Deterring Aggressive Space Actions with Cube Satellite Proximity Operations

A New Frontier in Defensive Space Control

Capt Michael Nayak, USAF, PhD*

Today, America's strategic advantage and military superiority are critically codependent on its space superiority.[1] Space-based systems provide critical information, intelligence, warning, and communication capabilities to commanders and warfighters across the spectrum of global conflict. As the reliance of the military enterprise on the effective use of space power grows, top leaders are consistently sounding the warning bell about a growing vulnerability to hostile action.[2] Calling the US dependence on space its "soft ribs," one Chinese analyst writes, "for countries that can never win a war with the United States by using [. . .] tanks and planes, attacking the U.S. space system may be an irresistible and most tempting choice. Part of the reason is that the Pentagon is greatly dependent on space for [. . .] its military action."[3] It is, therefore, no surprise that countries such as China, Russia, and India have chosen to aggressively invest in counterspace capabilities.[4]

Within this operating picture, it is vital to note the considerable recent progress of nanosatellites called *Cube Satellite* or *CubeSat*-sized spacecraft. A standard 1-unit (U) CubeSat form factor is 10 cm x 10 cm x 10 cm in dimensions, 1 liter in volume, and weighs approximately 1 kg in mass.[5] The number of CubeSat segments designates system size; a 10 x 10 x 30 cm system is a 3U, and a 10 x 20 x 30 cm system is a "6U" CubeSat, roughly 3 and 6 liters in volume respectively. Developed in the 1990s to train students in real-world satellite integration and testing, government and private entities have launched more than a thousand CubeSats.[6] Science requirements for sophisticated instruments, communications, propulsion, and three-axis

*This work is adapted from two other works by the author, "Cube-Satellite Proximity Operations: The Natural Evolution of Defensive Space Control into a Deterrence Initiative," published in *The Space Review* 18 January 2016; and "Fighting a War in Space: An Unusually Careful Selection of Staff," (in journal review as of October 2017) in *Astropolitics*.

stabilization have been demonstrated.[7] The commercial utility of CubeSats are increasing exponentially; the firm Planet Labs has launched more than seventy 3U CubeSats for responsive earth imaging.[8]

Extrapolating the explosive growth of satellite system miniaturization to a national security context, CubeSat systems are easier for adversarial nations with less sophisticated space programs to design, build, and launch. In considering the question of what the United States should do to better prepare to deter aggressive action in space, an active deterrence strategy to effectively combat small satellite-enabled hostile actions is of vital importance. In parallel with the development of new deterrence strategies that consider small satellites,[9] taking immediate steps to direct integration of CubeSat technologies into the US military space enterprise can help the United States respond proportionally and prevail should deterrence fail.

The Threat from Nations with Less Advanced Space Programs

In less than a decade, space miniaturization technology has come so far that students at a high-school level of education are now capable of designing, integrating, launching, and operating CubeSat systems.[10] Some university-designed systems boast sophisticated maneuvering and navigation capabilities and are capable of advanced military-relevant mission sets.[11] From a doctrinal and policy point of view, it is important to consider that CubeSat systems are far easier for nations with less sophisticated space programs to design, build, and launch. The price of failure in the small-satellite industry is less, making incremental growth more practicable. With the elimination of a need for heavy space lift and triple-redundant systems, it is almost certain that adversarial nations with smaller space programs can soon assemble and field capabilities they are today incapable of. It is feasible that within the next decade, we will see North Korea fielding a surveillance capability via a crude optical sensor on a CubeSat, in competition with South Korea, which is today developing a CubeSat-based telescope system.[12] Equally probable is Iran fielding a rudimentary missile warning system onboard a vehicle similar to the "Promise of Science and Industry" national satellite, recently built by Iranian university students and launched atop a modified long-range missile.[13]

Although systems centered on smaller spacecraft may not be as reliable, these development efforts prove that the technology is both mature and accessible. Today's clumsy student satellite feeds tomorrow's "wisdom of experience." Today's school-bus sized communication spacecraft (for example, the MUOS, the Mobile User Objective System) will tomorrow be the size of a shoebox (for example, lasercom on LADEE, the Lunar Atmosphere and Dust Environment Explorer).[14] Combining easy fabrication with access to space via ride-shares, small satellites are becoming a force to be reckoned with. At the rate of current development, the United States might find some of its actions or objectives deterred by the capabilities of its adversaries in the near future.

As it stands today, an adversary with basic space lift capability may be able to deny, disrupt, or degrade the US military enterprise by striking a few centers of gravity (COG) of space power that fulfill a critical defense or military enabling function.

This can be accomplished either through a direct-ascent antisatellite (ASAT) weapon, or a co-orbital ASAT weapon, where a satellite is placed into a similar or intercepting orbit as its target, and then maneuvered into a collision course with it. This threat dates back to the Cold War and the USSR's *Istrebitel Sputnikov* program.[15] Translated as *satellite killer*, the program focused on satellites capable of large maneuvers to rendezvous with their targets, prepositioned to execute a "kamikaze-style" takedown of US space systems if and when commanded.[16]

One immediate deterrent to hostile space action is therefore to distribute the US concentration of space power, lessening the reward for hostile action. Fielding duplicate, redundant systems to those in existence is unrealistic in a fiscally constrained environment. Distributed or disaggregated systems, on the other hand, are intrinsically less vulnerable. Since the capability is exerted through a larger number of redundant component parts, multiple component satellites can be lost before total system failure. The exploding growth of CubeSats, which have a reputation for being low-cost and easily reproducible, has a natural place in this discussion.[17]

While there are definite cost and size advantages to CubeSats, they are also significantly less capable than larger spacecraft, particularly in military applications. Larger spacecraft can lose multiple components and still have backup functionality. They host larger instruments better capable of fulfilling primary military functions. CubeSats are largely "single-string," not robust to single-point failure, and are size- and volume-limited in the instrumentation they can host. They are simply not a factor in signals intelligence, hyperspectral collection, or protected survivable secure communications. While they can fill a complementary role in ground-based imaging and imagery intelligence collection, larger optics, wider wavelength bands, and the need for cryocooling will always point in the direction of larger spacecraft.

The forte of CubeSats appears to be in the "numbers game." Even in the absence of direct conflict, a disaggregated system allows for cost and efficiency benefits in acquisition and operations. Such systems are resilient by nature. A distributed systems architecture serves to eliminate the US dependence on finite COGs of space power; with multiple systems in play, the payoff for an attack lessens. Therefore, in an environment where any small satellite in a similar orbit to a national security asset could be a potential ASAT threat, American space policies must ensure that capabilities in this arena are not left behind.

However, military space acquisition policy and business practices are both behind the times. Although policy papers by recent space acquisition leaders lean in favor of disaggregation, there has yet to be a push to implement this through enterprise leverage of small-satellite technology.[18] The only US government organizations actively involved in CubeSat development are either doing so for research and development (R&D) or because of cost constraints; the resolve to make small satellites a part of our national space architecture is simply not present. However, these systems are set to become an integral part of every other space-faring nation's military capability, likely within the next generation.

Therefore, there is an immediate need for decisive leadership action to focus US space acquisitions and operations into smaller, more agile systems, and more importantly, transition these capabilities into the mainstream "operational" space industry directly benefiting the warfighter. This will drive a strategic investment that will reduce the risk to space COGs. It will also support direct integration of small satellite technology into the national space enterprise, both military and civilian. Deploying mature technologies in parallel with ongoing R&D efforts for further development can help the United States widen the conversation on possible proportional and reciprocal dissuasion of enemy counterspace action, and preserve the "ultimate high ground" of space.

Applications of Cube Satellite Technology to Space Control

Any hostile action against a US spacecraft is considered tantamount to a declaration of war.[19] However, in reality, the distance of and limited access to space provides anonymity to offensive space actions, similar to cyber attacks. It is more likely that to maintain regional superiority, adversarial nations would seek to develop a denial of service counterspace capability against the United States. A satellite malfunction could be caused by space environment conditions, faulty, or inadequate satellite design, or even orbital debris factors.[20] Culpability, attribution, and retaliation are complicated by the lack of borders or sovereign regions in space and the infeasibility of total space situational awareness (SSA). This adversary may, therefore, be able to deny, disrupt, or degrade the US military space enterprise while maintaining plausible deniability. The uncertainty involved increases exponentially if hostile CubeSats are deployed as co-orbital ASAT devices. A low-velocity impact can be engineered to have just enough speed to shatter the impactor, causing disabling damage to the target, and leaving relatively little debris.

However, this is the crudest use of CubeSat technology as a counterspace tool. Rendezvous and proximity operations (RPO) are the ultimate tools for space surveillance, advanced space-based SSA, and even offensive action. In 2005 and 2007, respectively, the United States proved an experimental RPO capability with missions such as the Air Force Research Laboratory's XSS-11 and the Defense Advanced Research Projects Agency's Orbital Express.[21] While Orbital Express was more than 1,000 kg in mass and fielded two spacecraft that were aware of each another, XSS-11 was 150 kg and demonstrated advanced maneuvering around its own spent upper stage. It demonstrated the capability to safely approach an "uncooperative" object, image it, and retreat to a safe distance.

Small satellites in space control are not a near-future scenario; rather, they are today's emergency. China has developed a small satellite reputedly able to capture another satellite with a robotic arm.[22] Published work by US academic authors discusses the concept and ongoing design of a CubeSat-sized RPO mission, with precise attitude determination and control, pointing accuracy, real-time maneuver commanding, and even optimal trajectory design for docking applications from a future CubeSat platform.[23] A 10–25 kg (12U) CubeSat with optical sensors and agile maneuvering capability is a configuration that is easily achievable with today's technology; such vehicles have a negligible radar cross-sectional area. In geostationary orbit, they would be invisible from the ground.

Further, the delivery system for CubeSat is easily configurable. CubeSats can be released from stowed configurations designed to ride along with any launch vehicle.

Launch options include hosted payload services, a quickly growing industry that government payloads have utilized as secondary missions on commercial communications satellites. These payload services provide numerous launch opportunities per year to any desired orbit regime. This has even expanded to the commercial sector; international telecommunication satellites, as well as national security satellites, have demonstrated the capability to host CubeSats.[24]

As this technology becomes smaller and easier to launch, the detectability factor significantly decreases, which would allow adversaries to take autarchic actions against the US space enterprise with a lessened fear of retribution or discovery. One example is the Russian object 2014-28E. Initially thought to be drifting space junk associated with the launch of three Russian telecommunication satellites, it has since been observed to be maneuverable, and made a close approach to the rocket stage that boosted it into orbit as recently as November 2014.[25]

Apart from *satellite killer*, another translation of *istrebitel sputnikov* is *satellite fighter* (*istrebitel* translates as *fighter aircraft*). The big push in next-generation fighter aircraft is stealth, and it is not unreasonable to refer to small satellites as the stealth aircraft of space. The existence of 2014-28E was not announced, and the smaller the spacecraft, the less the probability of ground-based detection. If sensor avoidance techniques are employed during an approach, the target object may not ever detect another satellite in its local space.[26] Cumulatively, this reduces the culpability for space control actions, emboldening adversaries to move past proximity surveillance to offensive actions. . . all from a CubeSat platform.

RPO-capable CubeSats have the potential to be of critical importance to spaceborne intelligence gathering. They are capable of close approaches, surveillance, functionality, and material characterization, and battle damage assessment, all with a minimal fear of discovery. Even if discovered, close approaches are legal if they do not endanger the operation of the target body. Sociopolitical ramifications are likely inside a certain approach distance, but this is a gray area without much legal precedent or policy backing.[27]

This expanded reach of space-borne space control is the true jump in capability presented by burgeoning CubeSat technology. Never before has there been the capability for a force so large to be wielded from a body so small. CubeSats are poised to become the stealth aircraft of space technology. A nation capable of wielding a CubeSat-based offensive space control capability creates a real and present threat to US space superiority. This article will next address what the United States can do to deter aggressive action in space concerning this threat, and prevail should deterrence fail.

Combating the Threat of Hostile Cube Satellite Actions

One of the key factors for successful deterrence is the criterion of "proportionality, reciprocity, and coercive credibility." The more superior a nation's available instruments to inflict harm, the larger costs for non-compliance it may credibly impose.[28] The dissuasion of enemy escalation is accomplished by the threat of progressive retaliation, discouraging the enemy from an initial action.[29] The political will to exert this response is never in doubt.[30] The concept of proportionality drives the US's retaliatory action, but in the arena of space deterrence, each unique attack requires a unique response.

Three steps of escalating response and consequence are detailed below, derived from principles of force protection conditions (FPCON).[31] The proposed staged strategy ensures that the US response is proportional to the existing threat while maintaining both strategic advantage and technological superiority.

The base of the CubeSat threat pyramid may be considered to be FPCON Alpha, where there exists "a general threat of possible terrorist activity, the nature and extent of which is unpredictable."[32] This translates to no known deployment of RPO capability by an adversarial nation or RPO missions in a first-time R&D regime only. Given this threat level, a security posture of deterrence through ground detection and observation is proportional and must be capable of being maintained indefinitely. Methods currently utilized today, such as the Space Fence, the Space Surveillance Network, and the Space-Based Space Situational Awareness system are able tools for maintaining this ability to attribute.[33]

The next level on the CubeSat threat pyramid is FPCON Bravo, when "an increased and more predictable terrorist threat activity exists."[34] The threat increases when specific intelligence suggests the capability for possible aggression by a particular nation and is realized when there is a known, operational RPO capability beyond the first-time R&D phase. If an adversary is aware that their technology is sufficiently advanced that it may be able to attack and escape undetected, this can create an incentive to act. Dissuading an adversary nation from exercising mature RPO capabilities requires an escalation in the US's ability to detect and respond to such an action. Amputating the veil of invisibility around co-orbital RPO CubeSats can have a sizable impact on the political will to act. The small size and detectability of inbound CubeSats imply that ground-based SSA is likely inadequate to accomplish the objective of dissuasion by detection. The onus for deterrence falls on the shoulders of space-based SSA mission sets.

The implementation of a similar policy can be inferred with regard to recent news reports concerning the GEO Space Situational Awareness Program (GSSAP).[35] GSSAP mission sets were announced to the world by then-USAF Space Command head Gen William L. Shelton. [36] "GSSAP will bolster our ability to discern when adversaries attempt to avoid detection," General Shelton said at the 2014 Air Warfare Symposium, "and to discover capabilities they may have which might be harmful to our critical assets."[37]

The protection of space assets in the event of more direct threats is the final level on the threat pyramid and has larger geopolitical consequences, including impacts to warfighters in harm's way. Nations with less accomplished space programs are capable of developing CubeSat technology; these nations are also less likely to adhere to the classic psychology of deterrence. The threats become more diverse and immediate as well: for example, command of a co-orbital satellite could be assumed by cyber-offense, at which point it becomes an unintended ASAT weapon.[38] Alternately, a known CubeSat could have an alternate purpose and later exploit holes in US detection capabilities to maneuver into a new orbit. By the time this satellite is reacquired, it could have caused harm to a high-value asset. To assign attribution, respond proportionally, and deter this kind of threat, the United States must be able to characterize the motion, intent, and capability of inbound CubeSats, assign attribution, and avoid imminent harm to space COGs, all in a responsive manner.

Enabling the full awareness of local space in the vicinity of a high-value asset can ensure that any object, even CubeSat-sized, will be detected and characterized. The United States must, therefore, make a concerted effort to develop CubeSat RPO technology for utility in the operational realm, exert deterrence by possession of such space control capabilities, and employ these RPO-capable CubeSats in a defensive posture to perform proximity operations around high-value assets and monitor their local space. If justified and directed, interception attacks by the RPO "guardian" CubeSat may even be needed to ensure the safety of the asset.

Guardian CubeSats designed for RPO can ensure the safety and sanctity of local space, while simultaneously performing as a contributing sensor yielding information to global SSA systems. Designed for passive, autonomous proximity operations, such CubeSats would not interfere with the primary asset's mission. The presence of a responsive communication link between the Guardian and its high-value asset gives the COG sufficient time to maneuver out of the way of an interception. The Guardian would also be able to image the interceptor, perform orbital tracking, deliver responsive intelligence regarding the source of the attack, and provide a post-event battle damage assessment. This is apart from the deterrence aspect: the protective security function of the Guardian, the high likelihood of failure for hostile actions and subsequent negative consequences combine to dissuade the adversary from ever attempting the action. Critically, they also provide the United States the ability to respond to such an attack in a timely and proportional manner.

Conclusion

The natural evolution of a guardian paradigm becomes a truly revolutionary change to the status quo. Once the capability is established, and policy favors their continuous and rapid employment, deterrence becomes a function of uncertainty. In this scenario, Guardians are not deployed as continuous orbiters, but rather, "on demand." Designs exist for ride-along CubeSats within the spare storage space aboard commercial telecommunications satellites;[39] high-value assets could be similarly adapted to fit not one, but multiple RPO-capable CubeSats within their volume. In response to an increased threat or intelligence hinting at an impending attack, the high-value COG can deploy its Guardians to assess local space, determine threats, ensure safety, and provide responsive battlespace awareness. Deterrence by uncertainty can be achieved when adversarial nations are unable to determine if a particular target may (or may not) be hosting protector CubeSats within its volume. With the knowledge that these Guardians are RPO-capable, autonomous, and responsive to threats, the risk to invade the local space of a high-value asset will become too high to justify action, thus preparing the nation to deter aggressive action, while maintaining readiness to deflect an attack should deterrence fail. ✪

Notes

1. Michael Nayak, "CubeSat Proximity Operations: The Natural Evolution of Defensive Space Control into a Deterrence Initiative," *Space Review*, 18 January 2016, http://www.thespacereview.com/article/2902/1, 1–2.

2. *SPACENews* Editor, "Intelligence Director Cites Threats to U.S. Satellites," *SPACENews*, 10 February 2014, http://spacenews.com/39437intelligence-director-cites-threats-to-us-satellites/; Douglas Loverro, "Commentary: Space Resilience, Deterrence, Fast Ships, and Harm's Way," *SpaceNews*, 26 May 2014; and Mike Gruss, "U.S. Space Assets Face Growing Threat From Adversaries, STRATCOM Chief Warns," *SpaceNews,* 26 February 2014, http://spacenews.com/39669us-space-assets-face-growing-threat-from-adversaries-stratcom-chief/.

3. Wang Huacheng, "The US Military's 'Soft Ribs' and Strategic Weaknesses," *Liaowang* 27, reprinted in *Xinhua Hong Kong Service*, 5 July 2000, in FBIA—CHI—2000—0705.

4. Ashley J. Tellis, "China's Military Space Strategy," *Survival* 49, no. 3 (1 September 2007): 41–72, http://dx.doi.org/10.1080/00396330701564752; Jana Honkova, "The Russian Federation's Approach to Military Space and Its Military Space Capabilities," *George C. Marshall Institute Policy Outlook* 2013, http://marshall.org/wp-content/uploads/2013/11/Russian-Space-Nov-13.pdf; and Peter J. Brown, "India Targets China's Satellites," *South Asia Times*, 22 January 2010, http://www.atimes.com/atimes/South_Asia/LA22Df01.html.

5. Armen Toorian, Ken Diaz, and Simon Lee, "The CubeSat Approach to Space Access" (paper presented at the 2008 Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference), 20 May 2008, 1–14, http://ieeexplore.ieee.org/document/4526293/.

6. Josh Berk, Jeremy Straub, and David Whalen, "The Open Prototype for Educational NanoSats: Fixing the Other Side of the Small Satellite Cost Equation" (paper presented at the 2013 IEEE *Aerospace Conference*, 13 March 2013), 1–16, http://ieeexplore.ieee.org/document/6497393/; and Michael Swartwout, "Twenty (Plus) Years of University-class Spacecraft: a Review of What Was, an Understanding of What is, and a Look at What Should be Next," (paper presented at the 20th Annual American Institute of Aeronautics and Astronautics [AIAA]/Utah State University [USU] Conference on Small Satellites, North Logan, UT), 2006, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1532&context=smallsat.

7. Giovanni Minelli, Antonio Ricco, Christopher Beasley, et al., "O/OREOS Nanosatellite: A Multi-payload Technology Demonstration," (paper presented at the 2010 Small Satellite Conference, Moffett Field, CA); Milan Diaz-Aguado, Shakib Ghassemieh, Van Outryve et al., "Small Class-D Spacecraft Thermal Design, Test and Analysis-PharmaSat Biological Experiment," (paper presented at the IEEE Aerospace Conference, Big Sky, MT, 2009), 1–9, https://www.researchgate.net/publication/251884791_Small_Class-D_spacecraft_thermal_design_test_and_analysis_-_PharmaSat_biological_experiment; and Christopher Kitts, John Hines, Elwood Agasid et al., "The GeneSat-1 Microsatellite Mission: A Challenge in Small Satellite Design," (paper presented at the 2006 Small Satellite Conference, Moffett Field, CA), https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1558&context=smallsat.

8. Christopher R. Boshuizen, James Mason, Pete Klupar et al., "Results from the Planet Labs Flock Constellation," Staff Selection Commission (SSC) Paper 14-I-1, 2014, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=3016&context=smallsat.

9. Nayak, "CubeSat Proximity Operations", 1–2.

10. Carlos G. Niederstrasser, Alishan Hassan, Jake Hermle et al., "TJ3Sat–The First Satellite Developed and Operated by High School Students," SSC Paper 09-XII-5, 2009, https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1342&context=smallsat.

11. Stewart Davis, "Construction of a CubeSat Using Additive Manufacturing," *SAE* International Technical Paper 2011-01-2568, http://papers.sae.org/2011-01-2568/; Benjamin W. Longmier, Frans H. Ebersohn, J. P. Sheehan, and Timothy A. Collard, "The CubeSat Ambipolar Thruster: Earth Escape in a 3U CubeSat," (paper presented at the Joint Conference of the 30th Symposium on Space Technology and Science, 34th International Electric Propulsion Conference and 6th Nano-satellite Symposium), Hyogo–Kobe, Japan, 10 July 2015, http://pepl.engin.umich.edu/pdf/IEPC-2015-243.pdf; Gilbert Moore, Walter Holemans, Adam Huang et al., "3D Printing and MEMS Propulsion for the RAMPART 2U CubeSat," (paper presented at the AIAA/USU Conference on Small Satellites, North Logan, UT), https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1205&context=smallsat; Kristia Harris,

Michael McGarvey, Ha Youn Chang et al., "Application for RSO Automated Proximity Analysis and IMAging (ARAPAIMA): Development of a Nanosat-based Space Situational Awareness Mission," (paper presented at the AIAA/USU Conference on Small Satellites, North Logan, UT), 2013, 1–19, http://www.dtic.mil/dtic/tr/fulltext/u2/1034457.pdf; Bogdan Udrea, Michael V. Nayak, Adam Huang et al., "Mission Design and Concept of Operations of a 6U CubeSat Mission for Proximity Operations and RSO Imaging," (paper presented at the Fifth International Conference on Spacecraft Formation Flying Missions and Technologies, Munich, Germany, 2013), 1–15, https://www.researchgate.net/publication/280133315_Mission_Design_and_Concept_of_Operations_of_a_6U_CubeSat_Mission_for_Proximity_Operations_and_RSO_Imaging; and Michael Nayak, Jaclyn Beck, and Bogdan Udrea, "Real-time Attitude Commanding to Detect Coverage Gaps and Generate High Resolution Point Clouds for RSO Shape Characterization with a Laser Rangefinder," (paper presented at the IEEE Aerospace Conference, Big Sky, MT, 2013), 1–14, http://ieeexplore.ieee.org/document/6496861/.

12. Ho Jin, Youngju Kim, and Sanghyuk Kim, "Optical Design of a Reflecting Telescope for CubeSat," *Journal of the Optical Society of Korea* 17, no. 6, 2013, 533–37, https://www.osapublishing.org/josk/abstract.cfm?URI=josk-17-6-533.

13. Tarik Malik, "Iran Launches Small Earth-Watching Satellite Into Orbit," *Space.com*, 3 February 2012, https://www.space.com/14464-iran-launches-small-satellite-orbit.html.

14. J. Nicholson and B. T. Gerstein, "The Department of Defense's Next Generation Narrowband Satellite Communications System, the Mobile User Objective System (MUOS)," (paper presented at the MILCOM 2000: 21st Century Military Communications Conference, IEEE [Vol. 2], 2000), 805–09; and B.S. Robinson, D. M. Boroson DM, D. A. Burianek et al., "Overview of the Lunar Laser Communications Demonstration" (paper presented at *SPIE LASE*, International Society for Optics and Photonics, 2011, 792302). MUOS, or the Mobile User Objective System, is a narrowband tactical satellite communications system. LADEE, or the Lunar Atmosphere and Dust Environment Explorer, demonstrated high-bandwidth laser communications from lunar orbit using a receptor the size of two postage stamps.

15. Daniel A. Gallton, "The Challenge of Small Satellite Systems to the Space Security Environment" (master's thesis, Naval Postgraduate School, 2012), https://calhoun.nps.edu/handle/10945/6797. Examples include missile warning, protected communications, space-based position-navigation-timing, and China's Fengyun-1C Anti-Satellite Test, 2007.

16. Sergei N. Khrushchev, *Nikita Khrushchev and the Creation of a Superpower* (University Park, PA: Penn State Press, 2010), 351–60.

17. Disaggregated system is defined as "the dispersion of space-based missions, functions or sensors across multiple systems spanning one or more orbital plane, platform, host or domain."

18. Lt Col Ellen Pawlikowski, USAF, Doug Loverro, Defense Intelligence Senior Executive Service, and Col Tom Cristler, USAF, Retired, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly* 6, no. 1, 2012, 27–54, http://www.au.af.mil/au/ssq/2012/spring/pawlikowski.pdf; and Air Force Space Command (AFSC), *Resiliency and Disaggregated Space Architectures*, US government white paper (Peterson AFB, CO: AFSPC, 2013), https://fas.org/spp/military/resiliency.pdf.

19. Adam E. Frey, "Defense of US Space Assets: A Legal Perspective," *Air & Space Power Journal* 22, no. 4, 75–84, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-22_Issue-1-4/2008_Vol22_No4.pdf.

20. Michael Nayak, "Impact of National Space Policy on Orbital Debris Mitigation and US Air Force End of Life Satellite Operations," (paper presented at the SpaceOps 2012 Conference, Stockholm, Sweden, 2012), 1–9, https://arc.aiaa.org/doi/abs/10.2514/6.2012-1284611.

21. "XSS-11 Micro Satellite," *Kirtland.af.mil*, accessed 18 October 2017, http://www.kirtland.af.mil/Portals/52/documents/AFD-111103-035.pdf?ver=2016-06-28-110256-797; I. T. Mitchell, T. B. Gorton, K. Taskov et al., "GN&C Development of the XSS-11 Micro-satellite for Autonomous Rendezvous and Proximity Operations," (paper presented at the *29th Annual AAS Guidance and Control Conference*, Breckenridge, CO, 2006); David A. Whelan, E. Allen Adler, Samuel B. Wilson et al., "DARPA Orbital Express Program: Effecting a Revolution in Space-based Systems," (paper presented at the International Symposium on Optical Science and Technology, 2000), 48–56, https://www.spiedigitallibrary.org/conference-proceedings-of-spie/4136/1/DARPA-Orbital-Express-program--effecting-a-revolution-in-space/10.1117/12.406656.short?SSO=1; Andrew Ogilvie, Justin Allport, Michael Hannah et al., "Autonomous Satellite Servicing Using the Orbital Express Demonstration Manipulator System," (paper presented at the Ninth International Symposium on Artificial Intelligence, Robotics, and Automation in Space, Beijing,

China, 2008), 25–29, http://robotics.estec.esa.int/i-SAIRAS/isairas2008/Proceedings/SESSION%2014/m113-Ogilvie.pdf; and Robert B. Friend, "Orbital Express Program Summary and Mission Overview," (paper presented at the Society of Photographic Instrumentation Engineers *Defense and Security Symposium*, Orlando, FL, 15 April 2008), https://www.spiedigitallibrary.org/conference-proceedings-of-spie/6958/1/Orbital-Express-program-summary-and-mission-overview/10.1117/12.783792.short.

22. Bill Gertz, "China Launches Three ASAT Satellites," *Washington Free Beacon*, 26 August *2013*, http://freebeacon.com/national-security/china-launches-three-asat-satellites/.

23. Kristia Harris, Michael McGarvey, Michael Nayak, Bogdan Udrea et al., "Application for RSO Automated Proximity Analysis and IMAging (ARAPAIMA): Development of a Nanosat-based Space Situational Awareness Mission", SSC Paper 13-VI, 2009, http://digitalcommons.usu.edu/smallsat/2013/all2013/40/, 1–19; Bogdan Udrea, Michael Nayak, Michaella Ryle et al., "Mission Design and Concept of Operations of a 6U CubeSat Mission for Proximity Operations and RSO Imaging" (paper presented at the Fifth International Conference on Spacecraft Formation Flying Missions and Technologies, Munich, Germany, 2013), 1–15; Francisco J. Franquiz, Peter Edwards, Bogdan Udrea et al., "Attitude Determination and Control System Design for a 6U CubeSat for Proximity Operations and Rendezvous," (paper presented at the AIAA/American Astronautical Society Astrodynamics Specialist Conference, San Diego, CA, 2014), 1–18; Bogdan Udrea, Michael Nayak, and Finn Ankersen, "Analysis of the Pointing Accuracy of a 6U CubeSat Mission for Proximity Operations and Resident Space Object Imaging" (paper presented at the Fifth International Conference on Spacecraft Formation Flying Missions and Technologies, Munich, Germany, 2013), http://www.sffmt2013.org/PPAbstract/4139p.pdf; and Parv Patel, Bogdan Udrea, and Michael Nayak, "Optimal Guidance Trajectories for a Nanosat Docking with a Noncooperative Resident Space Object," (paper presented at the 2015 IEEE Aerospace Conference, Big Sky, MT, 2015), 1–11.

24. Linda M. Herrell, "Access to Space for Technology Validation Missions: a Practical Guide" (paper presented at the 2007 IEEE Aerospace Conference, Big Sky, MT, 2015), 1–8, http://ieeexplore.ieee.org/document/4161322/; and Phillip C. Kalmanson, Bryan Benedict, Michael Do et al., "Micro & Nanosatellite Launch Capabilities from the Star Bus GEO Commercial Communications Platform" (paper presented at the 22nd Annual AIAA/USU Conference on Small Satellites, Logan, UT, 2008), https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1408&context=smallsat. Example: Space Systems Loral hosted payloads on Intelsat and SES Astra space vehicles and has an established business model in place for government collaborations.

25. Mike Wall, "Is Russian Mystery Object a Space Weapon?" *Space.com,* 19 November 2014, https://www.space.com/27806-russia-mystery-object-space-weapon.html.

26. Michael Nayak, Jaclyn Beck, and Bogdan Udrea, "Design of Relative Motion and Attitude Profiles for Three-dimensional Resident Space Object Imaging with a Laser Rangefinger" (paper presented at the 2013 IEEE Aerospace Conference, 2013), 1–16, http://ieeexplore.ieee.org/document/6496837/; and Parv Patel, Bogdan Udrea, and Michael Nayak, "Optimal Guidance Trajectories for a Nanosat Docking with a Noncooperative Resident Space Object" (paper presented at the 2015 IEEE Aerospace Conference, 2015), 1–11. *Istrebitel* is the Russian word for "fighter aircraft."

27. Frey, "Defense of US Space Assets," 75–84.

28. Bruce W. Jentleson and Christopher A. Whytock, "Who Won Libya," *International Security* 30, no. 3, 47–86, https://lse.rl.talis.com/items/21C96C88-07BC-6BCB-EE7D-6BA3C5A73222.html.

29. Thomas T. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 202–33.

30. Shawn C. Fairhurst, "Realities of Deterrence and Retaliatory Options to Attacks in Space and Cyberspace," Technical Report (Maxwell AFB, AL: Air War College*,* 2012), 2–29.

31. Civil Air Patrol, "FPCON (Force Protection Condition) Categories," 22 August 2003, http://capnhq.custhelp.com/app/answers/detail/a_id/1023/-/fpcon%-%28force-protection-condition%29-categories.

32. Ibid.

33. Jayant Sharma, Grant H. Stokes, Curt von Braun et al., "Toward Operational Space-based Space Surveillance" *Lincoln Laboratory* 13, 2002, 309–34.

34. USAF, *AFD-110501-004*.

35. SpaceFlight 101, "GSSAP Satellite Overview," 25 July 2014, accessed 17 October 2017, http://spaceflight101.com/spacecraft/gssap/.

36. Stephen Clark, "Air Force General Reveals New Space Surveillance Program," *Space.com*, 3 March 2014, https://www.space.com/24897-air-force-space-surveillance-program.html.

37. Ibid.
38. Fairhurst, "Deterrence and Retailiatory Options."
39. Ian Garrick-Bethell, Robert P. Lin, Hugo Sanchez et al., "Lunar Magnetic Field Measurements with a Cubesat," in *Systems and Sensors for Space Applications VI*, ed. Khanh D. Pham, Joseph L. Cox, Richard T. Howard RT, et al., (Bellingham, WA: International Society for Optical Engineering, 2013).

Capt Michael Nayak, USAF, PhD

Captain Nayak (PhD, MS, University of California at Santa Cruz; BS, Embry-Riddle Aeronautical University) is a research scientist with the Directed Energy Directorate, Air Force Research Laboratory. Captain Nayak has published more than 35 journal and conference papers on interdisciplinary research ranging across aerospace engineering, planetary science, astrophysics, space mission design, guidance navigation and control, geophysics, and space policy. His experience outside the USAF spans work at three National Aeronautics and Space Administration centers, including as a certified space shuttle engineer, coprincipal investigator of a cube satellite program and a National Defense Science and Engineering Graduate Fellow at the University of California. He is also a commercial pilot and skydiving instructor.