What Happens If They Say No?

Preserving Access to Critical Commercial Space Capabilities during Future Crises

Lt Col Joseph Iungerman, USAF

In 2011 the *National Security Space Strategy* proclaimed that space was a "congested, competitive, and contested" domain. Since then, national security space professionals have paid considerable attention to the congested and contested aspects of the space domain. Alarmingly, despite the United States' dependence on commercial space capabilities for national security requirements, there has been little examination of the ways adversaries might influence commercial markets to obtain military advantages. Specifically, what would happen if US adversaries made the space and cyberspace business risks too great? Although some might find that concept outlandish, it is a plausible threat that warrants consideration. If the US government fails to prepare for such contingencies, the White House could lose decision and command and control (DC2) capability if worried vendors say no to the nation that needs them.

Why Would They Say No?

It is a simple business truth—the commercial space operators who augment US national space capabilities do so to generate revenues and other business opportunities that are "good for business." National security space professionals ignore this and assume that commercial

space operators will always be willing to offer their capabilities to Washington despite significant space and cyberspace risks. Instead, they mistakenly assume that commercial space operators universally view the loss of government service purchases as "bad for business" and they will tolerate great risks to avoid those losses. Although that was true previously, emerging market trends are diminishing that once considerable cachet. Space companies can tolerate losses of government business far better than they could ten years ago.

Currently, the US government relies on commercial augmentation for at least 40 percent of its military DC2 requirements. These include such operational staples as high-resolution satellite imagery, unmanned aerial systems (UAS), and Blue Force Tracking (BFT). However, Washington's purchases generate less revenue than demand from the energy (natural gas and oil), land management (forestry and mining), and commercial communications (television, radio, and broadband) sectors.[1] Respectively, those sectors represent greater potential for business growth than sales to the US government—especially when one considers the dilemmas posed by shrinking government budgets over the next decade. In the commercial satellite communications sector alone, some estimates project opportunities for five to 15 percent growth while government purchases of similar services only represent opportunities for a maximum of five percent growth.[2] In many cases, it is no exaggeration that a number of commercial space operators need Washington less than it needs them.

Adversaries can exploit that disparity of need to limit America's access to commercial space capabilities by holding revenues and growth opportunities at risk during crises. Many adversaries can launch missiles, operate lasers, create jamming, or wage cyber attacks that can make the cost of doing business with the US government too high with relative ease.

What Threats Could Influence Them to Say No?

As previously stated, adversaries opposed to US interests can bring an impressive array of threats to bear against commercial space operators to make it too risky for them to do business with the US government during a crisis. For example, DigitalGlobe and Astrium Geo-Information Services provide imagery to the US government using remote sensing platforms in low Earth orbit (LEO). Those assets are vulnerable to direct-ascent antisatellite (DA ASAT) missiles like the SC-19 that China used to destroy its FY-1C satellite- and ground-based lasers that illuminated US reconnaissance satellites.[3] For companies like DigitalGlobe, operating satellites costing $300 million in LEO without protective capabilities, destruction of a satellite, or damage to an imaging sensor could jeopardize revenues they depend on for survival.[4] Faced with such threats to expensive revenue-generating assets, companies might "turn off," reorient imaging sensors during passes over certain areas, or curtail business with the US government.

Satellites in geosynchronous Earth orbit (GEO) or stationary orbits that support UASs and BFT are safe from ground-based DA ASATs and lasers but remain vulnerable to radio frequency interference (RFI), which is easy to cause. In some cases, a hostile actor only needs to own an authorized equipment suite like the kind sold by Hughes or Intelsat and operate it in an improper configuration to overpower uplink signals on a satellite.[5] An adversary might also opt to keep a satellite signal from reaching a user on the ground by operating downlink jammers from companies like C.T.S. Technology and Aviaconversiya Ltd.[6] Although the commercial satellite industry has means to deal with uplink interference, it can do little to protect paying customers from downlink jamming. Knowing these things, an adversary could potentially cause RFI against transmissions from satellites carrying US government users such that the interference disrupted other paying customers using the same spacecraft. If a commercial operator were unable to mitigate RFI, clients might take their business to competitors and a commercial operator might choose to drop US government traffic.

Adversaries can also use a variety of cyberspace capabilities to influence commercial space operators during crises. For example, Internet denial of service attacks can prevent companies from communicating with their clients. Adversaries can also deploy malware to disable satellite command and control infrastructure and route terrestrial communications, or they can opt for complex command intrusions to reconfigure satellite subsystems in space.[7] At the same time, adversaries can execute industrial espionage to expose sensitive client data, compromise intellectual property, and reveal business plans from commercial space operators' computer networks. Such actions could cause stock devaluations, a loss of business, and undermine competitive advantages.[8] Many of those actions have already occurred. Cyber miscreants have attempted command intrusions against the US Geological Survey's Landsat-7 and NASA's Terra satellites and absconded with sensitive satellite design data from US space companies.[9] In the future, those trends will likely continue in volume and severity.

Why Would an Adversary Want to Make Them Say No?

It makes strategic sense for adversaries to target commercial space operators supporting Washington during future crises. Inviting swift retaliation with a "space Pearl Harbor" against America does not make asymmetrical sense. Cutting off the United States from commercial space augmentation in a gradual fashion could allow adversaries to slow down the red, white, and blue juggernaut.[10] Adversaries with enough patience could use the same methods to achieve larger strategic goals and avoid serious confrontations with the United States altogether.

For example, keeping commercial assets in LEO from imaging events in areas like the Ukraine and Sudan can limit the ability to justify sanctions or military actions against aggressors. As the Pentagon and Foggy Bottom struggle, hostile forces can take advantage of those delays to force native people off their lands, seize mineral wealth, and solidify territorial claims.[11] Meanwhile, interfering with commercial assets in GEO that support UASs would allow adversaries to limit a com-

batant commander's (CCDR) situational awareness in key areas like the East China Sea or the Straits of Hormuz.[12] If the United States did manage to observe aggressive acts, adversary interference could disrupt BFT and undermine large-scale distributed logistics needed to muster a response force to counter adversary moves.[13]

The most attractive aspect of disrupting commercial space support of the United States for an adversary during a crisis is an opportunity to degrade Washington's DC2 advantages without creating casus belli.[14] The United States is not required to retaliate for laser illumination of a commercial spacecraft that keeps it from sending imagery to an Air Force Eagle Vision platform.[15] Similarly, there is no obligation to respond to adversary-generated RFI against satellite links that support UAS and BFT.

In contrast, commercial space operators have contractual obligations to the customers paying premium rates for satellite services and to the investors who derive benefit from the value of those sales. Interference targeted against commercial space operators for doing business with Washington represents serious threats to company revenues. If the US government does not understand this or is unwilling to respond to such interference, commercial space operators might not have any recourse but to restrict or terminate their business with Washington in order to protect themselves.

Are There Precedents for Saying No?

Companies like Eutelsat, Intelsat, and Nilesat have dropped state-sponsored content from Russia, Iran, and Syria. They responded to world tensions caused by Moscow's forays into Georgia, Tehran's nuclear program, and the Arab Spring abuses in Damascus.[16] Those actions show that commercial satellite operators are willing to deny services to governments in the interest of preserving business with other clients. However, it is hard to consider those examples as precedents for the issues at the heart of this paper. None of those companies refused their

services to a government because they feared an adversary would target their businesses.

While the commercial space industry currently offers no historical precedent for those types of concerns, another industry does. For years, commercial augmentation has been essential to the United States' strategic force projection capability—particularly regarding long-range airlift. As with commercial space, the United States relies on the commercial sector for 37 percent of the long-haul airlift for rapid force projection capability, responses to crises, and delivery of aid to foreign partners. During the twilight of the Nixon administration, the situation was very much the same, but the White House's access to those capabilities suffered in the face of world tensions.[17]

In October 1973, Soviet-backed Arab forces attacked Israel across the Golan Heights and the Sinai Peninsula during what became known as the Yom Kippur War. As Israeli forces suffered terrible losses, Arab forces closed in and pushed the Jewish state to the edge of defeat.[18] Golda Meir's government called for resupply to their forces, and President Nixon expected to do so with a commercial airlift. Commercial flights would not disrupt the withdrawal of US forces from Southeast Asia or exacerbate tensions with the Soviets or oil-producing Arab states.[19]

To Washington's chagrin, American companies refused to place their planes, personnel, and profits at risk when the White House and Pentagon called on them. Companies feared that Arab states would drive up fuel prices, cut them off from transit routes, and contribute to increased air piracy that would undermine their bottom lines.[20]

As a result, Pentagon planners had to reallocate strategic airlift forces from the drawdown in Southeast Asia to support the Operation Nickel Grass (ONG) resupply of Israeli forces. Arab forces used the delay to inflict heavy losses on Israeli forces and secure territorial gains. Washington had no way to provide desperately needed aid to a key ally during a crisis because it had no plan to help the commercial sector offset risks associated with helping the White House during a crisis.

The basic lesson from ONG should speak loudly to national security space professionals. Despite Washington's cachet as a customer, American companies have refused to help when adversaries threatened business operations. It is simply a matter of time before the threat of adversary interference drives commercial space operators to do what their air cargo cousins did in 1973.

What Can We Do to Keep Them from Saying No?

Air Force Space Command (AFSPC) has an array of capabilities that could help commercial space operators overcome interference by an adversary.[21] However, it will be necessary to do more than ad hoc taskings of AFSPC units to deal with interference or to nominate important signals and networks for placement on a CCDR's defended asset list. In the future, the command will need to change how it interacts with commercial space operators fundamentally.

First, AFSPC needs to develop space and cyber professionals with a broader range of expertise than recent science, technology, engineering, and mathematics (STEM) recruitment efforts produce. In the future, it will not be enough to have a space and cyberspace workforce that understands the technical intricacies of space systems and their associated ground networks but knows little about the business operations behind them. AFSPC should consider adopting a "STEM-B" recruiting strategy that brings personnel with technically oriented business degrees into the space and cyber workforce. Further, once the command recruits those personnel, it needs to do a better job of tracking and utilizing them in the selection process for advanced academic degree programs.

To that end, AFSPC should create a commander's industrial research initiative (CIRI) to spur research into critical business matters that affect space. Shrinking headquarters staffs do not and will not have time or resources for that research. Under a CIRI, AFSPC could competitively select space and cyberspace personnel for attending the Air

Force Institute of Technology, National Intelligence University, Air Command and Staff College, and Air War College. These people should work on space industrial research topics and then go to follow-on assignments to AFSPC, Fourteenth Air Force, or Twenty-Fourth Air Force headquarters to put their research to practical use. To keep those officers' skills honed, the final element of CIRI would be a short-duration internship during the follow-on assignment to deepen their understanding of market forces and technical issues.[22]

AFSPC also needs to work with US Strategic Command (USSTRATCOM) for inclusion of threats to commercial space in the latter's 8000-series contingency plans.[23] Currently, it is not clear how much of those plans are applicable to commercial space operators or to the capabilities AFSPC and USSTRATCOM can use to protect them from targeted interference. There could be significant challenges under US Code Title 10 and Title 50. These define how AFSPC can use capabilities to protect terrestrial networks used by commercial space operators inside the United States. There could be liability concerns if the Pentagon used space and cyber capabilities to protect a commercial space operator and caused collateral damage in the process. The only way to address those challenges is to begin planning for them now. Failure to do so places the nation at risk of experiencing the same dilemma that occurred during ONG. Without meaningful plans to address threats directed at their business interests, commercial space operators will be no more likely to support the United States during future crises than the commercial air transport industry was in 1973.

With plans developed, they must be tested and evaluated, and AFSPC should work with USTRATCOM to create short-sprint exercises to test planning assumptions, courses of action, and authorities for critical commercial space capabilities. Ideally, such exercises would use industrial relations findings developed during AFSPC's "Schriever Wargames" and the National Reconnaissance Office's (NRO) "Thor's Hammer" war game." Commercial space operators need to be involved.[24]

Currently, industrial partners rarely participate in recurring exercises like Global Lightning and Global Thunder for a variety of security and procedural reasons. The same is also true for the Defense Information Systems Agency, the National Geospatial-Intelligence Agency, and at least five other federal agencies that act as the primary liaisons between the Department of Defense and commercial space vendors.[25] Because of that, personnel at the Joint Space Operations Center and US Cyber Command operations centers do not get the benefit of training with commercial representatives they would call for support during a conflict. Further, the infrequent participation of key federal agencies in recurring exercises means AFSPC and USSTRATCOM rarely get to evaluate how those organizations will fit within a joint interagency coordination group (JIACG) in a crisis. That kind of training needs to start happening as soon as possible. It will be too late to figure out how to preserve commercial augmentation after a crisis begins, and an adversary has already started interfering with commercial space operators.

Finally, AFSPC needs to organize better to facilitate its access to commercial space partners and their respective capabilities, which adversaries will likely target. AFSPC should organize an operations-focused commercial capabilities office (CCO) at the numbered air force level. The CCO would facilitate real-time information sharing, ease requirements updates, disseminate warnings of interference, and coordinate AFSPC and USSTRATCOM plans and responses.[26] Industry partners have asked the Pentagon to set up similar entities.Those efforts faltered for bureaucratic reasons or were diluted because they were formed under the auspices of obscure working groups better suited for policy development than for operations.[27] AFSPC should take the lead to reverse those trends and set up CCOs that can facilitate real-time interactions with commercial space operators and the operations centers and coordinate with intelligence community organizations such as the NRO Operations Center.

Conclusion

In the future, as the United States' dependence on commercial space capabilities increases, adversaries will be inclined to drive a wedge between the White House and the commercial space operators it depends on for DC2. Adversaries will want to make it too risky for commercial space operators to offer capabilities to the United States. If they succeed, the White House and the Pentagon might not be able to take decisive action. National security space professionals that AFSPC recruits and fosters need to reconsider current relationships with commercial space operators and better understand the business interests that drive them. With those space professionals, AFSPC and USSTRATCOM should develop plans to mitigate threats to commercial space partners. In addition, AFSPC must help test those plans and organize space and cyber professionals to support critical commercial space partnerships. Without these efforts, commercial space operators will have little reason to accept the business risks associated with helping the United States during a crisis. ✪

Notes

1. Sandra I. Erwin, "Satellite Shortages May Choke Off Military Drone Expansion," *National Defense*, April 2013, http://www.nationaldefensemagazine.org/archive/2013/April/Pages/SatelliteShortagesMayChokeOffMilitaryDroneExpansion.aspx; G. Ryan Faith and Mariel John, "Space Report 2011" in *Authoritative Guide to Global Space Activity*," ed. Micah Walter-Range (Colorado Springs, CO: Space Foundation, 2011), 14–15, 35–38, 42, 123–25; *2010 Futron Forecast of Global Satellite Services Demand Overview*, (Washington, DC: Futron Corporation, 2010); Satellite Industry Association, *State of the Satellite Industry Report* (Washington, DC: Futron Corporation, 2010 and 2012); and Defense Business Board, *Report to the Secretary of Defense: Taking Advantage of Opportunities for Commercial Satellite Communications Services*, Report FY 13-02 (Washington, DC: Department of Defense, undated). Although some industry estimates indicate the percentage of US government reliance on commercial space capabilities for decision and command and control requirements runs as high as 80 percent, this paper utilizes the lower end of the industry and government estimates for US government reliance on commercial capabilities. Even at the lower end of the estimates in current use, the concept that nearly half of the US government's space support requirements come from commercial sources is a significant planning consideration.

2. *2010 Futron Forecast of Global Satellite Services Demand Overview.*

3. Warren Ferster and Colin Clark, "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," *Space News*, 3 October 2006, http://www.spacenews.com/article/nro-confirms-chinese-laser-test-illuminated-us-spacecraft; Shirley Kan, "China's Anti-Satellite Weapon Test," Report RS22652 (Washington, DC: Congressional Research Service, 23 April 2007), http://fas.org/sgp/crs/row/RS22652.pdf; and Air University, *Space Primer*, AU-18 (Maxwell AFB, AL: Air University Press, September 2009), http://aupress.maxwell.af.mil/digital/pdf/book/AU-18.pdf, 276–77.

4. Peter B. de Selding, "DigitalGlobe Awards $307M in Contracts for WorldView-3 Satellite," *Space News*, 31 October 2010, http://www.spacenews.com/article/digitalglobe-awards-307m-contracts-worldview-3-satellite; Associated Press, "Longmont's Digitalglobe Gets Final Tests On Satellite," *CBS Denver*, 13 May 2014, http://denver.cbslocal.com/2014/05/13/longmonts-digitalglobe-getting-final-tests-on-satellite; and J. J. McCoy, "DigitalGlobe Orders WorldView 2 Satellite," *Via Satellite - Integrating SatelliteToday.com*, 3 January 2007, http://www.satellitetoday.com/telecom/2007/01/03/digitalglobe-orders-worldview-2-satellite/.

5. Robert Ames, "Satellite Interference; What It Means for Your Bottom Line," Kratos Integral Systems Service Solutions, Satellite Trends, undated, http://www.integ.com/IS3/whitepapers/SKTelecommNews.pdf; Giovanni Verlini, "New Efforts to Mitigate Satellite Interference," *Via-Satellite - Integrating SatelliteToday.com*, 1 March 2010, http://www.satellitetoday.com/telecom/2010/03/01/new-efforts-to-mitigate-satellite-interference; "World Broadcasting Union Adopts Carrier ID to Combat Satellite Interference," *TVTechnology*, 2 August 2013, http://www.tvtechnology.com/cable-satellite-iptv/0149/world-broadcasting-union-adopts-carrier-id-to-combat-satellite-interference/224999; and Air University, *Space Primer*, 274–77.

6. Jacob Kastrenakes, "FCC Issues Largest Fine in History to Company Selling Signal Jammers," *Verge*, 19 June 2014, http://www.theverge.com/2014/6/19/5824344/fcc-issues-signal-jammer-seller-largest-fine-ever-34-9-million; Bob Bewin, "U.S. Army Awarded Contracts to Russian GPS Jammer Vendor," *ComputerWorld*, 27 March 2003, http://www.computerworld.com/s/article/79783/U.S._Army_awarded_contracts_to_Russian_GPS_jammer_vendor; and Air University, *Space Primer*.

7. Mark Clayton, "Can Military's Satellite Links Be Hacked? Cyber-Security Firm Cites Concerns," *Christian Science Monitor*, 25 April 2014, http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0425/Can-military-s-satellite-links-be-hacked-Cyber-security-firm-cites-concerns; and Debra Werner, "Cover Story: Hacking Cases Draw Attention to Satcom Vulnerabilities," *DefenseNews*, 23 January 2012, http://www.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-Cases-Draw-Attention-Satcom-Vulnerabilities.

8. Leon Spencer, "Chinese Army Group Hacks US Satellite Partners: Crowdstrike," ZDNet, 10 June 2014, http://www.zdnet.com/chinese-army-group-hacks-us-satellite-partners-crowdstrike-7000030353.

9. Werner, "Cover Story"; John Walcott, "Chinese Espionage Campaign Targets U.S. Space Technology," *Bloomberg*, 18 April 2012, http://www.bloomberg.com/news/2012-04-18/chinese-espionage-campaign-targets-u-s-space-technology.html.

10. *Report of the Commission to Assess United States National Security Space Management and Organization [CAUSNSSMO]* (Washington, DC: CAUSNSSMO, 11 January 2001), 25, http://www.dod.gov/pubs/space20010111.html.

11. "Troops in the Demilitarized Zone; Confirmation of Violations by Sudan and South Sudan," Satellite Sentinel Project: Monitoring the Crisis in the Sudans, 2013, http://www.enough project .org/files/Troops-in-the-Demilitarized-Zone.pdf; Scott Neuman, "U.S.: Satellite Images Show Russian Rockets Hitting Ukraine," Two-Way: Breaking News from NPR, 27 July 2014, http://www.npr .org/blogs/thetwo-way/2014/07/27/335829570/u-s-satellite-images-show-russian-rockets-hitting -ukraine; and Tom Withington, "Space Paparazzi," *C4ISR Journal* 10, no. 3 (27 March 2011): 24–26.

12. Craig Whitlock and Anne Gearan, "Agreement Will Allow U.S. To Fly Long-Range Surveillance Drones from Base in Japan," *Washington Post*, 3 October 2013, http://www.washington post.com/world/agreement-will-allow-us-to-fly-long-range-surveillance-drones-from-base-in -japan/2013/10/03/aeba1ccc-2be8-11e3-83fa-b82b8431dc92_story.html; and Robert Johnson, "US Navy and Allies Showed Iran Who Really Controls the Strait of Hormuz," *Business Insider*, 27 September 2012, http://www.businessinsider.com/photos-the-us-navy-protects-the -gulf-2012-9?op=1; and Tony Capaccio, "Strait of Hormuz Attack Iran 'Last Resort,' Author Says," *Bloomberg*, 5 August 2012, http://www.bloomberg.com/news/2012-08-06/strait-of-hormuz -attack-iran-last-resort-author-says.html.

13. *AIT&ITV: Automatic Identification Technology and In-Transit Visibility*, US Transportation Command [USTRANSCOM], undated, http://www.transcom.mil/ait; Erwin, "Satellite Shortages"; Jeffrey Hill, "Blue Force Tracking System Upgrade Seen as Crucial," *Via Satellite - Integrating SatelliteToday.com*, 11 November 2008, http://www.satellitetoday.com/publications /eletters/military/2008/11/11/blue-force-tracking-system-upgrade-seen-as-crucial; Rick Lober, "Why the Military Needs Commercial Satellite Technology," *Defense One*, http://www .defenseone.com/technology/2013/09/why-military-needs-commercial-satellite-technology /70836/; and "Blue Force Tracking 2," *ViaSat.com*, https://www.viasat.com/government -communications/blue-force-tracking.

14. Although a debris-causing attack like a missile launch would likely generate a response based on the worldwide reaction to the Chinese SC-19 intercept of their FY-1C satellite, other publicly acknowledged attempts at interference—like the lasing of US reconnaissance satellites and attempted command intrusions on the Landsat-7 and Terra satellites—hardly evoked any public response from the US government.

15. Robert K. Ackerman, "Special Report—Commercial Eyes on the Battlefield Sharpen Focus," *Signal Online*, March 2001, http://www.afcea.org/content/?q=node/568; and Capt James A. Hartmetz, USAF, "Eagle Vision—Exploiting Commercial Satellite Imagery," *DISAM [Defense Institute of Security Assistance Management] Journal* 23, no. 4 (Summer 2001): 22—25, http://www.disam.dsca.mil/pubs/v.23_4/hartmetz.pdf.

16. "Iran's Press TV Taken Off Air in N America," Al Jazeera, 9 February 2013, http:// www.aljazeera.com/news/middleeast/2013/02/20132913263566603.html; Agence France-Presse, "Intelsat Blocks Iranian Channels in Europe," *RawStory*, 25 October 2012, http:// www.rawstory.com/rs/2012/10/25/intelsat-blocks-iranian-channels-in-europe/?onswipe _redirect=no&oswrr=1; Reuters, "Nilesat Stops Broadcasting Three Syrian Channels," *Egypt Independent*, 9 May 2012, http://www.egyptindependent.com/news/nilesat-stops-broadcasting-three-syrian-channels; and David Smith, "Satellite Saga" *New Atlanticist*, 23 July 2010, http:// www.atlanticcouncil.org/blogs/new-atlanticist/satellite-saga.

17. *USTRANSCOM Annual Command Report* (Scott AFB, IL: USTRANSCOM, 2012), 16, http://www.transcom.mil/documents/annual_reports/annual_report.pdf; *Airlift Operations of the Military Airlift Command During the 1973 Middle East War* (Washington, DC: US Government Accountability Office, 1975), http://www.gao.gov/assets/120/115367.pdf; and Maj

Thomas J. Riney, USAF, "Transforming Past Lessons to Mold the Future: A Case Study on Operation Nickel Grass," Graduate Research Project AFIT/GMO/ENS/03E-11 (Wright-Patterson AFB, OH: Air Force Institute of Technology, June 2003), http://www.dtic.mil/dtic/tr/fulltext/u2/a430910.pdf.

18. Abraham Rabinovich, *Yom Kippur War: Epic Encounter that Transformed the Middle East* (New York: Schocken Books, 2004). 175.

19. Nina Howland, Craig Daigle, and Edward C. Keefer, eds., *Foreign Relations of the United States [FRUS]: 1969–1976*, vol. 25, *Arab-Israeli Crisis and War: 1973* (Washington, DC: Government Printing Office, 2011), http://static.history.state.gov/frus/frus1969-76v25/pdf/frus1969-76v25.pdf; Walter J. Boyne, *The Two O'Clock War: The 1973 Yom Kippur Conflict and the Airlift That Saved Israel*, 1st ed. (New York: Thomas Dunne Books, 2002). 77–8; and Rabinovich, *Yom Kippur War*, 24, 323, 491.

20. Howland, Daigle, and Keefer, *FRUS: 1969–1976*, vol. 25, *Arab-Israeli Crisis and War: 1973*; Boyne, *Two O'clock War*; and Rabinovich, *Yom Kippur War*.

21. 21st Space Wing, "Fact Sheet: 16th Space Control Squadron," http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=8403; AFSPC, "Fact Sheet: Air Force Cyberspace Defense Weapon System," http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20871; AFSPC, "Fact Sheet: Air Force Cyberspace Defense Analysis Weapon System," http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20873; and AFSPC, "Fact Sheet: Air Force Cyberspace Vulnerability Assessment/Hunter Weapon System," http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20874. This list is not all-inclusive.

22. Due to staffing limitations, high organizational workloads, and cost concerns, internships probably should not last longer than two to three months and should be limited to opportunities with companies that reside in the same geographic area where the officer is assigned.

23. Chairman of the Joint Chiefs of Staff Manual 3130.03, *Adaptive Planning and Execution (APEX) Planning Formats and Guidance*, 18 October 2012, A-5. Personnel developed under a commander's industrial research initiative would be ideally suited for participation in joint planning working groups formed to develop, revise, and test planning assumptions and courses of action to preserve the nation's access to commercial space capabilities during a crisis

24. House, *Statement of Gen Keith B. Alexander, Commander, United States Cyber Command: Hearings before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities*, 112th Cong., 2d sess., 20 March 2012, 17, http://www.au.af.mil/au/awc/awcgate/postures/posture_cybercom_20mar2012.pdf; and Robert S. Dudney, "Hard Lessons at the Schriever Wargame," *Air Force Magazine* 94, no. 2 (February 2011), 88–89, http://www.airforce -magazine.com/MagazineArchive/Documents/2011/February%202011/0211wargame.pdf.

25. This passage considers the Federal Communications Commission, Federal Aviation Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, the National Aeronautics and Space Administration, and the Department of State's various space and arms control offices. As a contingency planner within US Strategic Command's Joint Functional Component Command for Space (JFCC-Space) and as a Headquarters Air Force staffer, the author has considerable firsthand experience with regard to interactions with commercial partners during exercises. The author of this paper also organized the JFCC-Space role in Schriever Wargames IV, V, and X as well as the Unified Engage-

ment Wargames that utilized the space and cyberspace game scenarios from Schriever Wargames V and X. The author also participated in Schriever Wargame XII as a member of the HQ AFSPC staff. Although game scenarios examine a wide variety of concerns, they do not normally explore underlying business concerns that affect the concerns of commercial space operators that augment national US capabilities. To explore such issues in depth, specific focus sessions are required before the main game events transpire.

26. The benefit of placing such an office at the numbered air force level is that each numbered air force has an operations center that commands and controls operations in support of a joint force commander. Placing the office at the staff level instead of within the operations center itself can alleviate many security and proprietary data concerns in the hectic environment of an operations floor and still offer close proximity to personnel commanding and controlling space and cyberspace operations.

27. Werner, "Cover Story."

Lt Col Joseph Iungerman, USAF

Lieutenant Colonel Iungerman (BA, Rider University; MS, National Intelligence University; MBA, Touro University International) is the executive officer for Air Force Space Command's Directorate of Programming and Financial Management. He is a joint-qualified space officer with previous operational experience as a contingency planner with the Joint Functional Component Command for Space, an intelligence analyst at the National Air and Space Intelligence Center, and a missile combat crewman with the 91st Missile Wing.