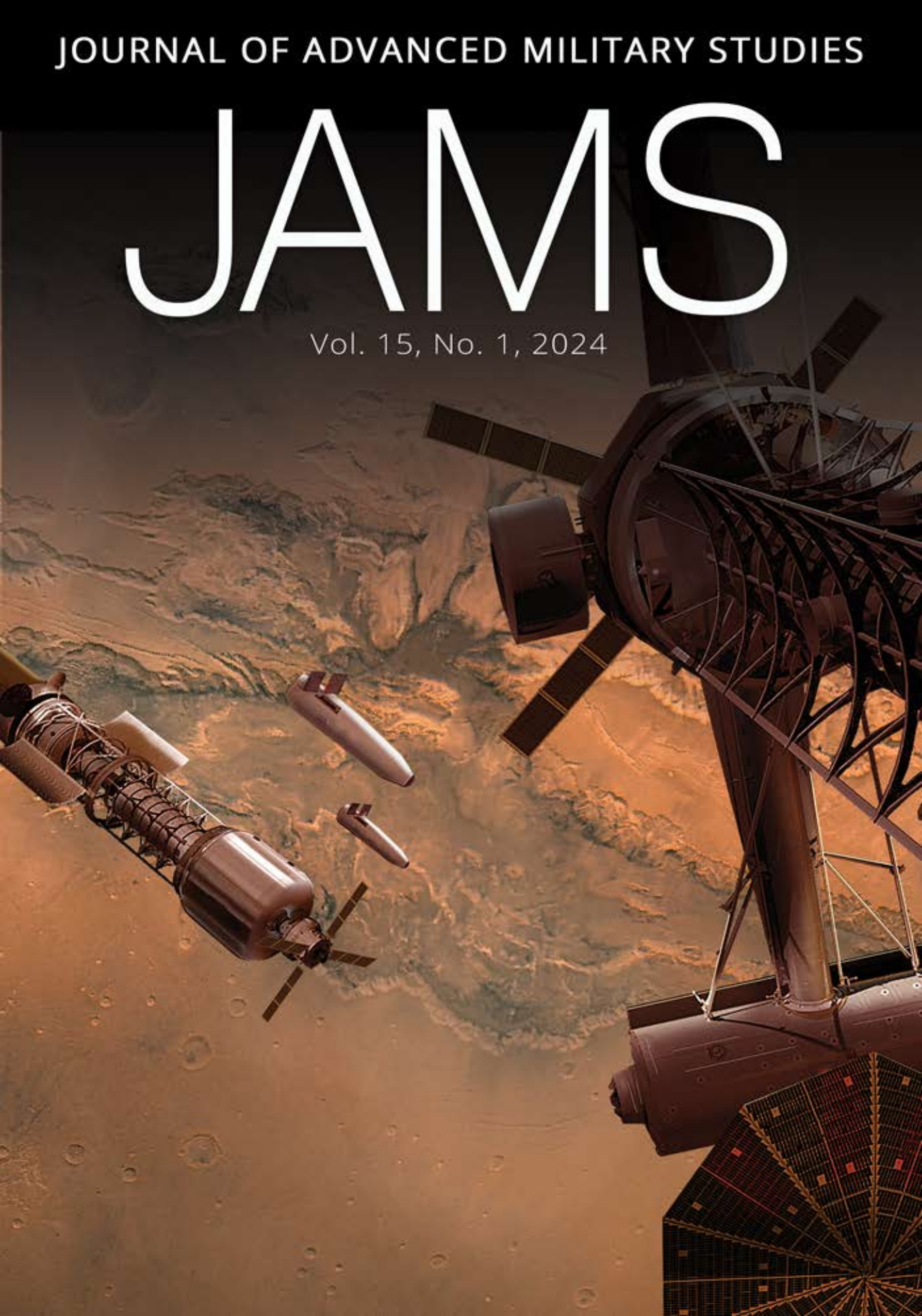
JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 15, No. 1, 2024



JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

MCUP

Published by Marine Corps University Press
2044 Broadway Street | Quantico, VA 22134

Journal of Advanced Military Studies
(Print) ISSN 2770-2596
(Online) ISSN 2770-260X

Established in 2008, MCU Press is an open access publisher that recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Journal of Advanced Military Studies* (JAMS) to provide a forum for interdisciplinary discussion of national security and international relations issues and how they have an impact on the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. JAMS is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS
The editors are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, and cybersecurity. To submit an article or to learn more about our submission guidelines, please email MCU_Press@usmcu.edu.

BOOK REVIEWS
Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS
Subscriptions to JAMS are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

ADDRESS CHANGE
Send address updates to MCU_Press@usmcu.edu to maintain uninterrupted delivery.

INDEXING
The journal is indexed by ProjectMUSE, Scopus, ScienceOpen, EBSCO, ProQuest, Elsevier, OCLC ArticleFirst, Defense Technical Information Center, Journal Seek, IBZ Online, British Library System, Lancaster Index to Defense and International Security Literature, and AU Library Index to Military Periodicals.

FREELY AVAILABLE AT
WWW.USMCU.EDU/MCUPRESS

Contents

Vol. 15, No. 1

The Void Above
The Future of Space Warfare and a Call to Update the Rule of International Space Law

Alan Cunningham

Abstract: In an age where space warfare is becoming more likely and a militarized space is already a reality, it is imperative to develop a strong legal framework to try and prevent nation-states from engaging in warfare. By implementing legal standards, improving on the existing legal framework, and taking input from outside legal sources, outer space can be made safer and the potential for armed conflict more protected against.
Keywords: outer space, international security, international law, space law, international relations, military affairs

Introduction

Cyberattacks, network intrusion, and other forms of electronic based warfare are becoming the way in which the military forces and intelligence services of the world conduct their operations to gain the upper hand on adversaries. The 2014–15 hack by Chinese intelligence of the Office of Personnel Management (OPM) remains one of the most serious data breaches in U.S. government history while the Chinese intrusion of the National Oceanographic and Atmospheric Administration's (NOAA) network and the ongoing Russia-Ukraine conflict shows how war will be waged in a new, highly technologically advanced digital age.[1]

Cyberattacks are becoming the name of the game, for both intelligence operatives and legitimate military states. And nowhere will this kind of warfare be waged more stringently and actively than in outer space. As such, with a new front growing in a geopolitical sense, it is important to examine the current

Alan Cunningham is a doctoral student in the University of Birmingham's Department of History. He is a graduate of Norwich University and the University of Texas at Austin. His research interests pertain to the U.S. intelligence community, Latin American affairs, and U.S. foreign policy. https://orcid.org/0009-0007-2746-2984.

Journal of Advanced Military Studies vol. 15, no. 1
Spring 2024
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20241501002

legal governance of space and how it can be updated or otherwise more readily relevant to current issues.

Warfare on the Final Frontier

What was once the final frontier for humanity is now the last true battleground in the cyberwar. For many hackers, with the development of privatized space travel and the creation of an entirely new Service branch for the U.S. armed forces, outer space has become a battleground with a growing sense of worry and fear regarding cyberattacks by nonstate actors disrupting internet access, interfering with the Global Positioning System (GPS), and turning "satellites into weapons."[2] Not only is the threat from nonstate actors growing, the greater level of concern is from state actors, like Russia and China, for strategic dominance in outer space.

Russia

Russia clearly is a significant geopolitical threat to the United States, easily one of the greatest foreign threats to American national security in the twenty-first century.

While their military may not be as strong as previously thought thanks to their lackluster performance in the Ukraine-Russia conflict, their cyber capabilities still rank highly among foreign adversaries and, if anything, have become more competent in their cyberattack abilities since the invasion.[3] Historically, Russia has been excelling in codebreaking, computer network intrusion, and waging warfare online since the downfall of the Soviet Union in 1991, doing so through the proliferation of "private cyber companies," some of which were started by former KGB (Committee for State Security) officers and further expanded by Vladimir Putin's oligarchs.[4] The state's cyberattack activities in Ukraine certainly, but also across Europe, Asia, and the Western Hemisphere show a highly capable and effective apparatus.[5]

The U.S. intelligence community (IC) has repeatedly identified Russia as a key cyber actor. Their 2022 annual threat assessment stated that the Russian Federation would "remain a top cyber threat [with a focus] on improving its ability to target critical infrastructure . . . in the United States as well as in allied and partner countries" while also using these cyber operations "to attack entities it sees as working to undermine its interests or threaten the stability of the Russian Government."[6]

The 2023 annual threat assessment reiterated this, in addition to highlighting Russia's commitment to warfare in space. The IC concluded that, in spite of the country's massive foreign and internal struggles during the past year, that Russia "is capable of employing its civil and commercial remote sensing satellites to supplement military-dedicated capabilities that reduce the U.S. ability to perform sensitive military activities undetected" while also "prioritizing and integrating" different highly technical capabilities (e.g., geolocation, advanced

GPS, intelligence, surveillance, and reconnaissance) to bolster their total space capabilities.[7]

The assessment goes into further detail, stating:

> Russia continues to train its military space elements, and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities. It is developing, testing, and fielding an array of nondestructive and destructive counterspace weapons—including jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based [antisatellite weapon] capabilities—to try to target U.S. and allied satellites . . . Russia is investing in electronic warfare and directed energy weapons to counter Western on-orbit assets. These systems work by disrupting or disabling adversary C4ISR [command, control, communications, computers, surveillance, and reconnaissance] capabilities and by disrupting GPS, tactical and satellite communications, and radars.[8]

Already, the United States has seen Russia's spatial capabilities in action. On the eve of Russia's invasion of Ukraine on 24 February 2022, exactly an hour before Russian troops moved into Ukraine, Russian hackers "launched destructive 'wiper' malware called AcidRain against Viasat modems and routers, quickly erasing all the data on the system" and, after being rebooted, these systems and "thousands of terminals . . . were permanently disabled."[9] Victor Zhora, the deputy chairman and chief digital transformation officer of the State Special Communications Service of Ukraine, stated that this cyberattack in the early hours of the conflict was "a really huge loss in communications in the very beginning of war" while others throughout Europe were affected by the cyberattack.[10]

By May 2023, it was the consensus of the U.S. intelligence community, the United Kingdom, and the European Council that Russian hackers were behind the downing of these key communications services, resulting in "tens of thousands of internet connections in at least 13 countries were going dead . . . making it much tougher for the [Ukrainian] military and intelligence services to coordinate troop and drone movements in the hours after the invasion."[11]

In December 2022, it was reported that the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) found that "the Russian military group known as Fancy Bear, or APT28 . . . [were] lurking inside a U.S. satellite . . . communications provider with customers in U.S. critical infrastructure sectors," this having gone on for months.[12]

In addition, Russia is also engaging in antisatellite weapons (ASAT) technology in support of their strategic and tactical goals. Having developed antisatellite weapons since 2007, Russia increased their abilities in November 2021 by launching a "PL19 *Nudol* interceptor [at] the now-defunct Soviet-era COSMOS 1408 satellite" resulting in a debris field "of at least 1,500 trackable pieces of debris in low orbit" causing immense geopolitical concern and threat-

ening any kind of military and spaceflight operations.[13] This can be seen as the culmination of decades-long desires for Russian aerospace superiority, which were steeped in the 1991 Persian Gulf War and the 1999 North Atlantic Treaty Organization (NATO) bombing of Yugoslavia.[14]

Russia's motivation behind this test was likely twofold, according to Deganit Paikowsky with Hebrew University of Jerusalem's Department of International Relations, as it signified to the international community that Russia is using antisatellite weapon technology to reassert its status as a superpower in space and "enhance . . . its defense and deterrence capabilities."[15]

Russia's capabilities for warfare in space are steadily increasing, having a robust cyberwarfare apparatus while also continually developing their ASAT competences for total aerospatial domination.

China

China, in many ways, surpasses Russia in terms of spatial domination. The IC's 2023 annual threat assessment made numerous assessments of China's abilities and capabilities, finding

> China's space activities are designed to advance its global standing and strengthen its attempts to erode U.S. influence across military, technological, economic, and diplomatic spheres [by way of continuing] to integrate space services—such as satellite reconnaissance and positioning, navigation, and timing—and satellite communications into its weapons and command-and-control systems in an effort to erode the U.S. military's information advantage. . . . Counterspace operations will be integral to potential [People's Liberation Army] PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites [already fielding] ground-based counterspace capabilities including electronic warfare systems, directed energy weapons, and ASAT missiles intended to disrupt, damage, and destroy target satellites.[16]

From an ASAT and counterspace weapons standpoint, China surpasses Russia in these threats. China first tested an ASAT-level weapon in 2007, destroying "an aging Chinese weather satellite" and has advanced their technology and capabilities steadily. [17] Due to this establishment of outer space as a military domain and solidifying their national space program under military control, China now "has an operational ground-based anti-satellite missile capability" and are testing scavenger satellites "which use grappling arms to capture other satellites" alongside having their satellites orbit "the geosynchronous belt . . . to sidle up to other satellites in space."[18]

China's development of hypersonic missile technology also has been assisting its rise in space dominance. In August 2021, China "launched a rocket that carried a hypersonic glide vehicle [through] low-orbit space before . . . [missing] its target by about two-dozen miles" in a test that caught the IC by surprise.[19]

Such developments of ASAT technologies and continued hypersonic missile development have resulted in the Pentagon announcing that China's military and defense posturing poses "the most consequential and systemic challenge to U.S. national security," essentially confirming what some have suspected.[20]

The IC found that China intends "to match or surpass the United States by 2045" and likely aims by 2030 to "achieve world-class status in all but a few space technology areas."[21] Based on the publicly available information and recent developments, it stands to reason that China, as in all other areas of military and national defense, will be a peer competitor to the United States for the next few decades.[22]

A Response from the U.S. Armed Forces

In response, the U.S. Department of Defense (DOD) aims to make space a priority alongside their adversaries. While most understand the "space race" of the Cold War to be an effort to beat the Soviet Union in scientific achievement, it also included developing intercontinental ballistic missile (ICBM) technology, unmanned aerial systems (UAS), and gaining an upper hand on U.S. adversaries by way of intelligence gathering and removing any first strike capabilities.[23] And to a large degree, the United States has never stopped innovating in space, continuing to be on the cutting edge of space warfare and innovating all manner of technologies originally meant for space operations.[24] With the growing militarization of space by Russia and China, the United States has engaged in many actions to combat this militarization, the most important of these being the creation of the U.S. Space Force.

With the creation of the Space Force in December of 2019, the culmination of decades of policy planning and theory, their entire goal is to protect and defend "U.S. interests in space from potential adversaries" strictly focusing on training troops in peacetime for spatial combat operations.[25] Since their creation, the Space Force has endeavored to make space a priority. This is evident in their policy and budget statements while they are also creating an entirely new unit "dedicated to targeting other nations' satellites and the ground stations that support them."[26] Coupling this with the U.S. Army's recent development of an office "to manage the portfolio of capabilities . . . [including] intelligence, electronic warfare and sensor," the DOD has substantially stepped up and recognized the growing trend of space militarization currently underway.[27]

From a policy standpoint, the Joseph R. Biden administration, in March 2023, released their *National Cybersecurity Strategy*, which called for "[rebalancing] the responsibility to defend cyberspace" toward larger federal institutions and private businesses as opposed to local governments and individuals alongside "[realigning] incentives to favor long-term investments" by recommitting the United States to international and industrial partnerships. This policy has been praised by many for seemingly calling for more tech and software regulation and reform, but also for helping to better define and outline what kinds of "offensive cyber operations" the Pentagon could undertake, which became

clearer when the Pentagon's own cyber strategy was released in May 2023. This policy called for financial and physical investment in cyber capabilities, aligning with international and private partners on direct operations, and better training/equipping forces for cyber missions.[28]

While this very real threat has been recognized by the United States as a serious and pressing issue, the matter of ensuring any kind of retaliatory or preventive action abides by and is enshrined in law, however, is another matter that must be readily addressed before any further action is taken.

Abiding by the Rule of Law

One of the main challenges to any U.S. outer spatial defense strategy comes from the lack of a clear and detailed international legal framework governing national security missions in space. Currently, "neither international law nor diplomacy has grappled effectively with space cybersecurity."[29]

Instead, there are manuals that offer guidance on space legal affairs to the international community and individual nation-states, though they are not legally binding nor official. The *Tallinn Manual 2.0* addresses the applicability of international law in cyberwarfare while both the Woomera International Law of Space Operations (a.k.a. *The Woomera Manual*) and the *Manual on International Law Applicable to Military Uses of Outer Space* (*MILAMOS*) "provide guidance on the international law applicable to space warfare."[30] It must be noted that these documents are largely theoretical in nature, not being produced by governments or any international legal or policy body, rather scholars and academics in the field. As such, while these are quite beneficial, there are challenges to their implementation given no governmental body or legally authoritative entity has embraced these works.

The current legal framework for global space governance is embodied within five United Nations treaties: the Outer Space Treaty (OST, or formally, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies) of 1967, the Rescue Agreement (formally, Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space) of 1968, the Convention on International Liability for Damage Caused by Space Objects of 1972, and the Convention on Registration of Objects Launched into Outer Space of 1976, all of which more represent the time period they were created in rather than addressing the current state and developing a framework for any future issues.[31] For example, the OST, while it does address a variety of issues in relation to proliferation, is only rather specific in principle as it addresses the use, placement, and control of weapons of mass destruction (WMDs) and nuclear weapons in space resulting in the difficult question of "what constitutes a weapon and [whether] its placement in space breach the requirement that outer space be used exclusively for peaceful purpose" in addition to failing to "provide any concrete rules that states must abide by in testing conventional weapons."[32]

Clearly, the international legal framework concerning military capabilities in space needs an update. Cyberattacks, antisatellite weaponry, and devices by which a foreign state could be able to neutralize another state's ability to engage in spatial warfare are no longer constrained to academic journals and conferences but are a current reality for governments, private corporations, and everyday civilians. The OST is still important and serves as an effective framework; however, its wide mandate has resulted in difficulty with it being the sole measure to "adequately govern space" and failing to consider more newer technologies.[33] Having a more robust, complete, and articulated rule of law for what military activities are and are not allowed in space would be the first step to secure space from such threats like China and Russia.

The unofficial or legally binding manuals (e.g., *Tallinn Manual 2.0*, *Woomera Manual*, *MILAMOS*) are all useful places for the international community to consult with and advise in developing laws necessary to safeguarding space; however, some experts caution they should not be implemented without extensive revisions or alterations. Some practitioners of space warfare have criticized the manuals for being "too-focused on legal theory, rather than real-world cases" while some authors of the manuals have openly stated that their work does not define what law "is should and ought to be" when it comes to space.[34] A thorough and complete analysis of these manuals, seeing what aspects of them are practical to real-world affairs and ensuring complete compliance with existing treaties, should be the first step for the international community in updating the world of space law for the modern, cyber age.

These new and more current updates to the current manuals and policies in place would not only help allied governments, nonstate actors, and civilian organizations in space travel and operations, but would also work to limit Chinese and Russian militarism in space as well as American militarization of this new strategic region. Some may argue for a ban of all weapons and the complete demilitarization of space; however, this is quite unrealistic as the issue of weaponry in space is already at hand, making any banning of conventional weapons or offensive operations problematic.[35] Surely this would assist in halting future militarization of space. Going forward, a more conciliatory effort should be applied instead to nation-states that work to militarize space.

This conciliatory view has been recommended by a multitude of individuals with experience in both space law, national security/defense, and in the space domain. Daryl G. Kimball, an executive director of the Arms Control Association, suggested as far back as 2007 the establishment of "stronger norms against dangerous activities in space, including flight tests that simulate hostile attacks against satellites and the deployment of anti-satellite and space weapon."[36] Others, including a former deputy director at the National Reconnaissance Office (NRO), a former undersecretary of energy for nuclear security, and a former senior diplomat working disarmament, all of whom are fellows with the Rand Corporation, argue for "deterrence . . . the capability to respond with overwhelming force to aggression . . . [pursuing] arms control agreements

as a complementary approach to enhancing stability, bolstering deterrence and avoiding costly arms races."[37]

David C. DeFrieze, then chief counsel for the U.S. Army Research Development and Engineering Command, wrote in 2014 that

> a standing committee is needed to provide a credible, knowledgeable, and equitable forum for regulating, monitoring, and adjudicating claims and disputes relating to the damage caused by objects launched into space, whether they are designed for destruction or not . . . [as well as] using the current economic deterrence and enforcement capability of the World Trade Organization to address and collect on unresolved adjudicated state liabilities. . . . A logical place for this committee would be the United Nations.[38]

It is important to note that some of this has already been undertaken by Western nations, including the United States, when developing ways to counter such space threats but also through the United Nations Open-Ended Working Group (OEWG) on Reducing Space Threats Through Norms, Rules, and Principles of Responsible Behavior.[39]

Nonetheless, some are hesitant to further codify space law. Laura Grego, a research director in the global security program at the Union of Concerned Scientists, detailed in a 2020 interview with the *Scientific American* that these "unofficial norms of behavior . . . registering new satellites sent into orbit, deorbiting their dying ones to avoid creating debris, not testing [direct ascent] DA-ASATs on their own satellites and not destroying another country's satellites" advocate, in the event a binding set of rules is unable to be articulated, for "a nonbinding international agreement based on current norms."[40] This interview was conducted prior to Russia's 2021 ASAT missile test and the Russian invasion of Ukraine, so it shows that such unofficial norms can be blatantly violated by nation-states with little to no repercussion.

Having these unofficial norms codified in law and using these, alongside the various manuals developed by legal practitioners, as a starting point for a more modern, internationally respected, and legally valid treaty is one of the best practices in ensuring the halting or pathway toward the demilitarization of space.

A diplomatic solution toward halting a further militarized outer space, in many cases, will be far more effective than an outright military solution. While a military solution would be on hand in the event there is a pressing matter that cannot be resolved diplomatically, the Department of Defense and U.S. armed forces can counteract some offensive operations in a way that would not be overly aggressive by using maneuverable satellites or engaging in jamming of enemy space equipment.[41] But diplomacy is and should remain the primary solution to any developments that occur in space to avoid a full on space race or any further debilitating and harmful activity using such weapons.

The research presented here suggests that addressing, redeveloping, and re-

organizing the legal framework currently in place by the international community into a codified, official legal treaty dictating what kind of military action is appropriate and what is not allowed in space would result in better outcomes for space. As mentioned above, the unofficial norms and the prior treaties all in place should be collectively considered in total and improved on or updated to reflect the current time. The more scholarly suggestions contained within the manuals should also be consulted and implemented on a case-by-case basis to adapt to the changing methods of warfare and plan for any potential, more theoretical issues that could arise.

Strengthening the international community's response to such spatial threats is imperative and essential in order to keep space as free of harmful conventional and unconventional weaponry as possible, ensuring militarism is kept to a limited manner in space.

Conclusion

Limiting the number of conventional weapons in space should be of utmost importance to the United States and the rest of the international community alongside lessening the impact of offensive cyber operations on Russia and China's part. Research and expert opinion have shown that diplomacy is by far one of the most assured measures by which the international community can be kept safe from man-made threats by way of space.[42] The United States should invest in their offensive capabilities, but also should make a strong push for diplomatic avenues and negotiations as a method of resolving the issues at hand.

The rule of law governing space must be updated, expanded, and developed to fully adapt to this modern, cyber age in which highly advanced technological weapons are becoming the primary way in which nation-states commit espionage and warfare against their adversaries.

Outer space offers many opportunities for humanity, namely deepening the understanding of our galaxy, the universe around us, and the origin of life as well as offering people the ability to explore and potentially find new planets in which to colonize. Placing conventional and unconventional weapons and allowing unfettered offensive cyber operations in space are not one of those uses.

Endnotes

1. Sean Gallagher, "NOAA Weather Data Interruption Due to Alleged Chinese Cyber Attack," *Ars Technica*, 14 November 2014; Josh Fruhlinger, "The OPM Hack Explained: Bad Security Practices Meet China's Captain America," CSO, 12 February 2020; and Grace B. Mueller et al., "Cyber Operations during the Russo-Ukrainian War," Center for Strategic & International Studies, 13 July 2023.
2. Bryan Bender, "What the Space Force Is, and Isn't," *Politico*, 3 February 2021; and Rebecca Heilweil, "For Hackers, Space Is the Final Frontier," Vox, 29 July 2021.
3. Simmone Shah, "The Russian Military's 4 Biggest Mistakes in Ukraine," *Time*, 24 February 2023; and Jon Bateman, Nick Beecroft, and Gavin Wilde, "What the Russian Invasion Reveals about the Future of Cyber Warfare," Carnegie Endowment for International Peace, 19 December 2022.
4. Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's

Capabilities," Center for European Policy Analysis, 8 September 2022; and Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's War on the Internet* (New York: PublicAffairs, 2015), 341.

5. Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," NBC News, 18 December 2016.
6. *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2022), 12.
7. *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2023), 16.
8. *Annual Threat Assessment of the U.S. Intelligence Community* (2023), 17.
9. Patrick Howell O'Neill, "Russia Hacked an American Satellite Company One Hour before the Ukraine Invasion," *MIT Technology Review*, 10 May 2022.
10. Lee Matthews, "Viasat Reveals How Russian Hackers Knocked Thousands of Ukrainians Offline," *Forbes*, 31 March 2022; and Corin Faife, "Russian Military Reportedly Hacked into European Satellites at Start of Ukraine War," *Verge*, 25 March 2022.
11. Faife, "Russian Military Reportedly Hacked into European Satellites at Start of Ukraine War"; Chris Vallance, "UK Blames Russia for Satellite Internet Hack at Start of War," BBC News, 10 May 2022; *Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union* (Brussels: European Council, 2022); and Katrina Manson, "The Satellite Hack Everyone Is Finally Talking About," Bloomberg, 1 March 2023.
12. Christian Vasquez, "CISA Researchers: Russia's Fancy Bear Infiltrated US Satellite Network," CyberScoop, 16 December 2022.
13. Ankit Panda, "The Dangerous Fallout of Russia's Anti-Satellite Missile Test," Carnegie Endowment for International Peace, 17 November 2021; and Shannon Bugos, "Russian ASAT Test Creates Massive Debris," *Arms Control Today*, no. 51 (December 2021).
14. Jaganath Sankaran, "Russia's Anti-Satellite Weapons: An Asymmetric Response to U.S. Aerospace Superiority," *Arms Control Today*, no. 52 (March 2022).
15. Deganit Paikowsky, "Why Russia Tested Its Anti-Satellite Weapon," *Foreign Policy*, 26 December 2021.
16. *Annual Threat Assessment of the U.S. Intelligence Community* (2023), 8.
17. William J. Broad and David E. Sanger, "China Tests Anti-Satellite Weapon, Unnerving U.S.," *New York Times*, 18 January 2007; and Bruce W. MacDonald, *China, Space Weapons, and U.S. Security* (Washington, DC: Council on Foreign Relations Press, 2008).
18. Taylor A. Lee and Peter W. Singer, "China's Space Program Is More Military than You Might Think," *DefenseOne*, 16 July 2021; and Bradley Bowman and Jared Thompson, "Russia and China Seek to Tie America's Hands in Space," *Foreign Policy*, 31 March 2021.
19. Demetri Sevastopulo, "China Tests New Space Capability with Hypersonic Missile," *Financial Times*, 16 October 2021.
20. Sandra Erwin, "Pentagon Report: China's Space Strategy Shaped by Technological Change," *SpaceNews*, 29 November 2022; and Ralph Jennings, "China Has Capability to Use Space for Military Purposes, Experts Say," Voice of America, 2 April 2022.
21. *Annual Threat Assessment of the U.S. Intelligence Community* (2023), 8.
22. Erik Seedhouse, "The Growing Chinese Space Threat," *SpaceNews*, 21 February 2023.
23. Craig Boucher, "On Space War," Modern War Institute, 1 June 2022.
24. George W. Bradley III, "The Air Force in Space Today and Tomorrow: An Overview," in *The U.S. Air Force in Space: 1945 to the Twenty-First Century*, ed. R. Cargill Hall and Jacob Neufeld (Washington, DC: USAF History and Museums Program, 1998), 163–67.
25. Margaret Hartmann, "Let's Get to Know Space Force, Trump's Most Misunderstood Creation," *New York*, 21 September 2022; and Stephen M. McCall, *Challenges to the United States in Space*, IFI0337 (Washington, DC: Congressional Research Service, 2021), 1.
26. Sandra Erwin, "U.S. Sharpens Plan for Military Space Race," *SpaceNews*, 11 July 2023;

and Brett Tingley, "US Space Force Creates 1st Unit Dedicated to Targeting Adversary Satellites," Space.com, 16 August 2023.

27. Mark Pomerleau, "Army Officially Creates New Offensive Cyber and Space Program Office," *DefenseScoop*, 28 July 2023.
28. Lauren C. Williams, "Sketching Out the Rules for Offensive Cyber Operations," *DefenseOne*, 5 March 2023; Elias Groll and Christian Vasquez, "Biden's National Cybersecurity Strategy Advocates Tech Regulation, Software Liability Reform," *CyberScoop*, 2 March 2023; "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy," White House, 2 March 2023; and Mark Pomerleau, "DOD Sends New Cyber Strategy to Congress, Releases Unclassified Fact Sheet," *DefenseScoop* 26 May 2023.
29. David P. Fidler, "Cybersecurity and the New Era of Space Activities," Council on Foreign Relations, 3 April 2018.
30. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation*s, ed. Michael N. Schmitt (Cambridge, UK: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524; Eytan Tepper, "The First Space-Cyber War and the Need for New Regimes and Policies," Centre for International Governance Innovation, May 2022, 3–4; and *Manual on International Law Applicable to Military Uses of Outer Space*, vol. 1, *Rules*, ed. Ram S. Jakhu and Steven Freeland (Montreal: Centre for Research in Air and Space Law, 2022).
31. Sophie Goguichvili et al., "The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier?," Woodrow Wilson International Center for Scholars, 1 October 2021; United Nations Convention on Registration of Objects Launched into Outer Space, New York, 15 September 1976; United Nations Convention on International Liability for Damage Caused by Space Objects, September 1972; Daryl Kimball, "The Outer Space Treaty at a Glance," Arms Control Association, October 2020; and Frans G. von der Dunk, "A Sleeping Beauty Awakens: The 1968 Rescue Agreement after Forty Years," *Journal of Space Law* 34, no. 2 (Winter 2008): 416–18.
32. Sa'id Mosteshar, "Space Law and Weapons in Space," in *Oxford Research Encyclopedia of Planetary Science* (Oxford, UK: Oxford University Press, 2019), https://doi.org/10.1093/acrefore/9780190647926.013.74; and Dale Stephens and Melissa de Zwart, "A Guide to Ensure Everyone Plays by the Same Military Rules in Space: The Woomera Manual," *Conversation*, 2 May 2019.
33. Adam G. Quinn, "The New Age of Space Law: The Outer Space Treaty and the Weaponization of Space," *Minnesota Journal of International Law* 17, no. 2 (2008): 487–89, https://core.ac.uk/download/pdf/217210297.pdf.
34. Theresa Hitchens, "New Legal 'Manual' on Peacetime Military Space Activities Could Aid Norms Drive," *BreakingDefense*, 8 September 2022; and Stephens and de Zwart, "A Guide to Ensure Everyone Plays by the Same Military Rules in Space."
35. Jeffery Nocton, "Ban Conventional Weapons in Space," *International Affairs Review*, 7 May 2019.
36. Daryl G. Kimball, "Avoiding a Space Arms Race," Arms Control Association, April 2007.
37. John Lauder, Frank Klotz, and William Courtney, "How to Avoid a Space Arms Race," *Hill*, 24 October 2020.
38. David C. DeFrieze, "Defining and Regulating the Weaponization of Space," *Joint Force Quarterly* 74, no. 3 (July 2014): 114.
39. David Vergun, "Official Details Space-Based Threats and U.S. Countermeasures," DOD News, 26 April 2023; and Theresa Hitchens, "Russia Spikes UN Effort on Norms to Reduce Space Threats," *BreakingDefense*, 1 September 2023.
40. Ann Finkbeiner, "How Do We Prevent War in Space?," *Scientific American*, 1 November 2020.
41. Finkbeiner, "How Do We Prevent War in Space?"
42. Alena Kuzub, "Why Diplomacy Is Needed Now to Set Rules for Outer Space," *Northeastern Global News*, 8 June 2023.