ESCALATION & DETERRENCE

IN THE SECOND SPACE AGE

AUTHORS

Todd Harrison

Zack Cooper

Kaitlyn Johnson

Thomas G. Roberts

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

OCTOBER 2017

A Project Report by the CSIS Aerospace Security Project

OCTOBER 2017

ESCALATION AND DETERRENCE
IN THE SECOND SPACE AGE

AUTHORS

Todd Harrison

Zack Cooper

Kaitlyn Johnson

Thomas G. Roberts

A Report of the

CSIS AEROSPACE SECURITY PROJECT

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgements

This report is made possible by the generous support of the Smith Richardson Foundation. The authors would also like to thank the experts from government, industry, and other think tanks that participated in our tabletop exercise and senior advisory panel. We are especially grateful for Brian Weeden and Victoria Samson from the Secure World Foundation for co-sponsoring the tabletop exercise.

Center for Strategic & International Studies

1616 Rhode Island Avenue, NW

Washington, DC 20036

202-887-0200 | www.csis.org

Table of Contents

THE EVOLUTION OF SPACE AS A CONTESTED DOMAIN

ON THE MORNING OF JANUARY 12, 2007, at approximately 6:28 a.m. local time, the People's Republic of China launched a rocket from the Xichang Space Center. This two-stage, solid propellant missile, believed to be a modified version of China's DF-21 medium-range ballistic missile, climbed to an altitude of 850 kilometers and intercepted a malfunctioning Chinese weather satellite.[1] The intercept produced more than 2,600 pieces of debris large enough to track (greater than 10 centimeters) and an estimated 150,000 pieces of debris larger than 1 cm. With this one test of a direct ascent anti-satellite (ASAT) weapon, China roughly doubled the amount of debris in space and sent a shockwave throughout the international space community.[2]

1 Shirley Kan, China's Anti-Satellite Weapon Test (Washington, DC: Congressional Research Service, April 2007), https://fas.org/sgp/crs/row/RS22652.pdf.

2 "Two Minor Fragmentations End Worst Debris Year Ever," *Orbital Debris Quarterly News* 12, no. 1 (January 2008), https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv12i1.pdf.

The 2007 test was the first successful intercept of a satellite by China, but it was not its first attempt. China had been developing this capability for years, with three previous test flights from September 2004 to February 2006.[3] More importantly, this test broke the informal moratorium on destructive ASAT tests that had been upheld since the last such test by the United States in 1985.[4] By conducting this test, China sent a clear signal to the rest of the world that the balance of power that had helped stabilize the competition in space throughout the Cold War was changing. For the United States, the test served as a wakeup call: it could no longer continue acting as if space was the sanctuary it had been throughout much of the Cold War. The United States needed a new concept of deterrence in space for a new space age.

– THE FIRST SPACE AGE (1957–1990)

THE SPACE AGE BEGAN ON OCTOBER 4, 1957 with the Soviet launch of Sputnik 1, the first human-made object to orbit the Earth. This event surprised many in the United States and raised fears that the Soviet Union was pulling ahead in missile technology. It ignited a frenetic competition for superiority in space. In pursuit of that superiority, both countries made significant investments in order to attain rapid technological advances in rockets, satellites, and human spaceflight. Because of these advances, the United States and Soviet Union quickly became the dominant powers in space. From 1957 through 1966, the United States launched 68 percent of the satellites orbited, the Soviet Union launched 30 percent, and all other countries combined launched less than 2 percent.[5] In the years that followed, other countries began to increase their space capabilities but still lagged far behind the United States and Soviet Union. From 1957 through 1990, the United States and Soviet Union were responsible for 93 percent of all satellites launched into space.

Militarization of Space

From the beginning, the U.S. and Soviet space programs were directly linked to military power, in particular nuclear forces. As such, approximately 70 percent of all satellites launched from 1957 to 1990 were military satellites.[6] As Air Force General Ellen Pawlikowski, Doug Loverro, and Tom Cristler have noted, "[f]rom the very beginning of the space age to the last days of the Cold War, most space systems were focused on strategic conflict."[7] Both the United States and the Soviet Union launched constellations of satellites (many of which were highly classified) with increasingly sophisticated capabilities

3 Mure Dickie, Stephen Fidler, and Demetri Sevastopulo, "Satellite kill likely to have equal impact on terra firma," *Financial Times*, January 20, 2007, http://www.ft.com/cms/s/0/9a943dac-a82a-11db-b448-0000779e2340.html?ft_site=falcon&desktop=true.

4 James Clay Moltz, *Crowded Orbits: Conflict and Cooperation in Space* (New York: Columbia University Press, 2014), 29.

5 Analysis of the space catalog data from Space-Track.org. See Appendix A.

6 Ibid.

7 Ellen Pawlikowski, Doug Loverro, and Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies ," *Strategic Studies Quarterly* 6, no. 1 (Spring 2012): 30, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-1/Pawlikowski.pdf?ver=2017-01-23-115910-680.

for intelligence collection, communications, and missile warning. These space systems were primarily intended to support "pre-conflict intelligence, nuclear attack warning and response, and continuity of nuclear command and control" and had limited applicability for conventional conflicts.[8]

Ironically, the proliferation of military satellites proved to be an important stabilizing factor that helped prevent attacks in space. For example, the space-based intelligence and surveillance capabilities developed by both sides allowed each to better understand the capabilities and capacity of the other's nuclear forces. This provided greater transparency, which helped ease suspicions and created a verification mechanism that underpinned arms control treaties and ultimately eased tensions.[9] The Accident Measures Agreement of 1971[10] required immediate notification of interference with missile warning and related communications systems, and the Hotline Modernization Agreement,[11] also signed in 1971, required that both sides protect the Direct Communication Link, which used Molniya and Intelsat satellites.[12] In the Anti-Ballistic Missile Treaty of 1972, both countries agreed to not interfere with each other's means of verification, which included reconnaissance satellites.[13] Because military space systems were primarily designed to support nuclear missions, the potential for conflict in space was often viewed as an extension of nuclear conflict on Earth. An attack on either country's military satellites would have been regarded as either a prelude or part of a nuclear war.[14]

Early Counterspace Programs

Space was not completely benign, however. Both the United States and the Soviet Union developed and tested a variety of counterspace weapons from the beginning of the space age. In 1959, the United States conducted the first anti-satellite weapons test with the launch of a Bold Orion missile from a B-47 aircraft. The missile flew within a few miles of the Explorer 6 satellite that was used as a target for the test. It was not equipped with a nuclear warhead, but it proved that, had it been armed, the target satellite would have likely been destroyed.[15]

In 1962, just three months before the Cuban missile crisis, the United States conducted the Starfish Prime nuclear test. In this test, the United States detonated a 1.4 megaton nuclear weapon at an altitude of approximately 400 km. Although it was not primarily intended to be an ASAT test, the experiment proved that nuclear weapons could be used to destroy satellites, although with indiscriminate

8 Ibid.

9 Pat Norris, *Spies in the Sky: Surveillance Satellites in War and Peace* (Berlin: Springer Praxis Books, 2008).

10 U.S. Department of State, "Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War Between The United States of America and The Union of Soviet Socialist Republics (Accidents Measures Agreement)," Bureau of International Security and Nonproliferation (September 1971), https://www.state.gov/t/isn/4692.htm.

11 U.S. Department of State, "Agreement Between the U.S. and the U.S.S.R. on Measures To Improve the U.S.A.-U.S.S.R. Direct Communications Link (With Annex, Supplementing and Modifying the Memorandum of Understanding With Annex, of June 20, 1963)," Bureau of International Security And Nonproliferation, (September 1971), https://www.state.gov/t/isn/4787.htm.

12 Laura Grego, "A History of Anti-Satellite Programs" *Union of Concerned Scientists*, (January 2012), 4, http://www.ucsusa.org/sites/default/files/legacy/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf.

13 Ibid., 3.

14 Pawlikowski et al., "Space: Disruptive Challenges," 30.

15 Robert Bowman, *Star Wars: A Defense Insider's Case Against the Strategic Defense Initiative* (Los Angeles: Tarcher Publications, 1986), 14.

"The defining characteristics of the second space age are that it is more diverse, disruptive, disordered, and dangerous than the first space age."

effects. The electromagnetic pulse from this nuclear detonation immediately destroyed satellites within line-of-sight. The blast also intensified the Van Allen radiation belts and created a ring of radiation in low Earth orbit (LEO) that gradually degraded the operation of other satellites over several months. According to some estimates, as many as one third of all satellites in orbit at the time were destroyed by the Starfish Prime test. Tests of nuclear weapons in space were banned by the Partial Test Ban Treaty the following year.[16]

In 1963, the Soviets began developing a co-orbital ASAT system capable of destroying satellites in LEO. The system had to be launched into the same orbital plane as the target satellite before gradually maneuvering close to its target and detonating a conventional warhead—a process that could take hours. In parallel, the United States pursued an anti-ballistic missile system, which had an inherent ASAT capability against satellites in LEO. Because guidance systems at the time were not sufficient to allow a direct intercept, the U.S. system relied on detonating a nuclear warhead in the general vicinity of a target satellite or incoming ballistic missile. In the 1970s, when NASA began development of the U.S. Space Shuttle, the Soviets viewed the Shuttle as a potential ASAT weapon because it was capable of retrieving satellites in LEO and deorbiting them.[17]

In the early 1980s, the United States began development of the Strategic Defense Initiative (SDI) and the Air-Launched Miniature Vehicle (ALMV). While SDI was primarily intended as a missile defense system, it would have had a latent capable to destroy satellites in LEO. ALMV was a direct ascent ASAT weapon launched from an airborne platform (an F-15 fighter jet), which gave it much greater flexibility for launch and a shorter response time than the Soviet co-orbital ASAT weapon. ALMV was tested only once against an actual satellite in 1985. The intercept occurred at 555 km altitude and produced several hundred pieces of orbital debris that persisted for decades. The U.S. military planned to conduct additional tests of this system, but Congress intervened in December 1985 with a ban on additional ASAT tests. The Air Force disbanded the ALMV program two years later.[18] The Soviets agreed to end testing of kinetic ASAT weapons against satellites as well, and no other debris-producing tests were conducted by any country until the Chinese ASAT test in 2007.

The relative peace that the world enjoyed in space throughout the first space age was not because space was an uncontested domain. Both the United States and the Soviet Union had the capabilities necessary to degrade and destroy one another's space systems. Despite periods of high tensions and proxy wars, conflict did not extend into space because both superpowers feared it would escalate into a nuclear conflict. Deterrence held in space because nuclear deterrence held on Earth.

16 "9 July 1962 'Starfish Prime', Outer Space" *CTBT Preparatory Commission*, 2017, https://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space.

17 Grego, "A History of Anti-Satellite Programs," 3-4.

18 Ibid.

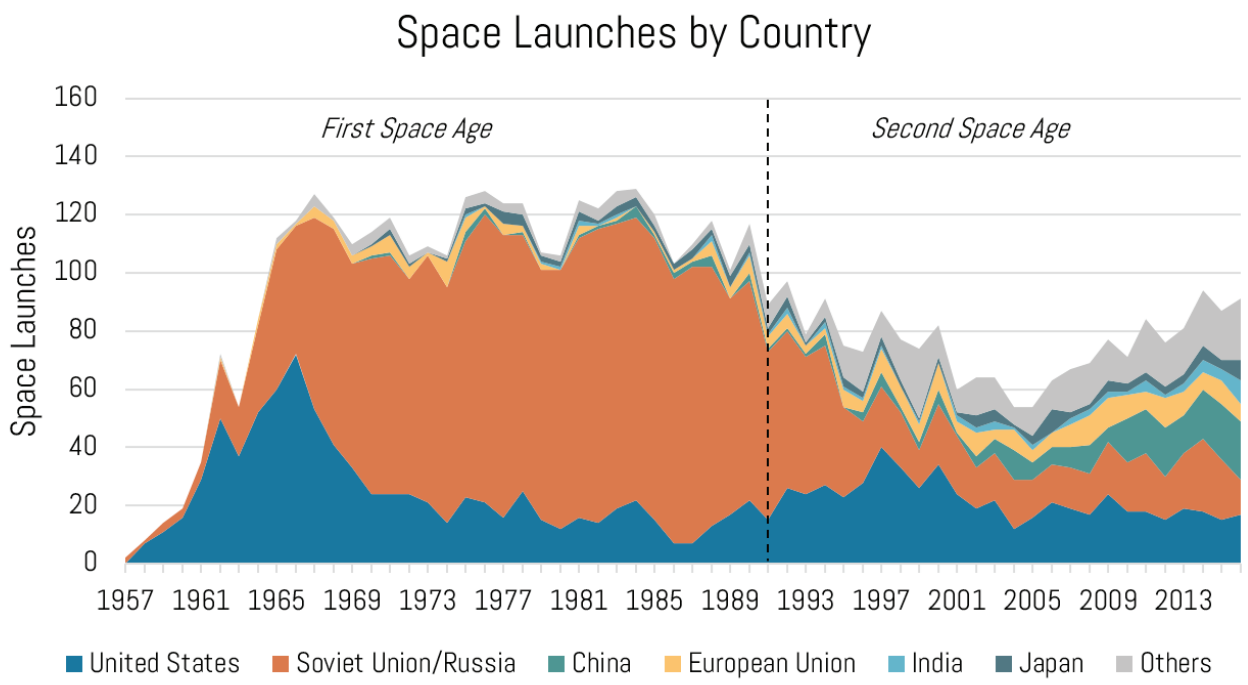

Figure 1: Space Launches by Country. This figure describes the total number of space launches completed per year for the United States, the Soviet Union and Russia, China, the European Union, India, Japan, and all other nations combined. For more information, refer to Appendix A. Source: Space-Track.org.

– THE SECOND SPACE AGE (1991–PRESENT)

AS THE COLD WAR CAME TO AN END IN 1991, the space domain began to transition into what has been called the "second space age."[19] This transition was the result of nearly simultaneous shifts in the commercial uses of space, the geopolitical environment on Earth, and the military balance of power. The fall of the Soviet Union meant that there were no longer two superpowers locked in a stable, long-term competition in space. Operation Desert Storm, also in 1991, proved to be a key turning point in the military use of space because it was the first time space-based capabilities played a major role in conventional military operations—what Air Force General Merrill McPeak called "the first space war."[20] Furthermore, beginning in the 1990s space capabilities began to spread to other countries and commercial firms, bringing more of the benefits of space to people around the globe.

The defining characteristics of the second space age are that it is more diverse, disruptive, disordered, and dangerous than the first space age. It is more diverse because space capabilities have proliferated to many other nations, despite several attempts by the United States at limiting the spread of space

19 Tom Cremins, "A New Space Age: Maximizing Global Benefits," *Strategic Foresight: Perspectives on Global Shifts* (New York: World Economic Forum, 2014), http://reports.weforum.org/global-strategic-foresight/thomas-e-cremin s-nasa-a-new-space-age/.

20 Craig Covault, "Desert Storm Reinforces Military Space Directions," *Aviation Week and Space Technology* (April 1991), 42.

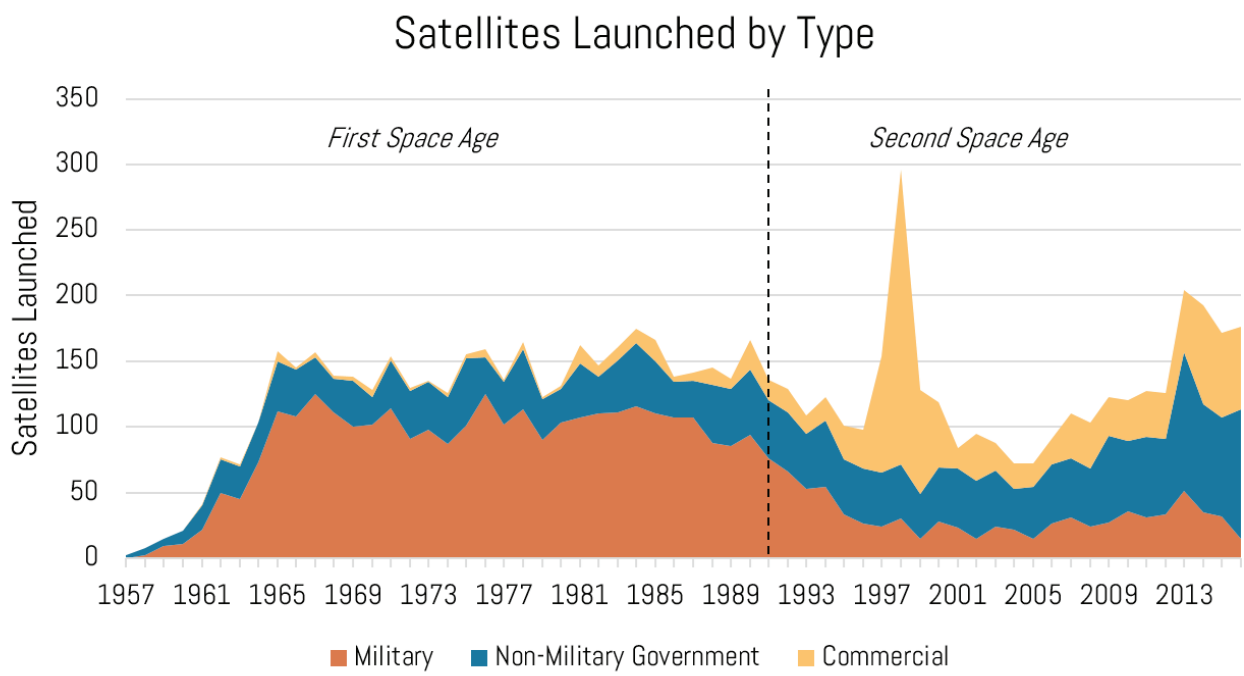

Figure 2: Satellites Launched by Type. This figure describes the total number of payloads launched per year, categorized by type. During one year in particular, 1998, an unusually large number of commercial satellites were launched. This anomaly corresponds to several different large- and small-satellite constellations being launched in a short amount of time. For more information, refer to Appendix A. Source: Space-Track.org.

technology.[21] From 1991 through 2016, 43 percent of new satellites and 39 percent of launches have been from nations other than the United States and Russia. Moreover, since 2014, a majority of satellites and a majority of launches have been from nations other than the United States and Russia—primarily China, Japan, Europe, and India.

A greater number and variety of commercial firms have also emerged since the end of the Cold War and the easing of government restrictions on space technologies. In the first space age (1957 to 1990) just 4 percent of satellites launched were commercial, while in the second space age (1991 to present) more than 36 percent of satellites launched have been commercial. Moreover, commercial firms have developed space capabilities in areas that were once dominated by governments, such as high-resolution satellite imagery, signals intelligence, and space situational awareness, and in some cases commercial firms are launching satellites with capabilities that rival or exceed those of the U.S. military. For example, one of ViaSat's recent communications satellites (ViaSat-2) has a total data throughput

21 In 1998, Congress transferred licensing authority for the export of satellites and space technology from the Department of Commerce back to the State Department, and in 1999 it further tightened export controls on missile technology and satellites. See United States Library of Congress, Congressional Research Service, "China: Possible Missile Technology Transfers from U.S. Satellite Export Policy - Actions and Chronology," by Shirley Kan, 98-485F, (2002), http://www.au.af.mil/au/awc/awcgate/crs/98-485.pdf.

capacity of 300 gigabits per second[22]—nearly 100 times that of the U.S. military's current generation of wideband communications satellites, Wideband Global SATCOM (WGS).[23]

The accelerating pace of innovation in commercial space is also leading to disruptive changes in the way space is used. A notable example is the space launch industry where a handful of billionaire-backed startups, such as Elon Musk's SpaceX, Jeff Bezos's Blue Origin, Richard Branson's Virgin Galactic, and Paul Allen's Stratolaunch, are competing to lower the cost of access to space and to create a space tourism industry. SpaceX and BlueOrigin in particular have disrupted the launch industry by developing first stages that can land vertically and be reused for multiple launches. Several commercial space firms are planning to launch constellations with hundreds—and in some cases thousands—of satellites for missions that include communications, imagery, and signals intelligence.[24] Since the total number of satellites in orbit today is roughly 1,459[25], these massive constellations could dramatically increase the number of objects that need to be tracked—and associated space traffic management issues—by an order of magnitude over the coming decade. Private companies are also planning space missions in new areas that go beyond what current laws and regulations were designed to accommodate, such as on-orbit servicing of satellites, asteroid mining, and on-orbit manufacturing.

The renewed energy in the commercial space sector has also led to a growing global space economy—now estimated at $323B annually—that creates high-tech, high-paying jobs and improves the lives of people around the world.[26] Government regulation of the space industry presents a sort of prisoner's dilemma: if one nation attempts to significantly limit commercial space activity on its own, it puts its own companies and citizens at a disadvantage relative to other less restrictive nations.

The increased use of space by more nations and the development of new commercial space capabilities is making the space domain more disordered. Policy makers are scrambling to understand the national security and foreign policy implications of this new environment, and some have argued that current laws and treaties are outdated and not designed to accommodate the way space is being used today.[27] One of the policy implications of the second space age is that the availability of advanced space capabilities on the commercial market can potentially bring the advantages of space within the reach of rogue nations and non-state actors. As a result, it could make the world more transparent to the public and weaken the ability of state actors—including the U.S. Government—to control the flow of information.

22 Steve Puterski, "ViaSat reveals newest satellite, which will increase speed, capacity," *The Coast News*, January 12, 2017, http://www.thecoastnews.com/2017/01/12/viasat-reveals-newest-satellite-which-will-increase-speed-capacity/.

23 "Backgrounder: Wideband Global SATCOM," *Boeing*, October 2013, http://www.boeing.com/assets/pdf/defense-space/space/bss/factsheets/702/wgs/docs/Bkgd_WGS_1013.pdf.

24 For example, SpaceX is planning a constellation of 4,425 satellites and OneWeb plans to launch a constellation of 700 satellites, both intended to provide broadband Internet access.

25 "UCS Satellite Database," *Union of Concerned Scientists*, 2016, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WUFLvlXytQI.

26 "The Space Report: 2016 The Authoritative Guide to Global Space Activity," *Space Foundation*, 2016, 1, https://www.spacefoundation.org/sites/default/files/downloads/The_Space_Report_2016_OVERVIEW.pdf.

27 "Support Grows for the American Space Commerce Free Enterprise Act of 2017," Committee on Science, Space, & Technology, June 8, 2017, https://science.house.gov/news/press-releases/support-grows-american-space-commerce-free-enterprise-act-2017.

"What is different in the second space age is not that war could extend into space, but rather that a wider array of adversaries can begin to fight back against U.S. space capabilities."

While space has become more diverse, disruptive, and disordered, it is also more dangerous because the targets in space—particularly U.S. military satellites—are more attractive for adversaries to attack in a wide range of scenarios with a wide array of counterspace weapons. The 1991 Gulf War, 1999 NATO bombing campaign in Yugoslavia, and 2003 Iraq invasion demonstrated the tremendous advantage that U.S. military space systems provide as a force multiplier in conventional conflict, particularly in command and control (C2) and the employment of precision-guided weapons.[28] While in the First Gulf War, less than 8 percent of the munitions used were precision-guided (including both laser-guided and GPS-guided), by the 2003 Iraq invasion, more than 60 percent of the munitions used were precision-guided.[29] This trend continued to grow, and by the opening phases of operations in Syria in 2014, some 96 percent of munitions used were precision-guided.[30] The demand for satellite communications (SATCOM) has also grown significantly, in many cases outpacing the capacity of military systems and forcing DoD to lease capacity from commercial satellite operators. The increase in demand for satellite communications bandwidth in U.S. military operations has grown exponentially, from 100 megabits per second (Mbps) in the 1991 Gulf War to 250 Mbps in Joint Task Force Noble Anvil in 1999, 750 Mbps in the early months of Operation Enduring Freedom in Afghanistan in 2002, and 2,400 Mbps in the opening phases of Operation Iraqi Freedom in 2003.[31]

Other nations have taken note of the many advantages space provides to the U.S. military and its critical dependence on space-based capabilities. Some have attempted to replicate U.S. space capabilities to provide similar advantages for their own forces. Other nations have developed counterspace capabilities to reduce or eliminate the advantages space provides for the United States. China and Russia appear to be pursuing both strategies.[32] These developments indicate that space is a more strategically important domain in modern warfare, not just for the U.S. military but for others as well, which increases the potential for conflict in space.

Senior leaders in the U.S. military are quick to point out that conflict in space is not something that occurs in isolation. Instead of talking about a war in space, military leaders routinely refer to a war

28 Pawlikowski et al, "Space: Disruptive Challenges," 32.

29 Barry Watts, *The Evolution of Precision Strike* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2013), 14.

30 Mark Thompson, "These Are the Weapons the U.S. Is Using to Attack ISIS," *TIME*, September 23, 2014, http://time.com/3422702/isil-isis-syria-obama/.

31 Patrick Rayermann, "Exploiting Commercial SATCOM: A Better Way," *Parameters*, Winter 2003-2004, 55.

32 See, for example, Dean Cheng, "Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC," The Heritage Foundation, January 21, 2016, http://report.heritage.org/hl1270; Alexei Arbatov and Vladimir Dvorkin, eds., Outer Space: Weapons, Diplomacy, and Security (Washington, D.C.: Carnegie Endowment for International Peace, 2010).

that "extends into space."[33] One could argue, though, that war already extends into space every time space-based capabilities are used in combat, from GPS-guided weapons to unmanned aircraft controlled through satellite data links. The U.S. military uses its space systems across the full spectrum of conflict, from gray zone conflicts to high-end major theater war. It is only natural to expect that adversaries will attempt to disrupt, degrade, or destroy these systems.[34] What is different in the second space age is not that war could extend into space, but rather that a wider array of adversaries can begin to fight back against U.S. space capabilities —both from the ground and from space.

Further complicating matters, military satellite constellations that were once intended primarily for nuclear missions, and were thus protected by the cloak of nuclear deterrence, are now being used routinely for conventional warfighting at lower ends of the conflict spectrum. This calls into question whether a nuclear or non-nuclear adversary would be deterred from attacking these systems in a conventional conflict—especially if these systems are actively providing the U.S. military with a substantial advantage in that conflict. The second space age is more dangerous because old notions of deterrence and controlling escalation in space may no longer be valid.

33 Alyssa C. Gibson, "Senior leaders discuss US space posture," Peterson Air Force Base, May 2017, http://www.peterson.af.mil/News/Display/Article/1187328/senior-leaders-discuss-us-space-posture/.

34 Dr. Frank Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," The Heritage Foundation, 2017, http://index.heritage.org/military/2016/essays/contemporary-spectrum-of-conflict/.

THREATS TO SPACE SYSTEMS

THE THREATS TO SPACE SYSTEMS CAN BE DIVIDED into four distinct categories based on the mechanism of attack: kinetic physical, non-kinetic physical, electromagnetic, and cyber. Attackers may prefer to use different methods of attack depending on their target, intended effects, and access to counterspace technologies. Attacks can vary widely in terms of the effects they create, the reversibility of those effects, and the ability of the defender to attribute the attack back to the attacker. Attack mechanisms also vary in the awareness a defender and/or the public may have about an attack, the ability of the attacker to assess the damage, and the risk of collateral damage. The following section discusses the types of counterspace attacks that are possible as well as some open-source information on what other countries are known to be developing and testing.

– KINETIC PHYSICAL ATTACKS

KINETIC PHYSICAL ATTACKS ATTEMPT TO STRIKE A SATELLITE or detonate a warhead in its vicinity, while non-kinetic physical attacks attempt to disrupt or degrade the physical operation of a satellite without physical contact. The 2007 Chinese test of a direct-ascent ASAT weapon provides a stark example of the effects of kinetic physical attacks.[35] Satellites in LEO, where many imaging satellites reside, are more vulnerable to the type of direct ascent kinetic ASAT weapons used in the Chinese test, because lower altitude orbits are easier for countries with limited missile capabilities to reach, and thus more countries can attain this capability.

Missile defense systems can be adapted to serve as ASAT weapons, as the United States demonstrated in 2008 by launching an SM-3 missile to intercept and destroy a disabled U.S. military satellite that was projected to re-enter the atmosphere within days.[36] Because the SM-3 intercept occurred at a much lower altitude (246 km[37] versus over 850 km[38] for the Chinese ASAT test), the debris it created did not linger in orbit and threaten other satellites. Attacking satellites at higher altitudes—such as medium earth orbit (MEO) where Global Positioning System satellites reside, or geosynchronous orbit (GEO) where many communications and missile warning satellites are located—requires a larger, more complex missile with multiple stages. Higher orbits also take longer to reach, providing greater warning for the satellite being attacked. For example, a typical launch trajectory to geosynchronous orbit takes more than four hours to reach apogee. China appears to be developing and testing missiles with the capability to reach higher orbits, but tests since 2007 have been non-destructive.[39] According to the Director of National Intelligence, Russia is developing and testing a new generation of direct ascent ASAT weapons, including an air-launched ASAT missile.[40]

Satellites are also vulnerable to co-orbital threats whereby a satellite already in orbit can be used to attack another satellite. A space mine, for example, can be used to quietly trail a target satellite and detonate a small charge when commanded. A co-orbital satellite can also grab another satellite to move or de-orbit it. It could also attach itself to the target satellite and interfere with that satellite's operation.[41] A satellite can also be maneuvered into a crossing orbit to intercept a target satellite while giving little warning. As previously discussed, Russia developed co-orbital ASAT weapons beginning in the 1960s and continued testing them through the 1970s. China, India, Japan, and several

35 Kan, "China's Anti-Satellite Weapon Test," 1.

36 Department of Defense, "DoD News Briefing with Gen. Cartwright from the Pentagon," News Transcript, February 21, 2008, http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=4152.

37 Ibid.

38 Kan, "China's Anti-Satellite Weapon Test."

39 See Brian Weeden, "Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space," *Secure World Foundation*, (March, 2014), https://swfound.org/media/167224/through_a_glass_darkly_march2014.pdf.

40 U.S. Congress, Senate Committee on Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record, Daniel R. Coats, Director of National Intelligence, May 11, 2017, 9, https://www.intelligence.senate.gov/sites/default/files/documents/os-coats-051117.pdf.

41 U.S. Congress, Office of Technology Assessment, *Anti-Satellite Weapons, Countermeasures, and Arms Control* (Washington, D.C.: Government Printing Office, September 1985), 7.

European nations also have the requisite technology to build and launch small satellites for this purpose, and other nations could soon join their ranks.[42] Recent activity in space indicates that China may be testing on-orbit servicing and debris removal satellites that could also be used as co-orbital ASAT weapons.[43]

Rather than attacking the satellites on-orbit, an adversary could achieve similar effects by attacking the ground stations that support them. Ground stations are perhaps more vulnerable to attack, because they are often highly visible, located in foreign countries, and relatively soft targets. For military communications satellites, the data transmitted to and from forward-deployed users is often sent via satellite to a teleport ground station, where it is relayed through another satellite or terrestrial networks to users around the world. To reduce the dependence on ground stations, some military space systems use inter-satellite links to transmit data directly between satellites without passing through an intermediary ground station.

Ground stations are vulnerable to kinetic physical attack by several means. Guided missiles and rockets can be used to attack ground stations from range, while rocket-propelled grenades and small arms fire can be used to disable ground station antennas at close range. Ground stations can also be disrupted by attacking the electrical power grid, water lines, and the high-capacity communications lines that support them. While attacks against ground stations could have large implications, the effects would not be permanent. Unlike satellites, which require years to build and often cannot be repaired once they are launched, ground stations can be repaired in a matter of days or weeks, depending on the level of damage incurred.

Kinetic physical attacks tend to have catastrophic, destructive effects on the satellites and ground stations they target. Moreover, kinetic attacks in space create space debris that can damage satellites belonging to other nations or commercial entities that are not directly involved in the conflict. Kinetic weapons are usually attributable, their effects are often irreversible, and the risk of collateral damage is high.

– NON-KINETIC PHYSICAL ATTACKS

Non-kinetic forms of physical attack can be just as effective at disrupting, degrading, and destroying satellites while being less visible and, in some cases, more difficult to attribute. Directed energy weapons, such as lasers and high-powered microwave systems, can target space systems more quickly (within seconds) and create effects that may not be immediately evident to the satellite operator. Furthermore, directed energy weapons can be based on ships, aircraft, other satellites, or the ground. A high-powered laser, for example, can be used to damage critical satellite components (such as solar

42 Brian Garino and Jane Gibson, "Space System Threats," *AU-18 Space Primer* (Maxwell Air Force Base, Alabama: Air University Press, September 2009), 277.

43 "China's new Orbital Debris Clean-Up Satellite raises Space Militarization Concerns," *Spaceflight101*, June 29, 2016, http://spaceflight101.com/long-march-7-maiden-launch/aolong-1-asat-concerns/.

arrays) by overheating parts of a satellite. Additionally, a relatively low power laser can be used to temporarily dazzle or permanently blind the sensors on a satellite. The attacker, however, may not be able to anticipate whether the effects of its attack will be temporary or permanent. Even once an attack is conducted, the attacker will not know for sure if it was effective, because there may be no readily-evident external indications that a satellite's sensors are not working.

Targeting a satellite from Earth with a laser requires high beam quality, adaptive optics, and the advanced pointing control needed to steer the laser beam as it is transmitted through the atmosphere. This technology is costly and not widely available.[44] In September 2006, China reportedly illuminated U.S. satellites using ground-based lasers in what may have been an attempt to blind or dazzle the satellites, which is an indication that this technology, while advanced, is not beyond the reach of potential adversaries.[45] Intelligence also indicates that Russia is developing an airborne lazing platform, which can be more difficult to track and can target a wider array of orbits in a timely manner.[46]

A high-powered microwave (HPM) weapon can be used to disrupt a satellite's electronics and potentially cause permanent damage at higher power levels. A "front-door" HPM attack uses a satellite's own antennas as an entry path, while a "back-door" attack attempts to enter through small seams or gaps around electrical connections and shielding. A front-door attack is more straightforward to carry out, provided the HPM is positioned within the field of view of the antenna that it is using as a pathway, but it can be thwarted if the satellite uses circuits designed to detect and block surges of energy entering through the antenna. In contrast, a back-door attack is more challenging because it must exploit design or manufacturing flaws, but it can be conducted from any angle relative to the satellite. Both front-door and back-door HPM attacks can be difficult to attribute to an attacker, and like a laser weapon, the attacker may not know if the attack has been successful.[47]

Nuclear weapons can be used as physical weapons by detonating them in space or at a high altitude in order to create an electromagnetic pulse that damages the electronics in satellites. This form of attack, however, is indiscriminate in its effects because the electromagnetic pulse produced affects all satellites within line-of-sight. Additionally, the highly charged particles left behind from the event create a high radiation environment that affects all satellites within an orbital regime.[48] Testing of such weapons has been prohibited since the signing of the Partial Test Ban Treaty in 1963. More than 100 nations have signed and ratified the treaty, although China and North Korea have not.[49]

44 Garino and Gibson, "Space System Threats," 277.

45 Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, September 25, 2006.

46 Coats, "Worldwide Threat Assessment of the US Intelligence Community," 9.

47 David Wright, Laura Grego, and Lisbeth Gronlund, *The Physics of Space Security: A Reference Manual* (Cambridge, MA: American Academy of Arts and Sciences, 2005), 131-132, https://www.amacad.org/publications/Physics_of_space_security.pdf.

48 Steven James Lambakis, *On the Edge of Earth: The Future of American Space Power* (Lexington, KY: University Press of Kentucky, 2001), 123.

49 United Nations Office for Disarmament Affairs, "Treaty Banning Nuclear Weapons Test in Atmosphere, in Outer Space and Under Water," (August 5 1963), http://disarmament.un.org/treaties/t/test_ban/text.

– ELECTRONIC ATTACKS

RATHER THAN ATTEMPTING TO DAMAGE THE PHYSICAL COMPONENTS OF SPACE SYSTEM, electronic attacks target the means by which space systems transmit and receive data. Jamming is an electronic attack that uses radio frequency signals to interfere with communications. A jammer must operate in the same frequency band and within the field of view of the antenna it is targeting. Unlike physical attacks, jamming is completely reversible—once the jammer is disengaged, communications can be restored. An uplink jammer is used to jam signals going up to a satellite by creating enough noise that the satellite cannot distinguish between the real signal and the noise. Uplink jamming of the control link, for example, can prevent satellite operators from sending commands to the satellite. But because the uplink jammer must be within the field of view of the antenna on the satellite receiving the command link, the jammer must be physically located within the vicinity of the command station on the ground.[50]

While an uplink jammer can have broad effects across many users of a satellite, a downlink jammer has more localized effects. Downlink jammers target the users of a satellite by creating noise in the same frequency as the downlink signal from the satellite. A downlink jammer only needs to be as powerful as the signal being received on the ground and must be within the field of view of the receiving terminal's antenna. This limits the number of users that can be affected by a single jammer. Since many ground terminals use directional antennas pointed at the sky, a downlink jammer typically needs to be located above the terminal it is attempting to jam. This limitation can be overcome by employing a downlink jammer on an air or space-based platform, which positions the jammer between the terminal and the satellite. This also allows the jammer to cover a wider area and potentially affect more users.[51] Ground terminals with omnidirectional antennas, such as many GPS receivers, have a wider field of view and thus are more susceptible to downlink jamming from different angles on the ground.

The technology needed to jam many types of satellite signals is commercially available and relatively inexpensive. For example, U.S. forces experienced jamming in Iraq well after the fall of the Iraqi government, with at least five instances of hostile jamming of commercial SATCOM links documented.[52] amming can also be difficult to detect or distinguish from accidental interference, making attribution and awareness more difficult. In 2015, General John Hyten, the commander of Air Force Space Command, noted that the U.S. military was jamming its own communications satellites an average of 23 times per month.[53]

Spoofing is a form of electronic attack in which the attacker mimics a legitimate radio frequency signal to trick a target into locking onto a fake signal. An attacker can "spoof" the downlink from a satellite, causing users to lock onto a bogus signal and then use that signal to inject false data. An attacker

50 Garino and Gibson, "Space System Threats," 274-275.

51 Garino and Gibson, "Space System Threats," 275.

52 Hank Rausch, "Jamming Commercial Satellite Communications During Wartime: An Empirical Study," *Proceedings of the Fourth IEEE International Workshop on Information Assurance*, April 2006.

53 Sydney Freedberg, "US Jammed Own Satellites 261 Times; What If Enemy Did?," *Breaking Defense*, December 2, 2015, http://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/

can also spoof the command and control uplink signal to a satellite and take control of the satellite for nefarious purposes. The best protections against this type of spoofing are encryption of the signal, because an attacker will need to crack the encryption to produce a signal that appears to be legitimate, and highly directional antennas that block out signals from other directions.

In 2011, Iran claimed to have downed a U.S. remotely piloted aircraft by using some combination of jamming and GPS spoofing.[54] Subsequent research has shown that even encrypted military GPS signals can be spoofed by a device that records the encrypted signal and rebroadcasts it with a slight delay, a process known as "meaconing."[55] This does not require cracking the GPS encryption, because the rebroadcast signal is merely a time-delayed copy of the original signal. By gradually adjusting the amount of time delay inserted, an autopilot system using GPS for navigation can be tricked into thinking it is flying straight and level, when in fact it is climbing, descending, or turning.

– CYBER ATTACKS

LIKE MANY OTHER MODERN MILITARY SYSTEMS, satellites are also vulnerable to cyber attacks. Cyber attacks can be used to intercept data, corrupt data, or seize control of systems for malicious purposes. Unlike electronic attacks, which interfere with the transmission of radio frequency signals, cyber attacks target the data itself and the systems that use this data. Any data interface in the system is a potential intrusion point, including the antennas on both the satellites and ground stations as well as the landlines connecting ground stations to terrestrial networks. The effects of a cyber attack on space systems can range from loss of data to widespread disruptions and can potentially lead to the permanent loss of a satellite. If an adversary could seize control of a satellite through a cyber attack, it could shut down all communications and destroy the satellite by expending its propellant supply or damaging its electronics. Moreover, it may be difficult for controllers to know what caused a satellite to lose control, since accidental malfunctions occur from time to time. Attribution for a cyber attack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

In 2009, it was revealed that insurgents in Iraq were using commercially available software to intercept and decode video over satellite communication links from U.S. surveillance aircraft. This was possible because some U.S. aircraft did not have the equipment needed to encrypt video feeds, and it enabled the insurgents to see what the U.S. military was seeing in near real-time.[56] The U.S.-China Economic and Security Review Commission has also cited examples in the past in which cyber attacks were used against the command and control systems of U.S. government satellites. According to the

54 Adam Rawnsley, "Iran's Alleged Drone Hack: Tough, But Possible," *WIRED*, December 16, 2011, https://www.wired.com/2011/12/iran-drone-hack-gps/.

55 Richard B. Langley, "Innovation: GNSS Spoofing Detection," *GPS World*, June 1, 2013, http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/.

56 Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal*, December 17, 2009.

Commission's 2011 report, one of the more successful attacks was targeted at NASA's Terra EOS satellite in 2008.[57] On two instances in June and October of that year, hackers reportedly gained control of the satellite for 2 minutes and 9 minutes, respectively, although they did not execute any commands.[58]

– SUMMARY OF THREATS

As shown in the table below, the threats to space systems vary significantly from relatively low-end threats to more sophisticated methods of attack. At one end of the spectrum are threats, such as direct ascent kinetic ASAT weapons, which are attributable, require advanced technology, are irreversible, and produce effects that are publicly visible. At the other end of the spectrum are threats such as uplink jamming, which are fully reversible, more difficult to attribute, and do not always require advanced technology. While U.S. national security space systems are used to support the full spectrum of conflict, they are not designed to be resilient against the full spectrum of threats. Nearly all of the military satellites in operation today were designed for a relatively benign space environment where threats were more limited and could be deterred by the threat of nuclear escalation.

– COMPLICATING FACTORS IN SPACE

SEVERAL FACTORS—some of which are unique to the space domain—serve to complicate planning and strategy development in space. One complication is the remoteness of the space domain. Satellites can range in altitude from just a few hundred kilometers above the Earth's surface in LEO to some 36,000 kilometers in GEO and beyond. Moreover, they must travel at high velocities to stay in orbit, ranging from 8 km per second in LEO to 3 km per second in GEO. The distance and speed at which satellites operate makes them difficult to physically inspect and track, and it makes awareness, attribution, and damage assessment from attacks more challenging. For example, an operator will know if its satellite stops functioning, but it can take days or weeks to determine precisely what occurred. Attribution can also be difficult because attacks can emanate from many different sources, and some forms of attack can easily be confused with accidental malfunctions. A satellite operator may need to conduct a root cause analysis long after an incident occurs in order to determine what happened and why.

Determining if an attack was successful can be difficult for the offensive side of an engagement because the remoteness of space makes direct inspection of the target satellite difficult. While the effects of a kinetic ASAT attack are readily visible from the orbital debris created, the attacker may not be able to see the effects of non-kinetic physical, electronic, and cyber attacks. To know if an attack is successful, the attacker may need to monitor a target satellite for days or weeks following an attack

57 U.S.-China Economic and Security Review Commission, *2011 Report to Congress*, 216.

58 Matthew Humphries, "Chinese hackers took control of NASA satellite for 11 minutes," *Geek.com*, November 9, 2011, https://www.geek.com/geek-pick/chinese-hackers-took-control-of-nasa-satellite-for-11-minutes-1442605/.

Type of Attack	Direct Ascent ASAT	Co-orbital ASAT	Ground Station Attack	High Altitude Nuclear Detonation	High-Powered Laser	Laser Dazzling / Blinding	High-Powered Microwave	Uplink Jamming	Downlink Jamming	Spoofing	Cyber—Data Intercept / Monitoring	Cyber—Data Corruption	Cyber—Seizure of Control
Attribution	Launch site can be attributed	Can be attributed by tracking previously known orbit; Irreversible	Variable attribution, depending on mode of attack	Launch site can be attributed	Limited attribution	Clear attribution of the laser's location at the time of attack	Limited attribution	Modest attribution, depending on mode of attack	Modest attribution, depending on mode of attack	Modest attribution, depending on mode of attack	Limited / uncertain attribution	Limited / uncertain attribution	Limited / uncertain attribution
Reversibility	Irreversible	Irreversible or reversible, depending on capabilities	Irreversible	Irreversible	Irreversible	Reversible or irreversible, although attacker may not be able to control	Reversible or irreversible, although attacker may not be able to control	Fully reversible	Fully reversible	Fully reversible	Fully reversible	Fully reversible	Irreversible or reversible, depending on mode of attack
Awareness	Publicly known, depending on trajectory	May or may not be publicly known	May or may not be publicly known	Publicly known	Only satellite operator will be aware	Only satellite operator will be aware	Only satellite operator will be aware	Only satellite operator will be aware	Satellite operator will be aware, may or may not be known to the public	Satellite operator and public may not be aware	Satellite operator and public may not be aware	Satellite operator and public may not be aware	Satellite operator and public may not be aware
Attacker Damage Assessment	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled	No confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled	No confirmation of success	Limited confirmation of success if monitoring of the local RF environment is possible	Limited confirmation of success if effects are visible	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success
Collateral Damage	Orbital debris could affect other satellites in similar orbits	May or may not produce orbital debris affecting other satellites in similar orbits	Ground station may control multiple satellites, potential for loss of life at the ground station	Indiscriminate effects from higher radiation levels in orbit that would persist for months or years	Could leave target satellite disabled and uncontrollable	None, only damages the target satellite's sensors	Could leave target satellite disabled and uncontrollable	Only disrupts the signals targeted and possibly adjacent frequencies	Only disrupts the signals targeted and possibly adjacent frequencies	Only corrupts the specific RF signals targeted	None	None	Could leave target satellite disabled and uncontrollable

to look for signs of whether the satellite is still functioning, such as routine orbital maneuvers and communications with a ground station. Even then, the attacker may not be able to discern the effect of the attack. For example, if a laser is used to blind an imaging satellite, the attacker may never know for sure if the satellite was permanently disabled, temporarily dazzled, or not affected at all unless the operator of the satellite chooses to disclose this information.

The space domain is also uninhabited, with the exception of the International Space Station and occasional Chinese human spaceflight missions. While some plans were considered early in the space age to develop inhabited military space stations, these plans were ultimately abandoned.[59] The added weight and cost of including humans in military space systems was not worth the marginal benefit in capabilities. There are no military targets in space with humans on board, which means warfighting in space could be conducted remotely by both the attacker and defender with little to no direct risk to human life. This may make it psychologically easier to attack targets in space because there is no direct threat to human life. In other domains, the potential for the loss of life, especially for non-combatants, can complicate decision-making for war planners and reduce the impetus to attack.

Another complicating factor in the space domain is the lack of borders. The only orbit in which satellites do not move relative to the surface of the Earth is geostationary orbit—a thin ring circling the Earth at nearly 36,000 km above the equator. Satellites in all other orbits, including LEO, MEO, HEO, and GEO orbits not aligned with the equator, move relative to the Earth and cross over the territory of other nations. Unlike the air, maritime, and ground domains, no nation has control of the orbital space above or adjacent to its territory. The physics of orbital mechanics makes space inherently a global domain where the actions of one nation can affect all others, and objects placed in orbit will often pass over the territory of other nations. For example, orbital debris created by one nation (or private actor) can intercept the orbits of all other satellites in a similar orbital regime. And unlike other domains, international law, treaties, and norms of behavior are less developed in the space domain.

59 Leonard David, "Declassified: US Military's Secret Cold War Space Project Revealed," *Space.com*, December 30, 2015, https://www.space.com/31470-manned-orbiting-laboratory-military-space-station.html.

SPACE DETERRENCE AND ESCALATION

ON NOVEMBER 29, 1957, less than two months after Sputnik was launched, U.S. Air Force Chief of Staff General Thomas White asserted, "[w]e airmen who have fought to assure that the United States has the capability to control the air are determined that the United States must win the capability to control space."[60] Sixty years later, the unique attributes of outer space continue to pose a challenge for both policymakers attempting to control space and scholars trying to understand deterrence and escalation dynamics.[61]

60 Quoted in Bob Preston, Dana J. Johnson, Sean J.A. Edwards, Michael Miller, and Calvin Shipbaugh, *Space Weapons: Earth Wars* (Santa Monica, CA: RAND Corporation, 2002), 9.

61 According to doctrine, space control is defined as "providing freedom of action in space for friendly forces while, when necessary, denying it to an adversary. It includes offensive and defensive operations by friendly forces to gain and maintain space superiority and situational awareness of events that impact space operations." Description based on U.S. Joint Chiefs of Staff, *Joint Doctrine for Space Operations*, Joint Publication 3-14, August 9, 2002.

As General White's quote indicates, experts often try to apply lessons from existing domains—ground, maritime, and air—to better understand dynamics in emerging domains. This is particularly true of a domain such as space, in which no major conflict has occurred. Indeed, space resembles other domains in some significant ways. Just as international waters and airspace cannot be claimed by any sovereign state and remain free for use by all actors, so too does space. As with nuclear weapons, military activities in space were initially limited to a small subset of highly advanced states, with policy implications that continue today. Similar to the cyber domain, space remains dependent on advanced communication technologies for which software is often more important than hardware. Finally, many space capabilities and users of space assets are resident on the ground, and escalation in space is more likely to emerge from terrestrial conflicts than begin in space itself.

Thus, there are many reasons to believe that lessons from the ground, maritime, air, nuclear, and cyber domains can be applied to space.[62] Yet, space is in many ways a peculiar domain. Unlike the nuclear or cyber domains, space is a physical region, not a capability type. Unlike the ground, maritime, and air domains, sovereign rights do not extend to space. Unlike all these domains, no major conflict has taken place in space, leaving experts without an empirical test of how a conflict in space would actually occur or escalate. These differences require scholars and policymakers to think carefully before applying the traditional literature on deterrence to space conflicts.

This chapter attempts to address this gap in the literature by examining space deterrence and escalation dynamics through a theoretical lens. It begins by describing the core tenets of deterrence theory and suggesting how basic deterrence logic might be applied to space.[63] The next section discusses similarities and differences between the evolution of deterrence in the second nuclear age and the second space age. The final section synthesizes these lessons and suggests key questions that policymakers should consider as they apply theoretical lessons to deter and respond to escalation in space.

– THE FOUNDATIONS OF DETERRENCE THEORY

DETERRENCE THEORY HAS A RICH HISTORY, largely rooted in early thinking about nuclear strategy. In one of its central texts, Glenn Snyder defines deterrence as "discouraging the enemy from taking

62 Scott Pace argues that "Deterrence in space is not different from deterrent on the land, seas or in the air: the focus is on understanding the thinking of an opponent." Scott Pace, "Strengthening Space Security," Harvard International Review, 33.4, (Spring 2012), 59.

63 A number of outstanding works address elements of these questions, including Forest E. Morgan, "Deterrence and First-Strike Stability in Space," *RAND Corporation*, 2010; Bruce W. MacDonald et al., Crisis Stability in Space: China and Other Challenges (Washington, D.C.: Foreign Policy Institute, 2016); Paul Stares, *Space and National Security* (Washington, D.C.: Brookings Institution Press, 1987); Joan Johnson-Freese, *Space Warfare in the 21st Century: Arming the Heavens* (New York, NY: Routledge, 2017); Bob Preston, Dana J. Johnson, Sean J.A. Edwards, Michael Miller, and Calvin Shipbaugh, *Space Weapons: Earth Wars* (Santa Monica, CA: RAND Corporation, 2002); Peter L. Hays, James M. Smith, Alan R. Van Tassel, Guy M. Walsh, *Spacepower for a New Millennium: Space and U.S. National Security* (New York: McGraw-Hill, 2000); James Clay Moltz, *The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests* (Stanford, CA: Stanford University Press, 2008).

military action by posing for him a prospect of cost and risk outweighing his prospective gain."[64] Deterrence therefore exists in the mind of one's adversary. As a result, deterrence of aggression against space systems is simply an extension of deterrence in other domains. Deterrence succeeds by altering the cost-benefit calculus of a potential aggressor. Snyder argues that an aggressor's risk calculus is the result of: "(1) his valuation of an objective; (2) the cost which he expects to suffer in an attack on the objective, as the result of various possible responses by the deterrer; (3) the probability of various responses, including 'no response'; and (4) the probability of winning the objective with each possible response."[65] Deterrence can succeed by altering any of these four components so that the expected costs are greater than the expected benefits.

"Deterrence succeeds by altering the cost-benefit calculus of a potential aggressor."

Most deterrence approaches tend to focus on increasing the costs that an aggressor expects to pay for taking an action (although it is also possible to increase the benefits for taking other actions). After all, as Richard Betts explains, "an enemy will not strike if it knows the defender can defeat the attack or can inflict unacceptable damage in retaliation."[66] Changing an aggressor's expected costs requires that the deterrer focus on three elements: capability, credibility, and communication.

Capability is necessary to convince an aggressor that the deterrer could respond to an attack. A deterrer's capability—which Snyder defines as "the capacity to affect object values by application of a power base"—must be sufficient to damage an aggressor's objects of interests.[67] The deterrer can utilize threats to escalate in the same domain (vertical escalation) or in a different domain (horizontal escalation). In many cases, a deterrer may wish to escalate in other domains, locations, or periods in order to leverage the deterrer's strengths against the aggressor's weaknesses. In the early Cold War period, for example, John Foster Dulles and others preferred to respond to Soviet attacks "at a time and place of our choosing" rather than replying directly.[68] Herman Kahn built on this concept by distinguishing among three types of escalation capabilities: "increasing intensity, widening the area, or compounding escalation."[69]

Credibility is necessary to persuade an aggressor that the deterrer would respond to an attack. Leading deterrence theorist Thomas Schelling warned, "We often forget that both sides of the choice, the threatened penalty and the proffered avoidance or reward, need to be credible."[70] Credibility, in turn,

64 Glenn Herald Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961), 3.

65 Glenn H. Snyder, "Deterrence and Power," *The Journal of Conflict Resolution* 4, no. 2 (1960), 167.

66 Richard K. Betts, "The Lost Logic of Deterrence," *Foreign Affairs* 92, no. 2 (March–April 2013). See also Patrick M. Cronin, *The Challenge of Responding to Maritime Coercion* (Washington, D.C.: Center for a New American Security, September 2014).

67 Snyder, "Deterrence and Power," 165.

68 Herman Kahn and Evan Jones, *On Thermonuclear War* (New Brunswick, CT: Transaction Publishers, 2007), 37.

69 Herman Kahn, *On Escalation: Metaphors and Scenarios* (New Brunswick, NJ: Transaction Publishers, 2010), 4.

70 Thomas C. Schelling, *Arms and Influence* (New Haven; London: Yale University Press, 1976), 75.

was defined by Snyder as "the perception by the threatened party of the degree of probability that the power-wielder will actually carry out the threat if its terms are not complied with or will keep a promise if its conditions are met."[71] Credibility is thus highly context dependent; credibility results from an assessment about the likelihood that a deterrer will respond to a specific action by a specific party in a specific way at a specific time.[72] More recent research has suggested that credibility may derive either from the deterrer's perceived power and interests or from their perceived reputation for resolve[73].

Communication is necessary to demonstrate that a deterrer is both capable and credible. After all, a highly capable and credible deterrent is worthless unless it is perceived that way by the potential aggressor. Despite incentives for clear communication, Robert Jervis writes that there are at least five reasons to expect communication challenges:

> First, in almost no interactions do two adversaries understand each other's goals, fears, means-ends beliefs, and perceptions… Second, the adversary will miss or misperceive many of the state's signals… Third, commitments by one actors that are objectively clear and credible… may not be perceived by another… Fourth, actors tend to overestimate the potency of threats and underestimate the utility of rewards and reassurances. Fifth, threats and conciliation generally need to be combined, but their optimal mixture and timing is extremely difficult.[74]

Additional complications in the space domain include the remoteness of space and the highly classified nature of some space systems, which can limit each side's awareness of what the other can do or is doing. Taken together, these reasons for communication failures suggest that there are abundant opportunities for deterrence to break down.

How can states effectively communicate their capability and credibility to deter? James Fearon suggests leaders can either "(a) tie hands by creating audience costs that they will suffer *ex post* if they do not follow through on their threat or commitment… or (b) sink costs by taking actions such as mobilizing troops that are financially costly *ex ante*."[75] Statements and actions of this sort should be particularly credible because they are costly to the deterrer and should therefore communicate real commitment. For example, an elected leader might publicly warn a potential aggressor against taking a specific action, suggesting that he or she would be punished at the ballot box if aggression were to occur, and the leader failed to act. Conversely, that leader could put military forces into danger, demonstrating commitment with a costly and risky action. Additionally, Keren Yarhi-Milo has shown that particularly vivid, non-costly actions and statements may also alter an aggressor's perception of a deterrer's credibility. After all, the inclination of leaders "to rely on their own judgments and subjec-

71 Snyder, "Deterrence and Power," 164.

72 Keren Yarhi-Milo, "In the Eye of the Beholder: How Leaders and Intelligence Communities Assess the Intentions of Adversaries," *International Security* 38, no. 1 (2013), 7-51.

73 Daryl G. Press, *Calculating Credibility: How Leaders Assess Military Threats* (Ithaca, NY: Cornell University Press, 2007); Joshua D Kertzer, Resolve in International Politics (Princeton, N.J: Princeton University Press, 2016), 8.

74 Robert Jervis, "Rational Deterrence: Theory and Evidence," *World Politics* 41, no. 2 (1989), 198.

75 James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs," *Journal of Conflict Resolution* 41, no. 1 (February 1997), 68.

tive reading of signals to infer political intentions is pervasive and universal."[76]

Having established the basic definition of deterrence and the importance of communicating capability and credibility to a potential aggressor, it is now possible to discuss deterrence strategies. Lawrence Freedman notes that deterrence can "be achieved by limiting gains as much as imposing costs."[77] Thus, a deterrer can either threaten to deny the aggressor its objective or threaten to punish an aggressor. Freedman observes that, "[p]reventing gain by means of a credible ability to stop aggression in its tracks became known as deterrence by denial, while imposing costs became deterrence by punishment."[78] Deterrence by punishment seeks to communicate to an aggressor that if it proceeds with a proscribed action, it will suffer pain that is too great to make the action worthwhile. Deterrence by denial involves convincing an aggressor that if it proceeds with a proscribed action, it will not achieve its goals.[79] Deterrence by punishment must typically threaten a severe response, as the United States did by threatening to use nuclear weapons in response to a Soviet conventional military attack in the early Cold War. Such major escalations, though, are often less credible than efforts to deter by denial. For this reason, Forest Morgan, Karl Mueller, Evan Medeiros, Kevin Pollpeter, and Roger Cliff argue that "a more reliable strategy for deterring deliberate escalation is one that buttresses threats of punishment with visible capabilities for denial."[80]

> "Thus, deterrence and defense go hand in hand, although the capabilities most valuable for deterrence may not be those most valuable for defense."

If deterrence succeeds completely, then an aggressor takes no action. Thus, general deterrence holds when a crisis does not arise at all.[81] This form of deterrence success is easy to overlook. Yet, deterrence failure is another matter. A failure of general deterrence can result in an immediate challenge. Robert Jervis comments that if an aggressor decides to challenge a deterrent commitment, then "[t]he very fact that a case of immediate deterrence arises means that the defender thought he had a defensible position and the challenger thought that he could get his way by force or coercion."[82] Unlike general deterrence, immediate deterrence occurs when an aggressor contemplates action, but a challenge is resisted without violence.[83] If an immediate deterrent threat fails, however, then the deterrer is left with no choice but to defend itself. Defense, in this context, means reducing "prospective costs and

76 Keren Yarhi-Milo, "In the Eye of the Beholder: How Leaders and Intelligence Communities Assess the Intentions of Adversaries," *International Security* 38, no.1 (2013), 13.

77 Lawrence Freedman, *Strategy: A History* (Oxford: Oxford University Press, 2015), 159.

78 Ibid.

79 Snyder, *Deterrence and Defense*, 14–16.

80 Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND Corporation, 2008), xiii.

81 Also see Paul Huth and Bruce Russett, "Testing Deterrence Theory: Rigor Makes a Difference," *World Politics* 42, no. 4 (1990), 474.

82 Robert Jervis, "Rational Deterrence: Theory and Evidence," *World Politics* 41, no. 2 (1989), 194.

83 Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: SAGE Publications, 1983), 31–43.

risks in the event that deterrence fails."[84] As Snyder notes, "[d]eterrence works on the enemy's intentions… Defense reduces the enemy's capability to damage or deprive us."[85] Thus, deterrence and defense go hand in hand, although the capabilities most valuable for deterrence may not be those most valuable for defense.[86]

The basics of deterrence theory are second nature to many who remember Cold War debates on deterrence strategy. However, before proceeding to apply this theory to the space domain, it is helpful to briefly review how deterrence evolved in the nuclear domain during the early Cold War.

– PARALLELS IN THE EVOLUTION OF NUCLEAR AND SPACE DETERRENCE

AS BRUCE MACDONALD NOTES, "[i]n certain respects, offensive capabilities in the contemporary space domain closely resemble nuclear assets in the early days of the nuclear era."[87] For this reason, the evolution of nuclear deterrence strategy can be a useful guide for those seeking to understand deterrence in space. Of course, the unique characteristics of space make applying nuclear deterrence theory difficult. Karl Mueller warns that "the parallels between nuclear and space deterrence are thought provoking and potentially illuminating. However, each of these domains involves key characteristics that are unique to it, so understanding one does not imply or constitute mastery of the other."[88] Yet, there are some valuable lessons across the two domains. Nuclear strategy may not provide the right answers, but it can highlight the right questions to ask.

The Evolution of Nuclear Deterrence

As scholars and policymakers in the United States developed deterrence theory during the early Cold War, they began to understand the basic dynamics of the nuclear domain. Robert Haffa, Ravi Hichkad, Dana Johnson, and Philip Pratt reflect that "[d]uring the first nuclear age, Cold War nuclear strategy was driven by clearly stated intentions and demonstrated capabilities of the two principals to ensure a bipolar nuclear

84 Ibid.

85 Snyder, *Deterrence and Defense: Toward a Theory of National Security*, 3.

86 Snyder notes "[t]he need to choose between deterrence and defense is largely the result of the development of nuclear and thermonuclear weapons and long-range airpower. Prior to these developments, the three primary functions of military force—to punish the enemy, to deny him territory (or to take it from him), and to mitigate damage to oneself—were embodied, more or less, in the same weapons… Long-range airpower partially separated the function of punishment from the function of contesting the control of territory, by making possible the assault of targets far to the rear whose relation to the land battle might be quite tenuous." Glenn Snyder, Deterrence and Defense: Toward a Theory of National Security (Princeton, NJ: Princeton University Press, 1961), 8.

87 Bruce W. MacDonald et al., *Crisis Stability in Space*, 15.

88 Karl P. Mueller, "The Absolute Weapon and the Ultimate High Ground: Why Nuclear Deterrence and Space Deterrence Are Strikingly Similar - Yet Profoundly Different," quoted in Michael Krepon and Julia Thomas, eds., *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations* (Washington, D.C.: Stimson Center: 2013), 48.

balance of power."[89] At the time, nuclear capabilities were dominated by the United States and the Soviet Union. Both superpowers constructed substantial nuclear forces, although the United States retained an edge for the first few decades of the Cold War. It took years for nuclear technology to proliferate, and when it did, other states built only limited nuclear arsenals. As a result, nuclear strategy was treated as a largely bipolar affair. The bipolar configuration made early nuclear strategy an ideal area for the application of complex deterrence logic that was rooted in the application of game theory.

One early challenge for nuclear strategists was whether to rely on nuclear deterrence to prevent not just a nuclear attack but a conventional conflict as well. The Soviet Union's size and rapidly modernizing military drove U.S. leaders to question their ability to stop a Soviet invasion without reliance on nuclear weapons.[90] Seeking to avoid another major land war on the Eurasian continent, or the creation of a garrison state, Dwight Eisenhower endorsed a "New Look," which relied on nuclear deterrence through massive retaliation, rather than a dramatic increase in the size of U.S. conventional forces. As John Foster Dulles explained in January 1954, "We want, for ourselves and the other free nations, a maximum deterrent at a bearable cost. Local defense will always be important. But there is no local defense which alone will contain the mighty landpower of the Communist world. Local defenses must be reinforced by the further deterrent of massive retaliatory power."[91] Deterrence by denial seemed untenable given growing Soviet military capabilities in Europe, so U.S. leaders adopted a strategy of massive retaliation and deterrence by punishment. In the early 1950s, then-Vice President Richard Nixon pushed for reliance on nuclear threats to avoid letting "the Communists nibble us to death all over the world."[92] Early views of deterrence in the nuclear domain seemed to favor the use of maximal threats, even against minimal attacks.

Massive retaliation relied on the U.S. capability advantage, but it soon created a credibility gap. Eisenhower and Dulles had relied on brinksmanship to deter Soviet attacks. As Dulles noted, "If you cannot master it, you inevitably get into war. If you try to run away from it, if you are scared to go to the brink, you are lost."[93] Yet, William Kaufman argued that U.S. strategy was not credible, because U.S. leaders "do not tend to retaliate massively against anyone except in the face of provocations as extreme as Pearl Harbor… the minimum requirements of credibility have not been fulfilled in the case of massive retaliation."[94] Thus, despite the vast U.S. nuclear arsenal, Snyder notes that the Soviets could still engage in "a range of minor ventures which they can undertake with impunity, despite the objective existence of some probability of retaliation."[95] This phenomenon became known as the stability-insta-

89 Robert P. Haffa, Jr., Ravi R. Hichkad, Dana J. Johnson, and Philip W. Pratt, "Deterrence and Defense in 'The Second Nuclear Age'," *Northrop Grumman*, March 2009, 5, http://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/Deterrence-and-Defense-in-seco.pdf.

90 See Frank C. Gavin, "What's in a Name? The Genius of Eisenhower," *War on the Rocks*, June 15, 2017, https://warontherocks.com/2017/06/whats-in-a-name-the-genius-of-eisenhower/.

91 John Foster Dulles, "The Evolution of Foreign Policy," Department of State, Press Release No. 81 (January 12, 1954), http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/article-dulles-retaliation_1954-01-12.htm.

92 Nixon quoted in *The New York Times*, March 14, 1954, 44.

93 Dulles quoted in James Shepley, "How Dulles Averted War," *Life*, 78, January 16, 1956.

94 Kaufmann, "The Requirements of Deterrence."

95 Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961), 226.

bility paradox, which Jervis describes by noting, "To the extent that the military balance is stable at the level of all-out nuclear war, it will become less stable at lower levels of violence."[96]

By the late 1950s, it was clear that a new strategy was required to reestablish U.S. credibility. U.S. leaders were forced to reassess their approach when the Soviets announced their intercontinental ballistic missile capability in August 1957, thereby negating the U.S. nuclear edge. By 1958, Albert Wohlstetter observed that "the notion of massive retaliation as a responsible retort to peripheral provocations vanished."[97] Soon McGeorge Bundy complained, "The only plan the United States had for the use of strategic weapons was a massive, total, comprehensive obliterating attack upon the Soviet Union… the Warsaw Pact countries and Red China."[98]

The alternative approach that the Kennedy administration chose was flexible deterrence. As Kennedy explained, "The primary purpose of our arms is peace, not war—to make certain that they will never have to be used—to deter all wars, general or limited, nuclear or conventional, large or small."[99] He sought improved command and control in order to establish strategic deterrence that was "more flexible, more selective, more deliberate, better protected and under ultimate civilian authority at all times."[100] This strategy provided the United States with a more robust deterrence-by-denial capability, by investing in U.S. capabilities that could defeat Soviet forces before they could obtain their territorial objectives. The central concept of flexible response was to give the United States graduated deterrence options, ranging from direct defense to deliberate escalation and finally culminating with a general nuclear response. This coupled deterrence by denial with deterrence by punishment. Indeed, Jervis notes, "since the 1960s, the United States has sought to make denial the first line of deterrence, keeping the possibility of extreme punishment as the ultimate threat."[101]

The Evolution of Space Deterrence

The development of deterrence concepts for space followed a similar track as those for the nuclear domain. Michael Krepon defines space deterrence as "deterring harmful actions by whatever means against national assets in space and assets that support space operations."[102] Initially, he notes that policymakers "considered warfare in space to be linked to nuclear warfare… attacks on critical assets and infrastructure in space commonly were viewed in the gravest terms, regardless of whether they were precursors to attacks on nuclear forces."[103] In the second space age, however, space has come to be seen as a separate domain with different characteristics and escalation dynamics.

96 Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca, NY: Cornell University Press, 1981), 31.

97 Albert Wohlstetter, "The Delicate Balance of Terror," *Foreign Affairs* 37, no. 2 (January 1959), 211–234.

98 Kennedy quoted in Richard Reeves, *President Kennedy: Profile of Power* (New York: Simon & Schuster, 1994), 179.

99 John F. Kennedy: "Special Message to the Congress on the Defense Budget.," March 28, 1961, Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*, http://www.presidency.ucsb.edu/ws/?pid=8554.

100 Ibid.

101 Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Cornell University Press, 1989), 12.

102 Michael Krepon, "Space and Nuclear Deterrence," quoted in Michael Krepon and Julia Thomas, eds., *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations* (Washington, D.C.: Stimson Center: 2013), 5.

103 Ibid., 26.

As previously discussed, early in the emergence of the space domain, efforts were made to prevent attacks in space. U.S. leaders warned explicitly against attacks on U.S. early warning systems or command and control satellites. As the space domain matured, however, the United States came to be reliant on space for a variety of conventional military requirements and commercial activities, which called into question long-standing U.S. deterrence policy. Indeed, by the turn of the millennia, the Commission to Assess the Ballistic Missile Threat to the United States (also known as the Rumsfeld Commission) found that "[t]he commercial revolution in space has eliminated the exclusive control of space once enjoyed by national defense, intelligence and government agencies."[104] As a result, U.S. leaders sought "tactical denial of capabilities" rather than "permanent destruction," which put a premium on "temporary and reversible" options.[105]

As the post-Cold War environment continued to develop, it became clear that old notions of deterrence in space would not suffice for new realities. In 2011, the Obama administration's National Security Space Strategy articulated a deterrence strategy with four key elements: 1) supporting norms of responsible behavior; 2) building coalitions to enhance collective security; 3) enhancing resilience; and 4) preparing to respond to an attack proportionally, but not necessarily symmetrically or in space, using any or all elements of national power.[106] This is a far cry from the traditional conceptions of massive retaliatory responses against attacks on space systems.

Yet, the U.S. military's reliance on space is growing and questions remain about the viability of the U.S. deterrent posture. General John Hyten, Commander of U.S. Strategic Command, has warned that the loss of U.S. space capabilities would send the U.S. military "back to World War Two… back to industrial age warfare."[107] Similarly, General Robert Kehler, former Commander of Air Force Space Command, has explained, "[t]he space capabilities we provide today are embedded in all of our combat operations. We cannot fight the way America fights without space capabilities. Space has become a contested environment, and we know that in any conflict our adversaries will try to deny us use of those space capabilities."[108] Combining the growing U.S. reliance on space and the increasingly contested nature of the domain, Bruce MacDonald worries that "U.S. space capabilities are critical enablers for joint forces, but they may become an American Achilles heel unless steps are taken to offset growing vulnerabilities in its space architecture."[109] How can the United States adopt a deterrence strategy for space that adapts to these new realities?

104 "Space: Today and the Future," prepared for the Commission to Assess United States National Security Space Management and Organization" (2001), 12.

105 John J. Hamre quoted in "U.S. Objectives for Space," prepared for the Commission to Assess United States National Security Space Management and Organization" (2001), 28.

106 "U.S. National Security Space Strategy", (summary, U.S. Government, 2011).

107 General John Hyten, U.S.-China Economic and Security Review Commission, "China's Space and Counterspace Programs," quoted in *2015 Report to Congress* (Washington, D.C.: USCC, November 2015), 317.

108 Bruce W. MacDonald et al., *Crisis Stability in Space*, 6.

109 Ibid.

– LESSONS FOR SPACE DETERRENCE

WHAT LESSONS DOES THE DEVELOPMENT OF NUCLEAR DETERRENCE THEORY hold for the current space age? Some of the historical parallels are obvious. For starters, both domains were initially dominated by two great powers—the United States and the Soviet Union. Along these lines, Karl Mueller notes, "Nuclear and military space capabilities both began as the exclusive domain of the superpowers, and subsequently have spread gradually to other countries."[110] This incentivized strategists to discount the importance of other actors. Reflecting on the development of nuclear strategy, Vipin Narang warns that "virtually the entire corpus of existing scholarship on nuclear strategy and deterrence focuses on these two globally dominant states with massive nuclear architectures. None of this work addresses the question of whether the smaller arsenals and different strategies of the regional nuclear powers are sufficient to deter nuclear and conventional attack."[111] The same is true of the literature on space deterrence. Too often, scholars have thought of space deterrence as a "two-body problem" using bipolar concepts developed during the Cold War, but a more diverse space environment is increasingly challenging these notions. For this reason, MacDonald argues, "Because the technologies involved are becoming widespread, a monopoly on space power, or a position of serious space dominance, is neither credible nor sustainable."[112]

Might new space players adopt different deterrence strategies than the superpowers did in the Cold War? If research on nuclear postures can be extended to the space domain, then the answer may be yes. For example, Narang suggests that states pursue one of three nuclear postures: assured retaliation, asymmetric escalation, or a catalytic strategy.[113] These postures might apply in space as well. Extending Narang's definitions, an assured retaliation strategy in space would threaten massive retaliation in the event that a state suffers any space attack. This was initially the U.S. position. A deterrence strategy of asymmetric escalation would involve threatening to attack space capabilities before an adversary does so. The United States has retained this right, even today.

Yet, the growth of new space powers means that a third approach—a catalytic strategy that attempts to catalyze superpower intervention on the state's behalf—is also possible. A catalytic space strategy would attempt to convince a great power patron (likely the United States) to intervene on behalf of one of its allies if that ally was attacked in space. For example, the Japanese reliance on payloads hosted on U.S. satellites could force the United States to consider responding to an attack made by China against Japanese space capabilities. This type of catalytic strategy is made possible by the proliferation of space capabilities in recent decades. With these types of approaches possible, simple deterrer-aggressor conceptions of deterrence will not suffice to avoid escalation. Thus, more complex

110 Karl P. Mueller, "The Absolute Weapon and the Ultimate High Ground: Why Nuclear Deterrence and Space Deterrence Are Strikingly Similar - Yet Profoundly Different," quoted in Michael Krepon and Julia Thomas, eds., *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations* (Washington, D.C.: Stimson Center: 2013), 56.

111 Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict* (Princeton, NJ: Princeton University Press, 2014), 6.

112 Bruce W. MacDonald et al., *Crisis Stability in Space*, 3.

113 Ibid., 4.

understandings of deterrence dynamics must take into account how new players, including allies, might adopt new deterrence strategies in space.

A second parallel in the nuclear and space domains is the initial U.S. reliance on massive retaliation. Both nuclear and space systems were initially seen as "off limits" to interference, except in a nuclear exchange, because they were associated with early warning as well as nuclear command and control.[114] MacDonald notes that the United States and the Soviet Union came to understand that "satellites were off limits, at least in situations short of full-scale nuclear conflict… satellites were protected by the threat of a nuclear response to any attack on so vital a component of their strategic architectures."[115] This threat of massive retaliation against any escalation in space was similar to the New Look policy that the Eisenhower administration embraced. As countries developed more exquisite nuclear and space capabilities over time, however, they came to rely on space for non-nuclear missions. As a result, interference with these non-nuclear activities led to questions about whether an attack on space capabilities would really trigger a nuclear exchange. Once again, massive retaliatory threats led to questions about the credibility of the strategy.

In summary, nuclear and space capabilities both proliferated and matured over time. More actors with more capabilities inherently lead to more complexity and greater opportunity for misperception and miscalculation.[116] Several types of escalation in space are possible. Borrowing from Barry Posen's work in the nuclear domain, one can differentiate between advertent and inadvertent types of escalation. Advertent space escalation includes "deliberate and sustained conventional attacks on [space] forces that are explicitly developed and approved to alter" the balance of forces in space.[117] On the other hand, inadvertent space escalation occurs when an unintended escalation affects space systems. Inadvertent space escalation includes "occasional accidental conventional attacks" on space as well as incidental "conventional attacks that self-consciously threaten [space] forces as a means to achieve a conventional mission."[118] Either type of space escalation can occur regardless of whether a space system resides in space or on the ground.

For the reasons described above, the likelihood of both inadvertent and advertent escalations in space are higher in the second space age than in the first space age. Inadvertent escalation is more likely because there are a growing number of space systems and actors, which increases the likelihood of unforeseen events. The physics of orbital mechanics makes space a tightly coupled domain, where actions by or against one satellite can quickly affect other satellites in similar orbits. Inadvertent escalation could also occur because, as Joan Johnson-Freese finds, "in order to maximize resources many countries, including China, France and Japan, deliberately develop technology or establish organizations and operations for dual-use purposes. They have far less a dichotomy between military

114 For more on this topic, see Paul Stares, *Space and National Security* (Washington, D.C.: Brookings Institution Press, 1987).

115 Bruce W. MacDonald et al., *Crisis Stability in Space*, 1.

116 On this point, see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 2015), 67.

117 This concept is adapted from Barry Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1992), 2.

118 Ibid.

and civilian space activities and organizations than in the United States."[119] As a result, disaggregating attacks on military and non-military systems may be difficult or impossible for many actors in the second space age.

Advertent escalations against space systems may be more likely in the second space age because states are more reliant on space systems for conventional missions, meaning that states have an incentive to interfere in space in order to degrade their adversary's operations at all levels of conflict. Some experts argue that "the greatest danger to the United States from cyberspace (as well as space) may be operational rather than strategic. If states with powerful militaries come to believe that a sudden cyberattack [or space attack] on the U.S. military could paralyze it long enough for conventional militaries to run roughshod over U.S. interests, the risks they run may endanger us all."[120] Adversaries might seek to intentionally interfere with intelligence collection assets or communications if the benefits of doing so appear higher than the costs.

Efforts to control inadvertent escalation tend to rely on risk reduction measures. For example, improving space situational awareness decreases the likelihood of unforeseen or unintentional events in space spiraling out of control. Meanwhile, developing rules and norms for behavior in space, through efforts such as the United Nations Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, can help to establish some "rules of the road" for space activity.[121] This decreases the likelihood of accidents and increases the confidence that leaders have in the expected actions of other state and non-state actors. These types of risk reduction measures have proven effective in decreasing the likelihood of an inadvertent conflict in other domains, including the nuclear domain. Yet, efforts to control inadvertent escalation are often at odds with maximizing deterrence against advertent escalations. After all, deterrence thinkers, such as Thomas Schelling, have long noted that deterrence relies on "the threat that leaves something to chance."[122] Risk minimization can, therefore, run counter to the risk manipulation efforts that are required for effective deterrence.

– DETERRENCE IN THE SECOND SPACE AGE

HOW CAN THE UNITED STATES AND ITS ALLIES and partners both minimize the risk of inadvertent escalation and maximize the effectiveness of deterrence and defense against advertent escalation in the second space age? A first step for U.S. policymakers is to clearly communicate its capabilities and credibility to withstand and respond to an attack now, before an attack occurs. Doing so will,

119 Johnson-Freese also states: "Categorization of Chinese space activities as military or civilian is complicated by the fact that the vast majority of space technology (>90%) is dual use." Joan Johnson-Freese, "Hearing on China's Space and Counterspace Programs (statement, U.S.-China Economic and Security Review Commission, February 18, 2015), 2.

120 Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA.: RAND Corporation, 2009), 6, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

121 For more details, see U.N. General Assembly Resolution 65/68, *Transparency and confidence-building measures in outer space activities*, A/RES/65/68, (January, 11, 2017),http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/68.

122 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard Univ. Press, 20), 187–204.

in turn, require a more refined U.S. declaratory policy that identifies and sequences U.S. escalation options in response to an attack in space. These options might include: applying international pressure, jamming communications to or from satellites, dazzling or blinding imaging satellites, temporarily disabling satellites through cyber attacks on satellite command and control systems, moving or de-orbiting satellites, executing special operations or missile attacks on ground-based command and control facilities, launching kinetic anti-satellite strikes, and using nuclear weapons. In addition to these vertical escalation options in space, the United States could escalate horizontally in other domains by taking military, diplomatic, informational, or economic measures. How should the United States assess which of these escalatory options to embrace and in what cases? To answer those questions, policymakers should focus on five key issues: attribution, reversibility, resilience, thresholds, and asymmetries. Each is discussed below and examined in greater detail in the chapters that follow.

ATTRIBUTION: In the first space age, attribution was less important and less complex than in the second space age. For many years, actions that interfered with space systems were viewed as attacks by the opposing superpower, so attribution was assumed. Today, however, attribution cannot be assumed. Just as in the nuclear domain, the increasing number of actors engaged in space means that it is not just one adversary with which U.S. military planners must concern themselves, but rather a host of state and, in some cases, non-state actors that have increasingly capable space and counterspace capabilities.[123] As U.S. strategists develop more tailored deterrence strategies, they will have to be sure that the United States can attribute aggressor actions in order to respond effectively and credibly. U.S. leaders will also have to demonstrate their ability to attribute attacks, lest an aggressor believe that it could avoid retaliation by relying on ambiguity. In so doing, U.S. leaders may want to demonstrate that the U.S. edge in attribution (based on its substantial investment in space surveillance and situational awareness capabilities) provides an asymmetric advantage that could permit escalation dominance over an adversary that is less well-equipped to quickly and reliably attribute hostile actions.

REVERSIBILITY: In the first space age, any action that disabled a satellite, even temporarily, was typically treated as a potential prelude to a nuclear attack. Yet, John Klein observes that today "[s]ome strategists question whether non-kinetic and reversible actions are hostile acts or armed attacks that warrant a military response."[124] Indeed, MacDonald agrees that "[t]here is no taboo against the use of many counter-space systems. The threshold for using temporary and reversible counter-space capabilities, such as electronic interference, is largely untested and likely much lower."[125] Even so, leaders should question whether reversible actions by one party are perceived as substantially less escalatory by other parties. Circumstantial evidence suggests that even reversible actions may be seen as major

123 As MacDonald comments, "[t]oday's space environment contrasts with earlier days of the Space Age in which only a handful of nations needed to be concerned with congestion. Now there are approximately 60 nations and government consortia that own and operate satellites, in addition to numerous commercial and academic satellite operators." Bruce W. MacDonald et al., *Crisis Stability in Space*, 12.

124 John J. Klein, "Space Warfare: Deterrence, Dissuasion and the Law of Armed Conflict," *War on the Rocks*, August 30, 2016, https://warontherocks.com/2016/08/space-warfare-deterrence-dissuasion-and-the-law-of-armed-conflict/.

125 For this reason, he finds, "The threat of an unstable escalation of space attacks is real during a crisis and jamming one or two GPS satellites in isolation would carry risks, but such action seems unlikely to precipitate an all-out space war..." Bruce W. MacDonald et al., *Crisis Stability in Space*, 36, 41.

"The U.S. edge in attribution provides an asymmetric advantage that could permit escalation dominance over an adversary that is less well-equipped to quickly and reliably attribute hostile actions."

attacks, as has been the case in the cyber domain, where distributed denial of services attacks have triggered major responses.[126] An adversary could use reversible attacks to drive wedges among allied nations if there are differences in how each of the allies view reversible attacks.

RESILIENCE: In a 2015 white paper, the U.S. Department of Defense noted that resiliency is distinctly different than defensive operations and reconstitution. It defined six ways to achieve resiliency (disaggregation, distribution, diversification, protection, proliferation, and deception) and noted that "all of these resilience measures, along with reconstitution and defensive measures, and alternate/cross domain abilities may be used individually and collectively to achieve warfighting mission assurance."[127] In the first space age, space resilience was largely an afterthought because a conflict in space would likely lead to or precede a major nuclear exchange. Instead, the focus was on cost-effective architectures that maximized the capabilities of satellites. Increasing resilience can be expensive, but some experts have argued persuasively that the resilience of key space systems could be sufficiently enhanced so that critical military operations would not be significantly impeded.[128] For example, Kevin Pollpeter suggests that "the United States could invest in smaller and more distributed satellite capabilities."[129] Such resilient capabilities would decrease adversary incentives to carry out first strikes because they are less likely to be successful and therefore bolster deterrence.

THRESHOLDS: In the first space age, minor escalations against space systems were treated as major events, since they typically threatened key elements of the superpowers' nuclear architectures. Given the wide array of possible attacks and the proliferation of counterspace capabilities observed in the second space age, many types of attacks against U.S. space systems are unlikely to warrant a nuclear response. Thus, it is critical that policymakers understand the likely break points in any conflict involving space systems. Such thresholds are often called "Schelling points" after nuclear strategist Thomas Schelling who identified these points as "finite steps in the enlargement of a war or a change in participation. They are conventional stopping places or dividing lines… They have some quality

126 See, for example, Nicky Woolf, "DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say," *The Guardian*, October 26, 2016, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

127 Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, "Space Domain Mission Assurance: A Resiliency Taxonomy," September 2015, 6-8.

128 Bruce W. MacDonald et al., *Crisis Stability in Space*, 36, 84.

129 Pollpeter notes, "Although smaller satellites would not be as capable and robust as larger satellites, the distribution of greater numbers of satellites would make the loss of any one satellite less catastrophic to the architecture as a whole." Kevin Pollpeter, statement to the U.S.-China Economic and Security Review Commission, *Hearing on China's Space and Counterspace Programs*, February 18, 2015, 9-10.

that makes them recognizable, and they are somewhat arbitrary."[130] In the nuclear domain, a taboo developed since 1945 against the use of any nuclear weapons. Even so, space may not benefit from this type of strong taboo, particularly given that few humans live in space. Strategists must explore whether the characteristics of different types of attacks against space systems create different thresholds, particularly the five characteristics explored in Chapter 2: attribution, reversibility, awareness of attack by the defender and general public, ability of attacker to assess effectiveness of the attack, and the risks of collateral damage (e.g., orbital debris).

In other domains, U.S. competitors—including Russia, China, and Iran—have used "gray zone" strategies to avoid crossing thresholds that might lead to direct combat with U.S. forces. The relative strength of the U.S. military makes threshold avoidance of this sort attractive to competitors. Thus, competitors have often relied on asymmetric capabilities in combination with ambiguity and incrementalism to minimize the likelihood of a forceful response by the United States or its allies and partners.[131] Competitors might adopt similar strategies in the space domain. For example, competitors could use non-kinetic weapons and reversible actions to stay below the threshold that would trigger a strong U.S. response. The United States will want to ensure that it has capabilities to respond both above and below these thresholds to ensure a full-spectrum of deterrence options. It is also likely that different actors may have different thresholds. For example, the United States may regard jamming of its satellite communications links that are used for nuclear command and control as highly escalatory, but its allies may view this form of attack as below such a threshold.

ASYMMETRIES: In the first space age, the two superpowers had largely symmetric capabilities and interests in outer space (with some notable exceptions). In the second space age, the space domain includes many disparate players with vastly different capabilities and interests. The United States is more reliant on space than any other country in the world, and it also retains greater space capabilities than any of its competitors, particularly when one takes into account U.S. allies and the U.S. commercial industry. The 2011 National Security Space Strategy states, "Space capabilities provide the United States and our allies unprecedented advantages in national decision-making, military operations, and homeland security."[132] Yet, as MacDonald notes, this also means that the United States "has more to lose in space than its adversaries."[133] The United States is particularly dependent on space because of its geography and global network of alliances. With two large oceans on either side, the U.S. military must be able to project power over great distances to secure its interests and those of its allies. The U.S. military's ability to conduct precision global surveillance and strike would not be possible without the use of space-based capabilities.

130 Schelling, *Arms and Influence*, 135.

131 Michael Green, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (Washington, D.C.: Center for Strategic and International Studies, 2017).

132 U.S. National Security Space Strategy, 2011. Also see U.S.-China Economic and Security Review Commission, "China's Space and Counterspace Programs," in *2015 Report to Congress* (Washington, DC: USCC, November 2015), 316.

133 Bruce W. MacDonald et al., *Crisis Stability in Space*, 10.

– CONCLUSION

THESE CHARACTERISTICS DESCRIBED ABOVE ARE DIRECTLY RELATED to the ability and credibility of the United States to quickly demonstrate its resolve, protect its power projection capabilities, encourage its opponent to de-escalate, and maintain its domestic and international support. One way to better understand how these dynamics operate is to conduct simulations (or war games) of crisis and escalation dynamics in space. Unfortunately, many space simulations are highly classified, limiting the amount of information available to the public. One concerning result of this classification is that U.S. leaders may have developed lessons from these simulations that are not shared by foreign counterparts, which could increase the likelihood of miscalculation in a real life crisis. Furthermore, many simulations tend to focus more on the warfighting aspects of a crisis than the early crisis phases. As MacDonald notes, "While space war games offer insights, participants too often rush through the crisis phase of the game and into the conflict itself, which is usually of greater interest to the participants and even to the game controllers. The crisis period is often viewed in these games as a necessary but minor prelude to the main event, but this phase should be a key focus of attention."[134] The next chapter discusses our efforts to test these principles in an unclassified space crisis exercise.

134 Ibid., 3.

LESSONS FROM A SPACE CRISIS EXERCISE

Background

ONE OF THE CRITICISMS OF U.S. SPACE POLICY is that the United States has not communicated a clear space deterrence framework to adversaries, allies, or the U.S. public. In order to test a range of scenarios in which conflict might begin or extend into space and understand how actions and reactions are perceived in those situations, the study team held a tabletop space crisis exercise. The exercise used three scenarios to explore three types of escalation: inadvertent escalation by miscalculation, inadvertent escalation by accident, and advertent escalation. The scenarios were used to understand how decision making on all sides of a conflict are affected by factors such as: the attack mechanism used (i.e., kinetic physical, non-kinetic physical, electronic, or cyber), the aggregation of strategic and tactical capabilities on military satellites, shared use and/or ownership of military space systems with allies and partners, and the use of commercial space systems for military missions. The findings from the exercise, which are described below, help inform analysis and recommendations for how U.S. national security space policy should be adapted to enhance deterrence in space.

On November 9-10, 2016, the Center for Strategic and International Studies (CSIS) and the Secure World Foundation (SWF), a private foundation that promotes cooperative solutions for space sustainability and the peaceful uses of outer space, co-organized a tabletop exercise entitled *Space Crisis Dynamics and Uncertainty*. Eighteen people participated in the exercise and were divided into four teams. The participants were drawn from government, academia, industry, and nongovernmental policy-organizations with backgrounds in national security, diplomacy, space policy, and civil and commercial space. This chapter provides an overview of what occurred during each scenario of the exercise and the key findings derived from an analysis of the actions and responses of the participants. A more detailed description of the exercise, methodology, and information provided to the participants can be found in the appendix.

As with any tabletop exercise (TTX) or war game, the specific outcomes that occur are dependent to a great extent on the people involved in the exercise. The participants in this exercise were specifically invited to participate because of their knowledge and expertise in space issues. Nevertheless, one should be careful not to extrapolate the results of a single exercise into broad generalizations. This tabletop exercise was used to help sharpen questions for analysis and uncover any unanticipated questions that should also be addressed in future research.

– METHODOLOGY

THE FOUR TEAMS USED IN THE EXERCISE each represented a fictional state actor. The teams were designated by a color code - Red, Orange, Yellow, and Blue - and were provided a background briefing that outlined their national objectives, military capabilities, and diplomatic relationships, which remained largely consistent throughout the TTX for each team. A more detailed description of the background provided for each team is provided in the Appendix, including the space and counterspace capabilities of each team. Throughout the three scenarios, Yellow and Orange had a pre-existing alliance, Orange and Blue were long-standing adversaries, and Red was relatively neutral; however, both Orange and Blue had the goal of bringing Red into their own sphere of influence. Real countries were not used in the scenarios to keep the tabletop exercise unclassified and ensure a broader array of experts could participate. Similarly, the scenarios were not based on real events, but rather realistic possibilities for what could happen between space-capable countries in a future crisis.

Participants were assigned to the same team for all three scenarios. Furthermore, participants played as themselves and represented their own personal experience, expertise, and opinions within bounds of their team's objectives. Participants were divided among the teams in a way that ensured that each team had a breadth of expertise in national security, diplomacy, and civil and commercial space.

The TTX was run by the Control Cell, which consisted of two CSIS experts and two SWF experts. Additionally, the TTX included two outside observers and four rapporteurs (one for each team). Each of the rapporteurs were embedded with one of the teams for the entire TTX, and were responsible for

handling communications with other teams and taking notes on their team's internal discussions. The Control Cell was responsible for adjudicating the actions taken by each team by using the probabilities of success and attribution for each action as specified by the capabilities of each team.

Each scenario consisted of three moves over a three-hour period. At the start of each scenario, Control Cell members briefed each of the teams on the background information and their starting status. At the end of the deliberation period of one hour per move (three moves in each scenario), each team provided their rapporteur with their decisions on what actions to take. The rapporteurs communicated the action(s) to the Control Cell, which then adjudicated the actions taken by all teams, according to the capabilities established by the scenario, and determined what outcomes would be seen by which teams. While the Control Cell adjudicated actions, each rapporteur worked with their team to document why the team made the decisions it did and also record any minority opinions. The rapporteur also served as the communicator between the teams and the Control Cell in the event that the teams had any questions; however, there was no direct communication between teams. As a result, any efforts to message the other teams had to go through the Control Cell.

At the end of each move, the Control Cell communicated to each team both the results of their action(s) and also any overt actions taken by other teams. This provided the starting status for the next move, and each scenario ended when all teams submitted their third action or set of actions. For a full synopsis of each scenario and all background materials presented to the teams during this exercise, please see the appendices.

SCENARIO 1

Inadvertent Escalation by Accident

In the setup for the first scenario, a longstanding territorial dispute over a nearby island chain between three of the four countries, Red, Blue and Orange, came to a head when Orange sanctioned a government-backed drilling company to prepare one of the disputed islands (colored grey in the map below), known as Skull Island, for commercial drilling. Blue and Red publicly denounced this action and moved naval and air forces into the island chain, but not onto the actual island in question. Orange then moved its own naval forces into the region in order to protect its commercial operations and established a military base on Skull Island for additional support. The military base on Skull Island included a military-grade PNT downlink jammer, which disrupted civil PNT signals in a 200-km radius around the island, but not military PNT signals.

Around the same time, a Blue helicopter was downed by an accidental collision with a UAV. The UAV was owned by Red and the PNT downlink jamming disrupted its ability to navigate, although only the Red Team knew this at the beginning of the scenario. Blue suspected that the helicopter was deliberately rammed by an Orange UAV and Blue began to mobilize additional military units, which included dispatching naval ships and establishing long-range ISR patrols over the island chain. Blue also put its land-based aircraft and conventional ballistic missile forces on alert. Yellow, a longstanding ally of Orange, then moved a carrier strike group into the region, while simultaneously calling for a diplomatic solution to the issue. Orange denied Blue's allegations that it was an Orange UAV that struck down the

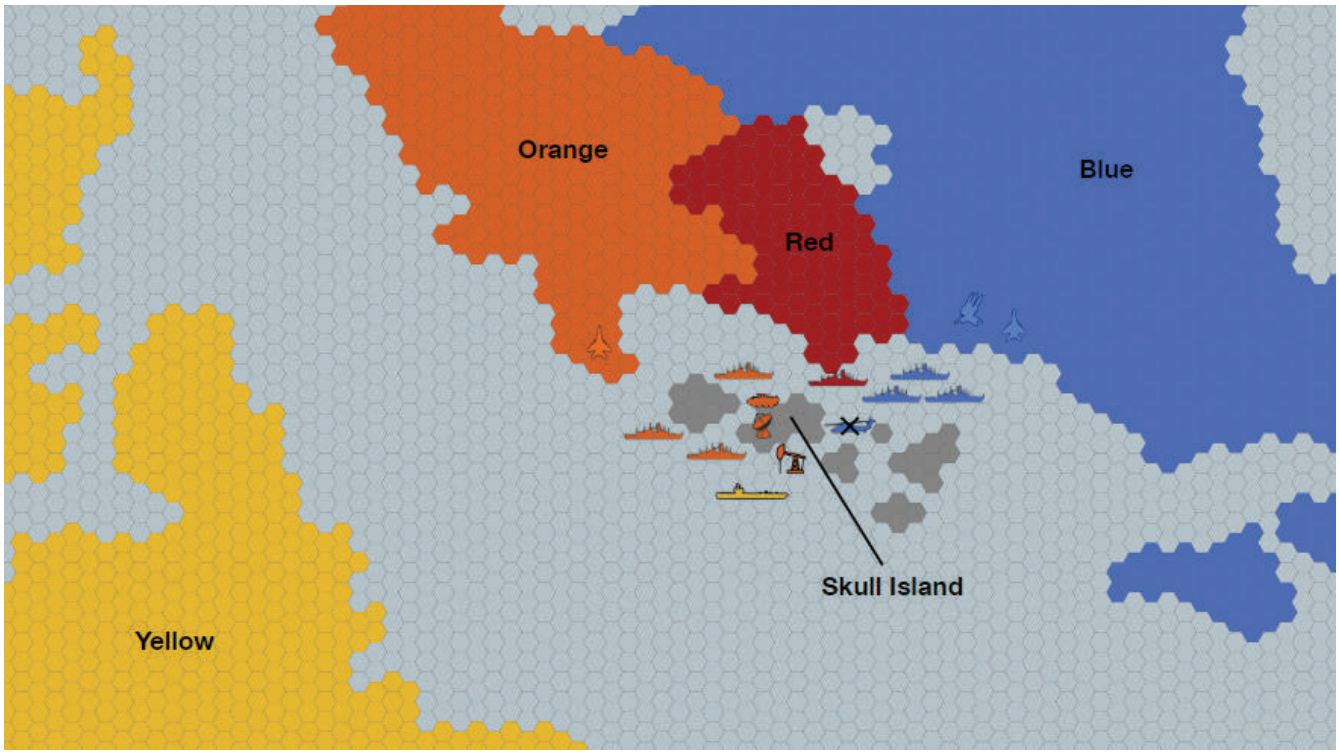

Figure 3: Location of forces at the beginning of Move 1 in the first scenario.

Blue helicopter and follows up by deploying two destroyers to the island chain, which were equipped with missile defenses that utilized satellites for detection and targeting of ballistic missiles.

Based on this setup, the scenario proceeded into actions by the individual teams, with each team pursuing different strategies to achieve their goals. Both Blue and Red worked towards removing Orange's presence, especially their military presence, off the disputed territories of Skull Island and returning to the status quo. Blue was especially concerned with removing Orange without provoking Yellow, who had much more robust military and space capabilities. Neither Blue nor Red had higher ambitions of claiming the island chain for themselves as long-term goals and preferred to leave the disputed island chain unclaimed by any country. Orange's main goal in this scenario was to allow their Standard Oil Company to continue to drill and to de-escalate the situation at-large. Yellow also wished to de-escalate the situation, but they wanted to do so from a distance and not have their national assets pulled into the conflict. These general goals were provided to the teams as part of the setup for the scenario.

During the moves, jamming was used by both Orange and Blue in an attempt to get the other nation to back down. Cyber attacks were also attempted by the Blue and Red teams to halt drilling and military activity by Orange. Imagery, or ISR, was used by both Yellow and Red as a soft-power outreach mechanism in an attempt to strengthen relationships with other nations. This publicly-released ISR from both teams was used to improve situational awareness across the board.

An effort to establish norms and responsible behavior was brought up by the Orange team, but not thoroughly explored during the first scenario. With all of the electromagnetic attacks occurring, Or-

ange suggested that a code of conduct for electromagnetic attacks might be drawn up to clarify the level of severity of these attacks. However, this idea was not picked up by any other team.

Yellow eventually pulled its naval forces out of the area in their final move to avoid getting entangled in a conflict between Red, Blue, and Orange. Yellow also hoped that this sign of de-escalation would encourage others to de-escalate as well. In its final move, Blue prepared for an air assault against the Orange forces on Skull Island by jamming both Yellow and Orange's commercial and military SATCOM and dazzled the two countries' ISR capabilities. More broadly, Blue stated that it was initially hesitant to directly attack space capabilities, because it felt that once the conflict moved to space, it would be hard to stop the conflict from escalating dramatically. This appeared to be a commonly held conviction by all the teams in the first scenario. However, as described above, Blue eventually resorted to jamming Orange SATCOM and dazzling Orange ISR in order to conduct an air assault on Orange's ground station and military forces that were stationed on Skull Island.

SCENARIO 2

Inadvertent Escalation by Miscalculation

The setup for the second scenario in the tabletop exercise began with a terrorist attack in an Orange province bordering Blue. The attack was linked to extremists in Blue, and the Orange military mobilized to secure the Orange-Blue border and prevent further attacks. Furthermore, Orange media broadcasted a report that claimed to show evidence linking the terror attack to Blue's intelligence services. Although Blue officially denied the link, the report had a strong influence on the Orange public, who demanded action from their government. Two days later, a Blue fighter aircraft shot down a Yellow helicopter on the Blue side of the Blue/Orange border, killing all on board. Media outlets in Blue then announced that the Yellow helicopter was carrying an Orange special forces team, which was on a covert mission to infiltrate Blue. In response, Blue mobilized multiple fighter patrols and armored and mechanized divisions to their border with Orange.

Privately, Yellow learned that its space surveillance capabilities detected a change in the orbital trajectory of three small objects in the GEO belt, which had originally been cataloged as debris from a Blue space launch five years ago. The three objects were now drifting around the GEO belt towards the region over the crisis area between Blue and Orange. While Yellow did not have sufficient space situational awareness coverage over the conflict area to independently confirm this, Red had a ground telescope with good visibility and was able to confirm the new trajectories. Yellow ISR satellites also showed that Blue's mobilization included increased readiness of its ASAT capabilities.

For the first move, the four teams operated mostly independently, with the exception of the pre-established longstanding Yellow-Orange military alliance. This alliance allowed for Yellow and Orange to deploy forces in tandem in the first move of the scenario. Independently, Yellow also decided to conduct cyber attacks against Blue's SSA ground sites and non-nuclear C2 sites without informing Orange. Like the previous scenario, the teams tended to view cyber attacks as fair game and a more moderate escalation tactic. Also, similar to the first scenario, Red used ISR as a soft power tactic and shared with Yellow that one of the suspected Blue co-orbital ASATs had moved near a Yellow missile-warning satellite.

Figure 4: Location of forces at the beginning of Move 1 in the second scenario.

Despite the scenario set-up and the possibility of an ASAT attack either co-orbitally from Blue on a Yellow missile-warning satellite or from a ground site in Blue on any other nation's space capabilities, there was a real reluctance to use kinetic force in space. The notion that this type of escalation was of the highest order prevailed throughout this scenario and Blue de-escalated by moving its inspection satellites to a non-threatening distance as one of its first actions. Instead of kinetic attacks in space, offensive cyber activities were common and were widely used throughout this scenario.

SCENARIO 3

Advertent Escalation

In the third and final scenario, a change in the government of Red was the focus of tension in the region. In a hotly contested election, Red elected a new government; however, the outgoing government refused to concede the election, and a civil war erupted. Most Red military leaders resigned their posts and joined forces with the ousted government to form an insurgent force, which began a civil war against the remaining military forces that were loyal to the new government. Yellow and Orange expressed public sympathy for the ousted government, and it was suspected that they were providing material support to the growing insurgency. Additionally, there were rumors that Orange military training camps were being used by Red insurgents. Blue openly supported the new government in Red and provided it with military aid and advisors so it could counter the insurgency.[135]

135 Note that in this scenario the Red team is playing as the newly elected government supported by Blue and the White Cell is acting as the ousted government and Red insurgency.

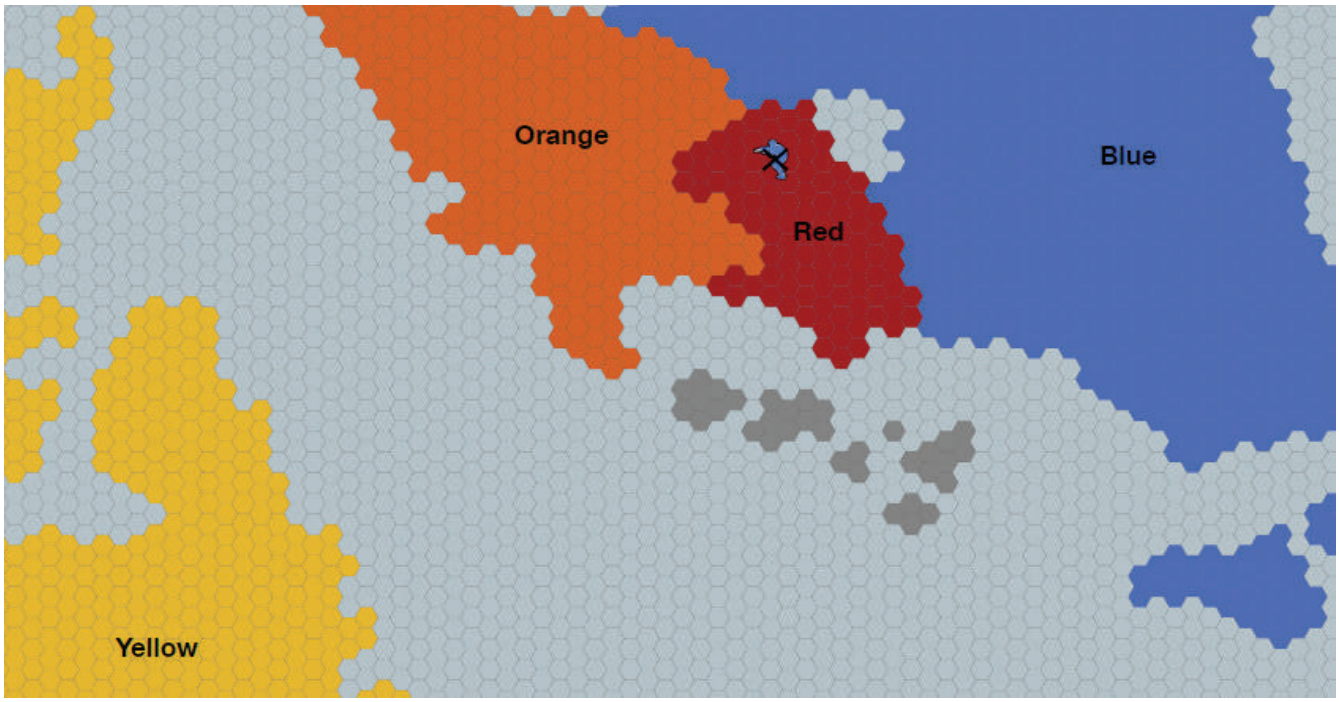

Figure 5: Location of forces at the beginning of the third scenario.

In the midst of this chaos, a solar storm occurs and causes widespread interference with satellite capabilities, which results in failures of several commercial and civil satellites. Concurrently, several Blue ISR satellites over Red's territory were knocked out. The solar storm interference played a role in the dynamics and perceptions of the ongoing conflict, as it created confusion between natural interference from the storm and jamming tactics used by adversaries. Following the storm, during a battle between Red insurgents and Red government forces, a dozen Blue military advisors were killed in an airstrike. Blue claimed that this was a deliberate attack on its military advisors by insurgents and that Yellow's space-based ISR capabilities provided intelligence to support the attack. In response Yellow's support of the ousted government, Blue blinded two Yellow ISR satellites, rendering them inoperable. However, Yellow decided to keep this information to itself and did not alert others (including Blue) that these two satellites were now dead.

In the first move, the teams coordinated with one another to respond immediately to events in the scenario in-briefing. Orange and Yellow coordinated jamming, dazzling, and cyber attacks on Blue and Red satellites. Simultaneously, Red opted to jam all PNT over its own territory to make offensive operations more difficult for Orange and Yellow. Again, as a common tactic throughout all three scenarios, cyber attacks were used to harm opposition space ground and command and control capabilities. This type of attack continued to be viewed by most of the teams as less escalatory than kinetic attacks on satellites in orbit. As Orange and Red insurgents made a push for the capital of Red in an effort to dispose of the new government, the Red team amped up their escalatory actions by putting their ASAT capabilities on alert. The Yellow and Orange alliance took this action by Red very seriously and made immediate moves

to counter any ASAT threat from Red. Orange immediately deployed two special operations teams and used cruise missiles to attack Red's ASAT ground sites to remove the threat to their space systems.

During the second move of the scenario, a kinetic ASAT attack occurred on Blue satellites. Yellow maneuvered its own dead ISR satellites, the two Blue had blinded earlier in the scenario, into active Blue ISR satellites in order to degrade Blue's ISR capabilities. However, Blue showed great resiliency and was able use increase its airborne ISR in order to make up for this gap in its space-based capabilities during the final move. In post-scenario deliberations, the Yellow team admitted that they did not weigh the consequences of putting a large amount of debris in orbit. They saw it as a tactical move that allowed them to make use of an otherwise unusable satellite.

– LESSONS

THROUGHOUT THE DAY AND A HALF EXERCISE, the three scenarios produced many interesting findings about how the groups acted with one another and perceived each other's actions. However, the most notable of these findings were pervasive and highly influential to the decision-making process.

ATTRIBUTION

Teams weighed attribution differently in decision-making depending on their own capability set. Throughout the exercise, the two teams with the least amount of space-based capabilities (Orange and Red) reported that they paid little to no heed to how attribution might affect their actions. However, attribution was a significant decision-making consideration for the two teams with more space-based capabilities (Yellow and Blue). In our exercise, teams with the most to lose in space held attribution of attack as a higher consideration than those teams with less to lose in space. Consideration of attribution may not have been very impactful for the decision-making of the less space-capable teams, but the consequences of attribution influenced reactions of all four teams. In-kind, responses or reactions to being attacked were often driven by whether or not an attack was attributed. For example, during the third scenario, a non-attributed attack was passed off as damage from the solar storm, and no response was taken. In other cases, teams were able to successfully manipulate perceptions of attribution and blame other teams for actions that they themselves had taken.

REVERSIBILITY

Teams viewed reversibility of attacks differently depending on whether they were the attacker or defender. One of the most common and impactful actions taken was the use of radio frequency interference. Jamming, sometimes even over one's own territory, proved to be an effective counterspace capability, and in several cases there was little an adversary could do in response. While the attacker tended to view jamming as less escalatory because it is fully reversible, it was viewed differently by the teams being jammed. Some teams perceived jamming and other reversible attacks as being just as threatening as an irreversible attack. They believed that if the capability could be denied or degraded once, then it could be lost again at any point in the conflict and was, therefore, an unreliable system.

RESILIENCE

Teams were often able to work around a debilitating attack on their space capabilities. By using non-space capabilities, purchasing commercial space capabilities, or utilizing allies' space capabilities, teams were often able to rebound after an attack on their systems. In particular, if a space-based ISR system was compromised, teams could resort to utilizing air reconnaissance or purchasing imagery from commercial companies or other teams. Resiliency was a significant advantage for those teams who had secondary systems or were able to work around the loss of a capability. It effectively denied or limited the benefits gained by an attacker.

"Resiliency was a significant advantage for those teams who had secondary systems or were able to work around the loss of a capability."

THRESHOLDS

Teams were generally reluctant to use kinetic attacks in space. The reluctance to deploy kinetic attacks on space systems appeared to stem from the perception that a kinetic attack is significantly more escalatory than even a non-reversible, non-kinetic attack. Only one kinetic attack occurred throughout all three scenarios, and it was viewed as an out of proportion, unnecessary escalation by the other teams. The Yellow ASAT attack on Blue satellites caused immediate negative responses from both Red and Blue, and also led to Blue's support for a ceasefire. Notably, Yellow agreed that without the threat of a Red ASAT attack, it might not have conducted a kinetic attack against Blue satellites. Similarly, during the second move in the final scenario, Red began to mobilize their ASAT capabilities. The opposing alliance of Orange-Yellow viscerally reacted to this by vowing to disrupt Red communications and deploying cruise missiles to attack Red ground-ASAT capabilities.

Teams used cyber attacks on space systems early and often. Cyber attacks were widely-used throughout all three scenarios and at least once by each team. These attacks were viewed as legitimate tools of conflict that allowed teams to interfere with their adversaries' ground and space systems without an overt kinetic attack. According to some players, cyber capabilities were viewed as being more usable and less threatening than kinetic physical attacks against space or ground systems. Notably, cyber hacking was used against one nation's central bank in a scenario, showing the versatility of cyber as a tactical asset. This instance, and others that involved spreading misinformation to the public, showed that the teams were thinking of other ways to influence events without escalating in the space domain.

Teams were willing to escalate and conduct kinetic attacks in other domains rather than in space. Throughout all three scenarios, teams escalated in other domains more often and more readily than escalating in the space domain. Escalating into space, especially kinetically, was a threshold that many teams appeared hesitant to cross without significant consideration or provocation. Instead, other conventional responses, including a variety of attacks on space ground systems were taken by the teams. In the first scenario, for example, a team responded to PNT downlink jamming with cyber attacks on ground stations against their opponents instead of responding in-kind. In the second sce-

nario, one team chose to send in special operations forces to overtake and disable SSA ground sites in an adversary's territory instead of attacking the satellites themselves. This reluctance might be tied to the fact that most of the participants were familiar with space and thus aware of the possible consequences of attacking satellites; if the TTX were to be run with a group of people unfamiliar with space, this reluctance might not be present.

The way an attack is perceived depends on the context in which it occurs. During the TTX, teams sometimes struggled to understand the intent of actions taken by other teams. In some cases, the teams assumed intent (and attribution) based on the military and geopolitical context in which the actions took place. This means that the thresholds and response elicited by a particular type of attack on space systems can vary depending on both when an attack occurs during a conflict and the situation on the ground at the time of the attack. For example, the only kinetic attack in space carried out by a team during the TTX did not cross the threshold to provoke a symmetric response. This was partially because it occurred in response to a debilitating non-kinetic attack, and it appeared to be an opportunistic move that was unlikely to be followed up by additional kinetic attacks.

ASYMMETRIES

Teams were not able to easily distinguish between strategic and tactical space systems. Adversaries were concerned during gameplay about affecting strategic space assets used to support nuclear missions, especially command and control satellites. Attacking these was seen as highly escalatory across all of the teams. For teams with more significant space-based capabilities, attacks on critical space assets were of more concern than they were for those teams with less-robust capabilities. Despite this, the distinction between tactical and strategic assets was not as great as the study team anticipated. Attacking teams reported that the lines between an opponent's' tactical and strategic space assets were unclear, and players reported that this made escalatory actions in space significantly more difficult and uncertain than escalatory actions on conventional forces.

Another interesting take-away was that establishing norms and behaviors was only brought up in the first and third scenarios, but it was not followed through beyond a team's initial inquiry. Possibly, the lack of enthusiasm and the length of a negotiations process deterred teams from reacting to these diplomatic proposals. It is also worth noting that the third scenario was held on a separate day as the first two scenarios, and thus the teams were more acquainted with the structure of the tabletop exercise, their fellow players, and the capabilities of each team. Although the White Cell intended for each of these scenarios to remain independent of one another, there was talk of the previous day and previous scenarios during this final round.

FINDINGS

THIS REPORT HAS EXPLORED ESCALATION AND DETERRENCE dynamics in the second space age through historical research, theoretical study, and a tabletop simulation. A key lesson from each of these efforts is that the United States must work with its allies and partners to develop tailored deterrence options that are better suited to the increasingly diverse, disruptive, disordered, and dangerous environment in outer space. Actions in space are not isolated from other domains, and the way an adversary views attacks and provocations in other domains may be a useful indicator for how it will regard attacks and provocations in space. The challenge is that space, especially during the second space age, presents a number of asymmetries that differ from other domains, and thus the way one deters actions in space may also need to differ from the way similar actions are deterred in other domains. Specific policy implications include the following:

- **Invest in attribution:** The United States needs better capabilities for attribution, particularly for non-kinetic attacks against space systems, such as the ability to quickly identify and geolocate sources of radio frequency interference and cyber attacks. Asymmetries in attribution capabilities could provide an important competitive edge to deter a potential aggressor's escalation against the United States' (or its allies and partners') space systems by increasing the likelihood and credibility of a response.
- **Increase resilience:** The United States and its allies and partners need more resilient capabilities to reduce or deny the potential benefits of an adversary's attacks on space systems. For example, rather than continuing to buy small numbers of large and expensive satellites for critical missions, such as missile warning and nuclear command and control, the U.S. military could transition to more resilient constellations that are populated by a larger number of smaller, less expensive satellites in a variety of orbits. This could include hosting military payloads on commercial and international satellites. In addition, the United States should demonstrate the ability to operate effectively using alternative commercial and non-space systems in order to augment or replace degraded military space systems, thereby limiting the benefits an adversary would attain by disrupting them.
- **Reexamine reversibility:** Reversibility is an important component of some methods of disrupting space systems, but reversibility may be perceived differently by an attacker and defender. Attackers should not assume that defenders will see reversible forms of attack as substantially less escalatory than non-reversible attacks. And attackers should be cognizant that the defender may not know at first whether the effects of an attack will be reversible or not, which could lead to inadvertent escalation through miscalculation. The United States should engage its allies and partners in discussions to articulate how each country regards different types of reversible attacks to ensure a more unified response should such an attack occur.
- **Identify escalation thresholds:** Developing a shared understanding of thresholds is key to deterrence, but many escalation thresholds in space remain contested and uncertain. Based on our findings, key thresholds include crossing between terrestrial attacks and attacks in space and moving from non-kinetic space attacks to kinetic space attacks. Although the difference between strategic and tactical systems often attracts attention, it may not be as important a threshold as is commonly assumed.
- **Demonstrate capabilities:** The nature of space capabilities often requires that these capabilities remain secret, but U.S. leaders may need to consider demonstrating and/or declassifying some space, counterspace, and attribution capabilities so they can more effectively communicate a credible deterrent to potential adversaries. While many space capabilities may need to remain secret to remain effective, senior leaders should be cognizant that capabilities that adversaries do not know exist cannot effectively contribute to deterrence.

In addition to these findings, this study raised several questions for further study:

- **Building coalitions:** How should the United States work with its allies and partners to maximize space-based capabilities while minimizing the cost and vulnerability of these assets? In particu-

lar, how might shared capabilities, such as joint technology development and hosted payloads, alter the willingness of potential adversaries to threaten U.S. or allied space systems? Which types of systems are best suited to such cooperative efforts, and with which partners?

- **Indemnification of commercial space systems:** Should the United States offer indemnification to cover the losses of commercial satellite operators that provide space services for the U.S. Government and / or the governments of U.S. allies and partners if they are attacked in a conflict? This could include commercial satellites that may host military payloads and (one day) satellites that service military satellites on-orbit. On the one hand, this would encourage companies to be willing to do business with the U.S. Government and its allies and partners by offsetting risks that commercial insurance is unlikely to cover. On the other hand, it may effectively put a "bullseye" on these commercial space systems by identifying which systems the U.S. Government is reliant upon, depending on how the indemnification program is structured. How would such a program be perceived by the commercial space industry, U.S. allies and partners, and potential adversaries?

The second space age is a period of turbulence and change. This study focused on understanding escalation and deterrence in this transitional period as norms are being contemplated and tested but are not yet widely accepted. Many of the commercial space ventures that are currently planning to launch large constellations of satellites and make space tourism a reality are implicitly based on a stable and predictable space environment that is suitable for commerce.

From the dawn of the first space age, Americans understood the many benefits that could come from the peaceful uses of space and the great harm that could result from hostile uses of space. In what has become known as his moon speech at Rice University in 1962, President Kennedy addressed the dilemma of how to reap the benefits of space without conflict:

> [O]nly if the United States occupies a position of pre-eminence can we help decide whether this new ocean will be a sea of peace or a new terrifying theater of war. I do not say the we should or will go unprotected against the hostile misuse of space any more than we go unprotected against the hostile use of land or sea, but I do say that space can be explored and mastered without feeding the fires of war, without repeating the mistakes that man has made in extending his writ around this globe of ours.[136]

For sixty years, space has been the exception – the one domain that has remained free from the scars of war. But the fractured balance of power and lack of norms in the second space age are leading space perilously close to the "new terrifying theater of war" of which President Kennedy warned. The hope is that by better understanding the dynamics of the current situation, a more stable equilibrium can be found to usher in a third space age–one that is defined by stability and widely accepted norms of behavior. The norms that govern the next space age could shape the balance of power in space—and on Earth—for a generation or more.

136 John F. Kennedy, "Address at Rice University on the Nation's Space Efforts" (speech, TX, Houston, September 12, 1962), https://www.jfklibrary.org/Asset-Viewer/MkATdOcdU06X5uNHbmqm1Q.aspx .

APPENDIX A

Analysis of the Space Environment

The analysis of the space environment presented in the first chapter of this report utilizes data from publicly available databases, including Space-Track.org (Space-Track),[137] the Union of Concerned Scientists' (UCS) website,[138] and Gunter's Space Page (GSP).[139]

– Satellite Databases

Space-Track Database

Space-Track is an online catalog that organizes and publishes historical and current space object data collected by the Joint Space Operations Center (JSpOC). The catalog contains over 40,000 individual entries, including both deorbited and in-orbit payloads, rocket bodies, and pieces of debris. This particular study focused only on payload objects.

Space-Track's catalog includes each space object's name, international designator, country of origin, and orbital parameters (as well as its launch site, date of decay if applicable, and radar cross section size if available) from *Sputnik 1*, launched in 1957 and deorbited in 1958, to the most recent object launched in 2017. This study focused only on objects launched before December 31, 2016.

UCS Satellite Database

The Union of Concerned Scientists organizes and publishes a catalog of satellites currently in orbit, updated quarterly, called the UCS Satellite Database. The most recently updated database is publicly available on their website, and earlier versions can be provided upon request. In addition to the information provided by Space-Track, the UCS database also includes information on each satellite's purpose and type (Civil, Commercial, or Military).

GSP Chronology of Space Launches

Gunter's Space Page provides a detailed, narrative description of most payloads' purpose, manufacturer, and operator. GSP is a privately organized, publicly available database.

– Key Definitions

International Designator (IntDes)

The international designator, or COSPAR number,[140] of a satellite describes a satellite's position in the history of all space launches. The first four digits denote the year the object was launched, the second

137 Space-Track.org, accessed September 13, 2017, https://www.space-track.org/.

138 "UCS Satellite Database," *Union of Concerned Scientists*, April 11, 2017, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WZb3wYjythE.

139 *Gunter's Space Page*, 2017, http://space.skyrocket.de/.

140 Committee on Space Research (COSPAR), 2017, https://cosparhq.cnes.fr/.

three digits denote the order in which that object was launched during the given year, and the final combination of letters differentiate individual satellites within a specific launch system. Objects that begin with the same seven digits were launched concurrently on the same launch system. Refer to Figure 3 for an example of an international designator.

Figure 6: International Designator for the International Space Station (ISS). The first module of the ISS, the Zarya, was the placed into orbit as the principal object (Object ID: A) on the 67th launch (Launch Number: 67) of 1998 (Launch Year: 1998).

Country of Origin

In Figure 1 of this report, the total number of space launches per year are displayed by country. While Space-Track includes the country of origin for each space object in its database, several assumptions were made to create the relevant figure. Space-Track lists all space objects launched by the Soviet Union and Russia as owned and operated by "CIS" or the Commonwealth of Independent States.[141] For clarity, the Commonwealth is written as "Soviet Union/Russia" in Figure 1.

Figure 1 also includes the number of space launches by the European Union (EU). This category is a combination of several more specific countries of origin included in Space-Track's database. It includes all member states at the time of publication.[142] Here, the European Union is defined as all current member states, the European Space Agency, the European Space Research Organization, the European Organization for the Exploitation of Meteorological Satellites, the European Telecommunications Satellite Organization (Eutelsat), Société Européenne des Satellites (SES), and also satellites launched by different combinations of EU member states.

Military, Non-Government Military, and Commercial

While the UCS Satellite Database includes the type (Civil, Commercial, or Military) of *currently* operating satellites, a majority of the space objects analyzed for Figure 2 are no longer in orbit. Thus, this study included a comprehensive catego rization of satellite types using the Gunther database.

If a satellite is owned and operated by a company that is more than 50% state-owned, it has been categorized as "Non-Military Government."

– Defining the Second Space Age

In the first chapter of this report, it was noted that the second space age can be principally defined by the collapse of the Soviet Union, which slowed Russia's launch pace, and the disruptive entrance of other non-U.S., non-Soviet actors into the space domain. Plotting the cumulative rate of space launches by country (United States, Soviet Union/Russia, Others) reveals a quantifiable expression of these statements.

The United States' launch rate remains approximately constant and linear, with a slight increase in the

141 Space-Track.org.

142 "EU member countries in brief," *European Union*, August 21, 2017, https://europa.eu/european-union/about-eu/countries/member-countries_en.

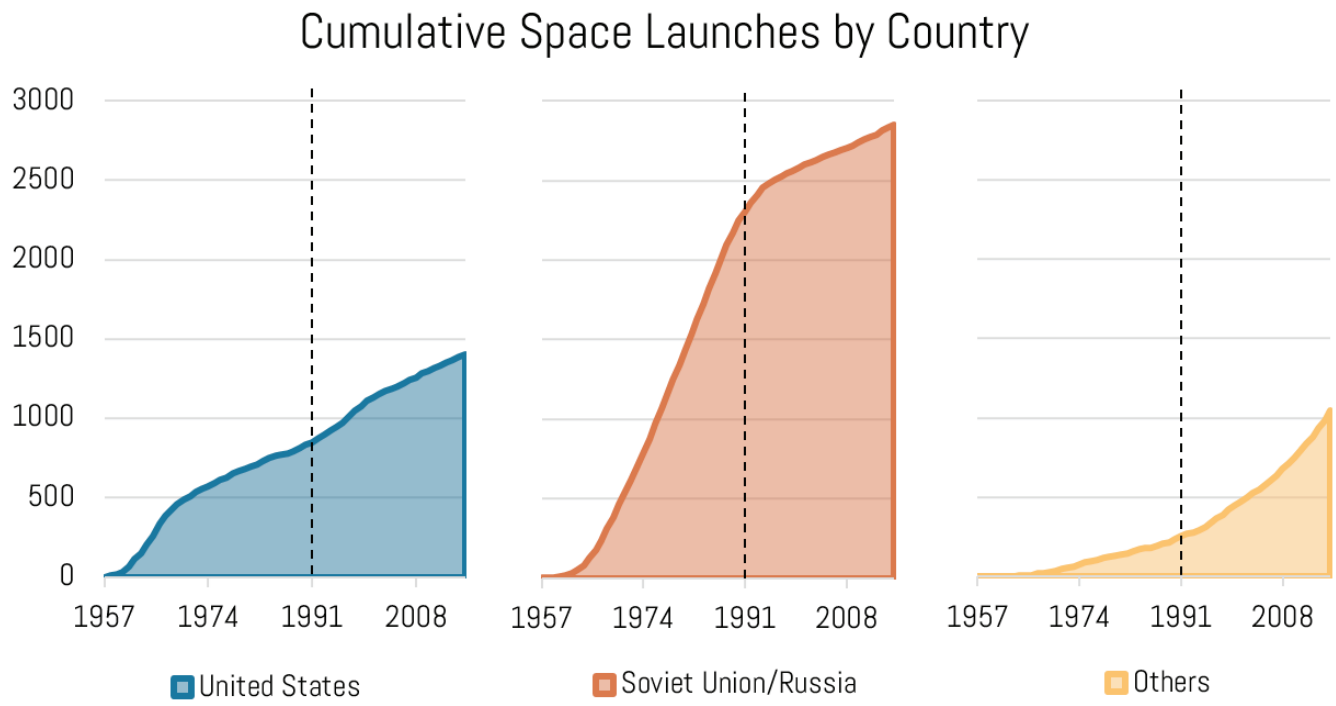

Figure 7: Cumulative Space Launches by Country. The total number of historical launches by year for the United States, the Soviet Union/Russia and all other space-faring nations.

1960s corresponding with NASA's Apollo Program. From 1967 (ten years after the launch of *Sputnik 1*) to 1990, the Soviet Union's launch rate was almost precisely linear, with about 90 new launches per year. After the dust settled from the collapse of the Soviet Union, Russia's launch rate sank to fewer than 17 launches per year from 1995 to 2016. Other actors, primarily Japan, China, and member states of the European Union, experienced a great increase in space launches following 1991. During the first space age, other countries successfully launched approximately 30 payloads per year. Afterwards, the launch rate more closely resembled an *exponential* increase with a 5.5% growth factor.

– Further Analysis

Only a fraction of the available data in Space-Track's online catalog was utilized for this study. Further analysis can be done to quantify certain characteristics of the first and second space age. Other categories of interest could include orbital regimes (which could be calculated from the orbital parameters provided with each line element of the catalog), launch sites, object size, and object lifespan.

APPENDIX B

Tabletop Exercise Background Materials

– Background Briefing

This exercise focuses on four countries: Yellow, Blue, Orange, and Red. The geographic locations of these countries are depicted in the attached map. Their respective military capabilities are explained in the attached force list.

Yellow has the world's second largest economy and the most technologically sophisticated and capable conventional military. Yellow also has a robust global presence through a longstanding network of alliances, which include a treaty commitment to defend Orange in the event of an attack on its territory or military forces. Yellow has advanced space capabilities that include missile warning; intelligence, surveillance, and reconnaissance (ISR); military satellite communications (MILSATCOM); and positioning, navigation, and timing (PNT). Yellow has the largest and most sophisticated commercial space sector in the world, which provides capabilities and services to both Yellow and the global market. Yellow also operates multiple commercial space stations in Earth orbit. Finally, Yellow has a significant nuclear deterrent on a 24/7 alert-ready and launch-on-warning posture.

Blue has the world's largest economy and a fairly sophisticated conventional military that is dominant in its immediate region but lacks global reach. Blue has moderate space capabilities across the national security and civil sectors but only minimal commercial capabilities. Blue has its own national space station, which hosts astronauts from other countries. Blue has no formal alliances but does have partnerships with several emerging countries. Blue has a minimal nuclear deterrent in a second strike posture.

Orange has the world's third largest economy and a small but technologically sophisticated military. Orange has significant capabilities in space-based communications and intelligence, reconnaissance, and surveillance, provided by both governmental and commercial satellites. Orange has a mutual defense treaty with Yellow and has access to some of Yellow's space capabilities. Orange has the ability to develop nuclear weapons but has not yet done so.

Red is a small, technologically sophisticated country with minimal conventional military capabilities. Red is not an ally of Blue, Yellow, or Orange. Red has very limited indigenous government space capabilities but does have some commercial satellite ISR and communications companies that provide services to Red and other global actors. Red disavows the possession and use of nuclear weapons.

	CAPABILITIES	Yellow*	Blue	Orange	Red
Ground	Personnel (active/reserve)	650K / 450K	1,500K / 800K	150K / 200K	150K / 300K
	Tanks	2,500	6,500	600	500
	Artillery	7,000	12,000	1,500	2,000
	SOF Groups	15	15	5	1
Naval	Carriers	10	3	1	-
	Destroyers	70	60	35	5
	Frigates	10	60	10	20
	Attack Subs	60	60	15	5
	Ballistic Subs	12	8	-	-
Air	Heavy Bombers (non/stealthy)	120 / 30	150 / 0	-	-
	Fighters (4th-gen/5th)	2,200 / 300	2,000 / 100	300 / 100	400 / 0
	Attack Helos	800	200	80	100
	Manned ISR	400	150	80	10
	Unmanned ISR	300	120	20	5
	Ballistic Missile Interceptors	50	10	-	-
	Conv.-armed Ballistic Missiles	20	90	-	-
Space	Protected Comms (GEO)	6	2	-	-
	Missile Warning (GEO/LEO)	4 / 2	-	-	-
	PNT (GEO/MEO/HEO)	3 / 30 / 0	5 / 25 / 0	1 / 0 / 4	-
	ISR (EO/SIGINT/Radar)	6 / 4 / 2	2 / 2 / 0	2 / 0 / 4	-
	SSA Satellites	4	4	-	-
	SSA Ground Stations	4	2	1	1
	Direct Ascent ASAT	Robust	Robust	Limited	Limited
	Co-orbital ASAT	Robust	Robust	-	-
	Jamming	Robust	Robust	Moderate	Moderate
	Dazzling/Blinding	Robust	Moderate	Limited	None
	Commercial Capabilities	Robust	Limited	Limited	Moderate
Nuclear	Nuclear Warheads	1000	300	-	-
	Tactical Nuclear Weapons	100	50	-	-

** Only ⅓ of Yellow systems are resident in region*

– Yellow Team Background

National Interests/Objectives

As one of the few countries with global military capabilities and alliances, Yellow's primary interest is in stabilizing the geopolitical landscape in order to protect its economic and political interests. Yellow is deeply dependent on the continued flow of trade, including access to natural resources. Yellow is increasingly concerned about the vulnerability of its space capabilities and its reliance on space-based capabilities to project global military power.

Diplomatic Relationships

Yellow has a mutual defense treaty with Orange.

Yellow has a longstanding peaceful diplomatic relationship and strong economic ties with Red.

Yellow's diplomatic ties with Blue are strained at best. Although both recognize the power and influence of the other, they are also economic and political competitors. Blue has recently sought to undermine Yellow's diplomatic and economic relationships with other countries, particularly Red .

Yellow Team Options

Your team can choose any combination of the example options shown below. You may also develop other options not listed here, but please check with the Control Cell in advance to make sure any new options are technically feasible given your team's capabilities.

Space	**Non-Kinetic** • **Jam commercial/protected SATCOM downlinks**, localized to the immediate area (Success: 90%; Attribution: 90%) • **Jam commercial/protected SATCOM uplinks**, would likely affect users not in local area (Success: 90%; Attribution: 60%) • **Jam civilian/military PNT signal**, localized to area (specify civil/military) (Success: 90%; Attribution: 90%) • **Jam civilian/military PNT signal**, beyond local area (specify civil/military) (Success: 70%; Attribution: 90%) • **Cyber attack (ISR/PNT/protected SATCOM) satellites**; protected SATCOM satellites are also used for nuclear C2 (Success: 70%; Attribution: 40%) • **Dazzle ISR satellites**, could permanently disable (blind) satellites. Effectiveness may be difficult to discern (Success: 60% dazzle / 10% blind; Attribution: 80% if successful)	**Kinetic** • **Move co-orbital ASATs near protected SATCOM** satellite(s) in GEO (Attribution: 80%) • **Use co-orbital ASATs to destroy protected SATCOM** satellite(s) in GEO, would produce debris in GEO (Success: 90%; Attribution: 80%) • **Use direct ascent ASAT missile to destroy ISR satellite(s) in LEO**, would produce debris in LEO (Success: 90%; Attribution: 100%)
Non-Space	**Non-Kinetic** • **Raise/lower the alert status** of forces in the region • **Deploy/withdraw aircraft** in the area (specify manned/unmanned and armed/unarmed) • **Deploy/withdraw maritime forces** in the area • **Deploy/withdraw ground forces** in the area	**Kinetic** • **Declare a no-fly zone** (give authority to shoot down aircraft) • **Attack naval forces** (Success: 90%; Attribution: 100%) • **Attack ground forces** (Success: 90%; Attribution: 100%) • **Attack SSA facilities** (Success: 90%; Attribution: 100%)
Diplomatic	**Public** • **Send public demarche** to Blue/Orange/Red • **Propose bilateral discussions** with Blue/Orange/Red • **Propose multilateral discussions** with Blue/Orange/Red • **Impose economic sanctions** against Blue/Orange/Red	**Private** • **Send private demarche** to Blue/Orange/Red • **Propose secret bilateral discussions** with Blue/Orange/Red • **Leak information** (or misinformation) to the media

– Blue Team Background

National Interests/Objectives

As a dominant regional economic and military power, Blue's primary national interest is in protecting and enhancing its regional influence. Blue seeks to minimize Yellow's influence in its region, particularly its alliance with Orange. Blue is concerned that Orange and Yellow wish to contain its regional influence, as evidenced by their alliance and economic partnerships with Blue's neighbors.

Diplomatic Relationships

Blue has no formal alliances with any countries but does have partnerships with several developing states.

Blue's relationship with Yellow is mixed. Blue and Yellow have historically been economic and political competitors, with Yellow wielding strong diplomatic influence among Blue's neighbors. Although Yellow has refrained from directly opposing Blue in recent years, it has not prevented its ally, Orange, from doing so.

Blue's relationship with Orange is strained. Over the last few years, Orange has made public denouncements of Blue and directly opposed Blue's political and diplomatic initiatives.

Blue has strong economic ties with Red and has recently sought to strengthen this relationship .

Blue Team Options

Your team can choose any combination of the example options shown below. You may also develop other options not listed here, but please check with the Control Cell in advance to make sure any new options are technically feasible given your team's capabilities.

Space	**Non-Kinetic** • **Jam commercial/protected SATCOM downlinks**, localized to the immediate area (Success: 80%; Attribution: 90%) • **Jam commercial/protected SATCOM uplinks**, would likely affect users not in local area (Success: 80%; Attribution: 60%) • **Jam civilian/military PNT signal**, localized to area (specify civil/military) (Success: 90%; Attribution: 90%) • **Jam civilian/military PNT signal**, beyond local area (specify civil/military) (Success: 70%; Attribution: 90%) • **Cyber attack (ISR/PNT/protected SATCOM) satellites**; protected SATCOM satellites are also used for nuclear C2 (Success: 60%; Attribution: 40%) • **Dazzle ISR satellites**, could permanently disable (blind) satellites. Effectiveness may be difficult to discern (Success: 50% dazzle / 10% blind; Attribution: 80% if successful)	**Kinetic** • **Move co-orbital ASATs near protected SATCOM / missile warning satellite(s)** in GEO (Attribution: 80%) • **Use co-orbital ASATs to destroy protected SATCOM / missile warning satellite(s)** in GEO, would produce debris in GEO (Success: 90%; Attribution: 80%) • **Use direct ascent ASAT missile to destroy ISR satellite(s) in LEO**, would produce debris in LEO (Success: 90%; Attribution: 100%)
Non-Space	**Non-Kinetic** • **Raise/lower the alert status** of forces in the region • **Deploy/withdraw aircraft** in the area (specify manned/unmanned and armed/unarmed) • **Deploy/withdraw maritime forces** in the area • **Deploy/withdraw ground forces** in the area	**Kinetic** • **Declare a no-fly zone** (give authority to shoot down aircraft) • **Attack naval forces** (Success: 80%; Attribution: 100%) • **Attack ground forces** (Success: 80%; Attribution: 100%) • **Attack SSA facilities** (Success: 70%; Attribution: 100%)
Diplomatic	**Public** • **Send public demarche** to Yellow/Orange/Red • **Propose bilateral discussions** with Yellow/Orange/Red • **Propose multilateral discussions** with Yellow/Orange/Red • **Impose economic sanctions** against Yellow/Orange/Red	**Private** • **Send private demarche** to Yellow/Orange/Red • **Propose secret bilateral discussions** with Yellow/Orange/Red • **Leak information** (or misinformation) to the media

– Orange Team Background

National Interests/Objectives

Orange's primary national objective is managing the military threat from Blue and maintaining the alliance with Yellow. Orange lacks any significant natural resources of its own, so it is highly reliant on international trade to supply its economy. Recent economic changes in Orange and in the global oil market have placed significant strain on Orange's ability to purchase the oil and other natural resources it needs to maintain its economy.

Diplomatic Relationships

Orange has a mutual defense treaty with Yellow, which is based on deep and longstanding economic ties. Orange has more limited intelligence and military ties with Yellow, which only shares information and capabilities with Orange on a case-by-case basis.

Orange has a strained relationship with Blue. Over the last decade, Blue has significantly increased its military and economic power in the region, to the detriment of Orange. Orange is deeply concerned that Blue is using its growing regional power to undermine Orange's economy and security.

Orange has a strained diplomatic relationship with Red. Although Orange and Red have some economic ties, they have never had a strong diplomatic relationship due to religious tensions that have sometimes triggered conflict. In recent years, Red has moved closer to Blue .

Orange Team Options

Your team can choose any combination of the example options shown below. You may also develop other options not listed here, but please check with the Control Cell in advance to make sure any new options are technically feasible given your team's capabilities.

Space	**Non-Kinetic** • **Jam commercial/protected SATCOM downlinks**, localized to the immediate area (Success: 90%; Attribution: 90%) • **Jam commercial/protected SATCOM uplinks**, would likely affect users not in local area (Success: 90%; Attribution: 60%) • **Jam civilian/military PNT signal**, localized to area (specify civil/military) (Success: 90%; Attribution: 90%) • **Jam civilian/military PNT signal**, beyond local area (specify civil/military) (Success: 70%; Attribution: 90%) • **Cyber attack (ISR/PNT/protected SATCOM) satellites**; (Blue/Yellow protected SATCOM satellites are also used for nuclear C2) (Success: 60%; Attribution: 40%) • **Dazzle ISR satellites**, could permanently disable (blind) satellites. Effectiveness may be difficult to discern (Success: 40% dazzle / 10% blind; Attribution: 80% if successful)	**Kinetic** • **Use direct ascent ASAT missile to destroy ISR satellite(s) in LEO**, would produce debris in LEO (Success: 70%; Attribution: 100%)
Non-Space	**Non-Kinetic** • **Raise/lower the alert status** of forces in the region • **Deploy/withdraw aircraft** in the area (specify manned/unmanned and armed/unarmed) • **Deploy/withdraw maritime forces** in the area • **Deploy/withdraw ground forces** in the area	**Kinetic** • **Declare a no-fly zone** (give authority to shoot down aircraft) • **Attack naval forces** (Success: 80%; Attribution: 100%) • **Attack ground forces** (Success: 80%; Attribution: 100%) • **Attack SSA facilities** (Success: 70%; Attribution: 100%)
Diplomatic	**Public** • **Send public demarche** to Blue/Red/Yellow • **Propose bilateral discussions** with Blue/Red/Yellow • **Propose multilateral discussions** with Blue/Red/Yellow • **Impose economic sanctions** against Blue/Red/Yellow	**Private** • **Send private demarche** to Blue/Orange/Red • **Propose secret bilateral discussions** with Blue/Orange/Red • **Leak information** (or misinformation) to the media

– Red Team Background

National Interests/Objectives

As a small but technologically-sophisticated country, Red's primary objective is to protect its economic and social stability. Red is heavily dependent on continued free trade between all the countries in the region, as well as access to natural resources.

Red has a history of religious strife and is governed by leaders of a religious minority. The current government has only been in power a short time and is keenly aware of their precarious situation. The government is supported by the Red military, whose leadership shares religious beliefs with the current government.

Diplomatic Relationships

Red does not have formal alliances with any of the other countries, but its diplomat relationships are mostly friendly. In particular, Blue is Red's largest economic trading partner and has shown interest in stronger diplomatic ties.

Red has a good economic relationship with Yellow but few security or political ties.

Red has a mixed relationship with Orange. Red and Orange have moderate economic ties but also political and cultural tensions due to historical animosities between religious groups in both countries.

Red Team Options

Your team can choose any combination of the example options shown below. You may also develop other options not listed here, but please check with the Control Cell in advance to make sure any new options are technically feasible given your team's capabilities.

Space	**Non-Kinetic** • **Jam commercial SATCOM downlinks**, localized to immediate area (Success: 90%; Attribution: 90%) • **Jam commercial SATCOM uplinks**, would likely affect users not in local area (Success: 90%; Attribution: 60%) • **Jam civilian/military PNT signal**, localized to area (Success: 90%; Attribution: 90%) • **Cyber attack (ISR/PNT/protected SATCOM) satellites**; (Yellow/Blue protected SATCOM satellites are also used for nuclear C2) (Success: 50%; Attribution: 40%)	**Kinetic** • **Use direct ascent ASAT missile to destroy ISR satellite(s) in LEO**, would produce debris in LEO (Success: 70%; Attribution: 100%)
Non-Space	**Non-Kinetic** • **Raise/lower the alert status** of forces in the region • **Deploy/withdraw aircraft** in the area (specify manned/unmanned and armed/unarmed) • **Deploy/withdraw maritime forces** in the area • **Deploy/withdraw ground forces** in the area	**Kinetic** • **Attack naval forces** (Success: 70%; Attribution: 100%) • **Attack ground forces** (Success: 70%; Attribution: 100%)
Diplomatic	**Public** • **Send public demarche** to Yellow/Blue/Orange • **Propose bilateral discussions** with Yellow/Blue/Orange • **Propose multilateral discussions** with Yellow/Blue/Orange	**Private** • **Send private demarche** to Yellow/Blue/Orange • **Propose secret bilateral discussions** with Yellow/Blue/Orange • **Leak information** (or misinformation) to the media

APPENDIX C

Scenario 1: Background

Orange, Blue, and Red have a longstanding dispute over an island chain that may contain natural resources. The island chain is within 1,000 nautical miles of all three countries. Yellow has attempted to act as a mediator to reduce tensions and avoid outright conflict in the region.

On November 1, the Standard Oil Company, a firm that is owned by the Orange government and enjoys substantial financial investment from Yellow companies, announces that it has found massive reserves of oil near Skull Island, which is part of the disputed island chain. Claiming that it has a drilling license from Orange, Standard Oil announces that it has moved offshore drilling equipment to the area to begin extracting oil.

On November 2, Blue and Red publicly protest the move and announce that they cannot allow such an illegal action to occur. Both countries move naval units into the territorial waters around the island chain for the stated purpose of monitoring the activity of Standard Oil and protecting their own claims. Orange announces that in order to protect its commercial activities, it is moving its own naval units into the territorial waters of the island chain.

On November 4, Orange lands a small military force on Skull Island and establishes a satellite ground station. Blue and Red denounce this action as a violation of international law and demand that Orange withdraw immediately. Yellow calls an emergency meeting of the United Nations Security Council (UNSC) to discuss the situation.

On November 6, a Yellow carrier strike group arrives near the island chain but stays beyond the territorial sea, where it conducts air patrols as well as ISR operations using manned and unmanned aircraft. Yellow publicly calls on all parties to refrain from hostile activities. The media reports that commercial shipping in the area is experiencing interference with civil PNT navigation systems.

On November 7, a Blue manned helicopter flying an ISR mission from a destroyer near Skull Island is struck by a small UAV and crashes, killing the pilot. Blue claims that the helicopter was deliberately rammed by an Orange UAV. Blue begins to mobilize additional military units, which includes dispatching naval ships to and establishing long-range ISR patrols over the island chain. Blue also puts land-based aircraft and conventional ballistic missile forces on alert. Blue declares publicly that it will defend itself against any further attacks on its military forces. Blue reiterates its demands that Orange cease the drilling operations and remove its forces from Skull Island, threatening to force an end to the drilling operations if Orange does not comply.

On November 8, Orange protests its innocence in the helicopter crash, claiming that a Red UAV hit the Blue aircraft. However, Orange also begins to mobilize additional naval and air units while declaring that it will defend itself against any aggression. Orange deploys two destroyers to the island chain, which are equipped with midcourse missile defenses that utilize satellites for detection and targeting of ballistic missiles.

On November 9, Red protestors stage mass demonstrations in the streets, calling for Orange to withdraw from Skull Island and for the Red government to do more to protect its national interests. The same day, the UNSC convenes an emergency meeting.

– Yellow Team - Scenario 1

Objective

Yellow's primary objective is to maintain stability in the region and prevent the outbreak of armed conflict that could jeopardize trade. At the same time, Yellow's government is also keen to uphold its alliance with Orange, while protecting its power projection capabilities, particularly its space-based systems.

Private Information

Orange did not consult with Yellow before moving its forces onto Skull Island.

After landing on Skull Island, Orange's forces established a ground-based PNT and satellite communications jamming capability. Orange then began jamming all civil PNT signals in a 200-kilometer radius around Skull Island. Orange's forces in the area are largely unaffected by this jamming as they are utilizing an encrypted military PNT signal provided by Yellow.

Blue's downed helicopter probably collided with a Red UAV because Red's UAVs rely solely on civil PNT signals.

Orange's ship-based midcourse missile defense relies on Yellow missile warning satellites.

Blue's alerting of its land-based missile forces included raising its conventional anti-ship ballistic missiles to their highest alert status. There are also indications that Blue has upped the tasking on its five ISR satellites that are capable of detecting, tracking, and targeting ships at sea.

There are indications that hardline elements within the Blue military are fueling domestic protests and are pushing for forceful action.

– Blue Team - Scenario 1

Objective

The Blue government's primary objectives are to force Orange to withdraw their forces from Skull Island and for Standard Oil to cease operations. Blue's secondary objective is to undermine Orange and Yellow's ability to use space capabilities to project power into the island chain.

Private Information

The Red UAV likely crashed due to Orange jamming of all public PNT signals near Skull Island. The jamming is not likely to affect the military PNT signals used by Blue, Yellow, or Orange.

Orange's ship-based missile defense system utilizes two of Yellow's space-based missile warning satellites in geosynchronous orbit for detecting missile launches. Orange shares military PNT capabilities with Yellow, using its own satellites to augment Yellow's constellation. Orange has its own limited

space-based ISR capability, consisting of six satellites providing both optical and SAR imagery, and it has limited access to some of Yellow's space-based ISR capabilities.

Yellow's carrier battle group is highly reliant on space capabilities (SATCOM in particular) to operate in the vicinity of the island chain.

– Orange Team - Scenario 1

Objective

Orange places the highest priority on defending its claims to Skull Island and the nearby oil fields, as well as deterring aggression by Blue.

Private Information

Orange did not consult with Yellow before moving its forces onto Skull Island.

Upon landing on Skull Island, Orange forces established a ground-based PNT and satellite communications jamming capability. As per standard operation procedure, Orange began jamming all civil PNT signals in a 200-kilometer radius around Skull Island. Orange forces in the area are largely unaffected by the jamming, as they are utilizing an encrypted military PNT signal provided by Yellow.

Orange intelligence services say it is likely that a Red UAV collided with the Blue helicopter near Skull Island, potentially due to Orange jamming.

Blue's alerting of its land-based missile forces included raising its conventional anti-ship ballistic missiles to their highest possible alert status. There are also indications that Blue has upped the tasking on its five ISR satellites capable of detecting, tracking, and targeting ships at sea.

There are indications that hardline elements within the Blue military are fueling domestic protests and pushing for forceful action.

– Red Team - Scenario 1

Objective

Red desires to avoid any perceived change in the sovereignty of the disputed islands. In addition, Red places a high priority on obtaining evidence that Orange is causing environmental damage and violating international law so that it can use the evidence to put international political and public pressure on Orange.

Private Information

On November 7, Red lost contact with one of its UAVs flying an ISR mission near Skull Island. Red technical experts say it might have been due to PNT jamming and that the most likely source is the Orange facility on Skull Island.

Since all Red UAVs rely heavily on civil PNT signals for navigation, it is unlikely Red will be able to successfully operate UAVs in the area.

Summary of Play- Scenario 1

Teams were NOT permitted to communicate privately with one another during each move. If they wished to privately communicate, they could send a message through the White Cell to pass to a different team. Actions and public messages may only be submitted at the end of a move.

Move 1

Blue's goal in Move 1 was to pressure and isolate Orange and sideline Yellow from the conflict by attempting to break the Orange-Yellow alliance. In Move 1 Blue decided to:

- Deploy additional air and naval forces to the region.
- Begin downlink jamming of the Yellow-commercial SATCOM used by Standard Oil for their drilling operations.
- Publically demarche Orange and accuse Orange of creating the PNT interference that caused the helicopter-UAV collision.
- Offered to host 3+1 talks, with Yellow as the observer, on regional challenges

Red's goal in Move 1 was to avoid escalating the situation and reassert Red sovereignty without provoking Orange or Blue. The actions they took were to:

- Increase the tasking of its commercial ISR satellites for the island chain.
- Task their commercial fishing fleet to collect water samples and place government scientists on the commercial fishing vessels to aid in the collection and analysis in order to try and learn more about the situation.

Orange's Move 1 goals were to diffuse the crisis while continuing their drilling operations on Skull Island and to use Yellow as an offset to a potential military response from Blue or Red. Orange's actions in Move 1 were to:

- Continue the PNT downlink jamming.
- Position its naval forces and sea-based missile defenses to defend Skull Island.
- Publicly express regret over the loss of life and offer compensation to Blue, while calling for restraint by all parties.

Yellow's goals in this move were to de-escalate the situation and establish communications with all other actors. In the first move Yellow decided to:

- Privately increase the alert status of its satellite dazzler and offensive cyber capabilities, in case they need to be used in the future.
- Investigate the PNT interference.

Adjudication

The Blue downlink jamming of Yellow's commercial SATCOM was successful, but also publicly attributed.

Orange's continued PNT downlink jamming was successful and not attributed.

Red's tasking of commercial ISR was successful and images are coming in.

Move 2

Blue's goal for this move was to increase the pressure on Orange without being the first to engage in an illegal use of force. They tried to collaborate with Red on both a joint-military exercise on the Red/Blue border and economic sanctions against Orange; however, Red refused to participate in either. Blue took the following actions in Move 2:

- Conduct a cyber-attack on the Orange ground station on Skull Island.
- Continue cyber-attacks against Standard Oil's global network.

In Move 2, Red's goal was to slow Blue down and to bring in Yellow to help pull Orange back from the island chain. Red's actions in this move were:

- Publically release imagery of Orange's deployment of missile batteries near Skull Island.

Yellow's goal in Move 2 was to reinforce de-escalation and return to a stable environment. To accomplish this, Yellow took the following actions:

- Publicly released satellite imagery of Skull Island and the island chain.
- Offered to provide Coast Guard personnel and military PNT receivers on Red fishing vessels to ensure safety of life.

Orange wanted to also de-escalate the situation, but without compromising their presence on Skull Island. In Move 2 Orange:

- Agreed, publically, to 3 + 1 talks if Yellow mediated.
- Expressed interest in discussing a code of conduct on electromagnetic interference.
- Leaked disinformation to the media that the initial samples from the drilling indicated a disappointing level of oil.

Adjudication

Blue's cyber-attack on the Orange ground station failed and was not attributed. Blue's continued cyber-attacks on Standard Oil also failed and were attributed to Blue.

Orange's leaked disinformation was successfully distributed and not attributed to Orange.

Move 3

For the final move in the scenario, Blue's main focus was to remove Orange forces from Skull Island. To achieve this Blue:

- Commenced downlink jamming of the Yellow/Orange commercial and military SATCOM being used by the Orange forces on Skull Island.
- Began dazzling of Yellow/Orange ISR satellites as they flew over Skull Island only for the short time period needed for Blue to conduct an air assault on Skull Island.

By Move 3 Red began to feel overshadowed and ignored by the other teams. Their goal for the final move was to get acknowledgement from the other teams of Red's sovereign and commercial rights. An additional goal was to remove Orange from Skull Island. To accomplish these goals and reassert themselves, Red:

- Raised the alert status of their forces in the region.
- Conducted an offensive cyber operation against the Orange military ground station on Skull Island.
- Encouraged its commercial industry to increase their activity in the island chain.
- Reaffirmed the protection of its commercial industries from Red's military.

Yellow's goal for Move 3 was to reinforce the actions of other teams to de-escalate the situation. To do this, Yellow acted to:

- Keep its satellite dazzler and cyber forces at a high readiness level.
- Pull its maritime forces (a carrier strike group) out of the area.

Finally, Orange's main goal in the final move was to maintain its presence on Skull Island, to make Blue seem as the aggressor in the situation, and the emphasize the commercial-nature of the situation at large. Orange took no specific actions in Move 3.

Adjudication

Blue's downlink jamming on Yellow's and Orange's commercial and military SATCOM was successful and attributed. Blue's dazzling of Yellow and Orange ISR satellites was also successful and attributed back to Blue.

Red's offensive cyber operations against the Orange military ground station on Skull Island was successful and without attribution.

Conclusion

The Blue Team stated that they wanted to find a way to get Orange off of Skull Island, without provoking a military response from Yellow. That drove Blue to look for ways to control escalation while still being coercive. As part of this, the Blue Team felt that Standard Oil could be treated as an independent actor from the Orange government. The Blue Team stated that they were hesitant to go directly to attacks on space capabilities, because they felt that once the conflict moved to space it would be hard to stop it from ratcheting up.

In the post-scenario discussion, the Red Team stated that their goal was to return the situation to the status quo ante, but felt that they were being ignored by the other teams and thus debated how early to launch the cyber-attack. The Red Team also stated that they fundamentally saw this as a territorial dispute, while both Yellow and Orange wanted to keep it an economic dispute.

The Yellow Team felt that Orange's decision to land forces in the island chain without prior consultation undermined their alliance and thus were not incentivized to strongly back Orange, *however it*

must be noted that this was part of the original given scenario and not an action taken by the Orange team during a move. Yellow's overall strategy was to de-escalate, communicate, find credible stakeholders, frame the scenario, and take initiative in the international fora. As part of this, the Yellow Team stated that they tried to use their space capabilities to increase transparency and hopefully peel Red away from Blue while deterring armed attacks. The Yellow Team stated that if there had been a Move 4, they probably would have responded to Blue's jamming and dazzling in kind, but probably also with a communication to Blue to try and resolve the situation. The Yellow Team also stated that they probably would have considered the jamming and dazzling to be equivalent to a permanent attack, because it could come at any time and they thus could not rely on those space capabilities.

The Orange Team stated that they resorted to lawfare, disinformation, and diplomacy to offset their weaker military position. Thus, the Orange Team focused on being conciliatory and offering economic incentives to Red and Blue, such as sharing in the commercial profits. The Orange Team said that they were surprised by Blue's decision to plan to escalate to an armed attack at the end and felt that up until then Orange was winning with diplomacy.

APPENDIX D

Scenario 2: Background

Geopolitical tensions are growing. Many countries are struggling to adapt to rapid changes being driven by globalization and the realignment of traditional political and economic relationships. Orange and Blue have been hit particularly hard by the changes, which have caused political and economic instability in both countries and reopened scars of past conflict between them. Hardline governments have risen to power in both countries on promises to restore each to their former glory and to right historical wrongs.

On November 1, Orange is struck by the largest terrorist attack in its recent memory in a province bordering Blue. Suicide bombers detonate multiple devices inside a packed train station in the largest city of the province, killing dozens and injuring hundreds.

On November 3, Orange media leaks that the preliminary investigation has linked the attack to extremists in Blue. Despite Blue's denial of any official involvement, public outrage in Orange forces action. A state of martial law is declared in the province, and Orange military forces are mobilized to secure the border between Blue and Orange. Blue expresses concern that the mobilization seems excessive. Blue media pundits warn that the build-up might be in preparation for a military attack by Orange.

On November 6, Orange media broadcasts a report that claims to show evidence linking the terror attack to Blue intelligence services. Although Blue officially denies the link, the report has a strong influence on the Orange public, who demand action from their government.

On November 8, a Blue fighter aircraft on patrol shoots down a Yellow helicopter within Blue territory near the border with Orange, killing all on board. Blue states that the helicopter violated its airspace. Blue media announces that the helicopter was carrying an Orange special forces team and that the team was on a covert mission to infiltrate Blue. The helicopter was launched from a joint Orange-Yellow base located in Orange's territory near the border with Blue. Pundits in Blue speculate that Orange and the Yellow are preparing to invade Blue.

Blue places its armed forces on their highest alert and mobilizes multiple armored and mechanized divisions to the border with Orange, along with fighter patrols. Blue publicly vows to defend itself against all threats.

– Yellow Team - Scenario 2

Objective

Yellow's primary objectives are to deter a ground invasion of Orange by Blue and to ensure the integrity of Yellow's nuclear deterrent, including the ability to detect and respond to a nuclear attack using space-based missile warning and protected communications.

Private Information

Yellow has been in discussions with Orange on possible responses to an attack by Blue, as well as options for retaliation or a pre-emptive attack to blunt a possible Blue offensive.

The Yellow helicopter was carrying an Orange special forces team to conduct a raid on the extremist border enclave in Blue from which the terrorists originated. The helicopter was supposed to be stealthy against radar detection by Blue but was detected by Red, which provided the tracking data to Blue.

In response to the deepening crisis, Yellow has made slight alterations to the orbit of several of its intelligence satellites to increase ISR of Blue forces in the crisis region.

Yellow intelligence services are moderately certain that Blue intelligence was at least aware of the terror attack beforehand, if not complicit in it. Intelligence sources show there is a high level of activity among Blue war planners and indicate potential preparations for a pre-emptive strike on Yellow space forces, which would be consistent with Blue doctrine of denying adversaries the use of space.

On November 8, Yellow space surveillance capabilities detected a change in the orbital trajectory of three small objects in the GEO belt, which had originally been cataloged as debris from a Blue space launch five years ago. The new trajectories have the three objects drifting around the GEO belt towards the region over the crisis area between Blue and Orange.

A few hours ago, the first of the small satellites was predicted to arrive at the location of one of Yellow's GEO missile warning satellites, which provides warning of missile launches from the crisis region as well as battlefield intelligence. Around the same time, the Yellow missile warning satellite began experiencing interference with its command and control channel, resulting in interruptions to its health and status reports, as well as interfering with Yellow's ability to send commands to the satellite.

Yellow does not have sufficient space situational awareness coverage over the conflict area to independently confirm, but Red does have a ground telescope with good visibility.

ISR satellites show that Blue's mobilization includes increased readiness of their ASAT capabilities. At least six of Blue's mobile direct ascent ASAT launchers have left their bases and their current whereabouts are unknown. Additionally, Blue's airborne laser dazzler platform is making daily patrols in the region bordering Orange. Blue has also deployed mobile PNT jammers to the border region.

– Blue Team - Scenario 2

Objective

Blue's primary objective is to deter a ground invasion or violation of Blue's territory by Orange or Yellow.

Private Information

An investigation has revealed that the terror attack was supported by a small rogue element within Blue's intelligence services, but there was not broad support within Blue's government.

The Yellow helicopter was shot down because it crossed the border into Blue airspace and was believed to be carrying a full Orange commando team. The helicopter was detected by a sophisticated Red civil air traffic tracking radar, after which Red warned Blue about the unknown aircraft.

As part of the mobilization, Blue has dispersed six mobile direct ascent ASAT systems, four ground-based mobile PNT jammers, and began regular flights of an airborne laser dazzler platform, all within Blue territory near the border region.

Several days ago, Blue activated three small inspection satellites in the GEO region and tasked them to move toward Yellow's GEO satellites over the crisis region to determine the ability of Yellow to use those satellites to support a potential conventional conflict on the ground. Blue has not yet activated its co-orbital ASATs hidden in the GEO belt.

One of the three inspection satellites arrived at the location of a suspected Yellow satellite providing missile warning and intelligence to the crisis area. Blue instructed its satellite to alter its trajectory to conduct rendezvous and proximity operations (RPO) of the Yellow missile warning satellite in order to assess its capabilities and functions. The other two Blue satellites continued drifting toward other Yellow satellites. Shortly after beginning its inspections, the Blue satellite conducting RPO near the Yellow satellite began experiencing interference with its command and control channel. This has interrupted its health and status reports, as well as Blue's ability to send commands.

Intelligence sources show a high level of activity among Yellow war planners and indicate potential preparations for a pre-emptive strike on critical command and control and air defense nodes that would be consistent with Yellow doctrine of seizing the initiative and dealing a decisive blow early in a campaign.

Yellow has altered the orbits of its ISR satellites to optimize collection over Blue territory. The satellites provide daily coverage of the border region and previously proved successful at identifying targets that were destroyed by PNT-guided munitions. Yellow will likely have fully mapped Blue's deployed forces and C2 architecture in a few days.

Blue has requested exclusive access to Red commercial ISR satellites over the conflict region, but has not yet received a response.

– Orange Team - Scenario 2

Objective

Orange's primary objective is to deter a ground invasion by Blue. Orange's secondary objective is to bring the perpetrators of the terror attack to justice and eliminate the terrorist threat.

Private Information

The Yellow helicopter was carrying an Orange special forces team to conduct a raid on the extremist border enclave in Blue from which the terrorists originated, with orders to capture or kill those responsible for the terror attack.

Orange has been in contact with Yellow to discuss possible responses to an attack by Blue, as well as

options for retaliation or a pre-emptive attack to blunt the offensive.

Yellow intelligence has alerted Orange that three small Blue satellites, suspected to be co-orbital ASATs, are drifting through the GEO belt towards important Yellow satellites, including ones that provide tactical warning of missile launches and battlefield intelligence of the border region.

Orange has requested exclusive access to Red commercial ISR satellites over the conflict region, but has not yet received a response.

– Red Team - Scenario 2

Objective

Red's primary objective is to deter an attack on its sovereign territory. Red's secondary objective is to prevent a conflict between Orange and Blue -- its two largest trading partners -- which would threaten political and economic stability in the region.

Private Information

Red has a very sophisticated civil air traffic control radar that detected the Yellow helicopter as it moved across the border. Red alerted Blue that it had detected an unknown aircraft but did not know it was a Yellow/Orange military mission.

Red has a scientific telescope located near the border with Orange and Blue, which provides data to a global tracking network operated by Yellow.

Red's telescope observed one of the three objects alter its trajectory to stay close to one of Yellow's missile warning satellites, while the other two have continued to drift further along the GEO belt.

Summary of Play - Scenario 2

Move 1

Teams are permitted to communicate privately with one another during each move. Actions and public messages may only be submitted at the end of a move.

In this move, Orange's goals were to deter Blue, solidify their alliance with Yellow, and deal with public discontent. Blue's goals were simply to de-escalate the situation in the region. Yellow hoped to keep Blue in a box, protect its nuclear C2 assets, and reassure its allies. Red played a smaller role, hoping to deter an attack on its sovereign territory by making themselves more valuable to Yellow and Blue in peacetime than in wartime.

At the start of this move, Orange immediately messaged Yellow to urge reinforcements of land forces, tanks, and artillery to establish a deterrent to Blue forces. Yellow agreed. In exchange for a Yellow senior delegation sent to the Red interior, Red agreed to share their information regarding the three space objects approaching Yellow GEO space assets. Blue expressed concern over the rogue element

within their government and warned against escalation.

At the end of the move, Orange took the following actions:

1. Call up reserve forces.
2. Deploy 10 attack submarines and 10 frigates, in coordination with Yellow.
3. Publicly release the following message: “We demand justice for our forces lost. We have no intention, however, on attacking Blue. We will not take offensive action against Blue except for our collective self-defense.”

Blue, took the following measures:

1. Raise the alert status of conventional forces, but not nuclear forces.
2. Increase ISR assets over Yellow mainland via commercial augmentation and cooperation with Red.
3. Move all small inspection satellites to a non-threatening distance.
4. Deploy additional ground, maritime, and air forces.
5. Send Orange an open letter, stating “we would like to communicate that we share a common enemy of hostile terrorist networks and we propose a phased reciprocal stand down of forces on the border.”

Yellow respected its pact with Orange:

1. Forward deploy a battalion, two carrier battle groups, 4 nuclear submarines, stealthy bombers, and 4th generation fighters into the region.
2. Conduct cyber attacks against SSA ground sites and non-nuclear C2 sites.
3. Release the following message publicly: “We urge everyone involved to deescalate, we are working with blue to try and find the elements within the blue government responsible for the terror attack.”

Red took the following actions:

1. Upgrade military preparation to high alert status.
2. Move tank, artillery, infantry, and aircraft assets to the northern region of the Red state to maintain the integrity of the Red border.
3. Signal preparation of ASAT capabilities.
4. Privately message Yellow the details of its GEO object identification: one object altered its trajectory to stay close to a Yellow missile-warning satellite.
5. Publicly announce: “The shifting of Red military assets in the northern regions of the Red state are completely defensive to maintain the integrity of our border.”

Adjudication

The cyber attacks that Yellow conducted against Blue’s SSA ground sites, was not successful, but it

was attributed. Additionally, Yellow's cyber attacks against Blue's non-nuclear C2 were also not successful; however, this action was not attributed to Yellow.

Move 2

Move 2 in this scenario could be considered the Round of the Observers. Red told Yellow that it'd "be happy to act on Orange's request to send observers" to the border regions. Blue not only welcomed the idea, but requested that Red also monitor de-escalation against space-based assets.

In a private message to Orange, Yellow suggests a confidence-building measure: share information with Blue to establish cooperative efforts to prevent terrorist elements from damaging Yellow collective attempts to de-escalate tensions.

At the end of the move, Red took the following actions:

1. Deploy border monitors along the Blue-Orange border to establish a demilitarized zone to aid in de-escalation.
2. Deploy a cyber operation against the Blue government to derive insights on the intentions and relationship of the government to the terror organization.
3. Publicly invite high-level delegations from all parties to the Red capital city, Rubyville, for peaceful de-escalation discussions.

Both Yellow and Orange elected to perform no actions this move.

Blue took a more aggressive approach:

1. Perform three simultaneous cyber attacks on military logistics sites in Yellow.
2. Intermittent, random PNT Jamming over Blue mainland.
3. Stage massive rally that demonstrates public support of government.
4. Propose a regional economic and security group with Orange and Red to stabilize the region and reduce violent extremism.
5. Send the following message to Orange and Red: "Regional issues should be addressed by regional actors not outside parties. Therefore, we propose working together to create a regional economic and security group.
6. Publicly call for peace talks.

Adjudication

Media reported intermittent civil PNT jamming over Blue mainland.

The Blue cyber attacks on Yellow military aerial refueling base, a major military port, and the logistics inventory system were all successful and not attributed.

Move 3

This move was riddled by miscommunication. First, Orange suggested unilaterally attacking Blue, but Yellow disagreed and felt that it would be too-escalatory. Then in order to sow confusion. Blue blamed Red for the cyber attacks on Yellow, which was accurate even though Blue originally initiated

the attacks. Red never formally responded to Yellow denying this falsity.

Yellow's goals for the round were to maintain the preservation of its objectives. Later, Red admitted they felt out of the loop on what the other teams' strategies were, which made them more hesitant to act aggressively. Blue's main goal was to deter Yellow and defend its borders, similar to the previous move. Orange's goals were the most aggressive: to disable Blue's offensive capabilities.

Red took just one action in this last round:

- Deploy a cyber operation on Orange to assess their intentions and involvement in the jamming of Blue's civil PNT and the cyber attacks in Yellow.

Yellow took no actions in the final move.

Orange acted against Yellow's behest and took stronger action:

- Jam SATCOM downlinks localized in the immediate areas of the two Blue SSA Ground Stations during the attack of the special forces.
- Send four SOF teams, two teams per each of Blue's SSA Ground Stations, to destroy the systems.

Lastly, Blue acted to protect itself against a Yellow attack:

- Place sea-based mine countermeasures on Blue coasts to the north and south.
- Conduct annual nuclear command and control exercises involving all levels of command;

Adjudication

Orange successfully jammed the SATCOM downlinks localized in the immediate areas of the two Blue SSA Ground Stations. Orange sent four SOF teams, two teams per each of Blue's SSA Ground Stations, and successfully destroyed the systems. The jamming and raids were both successful and also attributed to Orange.

Concurrently, Blue's move to place sea-based mine countermeasures was successful, as well as their decision to conduct annual nuclear command and control exercises.

Lastly, Red's cyber attacks were successful and not attributed.

Conclusion

All four teams convened for a discussion about the scenario.

The Red team's primary internal debate this round revolved around whether or not to posture a direct ascent ASAT as saber rattling with the intention of causing Blue and Orange to back down. In the post-scenario discussion, the Yellow team brought up that taking such a threatening posture confused them but did not affect the way they chose to play out the scenario.

Yellow noted that it didn't retaliate or escalate after the cyber attacks on homeland, because it felt its objectives were met and it was tit-for-tat with what they had done the round prior. They also noted that all of their objectives were met in the first move, so they didn't need to execute any more kinetic options.

In the first move, Blue chose to back away their inspection satellites from the Yellow satellites because of concern over their ability to avoid a collision that could escalate the scenario. This decision

was further influenced by Blue's knowledge of the link between those satellites and Yellow's nuclear warning system. Blue launched the multiple cyber attacks and jammed their own PNT, as a proportional response to Yellow's cyber attacks. They then tried to use lack of attribution to get back at Red. Once they realized that the main objective was not to be attacked, they were fine with letting people know it was a rogue entity. Blue's strategy was to both fracture the Yellow-Orange alliance and bring Red into the fold. They saw their biggest threat as Yellow's strategic and precision attacks.

The Orange team didn't respond to Blue's overtures because it didn't include Yellow. They couldn't agree to anything that excluded Yellow, and also did not want to get caught up in a big-power war. They also wanted Red to get involved,and then later felt that they had succeeded in getting Yellow and Red to deter Blue. Orange also attacked SSA ground stations to remove Blue's offensive co-orbital space capabilities, which also served well as a response to public demands for action.

APPENDIX E

Scenario 3: Background

Deepening economic stagnation and climate change have caused social and political upheaval in many developing countries. Governments have collapsed in several developing states, which are becoming breeding grounds for extremism and violence.

On November 1, in a hotly contested election, Red elects a new government that represents the religious majority. The outgoing government refuses to concede the election, and a civil war erupts. Most Red military leaders resign their posts and join forces with the ousted government to form an insurgent force, which fights a civil war against the remaining military forces wielded by the new government.

Yellow and Orange express public sympathy for the ousted government. Many suspect they are providing material support as well, and there are rumors that Orange training camps are used by Red insurgents. Blue openly supports the new government in Red and is providing them with military aid and advisors to counter the insurgency.

On November 4, Orange announces that one of its TV broadcasting satellites has experienced sustained, deliberate interference on a channel that is owned and operated by a Yellow company. Orange publicly blames the new government in Red and demands that the interference stop. The Red government accuses Orange of using the satellite TV channel to broadcast anti-government propaganda into Red.

On November 7, there is a major solar storm. A large coronal mass ejection strikes the Earth, causing widespread interruptions to power grids across the region. The storm causes widespread interference with satellite capabilities, resulting in failures of several commercial and civil satellites.

On November 9, during a battle between insurgents and Red government forces, a dozen Blue military advisors are killed in an airstrike. Blue claims that this was a deliberate attack on its military advisors by the insurgents and that Yellow's space-based ISR capabilities provided intelligence to support the attack.

– Yellow Team - Scenario 3

Objective

Yellow's primary objectives are to help restore the ousted government in Red to power and to protect Yellow's own space capabilities to maintain strategic deterrence against Blue.

Private Information

Yellow is covertly providing special forces, financial support, and intelligence to Red insurgents.

The Yellow special forces assisting Red insurgents are heavily dependent on satellite communications

and space-based PNT to provide support to the Red insurgents. Their primary source of satellite communications is from Yellow commercial satellites, which are also being used to downlink data feeds from Yellow UAVs supporting the insurgency, in order to provide plausible deniability.

Yellow intelligence has geolocated the uplink jamming of the TV satellite as coming from territory controlled by the new Red government. Technical experts say that the jamming bears the hallmarks of a military jamming system developed by the Blue military. The jamming is directed at the transponder used to carry a TV channel sponsored by the Orange government, but is strong enough to have intermittent effects on signals carried by other satellites in the region, including the commercial satellites carrying Yellow's UAV data feeds.

The solar storm did not have any significant effects on Yellow military satellites, but did have an impact on some civil and commercial satellites.

Yellow intelligence assesses that the Red jamming likely played a role in the airstrike on the Blue advisors. Yellow special forces had direct orders to avoid contact with Blue military advisors but may have been unable to determine their presence due to the intermittent interference from the Red jamming of commercial SATCOM links, used by stealthy Yellow UAVs in the area.

In response to the incident, Blue used an airborne laser platform against two of your military ISR satellites, which ended up blinding them.

– Blue Team - Scenario 3

Objective

Blue's primary objectives are to support the new Red government and to preserve Blue's own space capabilities to maintain strategic deterrence. Blue's secondary objective is to increase its power and influence in the region.

Private Information

Blue is overtly providing military advisors, intelligence, and material aid to the new Red government. Blue's support includes covert lending of a military SATCOM jammer to the Red government, which is likely being used to jam the TV broadcast satellite. The TV channel carried by the satellite is being funded by the Orange government and is highly critical of the new Red government.

The Red government reports that a stealthy Yellow UAV was overhead when the Blue military advisors were killed in the airstrike. There is evidence that Yellow UAVs have been providing intelligence to the insurgents.

Several Blue ISR satellites experienced anomalies at the time of the solar storm and are currently offline. Blue has very limited ISR coverage over the conflict area in Red.

Political pressure is building in Blue to avenge the deaths of its military advisors.

In response to the death of the advisor, Blue used an airborne dazzler against two Yellow military ISR satellites.

– Orange Team - Scenario 3

Objective

Orange's primary objective is to return the ousted government to power in Red. A secondary objective is to undermine Blue's influence and power in the region, including ending the jamming of the commercial SATCOM TV channel.

Private Information

The Orange government is funding the TV channel being broadcast into Red via satellite. While the channel is not being run by the Orange military, it naturally has been broadcasting material critical of the new Red government.

Orange has been cooperating with Yellow to provide support for opposition forces in Red. In particular, training camps located in Orange's territory are being used to train insurgent forces in Red.

– Red Team - Scenario 3

Objective

Red's primary objectives are to solidify its grip on the country and eliminate the ousted government as a political threat. Red also seeks to solidify its alliance with Blue.

Private Information

As part of Blue's military assistance to Red, Blue has covertly provided Red with a highly sophisticated SATCOM jammer that is designed to be effective against all commercial communication satellites. The Red government is currently using the jammer to surgically target the broadcast of an Orange-backed TV channel, which has been critical of the new Red government.

The Red government has detected stealthy Yellow UAVs operating over its territory. These flights have coincided with insurgent operations. One such Yellow UAV was detected in the area when the Blue military advisors were killed.

Summary of Play - Scenario 3

Move 1

Teams are permitted to communicate privately with one another during each move. Actions and public messages may only be submitted at the end of a move.

In this scenario, two strong alliances formed immediately in Move 1: Orange-Yellow and Red-Blue.

The Orange-Yellow Alliance

In this move, Orange's goals were to support Red insurgents in recapturing their homeland and prevent Blue from attacking Orange.

Yellow's goals were also to limit Red's new government's ability to retain control of their country and support the insurgency through an elimination of the Red government's counterspace capability. Additionally, Yellow wanted to eliminate Blue's space control capabilities, which attacked Yellow systems, without acknowledging their attacks were successful. In general, Yellow wished to remain covert in the aftermath of this crisis.

Towards the beginning of the move, Orange messaged Yellow to request assistance in restoring stability to the region by supporting the ousted government of Red with naval, ground, and air forces in order to establish a no fly zone, a blockade of Red's coast, and jamming communications in and around Rubyville, the capital of Red. Orange offered to establish a communications hub and missile defense on and around Skull Island to protect Yellow's forces. Yellow then counter-proposed that the Orange-Yellow alliance deploy a joint naval task force off the coast of Blue to determine Blue's true intentions and objectives. Orange accepted the offer and also agreed to supply naval forces.

As the turn ended, Yellow decided to take the following actions:

1. Target power stations via cyber beams, attributing power station attacks to solar storm.
2. Cyber-attack personnel supporting ISR and operations for the Blue airborne laser.
3. If the location of the operation center for the airborne laser is verified, then conduct two sea and two air cruise missile strikes against it, attempting to make the attack as non-attributable as possible.
4. Take action to limit the ability of the Red government to govern, including pervasive social media displays discrediting government officials, portraying them with women, without beards, drinking alcohol, and being blasphemous.

Orange, in what it called *Operation Restore Freedom*, took the following actions:

1. Activate reserves.
2. Jam all Red communications and ISR capabilities.
3. Mobilize all ground forces.
    a. Send two-thirds to the Orange-Blue border, postured as to deter a Blue attack on the Orange homeland.
    b. Send one-third of forces to the Orange-Red border to support the Red Insurgent invasion.
4. Forward deploy air forces to the intersection of Red-Orange-Blue to support the Red insurgent force and provide cover for our forces on the borders.
5. Place communications hub on and missile defense around Skull Island.
6. Deploy key elements of Orange naval forces to blockade the Skeleton Straits, between Skull Island and the southernmost peninsula of Red.
7. Hack Blue's main bank accounts funding the new illicit government of Red.
8. Put all space forces on high alert in anticipation of a Blue attack.

The Red-Blue Alliance

Red's goals in this move were to establish themselves as a legitimate government while trying to eject any Yellow and Orange insurgents, UAVs, and advisors from its territory and prevent future interventions. Blue's goals were to remain an economy of force and defense and prevent an escalated conflict in space.

At the onset of Move 1, Red proposed a broad strategic alliance with Blue. In a private message, Red made it clear that it was prepared to engage in the following activities in conjunction with the Blue team:

1. Jam all PNT with the effect of making Orange/Yellow precision operations ineffective within Red regions.
2. Use Red air forces to destroy all Yellow UAVs within the Red airspace.
3. Call up Red reserves and deploy land and air forces to the Orange border.
4. Engage in cyber operations against Orange/Yellow space-based ISR.

Red continued to agree that it would implement these activities immediately if Blue agreed to the following operations:

1. Strike the insurgent training camps within Orange.
2. Join the Red navy in joint naval operations to interdict all Yellow/Orange naval operations from the Red shoreline out through the Skull Island archipelago and along Red/Blue mutual shorelines.
3. Place anti-ship missiles in the Skeleton Straits.

Blue agreed to the mutual defense alliance and suggested a more diplomatic approach to deterring Orange's support to the Red insurgency.

As the turn ended, Red decided to take the following actions:

1. Jam all PNT within Red with the effect of making Orange/Yellow precision operations ineffective within Red regions.
2. Use Red air forces to destroy all Yellow UAVs within Red airspace.
3. Call up Red reserves and deploy land and air forces to the Orange border with the aim of interdicting the flow of supplies to the illegitimate Red insurgency.
4. Engage in cyber operations against Orange/Yellow ISR.
5. Deploy Red naval forces in a joint Red/Blue naval operation to the Red shoreline and Skull Island archipelago in order to interdict all Orange/Yellow naval operations within Red territorial waters.
6. Maintain the jamming of the Orange TV station.
7. Task Red commercial ISR to look for Orange-funded insurgent camps.
8. If Red ISR finds a training camp near the border, Red SOF will be deployed to disable the camps.

9. Leak intelligence to the media regarding the Yellow government using the disruption of the solar storm to cover their conduct in space, which includes targeting civilian space activities.
10. Announce publicly that Red and Blue have entered into a broad strategic defense alliance and that Blue has offered troops to defend the Red border should Orange or Yellow seek to invade.

Blue took the following actions:

1. Bolster protection of all space control infrastructure.
2. Deploy robust artillery and tanks on the Red-Orange border.
3. Support a no fly zone within Red to end Yellow UAV action.
4. Engage in a naval joint operation with Red as per the prior communications.
5. Place anti-ship missiles on the Skull Island Archipelago.
6. Perform a military exercise on the Blue-Orange border and raise alert level, but with no incursion across the border.
7. In a public message, underline that Blue's movement of forces to the Red-Orange border is in an attempt to stem the flow of insurgents and insurgent materiel into Red. Separately, make it clear that continued Orange support of the insurgency could lead to a more aggressive response from Blue and Red.
8. In private, demand an apology and reparations from Yellow for the killing of peaceful Blue advisors in Red as well as immediate cessation of Yellow's aggressive actions against Blue space assets.

Adjudication

This section represents the state of the environment at the end of Move 1.

Red's jamming of Yellow PNT over Red territory was active and working. Red successfully shot down all Yellow UAVs operating in Red airspace. Red was also made aware privately that their cyber-attack on Orange-Yellow ISR ground infrastructures was successful and they disabled data dissemination systems. Yellows knew this attack occurred but were unable to identify the perpetrator.

Orange TV stations were still being jammed.

Red was also experiencing widespread jamming of satellite ISR and communications, which was attributed to Orange. Red was also experiencing widespread power outages, but the media suggested it may have been linked to the solar storm.

Blue reports to Red that their bank accounts funding to the new Red government had been hacked and emptied.

Yellow conducted successful cruise missile strikes against a Blue military airbase from which a suspected airborne satellite dazzler was operating.

Blue and Red naval forces engaged with Orange forces, both attempting to land on Skull Island. Orange won the engagement and landed a communications hub and missile defenses on the island.

Multiple stories on social media portrayed the new Red government with women, without beards,

drinking alcohol and being blasphemous.

Blue noticed that Yellow failed in a cyber-attack against personnel supporting Blue's ISR and operations for Blue ABL. Yellow conducted a cruise missile strike against Blue's ABL C2 center. It was not successful and was attributed to Yellow.

Red insurgents, backed by Orange are moving to retake the Red capital.

Move 2

At the very start of this move, Yellow sent a private message to Blue clarifying its actions against Blue's airborne laser system. They believed that their attack was justified and proportional to Blue's prior actions and proposed to keep this conflict defined to terrestrial domains from then on.

Like the last move, Move 2 was dominated by two two-team alliances: the Red-Blue alliance and the Orange-Yellow alliance.

The Orange-Yellow Alliance

For this move, Orange's goals were to remove Red Team leadership and restore the previous government, with a close eye on a possible Blue ground invasion. Yellow's goals were to de-escalate in space, support the ousted Red government, and reassure support to Orange in support of the old Red government.

Yellow messaged orange to conduct a joint Electronic Warfare and cyber-attack against the Red government leadership to isolate them. They also recommended both of the alliance's commercial SATCOM companies to not support Red government leadership after these successful attacks. Orange accepted and requested that Yellow nuclear forces be placed on Stage 1 Alert while also sending a private message to Blue reiterating Yellow's commitment to defending Orange by any means necessary. Yellow reassured Orange of the strength of their alliance.

At the end of the move, Yellow took the following actions:

1. Maneuver dead ISR satellites into Blue's two ISR satellites for a kinetic kill with the intention of targeting them on the opposite side of the earth where their SSA capabilities are most limited.
2. Conduct EW against Red leadership C2 and restrict access to commercial satellite communications.
3. Provide support to Orange to ensure A2/AD in the Skeleton Straits and Skull Islands, including deploying heavy bombers to Orange to support border security.
4. Provide communications and propaganda channels to the ousted Red leadership to communicate the fact that they are in charge and are considered the legitimate government of the Democratic Republic of Red.
5. Vow to disrupt and negate communication links between blue SSA stations and satellites with Red ASATs.
6. Send the following message publicly: "Red your ASAT threats are dangerously irresponsible.

Blue do you know that Red is about to inflict great harm on your astronauts and those of other nations."

Orange took the following actions:

1. Deploy two SOF and cruise missiles to attack all of the Red Government's ASAT launch pads and ASAT facilities.
2. Deploy two SOF teams to remove Red leadership and restore the ousted regime to power.
3. Leak to the media that Orange enjoys a nuclear guarantee from yellow as part of the Orange-Yellow collective security alliance.

The Red-Blue Alliance

In this move, Red's goals were to push Orange off the territory and prove that a threat of escalation can work to de-escalate (and that threatening space is serious is enough to be an example of the concept). Blue's goals were to sustain the new Red government, avoid horizontal escalation, and think about their nuclear threshold.

Red messaged Blue to weigh in and support one of two operations in terms of military operations: eject the Orange presence from the Islands using naval forces, SOF, or a cyber attack or deploy a joint Red-Blue punitive ground mission to remove the terrorist camps. Blue suggests naval action and offers its full support.

Then Red sent a private message directly to every other team in the game, without Blue's consent. It read: "Unless you remove your support for the insurgency immediately, we will use our ASAT capabilities to render LEO INOPERABLE."

At the end of the move, Red took the following actions:

1. Deploy Red-Blue reserve forces to stop the Orange-backed insurgency.
2. Imprison all insurgent-supportive villagers.
3. Mobilize all ASAT capabilities and prepare for operation.
4. Defend ASAT sites with infantry and tank forces.
5. Airstrike attack all Orange-based insurgent camps that have been found.
6. SOF attack Orange ISR ground station.

Blue took the following actions:

1. Send naval forces for persistent counter maritime and land attacks on Orange forces on and around Skull Island.
2. Commit Blue forces into Red to defend against Operation Restore Freedom and support the duly elected Red government.
3. Jam and Dazzle Yellow commercial downlinks, civilian and military PNT satellites localized to the area, and dazzle ISR satellites localized to the area.
4. Massive airstrikes on Red insurgent move on the capitol.

5. Private message to Yellow: “Stay out of the region and we will cease our reversible attacks on your satellite.
6. Public message to all: “We condemn Yellow’s attack on Blue sovereign territory and continued attacks risks grave escalation between two nuclear powers.”

Adjudication

This section represents the state of the environment at the end of Move 2.

Each country was aware that Red’s ASAT capabilities had been mobilized and were at operational status, and Red infantry and tank forces were defending ASAT sites. In conjunction with Red, Blue successfully destroyed Orange forces on Skull Island.

Red successfully attacked insurgent training camps in Orange, but failed in their attack on an Orange ISR ground station in Orange territory. Blue moved forces into Red to defend government and Red insurgents were not able to retake the capital. Blue launched massive airstrikes against insurgents in Red territory.

Blue successfully jammed Yellow commercial SATCOM in Red territory. Orange conducted successful attack on Red ASAT facilities. Orange attempted a SOF and airstrike decapitation attack on Red that was Not successful.

Yellow successfully rammed its dead ISR satellite’s into Blue’s ISR satellites. Both were destroyed and several thousand pieces of debris were created in LEO. Yellow jamming attempt on Red C2 was not successful and not attributed.

Blue was successful in its attempt to destroy Orange forces on Skull Island, but in the process Yellow sunk several Blue naval vessels.

Move 3

The Red-Blue Alliance

Red’s goals in this last move were to stabilize the new Red government and regain internal control, while also further degrading Yellow’s space capabilities.

Blue’s goals were to consolidate the gains they had made earlier in the scenario and assert long-term influence in the region.

Through private communications, Red suggested Red-and-Blue-ordered cease-fire with Yellow and Orange. The round was too short for the two teams to agree on the details of such an action, so no cease-fire was called.

At the end of the move, Red took the following actions:

1. Continue to patrol Red’s villages with the support of Blue in search and prosecution of all insurgent forces.
2. Deploy a cyber attack on Yellow’s GEO communication satellite with the intent of pushing them into super-sync orbits where they do not pose conjunction threats, but are also no longer useful.

3. Deploy missile defense batteries surrounding the critical Red government assets.
4. Publicly communicate the following message: "Yellow, your hypocrisy is flagrant and through your reckless actions, you have set our planet's space-faring future back decades. COPUOS is really mad at you. The insurgency is being quashed and the legitimate government of Red is eager to fulfill the peaceful needs of its population."

Blue took the following actions:

1. Increase airborne ISR patrols to make up for lost satellite ISR.
2. Deploy all necessary military support in Red to counter Orange military aggression.
3. Continue Blue space control activities against Yellow from Move 2.
4. Communicate privately to Yellow: "We once again reiterate the danger of your actions within the region and call for you to stop engagement in region."
5. Communicate privately to Red: "We support a time-limited ceasefire with Yellow and Orange in order to negotiate a peace treaty that would result in the removal of any remaining Orange forces within Red territory and we offer to host the peace conference."
6. Publicly communicate the following message: "We condemn Yellow's reckless destruction of four satellites, degrading the LEO environment and we call for a negotiations of an International Code of Conduct for Outer Space Activities."

The Orange-Yellow Alliance

For this last move, Orange's goal was to fully withdrawal back to Orange territory.

Yellow's goals were to call peace talks to de-escalate tensions across the region, blunt Blue aggression indirectly through supporting Orange actions, and free up Orange ground and air forces by providing Yellow air forces in order to allow Orange to apply their forces to support the Red insurgency.

Orange and Yellow, through private communications during this round, were battered by miscommunication. Yellow's bombers, designed to support Orange's missions, were irksome to the Orange government.

At the end of the move, Yellow took no action, but did release the following public message: "Red's actions have resulted in a collision in space. We condemn Red's actions that have threatened lives and created debris in space. Blue along with the newly installed Red government have taken Skull Island for its oil resources to personally benefit the corrupt leadership. This grab for resources was enabled by the documented voter fraud on behalf of Blue and the Red government, which allowed them to take control as evidenced by the 110% voter participation in the Red capital of Rubyville. We are saddened by the loss of life that has transpired in recent days. We are calling for an immediate ceasefire and a peace conference between Yellow, Orange, Blue, and both the new and old Red governments."

Orange moved all Orange forces to defend the territorial homeland. They also released the following public message: "The attack on Orange soil by Red was unprovoked and peculiar due to the fact that there were no personnel in the training camps, as all Red Insurgents and Orange forces had been sent into Red territory to reestablish their rightful and historical government. Based on our assessment

that despite our superiority in numbers, the advantage of surprise, and the fact that Red commanders had defected; our forces in Red have nevertheless been defeated. Whatever mystical force defeated them is obviously a threat to Orange and therefore we are consolidating our lines of defense within our own territory."

Adjudication

This section represents the state of the environment at the end of Move 3.

Red deployed missile defense batteries surrounding the critical Red government assets. Orange forces moved into position to defend their homeland. Blue increased aerial ISR support over Red to make up for lost space-based ISR. Blue sent military support to Red to assist counter Orange military aggression

Conclusion

All four teams convened for a discussion about the scenario.

Yellow went after Blue ground stations instead of satellites because they didn't want to let Blue know the laser strikes were effective. Once Red made a public threat about using ASATs, Yellow thought it was a chance to use dead assets to attack Blue in a way that might not have been attributable. Yellow also noted that long-term increased risk of space debris was seen as a useful trade for taking out valuable Blue ISR assets. In the end, they were less worried about space debris than gaining a tactical advantage in the conflict. Furthermore, when asked if they would have used the kinetic attack had Red not made the ASAT threat, Yellow suggested that might not have done so. Had the cyber attack on Yellow protected SATCOM been successful, Yellow would have considered it a threat to strategic deterrent and placed its nuclear weapons on high alert.

For the Red team, after the Orange push on the capital, Red made the ASAT threat in an attempt to escalate to de-escalate without nuclear weapons. They recognized that in this instance, their plan backfired. Like many teams throughout the scenarios, the Red team reported that they found cyber capabilities to be consistently more useful than space control capabilities.

Orange felt limited in their space capabilities and therefore resorted to attacking Red ASAT ground stations. They also felt that there was serious miscommunication between them and both Yellow and Blue that hindered gameplay.

Blue's primary objective was to support the new Red government, so it focused military operations solely in Red. Additionally, Blue recognized that its attacks on Yellow were aggressive, but reversible. They intended to coerce Yellow through these aggressive moves, though they recognized that it didn't work out the way they intended. Blue believed that Yellow's kinetic attack gave Blue the diplomatic high ground. Lastly, Blue admitted that they didn't respond to attacks on their air bases because it felt the conflict in Red was resolving in its favor, and it didn't want to escalate the situation again.

About the Authors

Todd Harrison is the director of the Aerospace Security Project and the director of Defense Budget Analysis at CSIS. As a senior fellow in the International Security Program, he leads the Center's efforts to provide in-depth, nonpartisan research and analysis of space security, air power, and defense funding issues. Mr. Harrison joined CSIS from the Center for Strategic and Budgetary Assessments, where he was a senior fellow for defense budget studies. He previously worked at Booz Allen Hamilton where he consulted for the Air Force on satellite communications systems and supported a variety of other clients evaluating the performance of acquisition programs. Prior to Booz Allen, he worked for a small startup (AeroAstro Inc.) developing advanced space technologies and as a management consultant at Diamond Cluster International. He is a graduate of the Massachusetts Institute of Technology with both a B.S. and an M.S. in aeronautics and astronautics.

Zack Cooper is senior fellow for Asian security at the Center for Strategic and International Studies. Prior to joining CSIS, Dr. Cooper worked as a research fellow at the Center for Strategic and Budgetary Assessments. He previously served on the White House staff as assistant to the deputy national security adviser for combating terrorism. He also worked as a civil servant in the Pentagon, first as a foreign affairs specialist and then as a special assistant to the principal deputy under secretary of defense for policy. His research has appeared in *International Security* and *Security Studies*, among other outlets. He received a B.A. from Stanford University and an M.P.A., M.A., and Ph.D. from Princeton University.

Kaitlyn Johnson is a program manager and research associate for the Defense-Industrial Initiatives Group (DIIG) and a research associate for the Aerospace Security Project at CSIS. Her work focuses on supporting research staff, as well as specializing in research on defense acquisition and space policy. Previously, she has written on ultra-low-cost access to space, the RD-180 rocket engine, commercial remote sensing regulation reform, defense acquisition trends, and federal research and development contract trends. Ms. Johnson holds an M.A. from American University in U.S. foreign policy and national security studies with a concentration in defense and space security, and a B.S. from the Georgia Institute of Technology.

Thomas G. Roberts is a program coordinator and research assistant for the Aerospace Security Project at CSIS. His research interests include satellite architecture analysis, computational methodologies, and space policy in the United States Congress. Prior to his work at CSIS, Mr. Roberts worked with the government relations group at Orbital ATK. He holds a B.A. in astrophysical sciences with honors and an undergraduate certificate in Russian studies from Princeton University. In 2015, Mr. Roberts was named a Harry S. Truman Scholar.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org