engine, England's Fighter Command was able to win the fight for air superiority and blunt German bomber attacks to win the Battle of Britain.

The Allies learned the criticality of radar to effectively engaging penetrating aircraft during the Battle of Britain. As a result, they recognized that speed and altitude could not protect bombers from enemy fighters guided by radar. Ultimately, bomber survivability could be achieved only if the warning and information radar provided to enemy counterair capability could be sufficiently degraded or negated. As a result, Allied air forces initiated a concerted effort to develop electronic warfare capabilities. In 1940, immediately following the Battle of Britain, the Allies began a multiyear intelligence operation to learn everything they could about German air defense radar and communications in order to develop electronic warfare systems that could degrade or neutralize integrated German air defenses and increase Allied bomber survivability.[4] However, it would take two years for this intelligence operation to bear fruit.[5] In the meantime, US bomber strategy turned to formation tactics in the hopes of creating enough concentrated firepower from bomber self-protection guns to shield friendly aircraft from intercepting fighters. As the disastrous attack on Schweinfurt in 1943 showed, in which Allied bomber losses numbered 25 percent, either a new strategy was needed to protect Allied bombers or the Combined Bomber Offensive would fail.[6] Fortunately, the electronic warfare development effort delivered results just in time.

The Allies' new aircraft survivability strategy combined the use of electronic warfare capabilities, chaff, and airborne jammers with long-range fighter escorts to suppress German air defenses. In July 1943, Allied bombers first used chaff—thin strips of aluminum that create clutter on radar scopes.[7] Chaff degraded the performance of German ground control intercept radars used to vector Luftwaffe fighters onto attacking bombers.[8] Allied employment of airborne jammers like Airborne Cigar complemented the use of chaff. Airborne Cigar further degraded German air defenses by jamming the Lichtenstein radar aboard Luftwaffe night fighters so they could not effectively intercept Allied bombers attacking at night.[9] As a result of the electronic warfare advantage that systems like Window and Airborne Cigar bestowed upon the Allies, British bomber loss rates were cut by half compared to their average during the 1943 raids on Hamburg.[10]

The Air Force has never forgotten the importance of electronic warfare to aircraft survivability. As a result, it has developed stealth aircraft, modern jamming systems like the miniature air launched decoy jammer (MALD-J), and the high-speed antiradiation missile (HARM) to suppress and degrade enemy radar—the center of gravity of an air defense network. You cannot hit what you cannot see.

Unfortunately, the lesson of survivability and electronic warfare appears to have gone unnoticed within the Air Force's space operations community. While technology

could have quickly negated the survivability that orbital altitude and velocity initially afforded, this military evolution was suspended. The two principal antagonists during the early days of space capability development—the United States and the Soviet Union—established the international convention that outer space was international territory over which sovereignty would not be asserted and unrestricted overflight of any territory would be permitted.[11] This Cold War convention preserved space as a sanctuary for over 60 years. But it also arrested development of the Air Force's space Airmen in a state analogous to that of pilots prior to World War I in which responding to system malfunctions for basic safe operations was the focus rather than surviving in the face of enemy attack. Understandably, without a credible counterspace threat over the last 60 years, improving space system survivability has not received much of Airmen's attention.

Unlike its status during the Cold War period, though, the convention of space as a sanctuary is rapidly disappearing. For example, China conducted successful antisatellite missile tests in 2007 and 2014.[12] Additionally, antisatellite electronic jammers capable of degrading the use of GPS satellites for precision navigation and strike and communications satellites are readily available.[13] More importantly, states have recognized the asymmetric advantage that US forces gain from space and are implementing military strategies designed to deprive the United States of this advantage. For example, Chinese military writings "emphasize the necessity of 'destroying, damaging, and interfering with the enemy's reconnaissance . . . and communications satellites.' "[14]

Fortunately, counterspace networks share characteristics similar to those of counterair networks that the Air Force can exploit to improve survivability of US space systems—namely, dependence on electronic surveillance and reconnaissance via radar to find, track, and engage US satellites. Like counterair capabilities, counterspace capabilities integrated into a network of sensors and shooters will likely be most effective. In the air domain, this network of sensors and shooters is known as an integrated air defense system (IADS), and the extension of this war-fighting concept to space is the logical next step for potential adversaries seeking to deny the US military the advantage from the high ground of space.

An IADS is composed of several components to find, track, and engage aircraft to complete the kill chain. First, there are early warning radars that find aircraft and provide course speed, direction, and altitude information about incoming aircraft. Data from multiple early warning radars are fused into rough tracks and passed on to tracking and engagement radars. These more precise tracking radars then perform focused searches with early warning radar information as the starting point to refine the speed, direction, and altitude information about incoming aircraft. When tracked aircraft enter the lethal envelope of shooters, these aircraft are engaged with antiaircraft missiles that are terminally guided by radar or electro-optical sensors, typically housed on board the missile. Only if all of these steps are achieved successfully can the target aircraft be destroyed. Note that for each aspect of the find, track, and engage elements, a successful counterair engagement depends upon effective electronic surveillance—either electro-optical or radar. The ability of Air Force aircraft to survive in the presence of an IADS largely depends upon the capability to conduct effective suppression of enemy air defenses (SEAD) opera-

tions via stealth, kinetic strike, and electronic jamming to blind or deceive the IADS's electronic sensors.

Since World War II, US SEAD capabilities have grown in sophistication from releasing strips of aluminum (chaff) into the air to today's MALD and MALD-J systems.[15] In addition to jamming, the US military has developed kinetic strike options to destroy and suppress, by threat of destruction, enemy counterair systems by combining the capability to electronically locate enemy threat radars with high-speed missile technology, resulting in the HARM and its companion HARM Targeting System.[16] In addition to SEAD jamming and strike operations, self-protection jamming is another element of the electronic warfare system of systems that improves US aircraft survivability. Air Force systems like the ALE-50 towed decoy and Large Aircraft Infrared Counter-Measure (LAIRCM) are designed to degrade the performance of terminal guidance radar and electro-optical sensors housed within missile seekers.[17] Aircraft survivability in a contested environment has depended on superiority in electronic warfare going back to World War II—so too will it be in the contested space environment that the United States now faces.

Like an IADS, the effectiveness of potential adversaries' counterspace networks will depend upon electronic surveillance by radar and electro-optical sensors to find, track, and engage adversary spacecraft. Multiple countries already field networks of sensors, Space Object Surveillance and Identification (SOSI) radars, and telescopes in an effort to keep, find, and track satellites and debris in Earth orbit. Russia, China, and the United States each possess a network of SOSI sensors capable of finding and tracking spacecraft. The way the Air Force is likely to protect US spacecraft is through the conduct of suppression of adversary counterspace capabilities (SACC), which "neutralizes or negates an adversary offensive counterspace system through deception, denial, disruption, degradation, and/or destruction."[18] Like SEAD, success in SACC to protect US satellites will likely depend on the Air Force's capability to conduct successful electronic warfare operations to jam and strike adversary counterspace network sensors (i.e., SOSI sensors). Today, SOSI sensors are generally large, immobile facilities, so tactical systems to electronically locate them—like the HARM Targeting System—are typically unnecessary, but SOSI sensors can be expected to evolve to become smaller and more mobile, just as IADS sensors have over time. As this evolution occurs, the conduct of successful electronic warfare operations to locate and jam mobile SOSI systems and their companion counterspace strike batteries in support of SACC will become simultaneously more important and more challenging.

However, suppression of enemy counterspace alone will be insufficient to adequately protect US satellites. Spacecraft survivability, like aircraft survivability, will depend upon a system-of-systems approach that incorporates suppression operations as well as self-protection electronic jamming and possibly stealth technology to defeat counterspace systems at the point of engagement. Decoy and countermeasure systems like the ALE-50 and LAIRCM will be needed to defeat an antisatellite missile's terminal guidance sensors and protect targeted spacecraft from being destroyed by counterspace batteries that continue to function despite suppression efforts. Furthermore, while stealth technology could theoretically improve spacecraft survivability exponentially, as it has for aircraft, basic satellite operations requirements

for heat management and power generation using large solar arrays suggest that a stealth satellite is unlikely to emerge with today's technology.

In addition to the antisatellite missile threat, there are additional attack vectors against US satellites that manned aircraft are far less vulnerable to: cyber attack, kinetic strike on space system ground segments, and link jamming against both the command uplink and/or the data downlink. The fact that satellites are basically sophisticated robots/drones flying in space creates these additional vulnerabilities. Fortunately, there is a massive focus on cyber defense within AFSPC. AFSPC's Twenty-Fourth Air Force, the Air Force component to US Cyber Command, as well as the larger Air Force are in the midst of a massive recruiting, education, and training effort, the objective of which is to rapidly grow Airmen with the knowledge and expertise to defend Air Force assets from cyber attack. While Air Force space operators need to have knowledge of how cyber attacks could affect their systems, space operations will primarily find themselves in a supported role relative to cyber defense. Consequently, space operators do not need deep knowledge in cyber warfare at present, much as infantry does not need deep knowledge of air operations since the infantry most often finds itself in a supported role whereby it primarily needs to understand the effects that air operations can bring to bear. The same is true for space operators regarding cyber operations, and an introductory, familiarization-level of knowledge of cyber operations should suffice for space operators through broad courses like Undergraduate Space Training and Space 200/300. However, space operators require a significantly higher level of knowledge in electronic warfare because they will be directly engaged in it in order to protect their spacecraft.

Satellites are operated by personnel on the ground who send commands to the spacecraft via an electronic uplink. If this command uplink were to be successfully attacked electronically, a satellite would be rendered useless—if not immediately, then certainly over time. Moreover, because satellites' principal value is derived from the information they are able to acquire and communicate from their overhead vantage point and because that communication is via a wireless, electronic downlink to the ground, then effective electronic attack on that downlink immediately takes space systems out of the fight. For instance, jammers targeting the downlink from GPS satellites prevent users from receiving accurate and useful precision navigation and timing information from the spacecraft. However, if effective electronic support could be employed to geolocate and characterize enemy jammers, they could be destroyed, avoided, and negated via adaptive, real-time filtering or otherwise defeated by other electronic protection tactics like increasing transmitter power. Regardless, it is evident that skill in electronic warfare lies at the heart of successful defense against link jamming attacks on space systems.

Like aircraft survivability, spacecraft survivability will likely hinge on the ability to gain superiority in electronic warfare. To ensure space system survivability in a contested environment, space operators will have to holistically employ an electronic warfare system of systems comprised of electronic jammers and electronic countermeasures designed to degrade and defeat enemy SOSI systems and terminal guidance sensors of antisatellite weapons; electronic support equipment to geolocate and characterize enemy link jammers so they can be destroyed or otherwise neutralized; and electronic protection capabilities to defeat electronic attacks on

friendly satellites. If the United States wants to protect its satellites in a contested space environment, it is paramount to achieve superiority in the corresponding electronic warfare battle. Yet, despite the centrality of electronic warfare to defensive space control operations, few Air Force space operators have any training in the fundamentals of electronic warfare, and those who do typically have only an introductory level of knowledge or a very specialized set of training centered on link jamming rather than breaking the kill chain of adversary counterspace capabilities, the center of gravity of which is radar.

Conclusion and Recommendations

Fortunately, this shortfall in electronic warfare education and training for space operators can be readily alleviated. Several potential courses of action exist that could address the deficiency of the Air Force's space operations cadre in electronic warfare skill. First, the introductory electronic warfare course currently taught at the Advanced Space Operations School could be expanded to more fully address electronic warfare in relation to radar and electro-optical/infrared sensors that form critical parts of potential adversaries' counterspace kill chains. Alternatively, this introductory electronic warfare course could be folded into Undergraduate Space Training to ensure that all space operators possess a basic level of electronic warfare knowledge from which to develop effective defensive space control capabilities, tactics, techniques, and procedures. Third, response to electronic attack should become a focus area of initial weapon system qualification training for space operators as well as a focus area of recurring training and exercises. Finally, and perhaps most importantly, AFSPC should consider developing a cadre of space electronic warfare officers (EWO) who attend the relevant portions of the Air Force's initial training for its rated combat systems officers and EWOs. A logical group to form this cadre would be the space weapons officers, and the most logical time to receive this training would be immediately prior to attending the Space Weapons Instructor Course. This space EWO cadre should be developed with the view that over the long term, space EWOs should make up the majority, if not the entirety, of the space operations career field.

Space operator education and training historically has been rooted in conducting routine spacecraft flight operations and executing emergency procedures in response to satellite malfunctions. In the contested space environment the Air Force now faces, planning and executing electronic warfare operations absolutely must become a space operations core competency on par with traditional flight safety tasks. If the Air Force's space leaders and operators are not prepared to fight and win in electronic warfare, the tremendous war-fighting advantages that the US military enjoys from space will be at grave risk. ✪

Notes

1. Lee Kennett, *The First Air War: 1914–1918* (New York: Free Press, 1991), 220.
2. Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report* (Washington, DC: Office of the Secretary of the Air Force, 1993), 199; and Carl Conetta, Project on Defense Alternatives Briefing Memo no. 30, subject: Catastrophic Interdiction: Air Power and the Collapse of the Iraqi Field Army in the 2003 War, 26 September 2003, 2, http://www.comw.org/pda/fulltext/0309bm30.pdf.
3. Lt Gen T. Michael Moseley, *Operation IRAQI FREEDOM—By the Numbers* (Shaw AFB, SC: USCENTAF, 30 April 2003), 6, 11, http://www.afhso.af.mil/shared/media/document/AFD-130613-025.pdf.
4. Alfred Price, *Instruments of Darkness: The History of Electronic Warfare*, new expanded and updated ed. (London: Macdonald and Jane's, 1977), 77.
5. Ibid., 81–86, 93–95.
6. Cited in Maj Greg A. Grabow, "Schweinfurt Raids and the Pause in Daylight Strategic Bombing" (master's thesis, US Army Command and General Staff College, 2008), 56.
7. Price, *Instruments of Darkness*, 163.
8. Ibid., 164.
9. Randall T. Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command* (Toronto: University of Toronto Press, 2009), 155.
10. Ibid., 139; and Price, *Instruments of Darkness*, 151–60.
11. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (signed at Washington, London, Moscow, 27 January 1967), Art. II, US Department of State, accessed 14 October 2015, http://www.state.gov/t/isn/5181.htm.
12. Colin Clark, "Chinese ASAT Test Was 'Successful': Lt. Gen. Raymond," *BreakingDefense*, 14 April 2015, http://breakingdefense.com/2015/04/chinese-asat-test-was-successful-lt-gen-raymond/; and Leonard David, "China's Anti-satellite Test: Worrisome Debris Cloud Circles Earth," Space.com, 2 February 2007, http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html.
13. Cited in Maj Brian Garino and Maj Jane Gibson, "Space System Threats," in AU-18, *Space Primer*, prepared by Air Command and Staff College Space Research Electives Seminars (Maxwell AFB, AL: Air University Press, 2009), 276, http://aupress.maxwell.af.mil/digital/pdf/book/AU-18.pdf; and cited in Maj Dewitt Morgan III, "Space Power: A Critical Strength . . . and a Critical Vulnerability of the US Military," research report (Newport, RI: Naval War College, 10 May 2007), 11.
14. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: Office of the Secretary of Defense, 7 April 2015), 14–15, http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.
15. "Miniature Air Launched Decoy (MALD)," Raytheon, accessed 21 July 2015, http://www.raytheon.com/capabilities/products/mald/.
16. "High Speed Anti-radiation Missile Targeting System," US Air Force, 18 October 2007, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104602/high-speed-anti-radiation-missile-targeting-system.aspx.
17. "B-1B Lancer," US Air Force, 29 September 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104500/b-1b-lancer.aspx; and Capt Lauri Turpin, "Large Aircraft Infrared Countermeasures— LAIRCM," Pope Field, 2 May 2009, http://www.pope.afrc.af.mil/news/story.asp?id=123147362.
18. Curtis E. LeMay Center for Doctrine Development and Education, "Defensive Space Control," in "Annex 3-14, Space Operations," 19 June 2012, [4], https://www.doctrine.af.mil/download.jsp?filename=3-14-D34-SPACE-OPS-DSC.pdf.

Lt Col E. Lincoln Bonner, USAF

Lieutenant Colonel Bonner is commander of a space operations squadron at Aerospace Defense Facility–Colorado. He has also served as an airpower strategist at Headquarters Air Force and has held assignments as a space operator performing space-based missile warning and as a flight test engineer. He is a graduate of the Massachusetts Institute of Technology, the US Air Force Test Pilot School, Air Command and Staff College, and the School of Advanced Air and Space Studies—the Air Force's school for strategy. He holds a bachelor's and master's degree in aerospace engineering and is currently an Air University candidate for a doctorate of philosophy in military strategy.