

By Captain Andrew Compean and Mr. Daniel Selman

Introduction

Today's battles cannot be fought, nor the battlespace properly visualized, without being enabled by space-that's the bottom line and irrefutable reality of modern warfare. Our military today is as critically reliant on space as the ancient Greek army was on the phalanx to dominate that era's battlefields. Without crucial space-enabled capabilities ubiquitously supporting the various warfighting functions to joint, Service, and emerging multi-domain operations forces, the U.S. military would likely be unable to effectively plan, execute, sustain, or decisively win wars. By extension, the U.S. Army likely could not effectively conduct the breadth of land-based operations it must undertake to seize, control, and dominate that domain and defeat the enemy on the ground. Competition and conflict in the future will be reliant even more heavily on space. Coalition warfare further highlights the criticality and force-multiplying effects of space-enabling technologies by providing command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), and common operational pictures informed synergistically by space systems of the United States and many coalition partners.

Emerging Space and Counterspace Threats

When Army intelligence officers train for land operations, the reality of how space can affect both enemy and friendly actions, sometimes decisively, is virtually absent and is unwittingly taken for granted. This is because since the 1960s, the United States has maintained the world's largest and most sophisticated constellation of satellites in support of the Department of Defense and national policy; no other country was even close, with the exception of the Soviet Union during the bipolar era. In today's multipolar world, the battlespace is rapidly evolving, and space is no longer the exclusive domain of two dominant world powers to uniquely enhance all military operations. Nor is it the sanctuary it once was.

Competitors are developing and fielding sophisticated technologies that contest American space power. Global technology trends, and greatly reduced costs of commercial space technologies and launch services since the early 1990s, have supported explosive growth in the number of objects in space, provided near-universal access to space, and enabled even second- and third-world countries to acquire advanced technologies. Global technology trends are also creating or boosting nascent or developing scientific and engineering capacities that are countering the U.S. competitive advantage.¹ Some argue that in aspects of space utilization and technological advancements, Russia and China are on par with or have even surpassed the United States. Those same advanced commercial technologies

are used for military applications and support military and warfighting functions. Moreover, the increasing dual-use capabilities of these commercial systems can obscure end users and intent, and challenge the ability of the United States to provide unambiguous and advanced warning between peaceful and potentially hostile intent/use.²

Counterspace

Counterspace is a mission, like counterair, that integrates offensive and defensive operations to attain and maintain the desired control and protection in and through space. These operations may be conducted across the tactical, operational, and strategic levels in all domains (air, space, land, maritime, and cyberspace), and are dependent on robust space situational awareness and timely command and control. Counterspace operations include both offensive counterspace and defensive counterspace operations. Counterspace is also referred to as "space control."³

We, as intelligence professionals, must be aware of the existing and emerging space and counterspace threats that could significantly alter or affect the operational environment worldwide. With the recent re-establishment of U.S. Space Command and the creation of the U.S. Space Force, this sea change within the Department of Defense high-

lights the space domain's maturation and its vital concern for the United States—not only how the United States views space, but also how the adversary views and uses space. We will further discuss adversary and global advancement of space capabilities and the planning considerations that an Army intelligence professional should undertake when supporting land operations.

Space-Based Support for Military, Commercial, and Civilian Applications

Over the past couple of decades, the use of space has dramatically expanded in both the number

and types of satellites in orbit, as well as commercial entities making access to space and the various services they provide more affordable. Access to space is becoming more common and attainable by state and non-state entities that previously did not have the money, influence, or industrial and technological capacity to do so. As with any new advancement and opportunity, new risks are also introduced. Countries worldwide, regardless of economic status, are introducing, advancing, and expanding their space access and utilization after observing the revolutionary benefits of space applications, principally by the United States. They are achieving these feats by the use of diplomatic, information, military, and economic, also known as DIME, spheres, particularly for education, technology, and military sectors. In the military realm, it should come as no surprise that any new type of technological capability or advancement can be applied for both defensive and offensive purposes, and space-enabled capabilities are no exception. Figure 1 shows countries that have on-orbit satellites, the capabilities of those satellites, and the numeric representation of the satellites they own.

Protests to U.S. Space Operations

Both China and Russia, the United States main competitors in space, have taken overt and deliberate steps to challenge and restrain the United States use of and operations in space because both view the United States as seeking to dominate and militarize space. Both countries have openly protested, most notably and formally at the United Nations, the United States use of space as hostile. Both continued their protest by stating that any action they undertake in space is in direct response to their perceptions of the U.S.

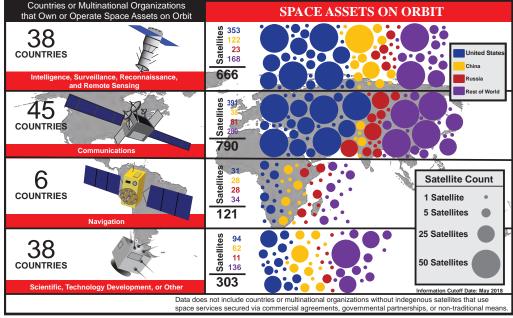


Figure 1. Space Assets on Orbit⁴

threat and is defensive in nature. In the following sections, you will see that their statements, actions, and protestations are hypocritical and ironic.

Chinese and Russian Views of Space and Counterspace

With the evolution and advancement of space-based capabilities, both Chinese and Russian military doctrines view space as an essential force multiplier and both view counterspace capabilities, ironically, as a means to reduce United States and allied operational effectiveness. In 2015, both countries reorganized their militaries and emphasized the utilization of space for modern military operations.⁵ Both countries developed or consolidated specialized space units and committed significant national funds to improve essential space services such as space lift, satellite communications (SATCOM), satellite navigation (satnav), spacebased ISR, space domain awareness, satellite control, and infrastructure. The advancement and employment of these capabilities will more effectively enable their governmental organs to conduct strategic communications, diplomatic functions, and economic strategies. They will also enable their military's ability to execute deployment; sustainment; maneuver; command, control, and communications; and full spectrum military operations regionally and worldwide. These capabilities will also enable them to search, track, identify, monitor, and possibly target U.S. and allied military forces operating in any area of operations. They are pursuing the same ability to maintain awareness of the space domain, particularly for U.S. and allied space assets.⁶ Both countries have put a premium on the ability to search, track, identify, characterize, and monitor satellites in all orbits. Having

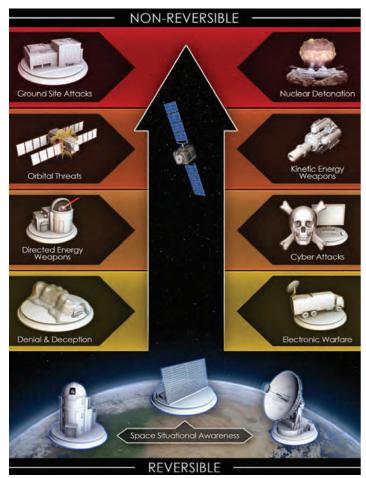


Figure 2. Counterspace Continuum–From Reversible to Nonreversible Effects⁷

this capability critically supports both Chinese and Russian space and counterspace programs. Having space domain awareness is the foundation of space and counterspace operations, and the counterspace continuum of threats, which range from reversible to nonreversible effects against space systems and supporting ground systems and infrastructure through kinetic and non-kinetic means. Both countries continue to develop a full range of counterspace capabilities, which include offensive jamming and cyberspace weapons, directed-energy weapons, on-orbit systems, and groundbased direct-ascent antisatellite missiles. Figure 2 shows the counterspace continuum that represents the range of threats to space-based capabilities, arranged from reversible to nonreversible effects. Reversible effects are nondestructive and temporary, while nonreversible effects can cause physical and permanent damage.

Russian Space and Counterspace Policy and Capabilities

Russia's space program is a source of national pride. Moscow views itself as a world leader in space development and particularly prides itself as being the first nation in space in 1957. After the Soviet Union dissolved in 1991, Russia inherited the extensive space infrastructure, technology, and the former Soviet Union's place among the global space powers.⁸ However, at the end of the Cold War, a combination of budgetary constraints, an economic implosion, and technological setbacks caused a decay of Russian space capabilities.9 Despite these setbacks, Russia implemented a set of programs and initiatives over the last decade to regain many of its Cold War-era space and counterspace capabilities and former prominence. Its counterspace program includes extensive electronic warfare (EW) systems to deny, degrade, and disrupt communications and Global Positioning System (GPS)/positioning, navigation, and timing (PNT); ground-based, mobile missiles to directly attack satellites in low Earth orbit; and directed-energy weapons to deny the use of space-based imagery.¹⁰

Russia's military doctrine and authoritative writings clearly articulate that Moscow views space as a warfighting domain and that achieving supremacy in space will be a decisive factor in seizing the initiative and winning future conflicts.¹¹ Russia considers the "intention to place weapons in outer space," an allusion to the United States military space program, a main external military danger, and describes establishing "an international treaty on [the] prevention of placement of any types of weapons in outer space" as a principal task for the Russian state in its military doctrine.¹² Moscow views space as a key enabler of U.S. precision strike and military force projection capabilities. When paired with United States missile defense systems, Russia believes United States space-enabled, conventional precision strike capabilities undermine Russia's strategic stability.¹³ At the same time, Russia views America's perceived dependence on space as the "Achilles' heel" of American military power, which can be exploited to achieve Russian conflict objectives.¹⁴ Russia is, therefore, pursuing counterspace systems and employment strategies to neutralize, deny, or limit United States military and commercial spacebased services to offset a perceived United States military advantage.¹⁵

Russian counterspace capabilities that directly affect United States and allied land operations will principally be EW attacks against GPS and SATCOM. The Russian military views EW as an essential tool for gaining and maintaining information superiority over its adversaries, allowing Russia to seize the operational initiative by disrupting adversary command, control, and communications; battlespace awareness; GPS/PNT; and intelligence capabilities. Russia has operational experience in the use of counterspace EW capabilities from recent and ongoing expeditionary military campaigns, enabling continual refinement of its tactics, techniques, and procedures, as well as use in Russia to protect strategic locations and VIPs.¹⁶ Russia has fielded a wide range of ground-based EW systems to counter GPS, tactical communications, SATCOM, and radars. Mobile systems include radar and SATCOM jammers. Russia aspires to develop and field a full spectrum of EW capabilities to counter Western C4ISR and weapons guidance systems with new technology, data transfer, and capabilities for peacetime and wartime use in the near term.¹⁷ Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of manned aircraft, unmanned aerial vehicles, guided missiles, and preground-based EW counterspace weapons both within its borders and abroad, the Russian state has repeatedly denied any wrongdoing.¹⁹ Russia is expected to continue developing ground-based EW weapons, and new evidence suggests Russia may be developing high-powered space-based EW platforms to augment the ground-based platforms.²⁰

Satellite command and data distribution networks expose space systems, ground infrastructure, users, and the links connecting these segments to cyber threats. Being aware of these vulnerabilities, Russia also considers offensive cyber capabilities as a key asset for maintaining military advantage, and as a result, is researching and developing cyber capabilities to affect these elements.²¹

United States and allied forces operating in areas with known Russian forces must be aware and expect that EW will most likely be encountered, intentionally or unintentionally. Having equipment properly encrypted and knowing the signs of an EW attack will help mitigate the effects. Military intelligence professionals can assist by helping to understand adversaries' EW capabilities and employment tactics, techniques, and procedures, and by anticipating and planning for their effects during the military decision-making process, and more specifically during the intelligence preparation of the battlefield (IPB) process. Putting forth an inject of jammed SATCOM or GPS during unit training and exercises will cause the planners, operators, and leaders to think about how military operations are affected by this asymmetric threat, and their response to these non-kinetic effects. As intelligence professionals, it is our responsibility to account for and characterize adversary non-kinetic capabilities and potential effects, and the way in which they enable adversaries' kinetic capabilities in support of their broader military operations.

cision-guided munitions, but it has no publicly known capability to interfere with the GPS satellites themselves using radio-frequency interference.¹⁸ Russian GPS jammers could also affect many United States military communications and other equipment enabled by the GPS timing function. Despite overwhelming evidence that Russia has operationally employed mobile,



Russia has invested heavily in developing sophisticated electronic warfare capabilities, including this Krashuka-4 jammer.

Chinese Space and Counterspace Policy and Capabilities

China is rapidly growing its space program by continually developing and operationally deploying new and technologically advanced space and counterspace capabilities. Beijing now has a goal of "[building] China into a space power in all respects."²² China is second only to the United States in the number of operational satellites, which are a source of national pride and part of President Xi Jinping's "China Dream" to establish a powerful and prosperous China.²³ China deploys both space and counterspace capabilities for both civil and military means. China officially advocates for peaceful use of space and is pursuing agreements at the United Nations on the non-weaponization of space.²⁴ Though it

advocates for the peaceful use of space, China continues to improve its counterspace weapons' capabilities and has enacted military reforms to better integrate cyberspace, space, and EW into joint military operations.²⁵

The People's Liberation Army (PLA) views space superiority as the ability to control the information sphere and deny adversaries the same; these are key components of conducting modern "informatized" wars.²⁶ The PLA uses "informatized" warfare to describe the process of acquiring, transmitting, processing, and using information to conduct EW weapons to suppress or deceive enemy equipment.³¹ Currently, China has the ability to jam common SATCOM frequency bands and GPS signals, and it has made the development and deployment of satellite jamming systems a high priority.³² China is further developing jamming systems that will target a large range of commercial SATCOM frequencies, as well as United States military-protected communication bands.³³ The PLA routinely incorporates jamming and anti-jamming techniques against multiple communication systems, radar systems, and GPS satellite systems in exercises.³⁴ In 2018, the Strategic Support Force even carried out advanced military exercises simulating a complex EW environment with the "[Strategic Support Force] SSF base pitted against five PLA Army, Air Force, and Rocket Force units."³⁵



and using information to conduct of China's Space Situational Awareness network.

joint military operations across the domains of land, sea, air, space, cyberspace, and the electromagnetic spectrum during a conflict.²⁷ The PLA historically has managed China's space program and continues to invest in improving China's capabilities in space-based ISR, SATCOM, and satnav, as well as human spaceflight and robotic space exploration.²⁸ As part of the military reforms announced in 2015, China established the Strategic Support Force to integrate cyberspace, space, and EW capabilities into joint military operations.²⁹ The Strategic Support Force forms the core of China's information warfare force, supports the entire PLA, and reports directly to the Central Military Commission, China's highest military governing body. The Strategic Support Force is likely responsible for the research and development of certain space and counterspace capabilities.³⁰

The PLA considers EW capabilities key assets for modern warfare, and the PLA's doctrine emphasizes using As with Russia, China considers offensive cyber capabilities as a key asset for maintaining military advantage and integrated warfare.³⁶ China is also researching and developing cyber capabilities to threaten satellite command and data distribution networks, space systems, ground infrastructure, users, and the links connecting these segments.³⁷

Although official Chinese statements on space warfare and weapons have remained consistently aligned to peaceful purposes, China has recently designated space as a military domain.³⁸ PLA military writings state that the goal of space warfare and operations is to achieve space superiority using offensive and defensive means in connection with their broader strategic focus on asymmetric cost imposition, access denial, and information dominance.³⁹ At its current and projected pace of advancement and employment, China's space and counterspace programs present one of the most profound threats to United States and allied space operations for the foreseeable future. China will continue to advance these capabilities to more effectively enable and directly support land and maritime operations, particularly within its regional sphere of influence, and to support its broader and long-term global strategic, military, diplomatic, and economic goals.

United States forces and allies operating within the United States Indo-Pacific Command area of responsibility have likely encountered Chinese space and counterspace effects. The ongoing geopolitical dispute within the South China Sea highlights China's resolve to obtain regional superiority. Regarding its counterspace systems within the South China Sea, China has deployed military-grade, truck-mounted jamming equipment in its buildup of military installations on its manmade islands. As of April 2018, U.S. officials confirmed two islands in the Spratly Island chain are equipped with jamming systems for targeting communications and radars.⁴⁰ China will continue to use these systems as a deterrence for any future conflict within the region.

Other Emerging Counterspace Threats

Many other countries, some with small or no space programs, are also developing counterspace capabilities to defend their existing assets or to counter perceived adversary threats in the electromagnetic spectrum. GPS and SATCOM jamming systems are the most prevalent counterspace weapon worldwide. These technologies are becoming easier to access, are more cost effective, and are simpler to operate for non-peer adversarial and lesser-developed countries than the more advanced counterspace weapons/ technologies-direct-ascent antisatellite missiles, directedenergy weapons, or on-orbit systems. Nonetheless, some are being developed outside of China and Russia. For example, India became the fourth country to successfully test a direct-ascent antisatellite missile, becoming the only other country to conduct a debris-producing test since China in 2007.⁴¹ Though the satellite that was destroyed was one of its own in low Earth orbit, all spacefaring nations rebuked this test as an unnecessary debris-causing event. In the end, India's strategic messaging goal, probably intended for Beijing, was most likely accomplished—to be seen as a space power. And by actually performing a kinetic test, New Delhi proved it has the means to acquire, track, and engage on-orbit targets. Though India's counterspace capabilities technically pose a threat to United States space systems in low Earth orbit, they are not considered a direct threat.

Two other primary adversaries of the United States, Iran and North Korea, continue to advance their rudimentary counterspace capabilities, primarily with GPS and SATCOM jamming systems, to affect these critically enabling technologies for United States and allied operations, within their areas of influence.

Iran has publicly recognized the strategic value of space and counterspace capabilities and will likely attempt to disrupt or deny the United States and allied forces' use of space capabilities during a conflict to the extent it is technically able to do so. Tehran also views its space program as a source of national pride, technological and economic development, and military modernization.⁴² Counterspace capabilities such as jamming and spoofing are considered regular tools in Iran's weapons arsenal. There are confirmed, documented cases of Iran using these capabilities against international and regional television broadcasts. In 2010, Iran jammed BBC and Voice of America SATCOM signals transmitting into Iran.43 It has publicly acknowledged that the Iranian government engaged in the jamming of foreign broadcast satellites and claimed the ability to spoof GPS receivers.⁴⁴ Iran has continually demonstrated successful EW attacks against both foreign government and civilian systems; United States and allied forces operating within Iran's regional influence will likely continue to experience these effects. Iran has expanded its development of EW counterspace capabilities, and it will likely further advance those capabilities to target a greater range of SATCOM frequencies used by the United States and allied militaries.

North Korea views denying the United States and its allies the ability to use space during a conflict as a top priority. Similar to Iran, North Korea has employed EW attack capabilities, as well as GPS and SATCOM jamming, against adversaries within the region; however, North Korea keeps its counterspace doctrine and operational concepts largely under wraps.⁴⁵ North Korea continually states that its space capabilities are for peaceful use and development and has spoken to the United Nations about its space program, seeking the acceptance and respect of its space program's right to help the country grow economically.⁴⁶ Despite continued statements that it only uses space for peaceful purposes, North Korea has acquired EW systems and conducted EW attacks against space systems. In 2010, South Korea's Defense Minister stated in a speech to parliament that "North Korea has imported vehicle-mountable devices capable of jamming GPS signals, from Russia." That same year, South Korean forces experienced GPS jamming but were unable to locate the jammers at the time because the jamming lasted only 10 minutes in each instance.⁴⁷ Since 2010, numerous GPS interference events have been attributed to North Korea, which affected both civil and military systems, including aircraft and maritime vessels. North Korea is

J.S. Army photo by SGT Jeremiah Woods, 358th Public Affairs Detachme

improving its EW capabilities, as demonstrated in continued GPS jamming and spoofing operations. U.S. and allied forces within the region are likely to experience these capabilities during combined exercises and border patrols, and possibly other high-interest peninsular events. Accounting for these EW capabilities through the IPB process, for North Korea, Iran, or any other potential adversary, will better position United States Army intelligence professionals to support operational planning and assist in mitigating these effects.

Despite the increasing, worldwide proliferation of counterspace systems, the greatest and most direct threats to United States and allied forces space

United States and allied forces space Resolve XII on August 5, 2019. operations are China and Russia. While both are pursuing, adver expanding, and fielding these capabilities, each has different employment strategies, doctrines, and end states, but all with the goal of denying U.S. freedom of action in space.

Conclusion

Persistent and reliable satnav/PNT, SATCOM, ISR, and other key space-enabled services have come to be expected and virtually assumed in peacetime and throughout the spectrum of conflict; however, these critical services are threatened globally today and are no longer assured. This reality can be worrisome and could mean the difference between victory and defeat, but too often, it is overlooked or dismissed until it occurs. Our adversaries are placing a premium on both space-enabled operations and counterspace applications, and we, as Army intelligence professionals, must be aware of their potential effects on land-based operations. When most intelligence officers participate in their formation's war games or combined arms rehearsals, the injects are often based on traditional kinetic strikes on a friendly formation or possibly some sort of external force (weather, terrain, or unforeseen civilian interaction) that could halt or alter a formation's movement.

The operational environment has forever changed, and we challenge Army intelligence professionals to now look and think outside the traditional box and present nontraditional injects and analytic processes based on real-world developments and activities. Presume the opposing force will employ GPS and SATCOM jamming during the operation. We must think like, and ahead of, the adversary in order to provide our leadership with greater insight into the adversary, the new threat paradigm, and a route toward mission success.

Today's Army intelligence professionals must continue to think critically and holistically about the negative or inhibiting effects that could be seen and experienced in the modern battlespace. In the landscape of military domains, space has emerged as a vital enabler for the spectrum of modern military operations, and we must now, more than ever, be aware of and understand its unique nature and threats. Therefore, it is our responsibility to characterize and advocate for incorporating the reality of these new threats to this newest domain. Ultimately, we must support the commanders, planners, and operators at every level and in every forum with accurate, timely, and actionable intelligence on adversary space and counterspace capabilities and intentions. We must assist their ability to operate in spite of, and through, these new and evolving threats.

Endnotes

1. Department of the Air Force, *Competing in Space* (Wright-Patterson Air Force Base, OH: National Air and Space Intelligence Center, December 2018), 2.

3. Department of the Air Force, Annex 3-14, *Counterspace Operations* (Washington, DC: U.S. Government Publishing Office, 27 August 2018), 9.

4. Department of the Air Force, Competing in Space, 4.

5. Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC, January 2019), iii.

6. Ibid.

7. Department of the Air Force, Competing in Space, 14.



Leadership and staff members from battalions across the 1st Armored Brigade Combat Team, 1st Infantry Division,

based out of Fort Riley, KS, participate in a combined arms rehearsal prior to a live fire event during Combined

^{2.} Ibid., 25.

8. Maxim V. Tarasenko, "Transformation of the Soviet Space Program after the 28 Cold War," *Science & Global Security* 4, no. 3 (1994): 339–361.

9. Asif Siddiqi, "Russia's Space Program Is Struggling Mightily," Slate, 21 March 2017.

10. Defense Intelligence Agency, Challenges to Security, 24.

11. Ibid., 23.

12. "The Military Doctrine of the Russian Federation," Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland website, December 25, 2014.

13. Defense Intelligence Agency, Challenges to Security, 24.

14. "This is the Achilles' Heel of Washington's Military Power," Sputnik News Online, 30 January 2016.

15. Defense Intelligence Agency, Challenges to Security, 24.

16. Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Washington, DC: Secure World Foundation, April 2020), 7.

17. Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC, 2017).

18. Weeden and Samson, Global Counterspace Capabilities, 7.

19. "Russia denies role in Israeli airport GPS jamming," BBC News, June 27, 2019; Thomas Nilsen, "Norway tired of Russia's electronic warfare troubling civilian navigation: 'Unacceptable and risky'," *Barents Observer*, January 20, 2019; and "Russia denies disrupting GPS signals during NATO Arctic exercises," *Guardian*, November 12, 2018.

20. Weeden and Samson, Global Counterspace Capabilities, 7.

21. Defense Intelligence Agency, Challenges to Security, 29.

22. The State Council of the People's Republic Of China, *Full text of white paper on China's space activities in 2016* (Beijing, 28 December 2016), quoted in Defense Intelligence Agency, *Challenges to Security*, 13.

23. Defense Intelligence Agency, Challenges to Security, 13.

24. Office of the Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC, 13 February 2018).

25. Defense Intelligence Agency, Challenges to Security, 13.

26. Ibid., 14.

27. Ibid.

28. Ibid.

29. Ibid.

30. Ibid.

31. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC, 2 May 2019).

32. U.S.-China Economic and Security Review Commission, 2015 Report to Congress of the U.S.-China Economic and Security Review Commission (Washington, DC, 2015), 297–298.

33. Defense Intelligence Agency, *Challenges to Security*, 20; Lin Jinshun, Feng Tao, Chen Binhui, and Jiang Chunshan, "Study on countermeasure against satellite adaptive null-steering technique," *Aerospace Electronic Warfare* 26, no. 3 (March 2010): 1-4; and H. Wang, "Analysis on Anti-jamming Measures of Mobile User Objective System," *Radio Communications Technology* 35, no. 2 (2009): 46–49.

34. Department of Defense, Annual Report to Congress.

35. Ibid., 23.

36. Defense Intelligence Agency, Challenges to Security, 20.

37. Department of the Air Force, Competing in Space, 19.

38. Weeden and Samson, Global Counterspace Capabilities, 6.

39. Ibid.

40. Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, and Makena Young, *Space Threat Assessment 2020* (Washington, DC: Center for Strategic & International Studies, March 30, 2020), 15.

41. Ibid., 44.

42. "DM: Iran to Give Crushing Response to Enemies' Space Threats," Fars News Agency, 13 November 2018.

43. Harrison, Johnson, Roberts, and Young, *Space Threat Assessment 2020*, 32.

44. Ibid., 33.

45. Ibid., 37.

46. "Stronger Rules Must Guarantee Outer Space Remains Conflict-Free, First Committee Delegates Stress, Calling for New Laws to Hold Perpetrators Accountable," United Nations website, 17 October 2017.

47. "N. Korea's jamming of GPS signals poses new threat: defense minister," Yonhap News Agency, October 5, 2010.

CPT Andrew Compean is an intelligence officer for the U.S. Army Space and Missile Defense Command (USASMDC) G-2 Current Intelligence Branch. He has more than 9 years of military intelligence experience, working primarily in support of tactical-level operations. In his current assignment, he focuses his analysis on adversarial space-counterspace intelligence, and he provides intelligence analytical expertise in foreign ballistic and cruise missiles and cyberspace. CPT Compean holds a bachelor of arts in history from Bowling Green State University.

Mr. Daniel Selman is the senior intelligence analyst and foreign space-counterspace subject matter expert for the USASMDC G-2 Current Intelligence Branch. Mr. Selman has 39 years of military intelligence experience. He served 11 years as an active duty U.S. Air Force (USAF) intelligence officer and 13 years as a USAF reserve intelligence officer, retiring with the rank of lieutenant colonel. He has been a U.S. Government civilian on the U.S. Space Command J-2 staff for 11 years as a foreign space-counterspace intelligence analyst, and on the USASMDC G-2 staff for more than 17 years as the G-2's principal space-counterspace intelligence analyst. He has also provided intelligence analytical expertise in foreign ballistic and cruise missiles, cyberspace, intelligence support to force protection, and counterintelligence. Mr. Selman holds a bachelor of science in geology from Southeast Missouri State University and a master's degree in management from Webster University.