Georgia Law Review

Volume 59 | Number 1 Article 3

2024

The Sixth Warfighting Domain?: Governing the Space-Cyber Nexus

Eytan Tepper
Indiana University Bloomington/Ostrom Workshop

Scott Shackelford
Indiana University Kelley School of Business

James B. Romano
Indiana University Maurer School of Law

Sergei Dmitriachev
Indiana University Maurer School of Law

THE SIXTH WARFIGHTING DOMAIN?: GOVERNING THE SPACE-CYBER NEXUS

Eytan Tepper,[*] *Scott Shackelford,*[†] *James B. Romano*[‡] *& Sergei Dmitriachev*[§]

This Article reviews the recent emergence of the space-cyber nexus as a distinct warfighting domain, solidified during the Russian invasion of Ukraine, and analyzes the (missing?) laws of space-cyber warfare. The Article further suggests a roadmap for the development of norms and rules under the constraints of contemporary geopolitics and difficulties in multilateral rulemaking. As space-based infrastructure became critical to modern militaries and economies, it has, as a result, become a prime target. While only four countries possess antisatellite missiles (United States, Russia, China, and India), cyberattacks require much less in terms of funds and technological sophistication and can also be launched by nonstate organizations. They are powerful asymmetric weapons that allow an attacker to cover their tracks, leaving the attacked country uncertain about attribution, thus rendering retaliation and deterrence challenging. The war in Ukraine, dubbed by some as "the first space-cyber war," saw, for the first time, the targeting of space-based services as part of a military campaign. Significantly, this was achieved through cyberattacks—a telling choice given that Russia, to which the attack was attributed, also possesses antisatellite missiles. This Article suggests that current multilateral regimes are insufficient to address the new space-cyber nexus and that there is an urgent

[*] Research Professor, Space Governance & Security, and Director, Space Governance Lab, Indiana University Bloomington/Ostrom Workshop.

[†] Provost Professor of Business Law and Ethics, Indiana University Kelley School of Business; Executive Director, Ostrom Workshop; Executive Director, Center for Applied Cybersecurity Research.

[‡] J.D. Candidate, Indiana University Maurer School of Law; Ostrom Fellow; Rumsfeld Foundation Fellow.

[§] LL.M., Indiana University Maurer School of Law.

This paper is based on research supported by the Carnegie Corporation of New York.

need to develop an integrated, flexible, multilateral regime. Considering the gridlock in traditional international lawmaking and the rise of nonbinding international agreements, the Article suggests a polycentric approach to regime building. Advocated by Nobel Laureate Elinor Ostrom for commons governance, polycentric governance is increasingly used to address a diverse range of global collective action challenges. The Article thus envisions multi-track diplomacy in which multiple forums introduce a series of nonbinding international agreements that together would amount to a feasible and flexible, albeit imperfect, corpus of the laws of space-cyber warfare.

TABLE OF CONTENTS

I. INTRODUCTION

The almost frantic discussions in Washington in February 2024 over revelations alleging Russia's nuclear counter-space capabilities and possible stationing of nuclear weapons in Earth's orbit[1] underscore the new reality: the United States is reliant on space-based infrastructure, the disruption of which would cripple its military and the economy. So much so that "[t]wenty years of training and wargaming to operate without space confirms that when space support is shut off, U.S. military operations grind to a halt."[2]

The real threat, however, comes from cyberattacks on space systems.[3] Indeed, the cybersecurity of space-based infrastructure has been a major cause of concern for both practitioners and policymakers following Russia's invasion of Ukraine and the cyberattack on Viasat, a U.S. commercial space company servicing the Ukrainian government and military.[4] This prompted White House Summits and a flurry of new frameworks and standards to

---

[1] *See* Julian E. Barnes, Karoun Demirjian, Eric Schmitt & David E. Sanger, *Russia's Advances on Space-Based Nuclear Weapon Draw U.S. Concerns*, N.Y. TIMES (Feb. 14, 2024), https://www.nytimes.com/2024/02/14/us/politics/intelligence-russia-nuclear.html ("The United States has informed Congress and its allies in Europe about Russian advances on a new, space-based nuclear weapon designed to threaten America's extensive satellite network . . . . At the moment, the United States does not have the ability to counter such a weapon and defend its satellites, a former official said.").

[2] Everett C. Dolman, *Space Is a Warfighting Domain*, 1 ÆTHER: J. STRATEGIC AIRPOWER & SPACEPOWER 82, 83 (2022).

[3] *See, e.g.*, Press Release, The White House, Readout of Space Systems Cybersecurity Executive Forum Hosted by the Office of the National Cyber Director and the National Space Council (Mar. 28, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/28/readout-of-space-systems-cybersecurity-executive-forum-hosted-by-the-office-of-the-national-cyber-director-and-the-national-space-council/ [https://perma.cc/X5Q6-B9RG] ("Government officials [have] noted the need for tangible, comprehensive guidance for government and commercial space system developers and operators to measurably improve the cybersecurity of their space systems in the current threat environment.").

[4] *See* Eytan Tepper, *The First Space-Cyber War and the Need for New Regimes and Policies*, CTR. FOR INT'L GOVERNANCE INNOVATION 3 (May 2022), https://www.cigionline.org/static/documents/PB_no.173_uPqYILM.pdf [https://perma.cc/A2DH-PRJR] (discussing Russia's invasion of Ukraine and its effect on Viasat).

help address vulnerabilities before they are exploited.[5] Cyberattacks on space assets can—and have been—launched by state and nonstate actors, including terrorist organizations and criminal groups.[6] They can cause significant disruption for advanced militaries and economies, making them the perfect asymmetric weapon.[7] Such space-cyberattacks can be launched during an armed conflict or as part of espionage and "below the threshold" activities.[8] Initially, however, the threat to space systems seemed to come from antisatellite (ASAT) missiles. In 2007, for example, China performed a successful ASAT test[9] that destroyed an aging weather satellite, thereby contributing more than 35,000 pieces of space debris[10] and instantly increasing the amount of total orbital space debris by approximately 25%.[11] While the test

---

[5] *See, e.g.*, Press Release, The White House, *supra* note 3 (summarizing the forum's goals and plans to address cybersecurity challenges); Grace Dille, *ONCD Launching Cyber Roadshow Focused on Space Sector*, MERITALK (Apr. 13, 2023, 1:37 PM), https://www.meritalk.com/articles/oncd-launching-cyber-roadshow-focused-on-space-sector/ [https://perma.cc/9FVL-RQZJ] (discussing the Office of the National Cyber Director's plans to grow cybersecurity in space systems).

[6] *See* Tepper, *supra* note 4, at 1 ("[C]yberattacks are likely to become the leading method of targeting space-based infrastructure for state actors, as well as non-state actors, notably criminal organizations and terrorist groups. There is evidence that such attacks have already occurred . . . .").

[7] *See, e.g.*, *id.* at 3 (discussing various examples of cyberattacks disrupting economics and militaries).

[8] *See* Mike Stone & Joey Roulette, *SpaceX's Starlink Wins Pentagon Contract for Satellite Services to Ukraine*, REUTERS (Jun. 1, 2023, 11:56 AM), https://www.reuters.com/business/aerospace-defense/pentagon-buys-starlink-ukraine-statement-2023-06-01/ ("Russia has tried to cut off and jam internet services in Ukraine, including attempts to block Starlink in the region, though SpaceX has countered those attacks by hardening the service's software.").

[9] *See* David Kestenbaum, *Chinese Missile Destroys Satellite in 500-Mile Orbit*, NPR (Jan. 19, 2007, 4:00 PM), https://www.npr.org/2007/01/19/6923805/chinese-missile-destroys-satellite-in-500-mile-orbit [https://perma.cc/X6VD-SE42] ("The United States says China shot down one of its own aging weather satellites last week, in a kind of target practice in low Earth orbit.").

[10] Nat'l Aeronautics & Space Admin., *Chinese Anti-Satellite Test Creates Most Severe Orbital Debris Cloud in History*, 11 ORBITAL DEBRIS Q. NEWS, Apr. 2007, at 2, 2.

[11] *See* Leonard David, *Ugly Truth of Space Junk: Orbital Debris Problem to Triple by 2030*, SPACE.COM (May 9, 2011), http://www.space.com/11607-space-junk-rising-orbital-debris-levels-2030.html [https://perma.cc/MKX3-2PSC] (citing Marshall Kaplan, an orbital debris expert in the Space Department at the Johns Hopkins University Applied Physics Laboratory).

demonstrated the weapon's capacity to destroy critical U.S. military assets, it also demonstrated the dangers that this weapon poses to the attacker's own space-based infrastructure, as the growing risk from space debris endangers all satellites in orbit.[12] Moreover, an ASAT missile attack exposes the perpetrator and escalates conflicts, while cyberattacks provide plausible deniability.[13] Indeed, Russia denied responsibility for the cyberattack on Viasat and there was no direct retaliation by the United States.[14] Launching an ASAT missile and physically destroying Viasat satellites, on the other hand, would have been an escalatory move forcing the United States to retaliate.[15] It is indeed telling that Russia—the first nation to develop and successfully conduct ASAT missile tests in 1968 and the one that conducted the most recent test three months before its large-scale invasion of Ukraine[16]—chose to use a cyberattack rather than an ASAT missile. This explains and demonstrates that cyberattacks are the main counter-space mode of warfare.[17]

For years, an active debate has been playing out concerning the different domains of conflict (land, sea, air, space, and cyberspace) and the extent to which they overlap in a hyper-connected environment.[18] This Article unpacks this debate by comparing and

---

[12] *See id.* (arguing that the location of China's ASAT test was more concerning than the actual increase in debris).

[13] *See* Tepper, *supra* note 4, at 1 ("[T]he attacker can attempt to cover its tracks, leaving the attacked country uncertain about attribution and its own response.").

[14] *See generally id.* (describing Russia's involvement as "alleged").

[15] *See* Eytan Tepper, *The Laws of Space Warfare: A Tale of Non-Binding International Agreements*, 83 MD. L. REV. 458, 463 (2024) (comparing the established, binding rules of traditional warfare to the emerging, largely nonbinding rules of space warfare).

[16] OFF. OF THE TECH. ASSESSMENT, STRATEGIC DEFENSES: TWO REPORTS BY THE OFFICE OF TECHNOLOGY ASSESSMENT 96 (1986); Daryl G. Kimball, *U.S. Commits to ASAT Ban*, ARMS CONTROL ASS'N (May 2022), https://www.armscontrol.org/act/2022-05/news/us-commits-asat-ban [https://perma.cc/8EEF-B62W]; *see also* Press Statement, Antony J. Blinken, Sec'y of State, U.S. Dep't of State, Russia Conducts Destructive Anti-Satellite Missile Test (Nov. 15, 2021), https://www.state.gov/russia-conducts-destructive-anti-satellite-missile-test/ [https://perma.cc/8YHP-P8ND] (implying that Russia's "destructive," "reckless," and "irresponsible" ASAT test was *successful* due to the amount of orbital debris produced).

[17] *See* Tepper, *supra* note 4, at 1 ("The most significant current security threat to space-based infrastructure and applications is from cyberattacks."); *see also* Stone & Roulette, *supra* note 8 (anticipating that the contract between the Department of Defense and Elon Musk will combat cyberattacks on Ukraine).

[18] *See* Michael P. Kreuzer, *Cyberspace Is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age*, THE STRATEGY BRIDGE (July 8, 2021),

contrasting the emergence of space, cyberspace, and eventually the new space-cyber nexus as warfighting domains. While United Nations (UN) rhetoric in the first resolution on space consistently focused on the *peaceful* uses of space and the joint desire "to avoid the extension of present national rivalries into [space],"[19] space exploration was intertwined with defense from the beginning, becoming a warfighting domain in 2019 when NATO declared it an "operational domain."[20] Cyberspace—computers and the Internet—similarly evolved to serve defense needs and, except for a short-lived tech utopia in the 1990s, saw both criminal and military uses.[21] In 2016, cyberspace officially became a warfighting domain as well when NATO also declared it to be an "operational domain."[22] Although holding no similar official declaration, the space-cyber nexus de facto became a distinct warfighting domain with the attack on Viasat.[23]

But while a new (sixth?) warfare domain has emerged, the laws of space-cyber warfare are yet to be developed. The laws of space warfare and the laws of cyber warfare are, themselves, in the early days of development; the forums working on the laws of space warfare mention cyberthreats and those working on cyber warfare mention space activities, but the required integrated approach has

---

https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age [https://perma.cc/8HYX-9TDC] (arguing that cyberspace differs from other domains of warfare because the boundaries of cyberspace are intangible, unfixed, and "rapidly evolving").

[19] G.A. Res. 1348 (XIII), Question of the Peaceful Use of Outer Space, at 5 (Dec. 13, 1958).

[20] *See* Press Release, N. Atlantic Treaty Org., London Declaration, https://www.nato.int/cps/en/natohq/official_texts_171584.htm (July 1, 2022, 4:43 PM) ("We have declared space an operational domain for NATO, recogni[z]ing its importance in keeping us safe and tackling security challenges, while upholding international law.").

[21] *See* Kreuzer, *supra* note 18 (providing a brief overview of the Internet and computers from the 1960s through the present day).

[22] Press Release, N. Atlantic Treaty Org., London Declaration, https://www.nato.int/cps/en/natohq/official_texts_171584.htm (July 1, 2022, 4:43 PM); *see also Cyber Defence*, N. ATLANTIC TREATY ORG., https://www.nato.int/cps/en/natohq/topics_78170.htm (July 30, 2024, 4:59 PM) ("In July 2016, Allies reaffirmed NATO's defensive mandate and recognized cyberspace as a domain of operations.").

[23] *See, e.g.*, Tepper, *supra* note 4, at 3 ("[T]he head of the Russian space agency Roscosmos, said that Russia will treat any hacking of its satellites as a *casus beli*—justification for war." (citation omitted)).

yet to emerge.[24] Indeed, the "[d]evelopment of a flexible, multilateral space and cybersecurity regime is urgently required."[25] The governance gaps are playing out in real time, but geopolitics renders international lawmaking ever harder.[26]

Recent decades have seen a rise in nonbinding international agreements.[27] Considering contemporary geopolitics, nonbinding international agreements may be a good fit for the development of the laws of space-cyber warfare.[28] Significantly, these would best emerge within a polycentric system of governance.[29] Elinor Ostrom's Nobel-winning study provides strong empirical proof supporting polycentric governance of the commons and complex systems.[30] This Article suggests adopting a polycentric approach for the governance of space-cyber activities where *nonbinding* agreements and instruments would be negotiated and introduced by multiple forums, notably including off-UN forums Track Two or Track 1.5 diplomacy.[31]

---

[24] *See* Tepper, *supra* note 15, at 516 ("While the rules of sea warfare had had more than 400 years to evolve, those of space warfare have had barely several decades. They are sparce [sic] and scarce and in early stages of development.").

[25] David Livingstone & Patricia Lewis, *Space, the Final Frontier for Cybersecurity*?, ROYAL INST. INT'L AFFS. 2 (Sept. 2016), www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf [https://perma.cc/2TLW-T4XC].

[26] *See id.* ("An international 'community of the willing'—made up of able states and other critical stakeholders within the international space supply chain and insurance industry—is likely to provide the best opportunity to develop a space cybersecurity regime competent to match the range of threats.").

[27] *See* Curtis A. Bradley, Jack Goldsmith & Oona A. Hathaway, *The Rise of Nonbinding International Agreements: An Empirical, Comparative, and Normative Analysis*, 90 U. CHI. L. REV. 1281, 1284 (2023) ("In the United States, executive branch use of binding international agreements has been declining for decades. In 2005, amidst that decline, a lawyer in the State Department Legal Adviser's Office observed that nonbinding agreements had shown a 'marked increased.'" (footnotes omitted)).

[28] *See* Tepper, *supra* note 15, at 509 ("The goal of any international regulation is to be adopted and followed by as many states as possible, and if a non-binding instrument achieves this goal, it has earned its place within international law.").

[29] *See id.* at 468 ("The transition from a fairly monocentric system to a polycentric one is intertwined with the rise of non-binding instruments.").

[30] *See generally* Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641 (2010) (describing prior research on the impact of international common-pool resources systems).

[31] For an introduction to two track diplomacy, see generally William D. Davidson & Joseph V. Montville, *Foreign Policy According to Freud*, 45 FOREIGN POL'Y 145 (1981).

The following Section II reviews the emergence of space—initially reserved for peaceful uses—as a warfighting domain, the emergence of cyberspace as a warfighting domain, and eventually, the emergence of the space-cyber nexus as a warfighting domain. Then, Section III reviews the in-progress national responses to the space-cyber nexus, including the introduction of policies and standards addressing the vulnerabilities and risks. The discussion of national responses is followed by a discussion on responses at the international level. Demonstrating the urgent need to adopt an integrated multilateral regime, Section IV discusses the laws of war in the new warfare domains: space, cyberspace, and the space-cyber nexus. Section V follows suit, suggesting multi-track international lawmaking as a feasible path forward for the introduction of multilateral norms and rules for the space-cyber warfare domain. This highlights a polycentric approach with multiple partially overlapping forums (including multi-stakeholder forums) and introduces mainly nonbinding international agreements and other instruments that, in the aggregate, result in identifying consensus and norm building. Section VI concludes with the key insights of the paper.

II. THE NEW WARFARE DOMAINS: SPACE, CYBERSPACE, AND THE SPACE-CYBER NEXUS

The traditional warfighting domains—land, sea, and air—were joined in recent decades with two new domains: space and cyberspace. Most recently, the space-cyber nexus has emerged as the newest warfighting domain. Indeed, as U.S. Space Force Major General and Chief of Space Operations Mobilization John Olson noted, "[T]here is no space without cyber."[32] The space-cyber nexus, arguably the newest, cross-domain theater—or even the sixth warfighting domain itself—presents unique challenges and is already poised "to become the primary battlefield for global power

[32] *Space Force Official Discusses Why the US Is Preparing for Potential Future Conflict in Space*, ABC NEWS (Apr. 14, 2023, 4:25 PM), https://abcnews.go.com/US/space-force-official-discusses-us-preparing-potential-future/story?id=98557388 [https://perma.cc/GJ53-K5E7].

in the twenty-first century."[33] Still, an active debate is swirling about whether it should be considered a separate, unique environment, or whether cybersecurity has become so ubiquitous that it should be considered a core element of security across all the other warfare domains.

A. SPACE AS A WARFIGHTING DOMAIN

On October 4, 1957, the Soviet Union launched the first artificial earth satellite *Sputnik 1*.[34] A year later, in December 1958, the UN General Assembly (UNGA) issued its first resolution dedicated to space, in which member states recognized "the common aim that outer space should be used for peaceful purposes *only*" while wishing "to avoid the extension of present national rivalries" into space.[35] The word "peaceful" reoccurs in almost every instrument in space law, from UN resolutions to legally binding space law treaties, and appears in the title of the annual UNGA resolution dedicated to space.[36] Noble aspirations—or rhetoric—aside, space exploration was originally intertwined with defense issues and the defense establishment in most countries.[37] For example, in Russia and China, it was the military that primarily executed the space program.[38]

---

[33] Marc Boucher, *The Emerging Space Cyberwarfare Theatre*, SPACEREF (Mar. 18, 2013), https://spaceref.com/newspace-and-tech/the-emerging-space-cyberwarfare-theatre/ [https://perma.cc/9KYU-AU32].

[34] *See* TODD HARRISON, ZACK COOPER, KAITLYN JOHNSON & THOMAS G. ROBERTS, ESCALATION AND DETERRENCE IN THE SECOND SPACE AGE 2 (2017) ("The space age began on October 4, 1957 with the Soviet launch of *Sputnik 1*, the first human-made object to orbit the Earth.").

[35] G.A. Res. 1348*, supra* note 19, at 1 (emphasis added).

[36] *E.g.*, G.A. Res. 1721 (XVI), International Co-Operation in the Peaceful Uses of Outer Space (Dec. 20, 1961).

[37] *See* John M. Logsdon, *Space Exploration*, ENCYC. BRITANNICA, https://www.britannica.com/science/space-exploration [https://perma.cc/3YWB-VT3A] (Dec. 9, 2024) (describing security concerns as a motivator for nationally sponsored space travel).

[38] The "fathers" of the Russian and Chinese space programs Sergei Korolev and Qian Xuesen, respectively, were employed by the military. *See* John B. West, *Historical Aspects of the Early Soviet/Russian Manned Space Program*, 91 J. APPLIED PHYSIO. 1501, 1501 (2001) ("Sergei Pavlovich Korolev (1907–1966) was the brilliant 'Chief Designer' who was responsible for many of the Soviet firsts, including the first artificial satellite and the first human being in space."); *Qian Xuesen: The Man the U.S. Deported – Who Then Helped China*

1. Early Space Activities and Military Uses. The launch of *Sputnik 1* shocked Americans, causing widespread "fear and awe" across the United States, steering fears from the capabilities of the rival superpower and its potential use of satellites to spy on the United States or even place nuclear missiles in orbit above it.[39] Democrat Senator Henry Jackson went as far as calling *Sputnik* "a devastating blow to the United States' scientific, industrial, and technical prestige in the world."[40] *Sputnik 1* not only marked the beginning of the space age but also initiated the first space race, a prominent fixture of the Cold War competition between the United States and the Soviet Union.[41] The United States, which had already been developing its first satellite, launched *Explorer 1* soon after on January 31, 1958.[42] Later that year, Congress provided increased funding for STEM education and established NASA.[43]

The use of space for strategic purposes began in earnest under the Eisenhower Administration. On August 25, 1960, pictures of Soviet airfields were delivered to President Eisenhower after the "first successful satellite photoreconnaissance mission" from the

---

into Space, BBC (Oct. 26, 2020), https://www.bbc.com/news/stories-54695598 [https://perma.cc/XMK7-KL4X] ("Qian is the father of China's missile and space programme. His research helped develop the rockets that fired China's first satellite into space, and missiles that became part of its nuclear arsenal.").

[39] The Bryant Park Project, *Revising America's Fear of Sputnik*, NPR, at 00:11 (Oct. 4, 2007, 7:00 AM), https://www.npr.org/2007/10/04/14980366/revisiting-americas-fear-of-sputnik [https://perma.cc/22XN-3KR4] ("Sputnik was about the size of a microwave oven, but it caused fear and awe in America because it had been launched by our enemies, the Soviets."); *see also* Tony Williams, *October 4, 1957: USSR Launches Sputnik, Shocks the United States into the Space Age*, CONSTITUTING AM. (Jun 25, 2020), https://constitutingamerica.org/october-4-1957-ussr-launches-sputnik-shocks-the-united-states-into-the-space-age-guest-essayist-tony-williams [https://perma.cc/4DKZ-X7VU] ("An important part of the Cold War was the space race which became a competition between the two superpowers.").

[40] Williams, *supra* note 39. For more discussion on the *Sputnik* scare, see generally YANEK MIECZKOWSKI, EISENHOWER'S SPUTNIK MOMENT: THE RACE FOR SPACE AND WORLD PRESTIGE (2013).

[41] *See* HARRISON ET AL., *supra* note 34, at 2 ("[The Soviet launch of *Sputnik 1*] 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.").

[42] Williams, *supra* note 39.

[43] *Id.*

Corona 14.[44] While far from the space domain we know today, outer space presented important opportunities for intelligence missions targeting the Soviet Union, for U.S. strategic nuclear force targeting, and for naval fleet support.[45]

The first Soviet satellites generally had the same functions as U.S. ones. The first Soviet photo reconnaissance satellite was the *Zenit-2*.[46] Created in 1960 and successfully launched into orbit on April 26, 1962, this satellite received the official designation *Kosmos-4*.[47] The communication satellites were developed and launched later; the first of which, *Molniya-1*, was launched on April 23, 1965.[48] These helped to develop Soviet radio communication systems used for governmental and military purposes and for television broadcasting.[49] *Kosmos-192*, launched in November 1967, was the first satellite to use the Soviet satellite navigation system Tsiklon ("cyclone"), which was initially intended to assist naval communications and navigation.[50] This system was the predecessor

---

[44] BRUCE BERKOWITZ, THE NATIONAL RECONNAISSANCE OFFICE AT 50 YEARS: A BRIEF HISTORY 1 (2011).

[45] *See id.* at 2 (discussing how, due to "nonexistent" information on Soviet nuclear weapons, the United States turned to "high-altitude aircraft").

[46] *Kosmicheskiye Apparati "Zenit-2"* [*Spacecraft "Zenit-2"*], ICTOPIIA POCCIIÏCKOÏ/COBETCKOÏ KOCMOHABTIKI [HISTORY OF RUSSIAN/SOVIET COSMONAUTICS], http://space.hobby.ru/projects/zenit_2.html [https://perma.cc/99G2-HXAM].

[47] *Id.* Most Soviet and subsequently Russian military satellites were given "Kosmos" designations, from *Kosmos 1* on March 16, 1962, to the recent *Kosmos 2564*, launched on November 28, 2022; however, the focus of these satellites can be different, starting with communication and the Internet and finishing with antisatellite weapons. *See Kosmos*, ENCYC. BRITANNICA, https://www.britannica.com/technology/Kosmos-satellite [https://perma.cc/ZL82-VUMB] (Feb. 28, 2020) ("Kosmos [refers to] any of a series of uncrewed Soviet and then Russian satellites launched from the early 1960s to the present day."); *see also Zapushenniy s Plesetska Voenniy Sputnik "Kosmos-2564" Vishel na Orbitu* [*Military Satellite "Cosmos-2564" Launched from Plesetsk Space Port Settled into Orbit*], IHTEPFAKC [INTERFAX] (Nov. 28, 2022), https://www.interfax.ru/world/874573 (discussing the launch of *Kosmos-2564*).

[48] *Development of Satellite Communication*, ENCYC. BRITANNICA, https://www.britannica.com/technology/satellite-communication/Development-of-satellite-communication [https://perma.cc/Q4P6-RNMU] (Dec. 2, 2024).

[49] The Soviet television system Orbita was built using these communication satellites, and Russian officials continue using today. *E.g.*, INTERFAX, *supra* 47.

[50] *See* Boris Ivanov, *Sputnik-Predshestvennik GLONASS Vpervie Bil Zapushen Sorok Let Nazad*, [*GLONASS's Predecessor Satellite Was First Launched 40 Years Ago*], RIA NOVOSTI (June 7, 2008, 1:35 PM), https://ria.ru/20071126/89619580.html [https://perma.cc/24KJ-PV7D] (outlining the history of Russia's first navigation satellite).

of the modern GLONASS satellite navigation system.[51] The 1960s also saw the United States develop its own satellite navigation system—what would later become the Global Positioning System (GPS).[52]

2. Satellites Providing Transparency, Reducing Risks of Conflict. The Soviet Union have had satellites for purely military purposes since the early 1960s: *Polyot-1*, launched on November 1, 1963, served as the first prototype of an automatic interceptor satellite.[53] By the end of the decade, the Soviet Union had developed counterspace capabilities in the form of the earliest antisatellite weapons; it succeeded with an actual interception and destruction of a specially designed target satellite in orbit on November 1, 1968, but this capability would not be fully operational for another decade.[54]

The satellite reconnaissance capabilities that both superpowers developed became especially vital for verifying arms control and disarmament agreements by monitoring the threat of missile launches in real time, allowing both the United States and the Soviet Union to obtain much needed information on the other's nuclear postures.[55] Soviet Premier Nikita Khruschev even noted that nuclear site inspections "[could] now be assumed by

---

[51] *Id.*

[52] *See Brief History of GPS*, THE AEROSPACE CORP., https://aerospace.org/article/brief-history-gps [https://perma.cc/5KUT-XP45] (detailing the development of the satellite navigation system in the United States).

[53] *See* Anatoly Zak, *The Hidden History of the Soviet Satellite-Killer*, POPULAR MECHS. (Nov. 1, 2013, 7:32 AM), https://www.popularmechanics.com/space/satellites/a9620/the-hidden-history-of-the-soviet-satellite-killer-16108970/ [https://perma.cc/LF7B-T9A2] ("[T]his highly maneuverable spacecraft was intended to test whether the Soviets could approach an 'enemy' satellite and blow it in smithereens.").

[54] *Id.*; *see also Istoriiа Sovetskogo Voennogo Kosmosa* [*History of Soviet Military Space*], BOEHHOE OBOZPEHIE [TOP WAR] (Jan. 17, 2013), https://topwar.ru/2018-istoriya-sovetskogo-voennogo-kosmosa.html (summarizing Soviet efforts to develop military space technology between the late 1950s and early 1990s).

[55] *Cf.* JAMES WALKER, LEWIS BERNSTEIN & SHARON LANG, SEIZE THE HIGH GROUND: THE ARMY IN SPACE AND MISSILE DEFENSE 157–58 (2003) ("Space-based systems also played an important part in tactical early missile attack warning by supplying critical information on missile launches. The early warning system was based on the Defense Support Program (DSP) satellite system developed in the 1970s. . . . The original DSP system was designed to track Soviet strategic missiles that flew longer, further and had brighter infrared signatures than tactical Scud rockets.").

satellites."[56] This had a stabilizing effect during the Cold War,[57] as the ability of each power to know and verify the other's deployment of nuclear weapons prevented a scenario of escalation based on unfounded suspicion. Indeed, "[t]ransparency create[d] predictability and minimize[d] the opportunities for misunderstanding and overreaction."[58]

3. Second Wave of Military Uses of Space. U.S. Navy experiments with satellite navigation for submarine system tracking in the mid-1960s evolved to become the Global Positioning System (GPS), a "multi-use, space-based radio-navigation system" operated by the U.S. Air Force.[59]

In the 1970s and early 1980s, there were several important events in the development of military spacecraft. On June 18, 1982, Eastern bloc countries participated in a series of military games called "Shield-82," sometimes referred to as the "Seven-Hour Nuclear War."[60] Shield-82 was one of the causes for the development and deployment of the U.S. antisatellite system announced by President Ronald Reagan in July 1982, a precursor to the Strategic Defense Initiative (the SDI).[61] The SDI, nicknamed "Star Wars," was announced on March 23, 1983, with the goal of building a space-based missile defense system to intercept ballistic strategic nuclear weapons.[62] While the SDI did not lead to the deployment of the

---

[56] BERKOWITZ, *supra* note 44, at 19 (citation omitted).

[57] *See* Harrison, *supra* note 34, at 3 ("[T]he proliferation of military satellites proved to be an important stabilizing factor that helped prevent attacks in space.").

[58] PAVEL PODVIG, UNITED NATIONS INST. FOR DISARMAMENT RSCH., TRANSPARENCY IN NUCLEAR DISARMAMENT 2 (2012), https://unidir.org/sites/default/files/publication/pdfs//transparency-in-nuclear-disarmament-390.pdf [https://perma.cc/Y3AA-6AAN].

[59] Catherine Manning, *GPS*, NAT'L AERONAUTICS & SPACE ADMIN. (Sept. 25, 2023), https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html [https://perma.cc/4TPB-DNJG].

[60] Roman Azanov, *Krupneĭshie Voennye Manevry za Vsiū Istoriiū Nasheĭ Strany* [*The Largest Military Maneuvers in the Entire History of Our Country*], TASS (Sept. 11, 2018, 8:20 AM), https://tass.ru/armiya-i-opk/5550476 [https://perma.cc/F6MG-UYWD].

[61] TOP WAR, *supra* note 54.

[62] *See Strategic Defense Initiative*, ENCYC. BRITANNICA, https://www.britannica.com/topic/Strategic-Defense-Initiative [https://perma.cc/8R9K-2DBW] (Nov. 9, 2024) ("[The SDI was a] proposed U.S. strategic defensive system against potential nuclear attacks—as originally conceived, from the Soviet Union. . . . Because parts

space component of the SDI shield, much of the program's theoretical research led to advances in space warfare technologies.[63]

The SDI threatened to change the delicate balance of power between the superpowers, and the Soviet Union had to meet this challenge. In 1986, the Central Committee of the Soviet Communist Party approved a counterprogram under which Soviet scientists and engineers developed the *Polyus* spacecraft, also known as *Skif-DM*,[64] an in-orbit weapons platform and laser-equipped space station designed to destroy low earth orbit satellites with a megawatt carbon-dioxide laser.[65] Some commentators suggest that

---

of the defensive system that Reagan advocated would be based in space, the proposed system was dubbed 'Star Wars' . . . .").

[63] *See Strategic Defense Initiative (SDI)*, ATOMIC HERITAGE FOUND. (Jul. 18, 2018), https://ahf.nuclearmuseum.org/ahf/history/strategic-defense-initiative-sdi/ [https://perma.cc/8Q4U-K9JB] ("By 1985, SDIO was serving as an umbrella for the 22 think tanks and aerospace firms working on the program. . . . [S]cientists and experts considered an enormous number of possibilities. Options included both space-based and ground-based lasers, as well as a wide variety of missiles and tracking systems . . . Later on, the program focused on smaller, space-launched missiles known as 'Brilliant Pebbles.'" (citation omitted)); *see also* Dwayne A. Day & Robert Kennedy, *Barbarian in Space: The Secret Space-Laser Battle Station of the Cold* War, THE SPACE REV. (Jun. 5, 2023), https://www.thespacereview.com/article/4598/1 [https://perma.cc/BFH6-RXN5] (detailing a number of research projects initiated by the SDI).

[64] The project was initially called *Skif-D*, but due to time restraints imposed by politicians, engineers had to present a "demonstration modification" of the spacecraft; thus, the project was labeled *Skif-DM* in 1985. *Polyus*, meanwhile, was a later name for the spacecraft and was "intended for public consumption when [it] was in orbit." Day & Kennedy, *supra* note 63.

[65] *See* Konstantin Lantratov, *"Zvezdnye Voĭny," Kotorykh Ne Bylo* [*The "Star Wars" That Never Was*], NPO MOLNIYA (Jan. 2005), http://www.buran.ru/htm/str163.htm [https://perma.cc/E4W7-K7ZX] (discussing the approval and development of the Soviet counterprogram). This older development "received an apparent boost" after the U.S. SDI program was announced. Pavel Podvig, *Did Star Wars Help End the Cold War? Soviet Response to the SDI Program*, 25 SCI. & GLOB. SEC. 3, 6 (2017), https://scienceandglobalsecurity.org/archive/2017/01/did_star_wars_help_end_the_col.html [https://perma.cc/A82W-2CMY]; *see also* Day & Kennedy, *supra* note 63 ("[*Skif*] was complicated enough that by 1985 the designers knew they would need more than one launch to test its components."). *Skif* was so labor-intensive that at least seventy firms within the Soviet aerospace industry were involved in its development. *Id*. *Skif-DM* was later successfully launched in May 1987, but a small software error led the spacecraft to plunge into the Pacific Ocean. *Id*. Soon after, the fall of the USSR and the end of the Cold War led to the abandonment of this ambitious project. *See* Podvig, *supra*, at 19 ("After the breakup of the Soviet Union there is no information on progress made on the rest of the programs that were still active in 1990 . . . . It is most likely that they were terminated shortly after that.").

the SDI led to the fall of the USSR, as the former presented the latter with a technological challenge it could not meet, or because the attempted response to the SDI drained the USSR's budget to the point of collapse.[66] To the extent this argument is correct, space exploration was not just a direct result of superpower competition and military rivalry; it also had the reverse effect of deciding the U.S.–Soviet rivalry, leading to the fall of the Soviet Union.[67]

4. The First Space War and Its Aftermath. The First Gulf War in 1991 saw, for the first time, the space domain's role shift from intelligence support to conventional military operations.[68] Called the "first space war" by Air Force General Merrill McPeak, Operation Desert Storm—as the war was officially called by the United States—revolutionized the role of space in military operations.[69] As an observer in China's Academy of Military Sciences noted, "The Gulf War marked a big step forward in both military theory and practice."[70] In particular, the shift towards operational capabilities provided a new and key dimension to military uses of space. Indeed, "Desert Storm ushered in what would be called 'the new American way of war.'"[71] The use of space to augment operations in the traditional domains of land, sea, and

---

Modern Russian medium-orbit satellites are also called *Skif*, but they have nothing to do with the Soviet *Skif-D* project.

[66] *See* Podvig, *supra* note 65, at 3–4 ("[T]he SDI program made the Soviet Union realize that its economic and social system could not sustain this new technological arms race with the United States, forcing the Soviet leadership to seek concessions and eventually accept defeat.").

[67] *Id.*

[68] *See* HARRISON ET AL., *supra* note 34, at 5 ("[I]t was the first time space-based capabilities played a major role in conventional military operations . . . .").

[69] *Id.*

[70] Dean Cheng, *China's Military Role in Space*, 6 STRATEGIC STUD. Q. 55, 58 (2012).

[71] Larry Lewis & Don Boroughs, *Wrong War, Right Weapons: Lessons for the Next Conflict*, CNA: IN DEPTH (Feb. 10, 2021), https://www.cna.org/our-media/indepth/2021/02/wrong-war-right-weapons [https://perma.cc/FVS4-G4ZP]. Precision-guided munitions can also be laser-guided, but the ones often discussed, such as munitions for the High Mobility Artillery Rocket System (HIMARS) in Ukraine, use GPS guidance. *See* CONG. RSCH. SERV., IF11353, DEFENSE PRIMER: U.S. PRECISION-GUIDED MUNITIONS (Dec. 5, 2024), https://crsreports.congress.gov/product/pdf/IF/IF11353 (detailing various guided munitions); *see also* Carlotta Gall & Vladyslav Golovin, *Some U.S. Weapons Stymied by Russian Jamming in Ukraine*, N.Y. TIMES (May 25, 2024), https://www.nytimes.com/2024/05/25/world/europe/us-weapons-russia-jamming-ukraine.html (noting that HIMARS relies on GPS).

air changed perceptions of space and led to the multidomain joint force operations we experience as a hallmark of twenty-first century warfare.[72] Since the Gulf War, the percentage of U.S. munitions that were precision-guided, including those using satellite guidance systems, increased from 8% in 1991 to 60% during the 2003 Iraq War to a staggering 96% during operations in Syria in 2014.[73]

The first Gulf War marked a turning point in the history of warfare, demonstrating that the success of a military campaign has become dependent on the possession and successful operation of space-based capabilities; henceforth, the use of space for military purposes has entered the defense strategy of advanced militaries.[74] Consequently, as space-based systems became powerful tools in the hands of the U.S. military, so emerged the need of other powers either to match these capabilities or at least to counter them.[75] Antisatellite weapons, or ASAT weapons—and in particular ASAT missiles—were thus developed by Russia, China, and, most recently, India (with the United States also possessing such weapons).[76] ASAT weapons have thus become part of the defense strategies of the main powers.[77] While Russia and China are developing their own military space assets, ASAT missiles allow

---

[72] *See* HARRISON ET AL., *supra* note 34, at 8 ("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.").

[73] *Id.*

[74] *See id.* ("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. Other nations have developed counterspace capabilities to reduce or eliminate the advantages space provides for the United States.").

[75] *Id.*

[76] *See* Tepper, *supra* note 15, at 486, 486 n.170 (discussing the international development of ASAT weapons); *see also* Ashley J. Tellis, *India's ASAT Test: An Incomplete Success*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Apr. 15, 2019), https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884 [https://perma.cc/423Q-4J3U] (discussing India's endeavor to join China, Russia, and the United States in conducting ASAT tests).

[77] *See* Tepper, *supra* note 15, at 476 ("Defense institutions around the world, mainly those of the big powers, are developing strategies and tactics for warfare in the theater of space, making the question of governing these conflicts increasingly vital.").

these near-peer competitors to hedge against potentially superior U.S. space capabilities.[78]

5. Recent Developments and the Recognition of Space as a Warfighting Domain. In recent years, there have been several advancements in counterspace capabilities, including direct-ascent ASAT, co-orbital ASAT, and directed energy weapons in space.[79] Co-orbital weapons are space-based weapons—essentially a satellite with the capability to harm other satellites,[80] like Russia's *Kosmos 2543*, which was able to discharge an object from the satellite at a high velocity.[81] Another class of weapons in development are directed-energy weapons, which, unlike the other ASAT weapons mentioned, deliver destructive energy to a target without needing to deliver much mass.[82] Examples of these include electromagnetic pulse attacks (EMPs), high-powered lasers, high-powered microwaves, signal jamming, and spoofing.[83] High-powered lasers in particular can be used to overheat components or "dazzle" optical

---

[78] *See, e.g.*, Jaganath Sankaran, *Russia's Anti-Satellite Weapons: A Hedging and Offsetting Strategy to Deter Western Aerospace Forces*, 43 CONTEMP. SEC. POL'Y 436, 450 (2022) ("[T]he vast majority of Russian analysts continue to display a severe 'fear of Western technological superiority' and the possibility that a coordinate high-precision aerospace strike 'may render these defenses obsolete.' As a result, Russian military exercises are now designed to repel massive strikes by hypersonic weapons and short- and medium-range cruise and ballistic missiles . . . ." (citations omitted)).

[79] *See generally* SECURE WORLD FOUND., GLOBAL COUNTERSPACE CAPABILITIES: AN OPEN SOURCE ASSESSMENT (Brian Weeden & Victoria Samson eds., 2018), https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf [https://perma.cc/852C-PD3G] (compiling and assessing available information on the counterspace capabilities developed by multiple countries).

[80] *See id.* at xviii (defining co-orbital weapons).

[81] *See, e.g.*, Theresa Hitchens, *Russian Sat Spits Out High-Speed Object in Likely ASAT Test*, BREAKING DEF. (Jul. 23, 2020, 4:34 PM), https://breakingdefense.com/2020/07/russian-sat-spits-out-high-speed-object-in-likely-asat-test/ [https://perma.cc/K89V-WW32] (reporting on Russia's testing of its *Kosmos 2543* satellite).

[82] *See* BOB PRESTON, DANA J. JOHNSON, SEAN J.A. EDWARDS, MICHAEL MILLER & CALVIN SHIPBAUGH, RAND, SPACE WEAPONS EARTH WARS xvi (2002) (comparing directed-energy weapons to other ASAT weapons).

[83] *See, e.g.*, Tyler Way, *Counterspace Weapons 101*, AEROSPACE SEC. PROJECT: AEROSPACE 101, https://aerospace.csis.org/aerospace101/counterspace-weapons-101/ [https://perma.cc/6UTV-AZFP] (June 14, 2022) (describing various counterspace weapons).

sensors, as was the case with a U.S. satellite that was temporarily "blinded" when it passed over China in 2006.[84]

The evolution of military uses of space, as well as counterspace capabilities, has reached a turning point where space, once reserved for peaceful uses, has become a warfighting domain.[85] In 2015, Russia established a Space Force as a separate branch of armed forces.[86] Four years later, the United States established the Space Force as the sixth branch of the U.S. military[87] and officially declared space a warfighting domain,[88] as did NATO[89] and China.[90] In 2021, Russia declared that a rival country's stationing of weapons in space would constitute a grave military threat,[91] and in August

---

[84] *Id.*; *see also* Matthew Mowthorpe & Markos Trichas, *A Review of Chinese Counterspace Activities*, THE SPACE REV. (Aug. 1, 2022), https://www.thespacereview.com/article/4431/1 [https://perma.cc/2ABB-4P37] (reviewing Chinese counterspace activities and referencing the 2006 incident).

[85] *See* Tepper, *supra* note 15, at 463 ("In a span of a little more than two years, from NATO's December 2019 announcement to the war in Ukraine, space . . . has been re-imagined as a war zone." (footnote omitted)).

[86] Vladimir Motorin, *Zvezdnaiа Voĭna: Kak Kosmos Stanovĭtsiа Novoĭ Arenoĭ Dliа Protivostoiӑniiа Rossii i SSHA* [*Star Wars: How Space Is Becoming a New Arena for Confrontation Between Russia and the United States*], FORBES (July 24, 2020), https://www.forbes.ru/obshchestvo/405681-zvezdnaya-voyna-kak-kosmos-stanovitsya-novoy-arenoy-dlya-protivostoyaniya-rossii [https://perma.cc/VA99-KQDS]; *see also* Franz-Stefan Gady, *Russia Creates Powerful New Military Branch to Counter NATO*, THE DIPLOMAT (Aug. 7, 2015), https://thediplomat.com/2015/08/russia-creates-powerful-new-military-branch-to-counter-nato/ [https://perma.cc/YY9E-XD86] ("The new service branch, officially called the Aerospace Forces of the Armed Forces of the Russian Federation, became operational on August 1, according to Russian Defense Minister Sergey Shoigu.").

[87] 10 U.S.C. § 9081.

[88] The National Space Policy, 85 Fed. Reg. 81755, 81769 (Dec. 16, 2020).

[89] *See NATO's Approach to Space*, N. ATLANTIC TREATY ORG., https://www.nato.int/cps/en/natohq/topics_175419.htm (Mar. 21, 2024, 3:11 PM) ("In 2019, Allies adopted a new Space Policy and declared space an operational domain.").

[90] STATE COUNCIL INFO. OFF. OF THE PEOPLE'S REPUBLIC OF CHINA, CHINA'S NATIONAL DEFENSE IN THE NEW ERA (2019), https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html [https://perma.cc/9SXP-UB49].

[91] ELEKTRONNYĬ SPRAVOCHNIK RUKOVODITELIĂ PO VOENNO-PATRIOTICHESKOMU VOSPITANIIŬ [ELECTRONIC HANDBOOK OF THE HEAD OF MILITARY-PATRIOTIC EDUCATION] 90–91 art. 11 (2023), https://adu.by/images/2023/03/spravochnik_ruk_VPV.pdf [https://perma.cc/E72D-LSZ6].

2022, the U.S. Department of Defense issued a new space policy.[92] Thus, the scene was set for conflicts in or involving space.

B. CYBERSPACE AS A WARFIGHTING DOMAIN

1. Computers and the Internet Developed for Military Purposes. Besides a short tech utopia during the 1990s, the history of computing has been intertwined with military history since the inception of the first computer. In 1943, British mathematician Alan Turing developed the first computer—the Colossus—to perform the intensive calculations needed for ballistics and cryptography during WWII; it was also famously used to decode messages from the German Enigma cipher machine.[93] Three years later, the United States unveiled the Electronic Numerical Integrator and Calculator (ENIAC), the first modern "general purpose, electronic digital computer," developed to calculate artillery firing tables for the U.S. Army's Ballistic Research Laboratory.[94] From the 1940s to 1960s, "the armed forces of the United States [would become] the single most important driver of digital computer development."[95] In conjunction with commercial firms, universities, and military research organizations, the U.S. military was the proving ground for prototype computer machines,[96] such as IBM's SAGE (Semi-Automatic Ground Environment) in the

---

[92] U.S. DEP'T OF DEF., DOD DIRECTIVE 3100.10: SPACE POLICY (Aug. 30, 2022), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/310010p.pdf [https://perma.cc/RW6F-YMGJ].

[93] *See* PAUL N. EDWARDS, THE CLOSED WORLD: COMPUTERS AND THE POLITICS OF DISCOURSE IN COLD WAR AMERICA 17 (1996) (describing Alan Turing's contributions towards computing and the war effort); *see also* Raymond R. Hill & Andreas Tolk, *A History of Military Computer Simulation*, *in* ADVANCES IN MODELING AND SIMULATION 277, 280 (Andreas Tolk, John Fowler, Guodong Shao & Enver Yücesan eds., 2017) ("It was the intense calculations associated with military system engineering and analysis that really raised interest in mechanical computing calculators. Areas such as ballistics and crypto-analysis, which had required many hours of manual calculations, could be done in seconds when using the automated device.").

[94] William T. Moye, *ENIAC: The Army-Sponsored Revolution*, U.S. ARMY RSCH. LAB'Y (Jan. 1996), https://ftp.arl.army.mil/~mike/comphist/96summary/ [https://perma.cc/W667-L492].

[95] EDWARDS, *supra* note 93, at 43.

[96] *Id.*

1950s. Used for the air defense system,[97] SAGE was "spun-off" into the commercial market and contributed to the commercial rise of IBM in the computer world.[98] With the later development of the transistor, computers could be small enough for use on U.S. Navy ships.[99] The Soviet Union tried to keep up, and Soviet scientists worked to copy U.S. technology, with the main use being for military purposes—mainly nuclear weapons, ballistic missiles, and antimissile defense.[100] To stem the flow of computer technologies to Soviet bloc countries, the United States worked with the U.K. and Japan to embargo Eastern Europe and China.[101]

The Internet was likewise a product of defense spending and R&D. During the Cold War, the United States sought to maintain operational command-and-control even in the event of a Soviet preemptive strike.[102] The solution was distributed networks.[103] A project of the U.S. Advanced Research Projects Agency (ARPA), the predecessor of DARPA,[104] resulted in the introduction of ARPANET

---

[97] *See SAGE*, IBM: IBM HERITAGE, https://www.ibm.com/history/sage [https://perma.cc/GK9Q-K64X] ("When the Soviet Union detonated the first atomic bomb, in 1949, it triggered the US government to call on [MIT] to create a real-time, state-of-the-art defense system covering the entirety of North America.")

[98] *Id.*

[99] George Gray & Ron Smith, *Sperry Rand's Transistor Computers*, 20 IEEE ANNALS HIST. COMPUTING 16, 19 (1998).

[100] *See* Slava Gerovitch, *'Mathematical Machines' of the Cold War: Soviet Computing, American Cybernetics and Ideological Disputes in the Early 1950s*, 31 SOC. STUD. SCI. 253, 256 (2001) ("The high demands placed on Soviet computing by the three top-priority defence programmes—nuclear weapons, ballistic missiles, and anti-missile defence—left little room for civilian applications.").

[101] *See* Frank Cain, *Computers and the Cold War: United States Restrictions on the Export of Computers to the Soviet Union and Communist China*, 40 J. CONTEMP. HIST. 131, 132–133 (2005) (describing congressional efforts to restrict the export of computers).

[102] *See* John Naughton, *The Evolution of the Internet: From Military Experiment to General Purpose Technology*, 1 J. CYBER POL'Y 5, 7 (2016) ("[T]he doctrine [of mutual assured destruction] could give an advantage to the aggressor if his pre-emptive strike was so devastating that it rendered the enemy's command-and-control system inoperative, thereby making it impossible to retaliate. There was therefore an urgent need to design a communications system capable of surviving a devastating thermonuclear attack.").

[103] *See id.* at 7–8 (The problem was that [machines that could deter foreign attacks] were incompatible with one another, and therefore could not function as shared resources . . . . From this came the idea, and the funding, for a network that would enable these valuable resources to be shared.").

[104] *See Innovation Timeline*, DEF. ADVANCED RSCH. PROJECTS AGENCY, https://www.darpa.mil/about/innovation-timeline [https://perma.cc/3KML-2RR9] ("The

in 1972, the precursor to the modern Internet.[105] In 1983, MILNET was split from ARPANET to create separate civilian and military networks.[106] During the 1990s the Internet was gradually opened to universities, commercial companies, the public, and eventually the world, creating the World Wide Web (WWW).[107]

2. The Tech Utopia. There was a short-lived tech utopia of the internet.[108] The opening of the Internet to everyone and everywhere in the world coincided with the new spirit of the 1990s: the backdrop of the fall of the Soviet Union, the end of the Cold War, the fall of the Berlin Wall, the spread of democracy in eastern Europe and elsewhere, and globalization. It was a time of optimism captured by Francis Fukuyama's declaration of the "end of history."[109] This was indeed the perfect background for a tech utopia. A strong community of tech people promoted a vision of a free Internet, and many scholars of the medium saw a lawless, open space, beyond the control of state authority. There were hopes that the Internet could be policed by its own users and that new, dynamic regimes of conduct would evolve with the technology. This tech utopia manifested in John Barlow's classic *Declaration of the Independence of Cyberspace*:

Advanced Research Projects Agency (ARPA) gained a 'D' when it was renamed the Defense Advanced Research Projects Agency (DARPA) in 1972. The Agency's name briefly reverted to ARPA in 1993, only to have the 'D' restored in 1996.").

[105] *See* Naughton, *supra* note 102, at 8–9 (explaining ARPANET's completion and its impact on the modern Internet).

[106] *See id.* at 10 ("[C]oncern about the security of the network had led to a decision to split [ARPANET] into civilian and military domains. From October 1982, one domain—the ARPANET—would continue as a research enterprise; the other—labelled MILNET—would henceforth be entirely devoted to military communications. The switchover was implemented in April 1983.").

[107] *See id.* at 11–12 (outlining the Internet's transition from heavily restricted, military technology to a publicly accessible resource).

[108] *See* Matt Novak, *Tech Nerds Who Predicted an Internet Utopia Are Sorry for Being So Wrong*, GIZMODO (Dec. 26, 2017), https://gizmodo.com/tech-nerds-who-predicted-an-internet-utopia-are-sorry-f-1821585477 [https://perma.cc/DE4R-6JKY] ("You probably remember those tantalizing tech predictions from the 1990s. The world wide web was going to become a paradise for access to information and civil discourse. The internet would allow people of different cultures to come together and learn from each other.").

[109] FRANCIS FUKUYAMA, THE END OF HISTORY AND THE LAST MAN (1992).

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[110]

3. Cybercrime, Cyber Warfare, and the Rise of Cybersecurity. Despite and alongside the tech utopia, the Internet was used, even during the 1990s, for defense *and* cybercrime, including for human trafficking.[111] Indeed, cybercrime is so prevalent and harmful that the World Economic Forum ranked it as one of the top ten risks facing the world in the coming decade in its 2023 Global Risk report.[112] The focus herein is nevertheless on cyberattacks, the history of which goes back to the 1980s[113]: Hacking and cyberattacks intensified during and after the 1990s Internet boom (and bubble), reached new heights in the 2000s, and has exploded since the 2010s, both for military purposes and, by 2018, as a $1.5 trillion industry, surpassing even the size of the illegal drug trade.[114] The 1980s also saw the rise of hackers and a greater concern for cybersecurity in the cultural zeitgeist and in government networks.

---

[110] John P. Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/W3A9-M2QW].

[111] *See, e.g.*, *Technology Facilitating Trafficking in Persons*, UNITED NATIONS OFF. ON DRUGS AND CRIME (May 2019), https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html [https://perma.cc/F82A-J75H] ("Technology and the Internet—both cybercrime tools—are harnessed by the sophisticated end of the trafficker spectrum. They can use these tools at each stage of the process, from the identification and recruitment of potential victims, through the process of coercion and control, to advertising and selling goods and services produced from their exploitation and finally to the laundering of profits.").

[112] *See* WORLD ECON. F., THE GLOBAL RISKS REPORT 2023: INSIGHT REPORT 6 fig.A (18th ed. 2023), https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf [https://perma.cc/4GFG-AYJV] (ranking "widespread cybercrime and cyber insecurity" as the eighth most severe risk the world faces in the next ten years).

[113] *See generally* Hilarie Orman, *The Morris Worm: A Fifteen-Year Perspective*, 1 IEEE SEC. & PRIV. 35 (2003) (discussing the "first worm to hit the Internet" in 1988).

[114] Press Release, Delegates Call for Global Instrument to Curb Cybercrime, as Third Committee Discusses Crime, Communications Technologies and Drugs, U.N. Press Release GA/SHS/4344 (Oct. 3, 2022), https://press.un.org/en/2022/gashc4344.doc.htm [https://perma.cc/A432-HGKP]; *Spending on Illegal Drugs*, WORLDOMETER, https://www.worldometers.info/drugs/ [https://perma.cc/ZWW7-2WZC].

The popular 1983 film *WarGames* depicted a teenager accidentally hacking into the North American Aerospace Defense Command (NORAD) computer system, thinking it was a game, and nearly starting WWIII.[115] Among the many viewers of the film was U.S. President Ronald Reagan, who brought together leaders from the Executive and Legislative branches to study the issue.[116] At the meeting, Reagan asked General John Vessey, the Chairman of the Joint Chiefs of Staff, if something like that in the film could happen.[117] Vessey responded, "Mr. President, the problem is much worse than you think."[118] Soon, the 1986 Cuckoo's Egg hack, the first significant cyber espionage attack, saw an infiltration of U.S. research and military computers by East German hackers with handlers from the Soviet KGB.[119] The 1988 Morris Worm hack, which started as a prank by a Cornell student, ended up infecting 10% of the Internet at the time.[120] It served as a wakeup call for the U.S. intelligence community, which began to address the security issues presented by hackers.[121] The hack even prompted DARPA to create the Computer Emergency Response Team (CERT), designed to provide solutions for cyberattacks.[122]

The 1990s witnessed an increase in the volume and complexity of cyberattacks on military assets; the Department of Defense

---

[115] *See* Charles Kaiser, *Dark Territory Review – How* WarGames *and Reagan Shaped US Cyberwar Battle*, THE GUARDIAN (Mar. 20, 2016, 9:58 AM), https://www.theguardian.com/technology/2016/mar/20/dark-territory-review-ronald-reagan-matthew-broderick-war-games-american-cyberwar [https://perma.cc/KME7-FMRZ] (describing the plot of *WarGames*).

[116] *See id.* (describing Reagan's fascination with the film and concern over the realistic possibility of such a plot).

[117] *Id.*

[118] *Id.*

[119] *See* Omry Haizler, *The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking*, 1 CYBER, INTEL., & SEC. 31, 33 (2017) (comparing the 1986 Cuckoo's Egg attack to the Morris Worm); *see also* CLIFF STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE 366–67 (1990) (discussing the KGB's involvement with the hack).

[120] Haizler, *supra* note 119, at 33.

[121] *See id.* ("The Morris Worm acted as a catalyzer for the first steps towards a more regulated cyberspace and led to dramatic changes, both conceptually and operationally.").

[122] *Id.*

sustained as many as 250,000 cyberattacks in 1995 alone.[123] The 1998 Moonlight Maze hack[124] saw the infiltration of computer networks of the Pentagon, NASA, and the Department of Energy.[125] The hack also raised the attribution issue presented by cyberattacks[126]: while the hack was traced to the Russian Federation, its officials did not take responsibility for it. That same year, in another "hack for fun," an 18-year-old Israeli named Ehud Tenenbaum (known as "the Analyzer") hacked NASA, the Pentagon, the U.S. Air Force and Navy, MIT, and the Israeli Parliament in what was described as "the most organized and systematic attack to date" on U.S. military systems.[127] This demonstrated the potential of cyberattacks as asymmetric warfare because they could be launched using very limited means.

The attribution problem would become even more relevant in the 2000s and 2010s. Entire countries experienced significant cyberattacks with disparate origins, including: Estonia in 2007,[128] Georgia in 2008,[129] Iran in 2009,[130] and Tunisia in 2011.[131] For

---

[123] U.S. GOV'T ACCOUNTABILITY OFF., GAO/AIMD-96-84, INFORMATION SECURITY: COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS 2 (1996).

[124] In 2017, a connection was proven between the Moonlight Maze hack and the Russian-language threat actor TURLA, well known for its method of hijacking satellite links to disguise itself—demonstrating that hacking spacecraft could be understood as a next stage development into using more sophisticated methods to risk global peace. *See Moonlight Maze Lives On? Researchers Find 20-Year-Old Link to Current APT*, SECUREWORLD (Apr. 3, 2017, 3:08 PM), https://www.secureworld.io/industry-news/moonlight-maze-lives-on-researchers-find-link-to-current-apt [https://perma.cc/4BR7-P6X2]; *see also* Stefan Tanase, *Satellite Turla: APT Command and Control in the Sky*, KASPERSKY: SECURELIST (Sep. 9, 2015), https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/ [https://perma.cc/6KJ4-MPLC].

[125] Haizler, *supra* note 119, at 34.

[126] *See id.* ("[The Moonlight Maze hack] emphasized the crucial need for firewalls and encryptions and, above all, the difficulties of identifying and *attributing* an attack to a specific adversary." (emphasis added)).

[127] Kim Zetter, *"The Analyzer" Released on Bail; Mom Says FBI Out to Get Her Son*, WIRED (Sep. 29, 2008, 2:57 PM), https://www.wired.com/2008/09/the-analyzer-re/.

[128] Chris McGuffin & Paul Mitchell, *On Domains: Cyber and the Practice of Warfare*, 69 INT'L J. 394, 396 (2014).

[129] *Id.*

[130] *Id.*

[131] Evan Hill, *Hackers Hit Tunisian Websites*, AL JAZEERA (Jan. 3, 2011), https://www.aljazeera.com/news/2011/1/3/hackers-hit-tunisian-websites [https://perma.cc/APS6-29QV].

example, after the 2007 Distributed Denial of Service (DDoS) cyberattacks in Estonia, some observers from NATO noted how the difficulty in attribution hindered both future prosecution and discovery of a state sponsor.[132] Perhaps one of the best examples of the difficulties of attribution of cyberattacks is the 2010 Stuxnet attack. While many observers claim that the Stuxnet attack was a joint Israeli–U.S. operation, the origins of the attack are still unconfirmed.[133] The Stuxnet attack was one of the most sophisticated cyberattacks ever recorded, physically damaging Iranian centrifuges and hindering its uranium enrichment efforts.[134] The Stuxnet attack further proved that cyberattacks could be just as effective as conventional weapons, being able to inflict physical damage—with the added benefit of obscured attribution.

4. The Recognition of Cyberspace as a Warfighting Domain. The late 2000s and early 2010s saw more complex cyberattacks and the recognition of cyberspace as a warfighting domain. In 2009 alone, the U.S. military established the Cyber Command,[135] China's People's Liberation Army established its Cyber Centre,[136] and Russia was formulating its plan for permanent cyber military units.[137] A year later, the U.S. Department of Defense published its Strategy for Operating in Cyberspace, declaring that "[a]lthough it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[138] That same year, Russia published its strategy for

---

[132] *See* James Pamment et al., *Hybrid Threats: 2007 Cyber Attacks on Estonia*, NATO STRATCOM COE (June 6, 2019), https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86 [https://perma.cc/VJH2-DQ74] (select "read online" to access PDF) ("[The attack] underscores the requirement for governments to achieve political consensus on attribution in a timely manner based on the available evidence and be able to communicate this in a clear and understandable way to the general public.").

[133] Haizler, *supra* note 119, at 35–36.

[134] *Id.* at 36.

[135] McGuffin & Mitchell, *supra* note 128, at 407.

[136] *Id.* at 397.

[137] *See generally* DANIIL TUROVSKĬ, VTORZHENIE: KRATKAIĀ ISTORIIĀ RUSSKIKH KHAKEROV [INVASION: A BRIEF HISTORY OF RUSSIAN HACKERS] (2019) (describing the development of Russian cyber strategy).

[138] U.S. DEPT. OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011) (citation omitted),

military cyber operations.[139] While declaring that Russian Military Forces must obey the principle of noninterference of internal affairs of foreign countries,[140] the strategy preserves the right to deploy cyber forces in the territory of other states to provide a response to "informational threats" (i.e., cyber threats).[141] Moreover, while the document does not specify the measures that the Russian Military Forces can use to respond to cyber threats, it may be interpreted to allow responding to a threat in virtual space with traditional warfare methods.[142]

In 2013, General Valery Gerasimov, appointed a year earlier as the Chief of the General Staff of the Russian Armed Forces, published a report building on the previous Conceptual Views report.[143] This report described the concept of hybrid war with the use of cyber forces for subversive activities to prepare the battlefield before an intervention.[144] Where Conceptual Views discussed the use of cyber forces for self-*defense*, this new report discussed *offensive* usage of cyber operations. Moreover, General Gerasimov continued to head the Russian military in 2022 and was one of the key planners of the full-scale invasion of Ukraine.[145] He was also

---

https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [https://perma.cc/5GNB-MDKY].

[139] MINISTERSTVO OBORONY ROSSIĬSKOĬ FEDERATSII [MINISTRY OF DEFENSE OF THE RUSSIAN FEDERATION], KONTSEPTUALNYE VZGLIĀDY NA DEIĀTELVNOSTV VOORUZHENNYKH SIL ROSSIĬSKOĬ FEDERATSII V ĬNFORMATSIONNOM PROSTRANSTVE [CONCEPTUAL VIEWS ON THE ACTIVITIES OF RUSSIAN MILITARY FORCES IN INFORMATIONAL SPACE] (2011) https://nsarchive.gwu.edu/document/29297-32-conceptual-views-activities-military-forces-russian-federation-informatio [https://perma.cc/DF6Y-86N2].

[140] *Id.* § 2.1.

[141] *Id.* §§ 3.1.2, 3.2.5. However, note that Russian legislation uses more vague terms like "informational threats"—as opposed to "cyber threats."

[142] *See id.* § 3.2.3 (stating that Russia reserved the right to traditional self-defense measures that did not violate general international law).

[143] Valery Gerasimov, *Tsennostv Nauki v Predvidenii* [*The Value of Science Is in Foresight*], VPK (Feb. 27, 2013), https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html [https://perma.cc/VFH7-WYWD].

[144] *See id.* (discussing the use of technology and cyber warfare against enemy combatants abroad).

[145] *See* Paul Kirby, *Ukraine Conflict: Who's in Putin's Inner Circle and Running the War?*, BBC (June 24, 2023), https://www.bbc.com/news/world-europe-60573261 [https://perma.cc/22E3-ZQ4R] ("As chief of staff, it was [Gerasimov's] job to invade Ukraine and complete the job fast . . . .").

later appointed overall commander of the war.[146] As the next section elaborates, this war was the first to feature cyberattacks on space assets as part of a military campaign.

But as Russia developed its cyber warfare capabilities, so did NATO. The 2014 NATO Wales Summit Declaration signaled that cyberattacks could trigger Article 5 of the NATO Treaty, which would trigger member states' obligations to defend fellow members,[147] and by 2016, NATO declared cyberspace a new operational domain.[148] All in all, between 2010 and 2016, cyberspace has become a warfighting domain for the superpowers.

C. THE SPACE-CYBER NEXUS AS A WARFIGHTING DOMAIN

1. The Motivation: Space Assets as a Prime Target and the Superiority of Cyberattacks. The wartime superiority that space assets provide makes them a prime target for an adversary. Indeed, Russian military scholars recognize that "high-precision aerospace weapon[s] supported by satellite-enabled data [have] become indispensable to the American way of war"—an observation that has driven their own development of ASAT weapons and the development of counterspace weapons more generally.[149] Moreover, space-based infrastructure has become critical infrastructure for the economy and many aspects of everyday life, thereby making it a

---

[146] *Id.*

[147] *See generally* Michaela Prucková, *Cyber Attacks and Article 5 – A Note on a Blurry but Consistent Position of NATO*, THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE (2022), https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/ [https://perma.cc/CY5T-ZZ54] (explaining the responsibilities under Article 5 of NATO's founding document should cyberattacks occur against a NATO member state).

[148] *See id.* ("At the next NATO summit in 2016, the Allies went even further by declaring cyberspace a new operational domain, taking its place alongside air, land and sea.").

[149] *See* Sankaran, *supra* note 78, at 447, 449 (suggesting that Russia's development of aerospace weaponry "will 'deter aggression' by the US and its allies 'reliant upon space' to execute such military campaigns").

prime target for adversaries.[150] Indeed, disturbances and disorder of space systems can ultimately lead to chaos on Earth.[151]

ASAT missiles are a proven counterspace weapon, but there is a high financial and technological barrier for achieving them.[152] Indeed, only four countries have done so to date: Russia, the United States, China, and India.[153] A cyberattack targeting space systems, on the other hand, has a much lower financial and technological barrier and is therefore superior as it enables even smaller, less equipped actors—including terrorist organizations and criminal groups—to target space assets.[154] The space domain maintained relative stability because of "limited accessibility, attributable norms, and environmental interdependence."[155] But cyberattacks on space systems potentially counteract these stabilizing factors because they are less technologically intensive than traditional ASAT missiles, obscure attribution better than traditional ASAT missiles, and have less of a risk of affecting the space assets of the attacker, especially if the attacker is a nonstate actor.[156] Specifically, the use of ASAT missiles exponentially increases space debris, thus risking countries that would launch such missiles.[157]

---

[150] *See* David Neuman, *Cybersecurity in the Space Domain: Safeguarding Our Future*, *in* TAG 2023 SECURITY ANNUAL: SPECIAL REPORT EDITION 12, 14 (2023) (describing the overlap of everyday society and the space domain, the impact that a space attack would have on day-to-day operations, and the need for protecting space-based assets from attack).

[151] *See id.* ("The repercussions such an event could have on society and businesses worldwide, from disrupting air travel and telecommunications to causing catastrophic power failures and affecting financial markets, are alarming.").

[152] *See* James Pavur & Ivan Martinovic, *The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space*, *in* 2019 11TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: SILENT BATTLE 213, 216 (2019) ("[A] launch programme alone does not guarantee the resources and precision required to operate a meaningful ASAT capability. . . . Limited access to orbit [also] necessarily reduces the scenarios which could plausibly escalate to ASAT usage.").

[153] *See* Tepper, *supra* note 15, at 486 ("ASATs are a conventional way to destroy satellites in orbit and so far have been successfully tested by Russia, the United States, China, and India.").

[154] *See id.* at 493 ("Cyber-attacks have a low barrier to entry, and offense is cheaper than defense, which makes them available to states that are not top space powers and even non-state actors like criminal organizations and terrorist groups.").

[155] Pavur & Martinovic, *supra* note 152, at 215.

[156] *See id.* at 217–18 (discussing the widespread accessibility, low risk of attribution, and lower risk of collateral damage of cyberattacks as threats to stability in space).

[157] *Cf.* Donald J. Kessler, Nicholas L. Johnson, J.C. Liou & Mark Matney, *The Kessler Syndrome: Implications to Future Space Operations*, 137 ADVANCES ASTRONAUTICAL SCIS. 47,

ASAT missile attacks are also highly visible, escalatory, and likely to lead to retaliation.[158] Conversely, in the case of a cyberattack, the perpetrator can attempt to cover its tracks and deny responsibility,[159] and a cyberattack is not distinctly escalatory and may not lead to retaliation.[160]

This is not merely conjecture. As noted herein, Russia did not take responsibility for the cyberattack on Viasat on the eve of its invasion to Ukraine, and although the United States attributed responsibility to Russia, it did not retaliate directly;[161] otherwise, if Russia had launched an ASAT missile that destroyed one of Viasat's satellites, one could assume the United States would have been compelled to retaliate. Furthermore, cyberattacks are easier to launch, can target even remote satellites, and can attack multiple space assets in a shorter period of time than with ASAT missiles.[162] For these reasons, space cyberattacks will be the primary mode of space warfare. As the next section demonstrates, space systems are especially vulnerable to such cyberattacks.

---

60 (2010) ("A more focused collision avoidance capability may help, but without adherence to current guidelines and an active debris removal program, future spacecraft operators will face an increasing orbital debris population that will increasingly limit spacecraft lifetimes.").

[158] *See* Pavur & Martinovic, *supra* note 152, at 216–17 ("For kinetic ASAT technology, plausible deniability and stealth are essentially impossible. The literally explosive act of launching a rocket cannot evade detection and, if used offensively, retaliation.").

[159] *See id.* at 218 ("[F]ew on either side would contend that cyber attacks are as attributable as the launch of an orbital rocket from sovereign territory. A kinetic ASAT would be noticed and credibly attributed within minutes, but the average data breach evades detection for 200 days, even for critical systems.").

[160] *See id.* ("[C]yber attacks have low risk of attribution and, by extension, low risk of retaliation . . . .").

[161] *See* James Pearson, *Russia Downed Satellite Internet in Ukraine – Western Officials*, REUTERS (May 10, 2022, 11:16 PM), https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/ ("Russia routinely denies it carries out offensive cyber operations.").

[162] *See* RAJESWARI PILLAI RAJAGOPALAN, U.N. INST. FOR DISARMAMENT RSCH., SPACE DOSSIER 3: ELECTRONIC AND CYBER WARFARE IN OUTER SPACE 9 (2019) ("[A cyber attack] can be developed and deployed much faster than an ASAT and is much cheaper. . . . The more satellites are linked to cyber nodes, the more vulnerable these are to cyber attacks. There are several points of intrusion for an attacker, including the landlines that link ground stations to terrestrial networks, user terminals that link satellites, and antennas on satellites and ground stations.").

2. The Heightened Cyber Vulnerabilities of Space Systems. Cyberattacks on space systems[163] present new and evolving challenges. As noted by David Fidler, "The tasks of securing outer space and cyberspace are converging. The internet increasingly depends on space-enabled communication and information services. Likewise, the operation of satellites and other space assets relies on internet-based networks . . . ."[164] The different challenges presented by space systems and other complex computer systems thus lies in the nature of spacecraft and their auxiliary systems.[165] First, space systems are "systems of systems" presenting several attack vectors; each space system has at least three structural components that are vulnerable to attack: the space segment (the spacecraft itself, e.g., a satellite), the ground segment (or a ground control system on Earth), and the information transmission systems that connect the previous two.[166] Each structural component at each stage of its lifecycle contains different procedures, hardware, and software that could have their own vulnerabilities for future cyberattack.[167]

Furthermore, space systems have, in addition to the general cyber vulnerabilities, unique and heightened vulnerabilities. Space-specific cyber challenges include limited processing power due to energy (e.g., relying on solar panels), which mandates the prioritization of essential operations while minimizing resource

---

[163] Space systems are defined in different ways, for example: "[V]ehicles and infrastructure working together to perform a task in the space environment. We depend on space systems every day for communication, navigation, and weather prediction services." *Space Systems*, UNIV. ILL. URBANA-CHAMPAIGN, https://aerospace.illinois.edu/research/research-areas/space-systems [https://perma.cc/5SDU-WE33].

[164] David P. Fidler, *Cybersecurity and the New Era of Space Activities*, COUNCIL ON FOREIGN RELS. (Apr. 2018), https://www.cfr.org/report/cybersecurity-and-new-era-space-activities [https://perma.cc/YA5Q-VRY6].

[165] *See* Vijay Varadharajan & Neeraj Suri, *Security Challenges when Space Merges with Cyberspace*, 67 SPACE POL'Y 1, 2 (2024), https://www.sciencedirect.com/science/article/pii/S026596462300067X ("From an operational perspective, the space environment presents certain unique challenges leading to situations which few consumer hardware systems will encounter.").

[166] *See id.* at 1 (describing the "three technological and operational segments" of space systems).

[167] *See id.* at 2 tbl.1 (providing a summary of "threats and vulnerabilities" to the different segments of space systems).

consumption.[168] This results in security mechanisms such as authentication, access controls, encryption, or intrusion detection systems that are weak or absent.[169] Due to the constraints on fuel and charging capabilities in space, software designed for space systems must also be optimized to consume minimal energy.[170] As a result, processors and software used in space missions are often weaker compared to those found in modern smartphones or computers.[171] This inherent limitation in processing power therefore raises concerns about the level of protection provided by such systems,[172] as the nature of spacecraft components and their location in space limit the ability to maintain, replace, or upgrade individual parts.[173] Moreover, the link between the ground segment

---

[168] *See* Abebe Diro et al., *Anomaly Detection for Space Information Networks: A Survey of Challenges, Techniques, and Future Directions*, 139 COMPUTS. & SEC. 1, 3 (2024) ("Space systems often operate under stringent resource constraints, including limited power, processing capabilities, and memory. Implementing sophisticated security measures can be challenging when they significantly impact system performance.").

[169] *See id.* at 7 ("Governments, space agencies, and cybersecurity experts must work together to develop effective defense mechanisms, encryption protocols, and intrusion detection systems tailored for space-based operations.").

[170] *See, e.g.*, Janessa Lynne Burford, Dawn H. Trout & Joseph I. Minow, *Spacecraft Charging Issues for Launch Vehicles*, NASA TECH. REPS. SERVER (June 23, 2014), https://ntrs.nasa.gov/api/citations/20150001479/downloads/20150001479.pdf [https://perma.cc/S2FA-6Q5D] (discussing the difficulties of charging space systems in outer space).

[171] *See* Graham Kendall, *Apollo 11 Anniversary: Could an iPhone Fly Me to the Moon?*, THE INDEPENDENT (July 9, 2019, 3:12 PM), https://www.independent.co.uk/news/science/apollo-11-moon-landing-mobile-phones-smartphone-iphone-a8988351.html (noting that memory and processing speeds today are much faster than in the guidance computers of previous space missions).

[172] *See supra* note 168 and accompanying text.

[173] *See Frequently Asked Questions About the International Space Station*, NAT'L AERONAUTICS & SPACE ADMIN., https://www.nasa.gov/international-space-station-frequently-asked-questions/ [https://perma.cc/J2SX-6RPT] ("Altitude control and propulsive reboost capability is a continuous requirement, which means the space station needs a continuous supply of propulsion spacecraft. Changes to the current propulsion scheme would take considerable new hardware/software development, and significant time and funding to implement."); OFF. OF INSPECTOR GEN., REP. NO. IG-22-005, NASA'S MANAGEMENT OF THE INTERNATIONAL SPACE STATION AND EFFORTS TO COMMERCIALIZE LOW EARTH ORBIT 12 (2021), https://oig.nasa.gov/docs/IG-22-005.pdf [https://perma.cc/6RFJ-R8KN] ("Station maintenance involves keeping items and equipment in an operational condition through installation, inspection, repair, servicing, removal, and replacement. . . . Resolving

and space segment is transmitted by radio, which is more susceptible to hacking, especially since many satellites do not encrypt their radio communications.[174] As NASA's former chief information security officer Jeanette Hanna-Ruiz portended, "[I]t's a matter of time before someone hacks into something in Space."[175] Within five years, this risk became a reality when hackers targeted Viasat's link segment in 2022.[176]

The reliance on older hardware and software in space systems for reasons like backward compatibility introduces additional security challenges. For example, the use of legacy systems may mean that these technologies lack the latest security features and updates that would protect against emerging threats.[177] As technologies evolve rapidly on Earth, the outdated components of space systems become more susceptible to vulnerabilities that have been discovered and addressed in newer versions; the lack of regular updates and patches for older systems increases the risk of security breaches and compromises. This problem has been exacerbated by the emergence of the commercial space industry, with complex supply chains and many different providers. The task of auditing aging hardware and software has thus become even more difficult.[178]

---

unexpected problems can be challenging and often requires the crew to make repairs in space with the aid of teams on Earth.").

[174] *See* Kimberly Lukin & Maximilian Haselberger, *Hacking Satellites with Software Defined Radio*, IEEE XPLORE (Nov. 18, 2020), https://ieeexplore.ieee.org/document/9256695 [https://perma.cc/X5N6-YNEY] (proving the ease with which satellite connections can be hacked and offering recommendations on how to prevent such attacks).

[175] Brianna Bace, Yasir Gökce & Unal Tatar, *Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems*, 48 TELECOMMS. POL'Y 1, 1 (2024), https://www.sciencedirect.com/science/article/abs/pii/S0308596124000363.

[176] *Id.*

[177] *See* Katie Terrell Hanna, *What Is Backward Compatible (Backward Compatibility)?*, TECHTARGET, https://www.techtarget.com/whatis/definition/backward-compatible-backward-compatibility [https://perma.cc/9WSY-JBZQ] (Sept. 2021) (explaining the incompatibility of these technologies due to the speeds utilized); *see also* M. Manulis, C.P. Bridges, R. Harrison, V. Sekar & A. Davis, *Cyber Security in New Space: Analysis of Threats, Key Enabling Technologies and Challenges*, 20 INT'L J. INFO. SEC. 287, 293 (2020) ("Unpatched versions of the software expose the application with openly documented attack vectors available for exploitation.").

[178] *See* Bace et al., *supra* note 175, at 3 ("Due to the commercialization of the space sector, more companies have begun manufacturing components for space segment infrastructure.

Overall, the combination of limited energy resources, weaker processors, and outdated hardware and software in space systems creates vulnerabilities that pose significant security risks.[179] But despite these heightened risks and potential damages, "[t]he cybersecurity posture of the space infrastructure, in terms of threats, vulnerabilities, and risks, has not been fully studied."[180] Moreover, cybersecurity threats are too often overlooked at the design stage. As Mitchell Kirshner notes, "[o]ne crucial factor of space systems development that is often overlooked is cybersecurity. As space systems become more complex and cyberphysical in nature, cybersecurity requirements become more difficult to capture."[181]

3. Electronic Interference. Space-based services are also vulnerable to electronic interference. GPS signals are vulnerable to jamming (denying the signal) and spoofing (providing a fake, misleading signal).[182] GPS jamming has become an especially salient problem in recent years as a cost-effective way of interfering with an adversary's capabilities, particularly in the case of drones.[183] Even the National Security and International Affairs

---

This has led to a more complicated supply chain, where it is harder to investigate sufficiently and audit suppliers.").

[179] *See* Manulis et al., *supra* note 177, at 288 (surveying the vulnerabilities of space satellite security); *see also* Brandon Bailey, *Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices*, THE AEROSPACE CORP. 11 fig.4 (Oct. 15, 2020), https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf [https://perma.cc/E3HE-UTWE] (listing threats and vulnerabilities to mitigate for space security).

[180] Georgios Kavallieratos & Sokratis Katsikas, *An Exploratory Analysis of the Last Frontier: A Systematic Literature Review of Cybersecurity in Space*, 43 INT'L J. CRITICAL INFRASTR. PROT. 1, 1 (2023), https://www.sciencedirect.com/science/article/pii/S1874548223000537.

[181] Mitchell Kirshner, *Model-Based Systems Engineering Cybersecurity for Space Systems*, 10 AEROSPACE 1, 1 (2023), https://www.mdpi.com/2226-4310/10/2/116 [https://perma.cc/ML8Z-PDT5].

[182] *See How to Deal with GPS Jamming and Spoofing*, CAMBRIDGE RADIO FREQUENCY SYS.: BLOG, https://www.crfs.com/blog/how-to-deal-with-gps-jamming-and-spoofing [https://perma.cc/LZ66-8WUY] (July 2020) (describing the basic differences between GPS jamming and spoofing).

[183] *See generally* Renato Ferreira, João Gaspar, Pedro Sebastião & Nuno Souto, *Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms*, 115 WIRELESS PERS. COMMC'NS 2705 (2020) (using experimental results to conclude that drone flights can be blocked with low-cost GPS jamming platforms).

Department of the U.S. Government Accountability Office noted as early as 1997 that the GPS equipment used during the Gulf War could become vulnerable to jamming.[184] This is precisely what happened during the 2003 invasion of Iraq when the Iraqi Army used jammers allegedly purchased from Russia.[185] Most recently, Israel faced GPS jamming in the Golan Heights, ostensibly from Russian elements in Syria.[186] This vulnerability spurred Israel's production of kinetic positioning systems that do not rely on satellites for positioning,[187] as well as anti-jamming systems.[188] Additionally, the number of GPS jamming incidents in civil aviation significantly increased in the Baltic Sea during the spring of 2024, which experts widely attribute to Russian military activities.[189] An interesting case of self-GPS jamming also occurred in 2024 when Israel, in order to disrupt missiles launched from Lebanon and Iran,

---

[184] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO/NSIAD-97-134, OPERATION DESERT STORM: EVALUATION OF THE AIR CAMPAIGN, at 25 n.20 (1997) ("[S]ome experts have expressed the concern that GPS guidance may be vulnerable to jamming. Thus, until system testing and possible modifications demonstrate . . . resistance to electronic countermeasures, it is possible that the solution to the TERCOM limitations—GPS—may lead to a new potential vulnerability—jamming.").

[185] Anne Marie Squeo, *U.S. Bombs GPS-Jamming Sites in Iraq, Possibly Sold by Russia*, WALL ST. J. (Mar. 26, 2003, 12:01 AM), https://www.wsj.com/articles/SB104863606076925200.

[186] *See* Arie Egozi, *Israeli Solutions Against the Most Advanced Electronic Warfare Systems*, DEF. INDUS. EUR. (Apr. 16, 2023), https://defence-industry.eu/israeli-solutions-against-the-most-advanced-electronic-warfare-systems/ [https://perma.cc/J85U-ET4W] (reporting that Russian GPS denial systems in Syria have "caused problems in Israel"); *see also* Avi Scharf, *GPS Jamming in Israel Spikes Amid Regional Flare-Up*, HAARETZ (Apr. 10, 2023), https://www.haaretz.com/israel-news/security-aviation/2023-04-10/ty-article/.premium/gps-jamming-in-israel-spikes-amid-recent-flareup/00000187-6589-dcdb-a9af-eda9f9330000 [https://perma.cc/7BJH-RMLZ] (discussing recent GPS jamming incidents in Israel amidst a period of significant unrest in the region).

[187] *See* Seth J. Frantzman, *Israel Starts Research Center for GPS-Free Navigation*, C4ISRNET (Mar. 18, 2021), https://www.c4isrnet.com/battlefield-tech/2021/03/18/israel-starts-research-center-for-gps-free-navigation/ [https://perma.cc/Z63X-Z9EC] (discussing Israel's research center to develop navigation systems less vulnerable to GPS disruption).

[188] *See* Egozi, *supra* note 186 (announcing that advanced anti-jamming systems were being integrated into Israeli Air Force platforms).

[189] *See* Vitaly Shevchenko, *Russia Blamed for GPS Interference Affecting Flights in Europe*, BBC (May 2, 2024), https://www.bbc.com/news/articles/cne900k4wvjo [https://perma.cc/Z87K-MCQH] ("Russia is causing disruption to satellite navigation systems affecting thousands of civilian flights, experts say. . . . [W]hile the problem existed before the Russian invasion of Ukraine in February 2022 it is worsening.").

disrupted GPS signals within its own territory—to the effect that Israelis' locations showed them in Beirut or Cairo.[190]

4. The First Space-Cyber War. Over the years, space assets were used in military campaigns to *support* the traditional warfighting domains of land, sea, and air for combined operations.[191] The targeting of space assets as a *distinct* part of a military campaign has now become an early defining feature of the war in Ukraine.[192] It started with a Russian cyberattack on Viasat on the eve of its full-scale invasion of Ukraine and continued with both parties launching cyberattacks on the space assets of their respective enemy.[193] Indeed, Ukraine marks the arrival of warfare in space and, significantly, cyber warfare on space assets.[194] If the Gulf War of 1991 was called the "first space war," the war in Ukraine has already been dubbed the first "space-cyber war."[195]

Both sides in Ukraine have launched cyberattacks on the space-based services of their rival. Indeed, just hours before Russia's full-scale invasion of Ukraine on February 24, 2022, it launched a cyberattack on Viasat's satellite network[196] serving the Ukrainian

---

[190] *See* Jane Arraf, *Israel Fakes GPS Locations to Deter Attacks, but It Also Throws Off Planes and Ships*, NPR (Apr. 22, 2024, 10:02 AM), https://www.npr.org/2024/04/22/1245847903/israel-gps-spoofing [https://perma.cc/X6XW-8PXR] (describing the ramifications of Israel's practice of "spoofing" GPS systems); *see also Israeli and Lebanese Users of Dating Apps Are Made Strange Bedfellows by War-Baffled GPS*, THE TIMES OF ISR. (Mar. 11, 2024, 12:16 PM), https://www.timesofisrael.com/israeli-and-lebanese-users-of-dating-apps-are-made-strange-bedfellows-by-war-baffled-gps/ ("Since the early days of the war, motorists using navigation apps like Waze and Google Maps would often see their locations show up completely wrong. Users in Tel Aviv would be marked in Cairo, while people in Haifa would show up as in Beirut.").

[191] *See* discussion *supra* Section II.A.

[192] *See* Tepper, *supra* note 4, at 2 ("The current war in Ukraine might be remembered as the first space-cyber war. It is demonstrating the potential and temptation of targeting space assets during an armed conflict.").

[193] *Id.* at 3.

[194] *Id.* at 2.

[195] *Id.*

[196] Viasat is an American telecommunication company, the biggest provider of satellite internet in the world. Its European subsidiary Eutelsat, a French company, owns the *KA-SAT* satellite. *See* Press Release, Viasat, Viasat Completes Acquisition of Remaining Stake in Its European Broadband Joint Venture, Inclusive of the *KA-SAT* Satellite and Ground Assets (Apr. 30, 2021), https://news.viasat.com/newsroom/press-releases/viasat-completes-acquisition-of-remaining-stake-in-its-european-broadband-joint-venture-inclusive-of-the-ka-sat-satellite-and-ground-assets [https://perma.cc/7FR9-RY6E] (describing the structure of

army.[197] The most likely aim of this cyberattack was "to disrupt Ukrainian command and control during the invasion."[198] The United States and NATO attributed the attack to Russia, which has consistently denied involvement in the attack.[199] However, SpaceX's Starlink appeared in Ukraine in March 2022, provided space-based broadband Internet, and immediately became a vital replacement for disrupted regular Internet service.[200] Then, Starlink itself became a target for Russian attempts to disrupt its services, though

---

Viasat Inc. and its ownership of the *KA-SAT* satellite); *see also* Matt Burgess, *A Mysterious Satellite Hack Has Victims Far Beyond Ukraine*, WIRED (Mar. 23, 2022, 7:00 AM), https://www.wired.com/story/viasat-internet-hack-ukraine-russia/ ("More than 22,000 miles above Earth, the KA-SAT is locked in orbit. Traveling at 7,000 miles per hour, in sync with the planet's rotation, the satellite beams high-speed internet down to people across Europe.").

[197] *See Vtorzhenie Rossii v Ukrainu Povysilo Trebovaniiā k Kiberbezopasnosti* [*Russia's Invasion of Ukraine Increases Cybersecurity Needs*], UNIVERSE SPACE TECH (Apr. 14, 2022), https://universemagazine.com/ru/vtorzhenie-rossii-v-ukrainu-povysilo-trebovaniya-k-kiberbezopasnosti/ [https://perma.cc/575Z-88SZ] ("Russia tried to jam Starlink signals near the border with Ukraine. Hackers also tried to attack Viasat satellites and get customer data. According to American experts, the purpose of these actions was to damage infrastructure.").

[198] Pearson, *supra* note 161.

[199] *Id.*; *see also* Carly Page, *Viasat Cyberattack Blamed on Russian Wiper Malware*, TECHCRUNCH (Mar. 31, 2022, 10:00 AM), https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/ [https://perma.cc/FXC6-M6CN] (noting the similarities between the Viasat attack and other Russian cyberattacks). Following the Viasat attack, researchers at SentinelLabs suggested that Russia had orchestrated the attack and that it was the result of a new strain of wiper malware called AcidRain, which resembled VPNFilter malware American security agencies had previously attributed to Russian-backed hacking groups Fancy Bear, or APT28. Notably, this malware was designed to remotely erase vulnerable modems and routers. *See* Juan Andrés Guerrero-Saade & Max van Amerongen, *AcidRain: A Modem Wiper Rains Down on Europe*, SENTINELLABS (Mar. 31, 2022), https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ [https://perma.cc/F3Q6-P9JR]; *see also FBI Warns Russians Hacked Hundreds of Thousands of Routers*, CNBC, https://www.cnbc.com/2018/05/29/fbi-warns-russians-hacked-hundreds-of-thousands-of-routers.html [https://perma.cc/W33F-NSWT] (May 29, 2018, 12:12 PM) (citing recent hackings by the Sofacy hacker group in Russia and noting their ties to the Fancy Bear hackings); *cf. CISA Warns of New Malware Framework Used by Russian 'Sandworm' Hacking Team*, DARK READING (Feb. 23, 2022), https://www.darkreading.com/vulnerabilities-threats/cisa-warns-of-new-malware-framework-employed-by-infamous-sandworm-hacking-team [https://perma.cc/LRR2-8L7A] (discussing how the hacking groups Sandworm and Voodoo Bear are the same entity, both tied to the Russian security agency GRU).

[200] *See generally* Babbage, *How Elon Musk's Starlink Has Changed Warfare*, THE ECONOMIST (Jan. 11, 2023), https://www.economist.com/starlink-pod [https://perma.cc/G82F-CSE8] (discussing how Starlink's collaborations with Ukraine became "vital to the country's war effort").

so far no such disruption has materialized.[201] Most recently, there have been reports of Russia purchasing third-party countries' Starlink terminals, supposedly to use its Internet service and potentially disrupt the network.[202]

There were also several cyberattacks targeting Russian satellites and space infrastructure, including by intercepting the signal of the satellite *Yamal-402* and broadcasting Ukrainian-placed content to Russian radio and TV channels.[203] Russian hackers sometimes

---

[201] *See* Valerie Insinna, *SpaceX Beating Russian Jamming Attack Was 'Eyewatering': DoD Official*, BREAKING DEF. (Apr. 20, 2022, 4:29 PM), https://breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/ [https://perma.cc/Q9BZ-MZJT] ("After SpaceX sent Starlink terminals to Ukraine in February in an apparent effort to help Ukraine maintain its internet connection amid war with Russia, SpaceX . . . claimed that Russia had jammed Starlink terminals in the country for hours at a time. After a software update, Starlink was operating normally . . . ."); *see also* Alex Horton, *Russia Tests Secretive Weapon to Target SpaceX's Starlink in Ukraine*, WASH. POST, https://www.washingtonpost.com/national-security/2023/04/18/discord-leaks-starlink-ukraine/ (Apr. 18, 2023, 8:27 PM) ("Russia's quest to sabotage Ukrainian forces' internet access by targeting the Starlink satellite operations . . . appears to be more advanced than previously known . . . .").

[202] *See* James Marson & Thomas Grove, *Russia Using Thousands of Musk's Starlink Systems in War, Ukrainian General Says*, WALL ST. J., https://www.wsj.com/world/russia-using-thousands-of-musks-starlink-systems-in-war-ukrainian-general-says-29303242 (Feb. 15, 2024, 2:09 PM) ("Ukraine's top military-intelligence officer said Russian invasion forces in his country are using thousands of Starlink satellite internet terminals, and that the network has been active in occupied parts of Ukraine for 'quite a long time.' . . . Russian private firms buy the terminals off intermediaries who pass off purchases as for personal use and deliver the equipment to Russia via neighboring countries . . . ."); *see also* Matt Burgess, *The Hacking of Starlink Terminals Has Begun*, WIRED, https://www.wired.com/story/starlink-internet-dish-hack/ (Aug. 10, 2022, 5:00 PM) ("This [Starlink] satellite network beams internet connections to hard-to-reach locations on Earth and has been a vital source of connectivity during Russia's war in Ukraine."); Sakshi Tiwari, *War Trophy for Russia: Starlink Terminals That Ukraine Was Using Against Russian Military Reportedly Seized by DPR Fighters*, EURASIAN TIMES (Jan. 23, 2023), https://www.eurasiantimes.com/war-trophy-for-russia-starlink-terminals-that-ukraine-was-using/ [https://perma.cc/D5J5-MEPU] ("[L]ocal Russian media was quick to conclude that since the Russian side had acquired the Starlink subscriber equipment, there were chances for Russians to study these terminals or use them in the battle against Ukraine.").

[203] *See MCHS Ob"i͡asnilo Lozhnoye Soobshchenie o Vozdushnoĭ Trevoge v Moskve*, [*The Ministry of Emergency Situations Explains the False Air Raid Alert in Moscow*], RBC (Mar. 9, 2023), https://www.rbc.ru/society/09/03/2023/6409daa69a7947252d17b932 [https://perma.cc/BEZ3-EGPS] (discussing several false air raid alarms in Russia caused by the hacking of Russian radio stations and television channels); Denis Chuprov, *Al'ternativnai͡a Dostavka: Ataki na Rossiĭskie Sputniki Zastavli͡aiu͡t Veshchateleĭ Iska' Novye*

retaliate by spoofing Ukrainian TV broadcasts, which causes collateral damage in other countries due to satellite transmission.[204]

In September 2022, hacktivists from Team OneFist attacked the satellite from Russia's LEO satellite constellation Gonets, owned by a company whose majority shareholder is Roscosmos, the Russian space agency.[205] Another significant attack happened at the end of June 2023 with a large disruption of the services of Russian satellite communications provider Dozor-Teleport,[206] a subsidiary of Amtel-

---

Sposoby Polucheniiа Signala [*Alternative Delivery: Attacks on Russian Satellites Force Broadcasters to Look for New Ways to Receive Signals*], TELESPUTNIK (May 5, 2023, 1:30 PM), https://telesputnik.ru/materials/tech/article/alternativnaya-dostavka-ataki-na-rossiyskie-sputniki-zastavlyayut-veschateley-iskat-novye-sposoby-polucheniya-signala [https://perma.cc/89SX-5GK9] (noting recent cyberattacks on the *Yamal* satellite series and their effect on Russian broadcasters); *see also* Ivan Zhukovsky & Ekaterina Zakaryan, *"Signal Byl Podmenen." Kak Zelenskiĭ Vystupil Pered Rossiianami v Svoĭ Den' Rozhdeniia* [*"Signal Was Replaced." How Zelensky Spoke to the Russians on His Birthday*], GAZETA (Jan. 25, 2023, 8:22 PM), https://www.gazeta.ru/social/2023/01/25/16145107.shtml [https://perma.cc/4JZ3-YBV2] ("In Crimea and the Belgorod region, TV viewers saw an address by Ukrainian President Volodymyr Zelensky instead of the usual federal channel programs. Regional authorities explained this by an unauthorized substitution of the broadcast signal. . . . The press service of the Belgorod regional administration told journalists that the replacement of the television signal was carried out from outside.").

[204] *See* Alena Fomina, *"Segodnia Den' Nasheĭ Obshcheĭ Pobedy": Rossiĭskie Khakery Vzlomali Ukrainskie Telekanaly i Saĭty* [*"Today Is the Day of Our Common Victory": Russian Hackers Hacked Ukrainian TV Channels and Websites*], GAZETA (May 9, 2024, 2:29 PM), https://www.gazeta.ru/tech/2024/05/09/19051345.shtml [https://perma.cc/2AQ3-N2Z4] (stating that the Russian group Kilobyte V hacked Ukrainian websites, leading Ukrainian hackers to hack Russian television stations in Ufa and Crimea); *see also Latvia: Hackers Replace Ukrainian Channel with Russian Propaganda*, TVP WORLD (April 19, 2024, 6:15 AM), https://tvpworld.com/77079182/latvia-hackers-replace-ukrainian-channel-with-russian-propaganda [https://perma.cc/C3QD-H4ML] (discussing how Russian satellite hacks affected a Russian-language Ukrainian state television broadcast in Latvia).

[205] *See* Vilius Petkauskas, *We Breached Russian Satellite Network, Say Pro-Ukraine Partisans*, CYBERNEWS, https://cybernews.com/cyber-war/we-breached-russian-satellite-network-say-pro-ukraine-partisans/ (Oct. 10, 2022, 2:19 PM) ("Hackers claim to have penetrated Gonets, a Russian low Earth orbit (LEO) satellite communications network, deleting a database that is crucial to its functioning. . . . A member of OneFist, known as Thraxman, claims it successfully penetrated Gonets' [CRM] system, discovering a misconfiguration error that allowed him to access the satellite network as a legitimate user.").

[206] *See* Vilius Petkauskas, *Russian Satellite Telecom Dozor Hit by Hackers*, CYBERNEWS, https://cybernews.com/cyber-war/dozor-russian-satellite-telecom-hacked/ (June 30, 2023, 11:57 AM) ("Dozor-Teleport, a Russian satellite communications provider used by the country's Ministry of Defense and security services, was hit by hackers aligned with the private military corporation (PMC) Wagner.").

Svyaz, which operates one of the largest satellite networks in Russia and provides services to Russian security services (including the military and FSB).[207]

With both sides of the war launching cyberattacks targeting space-based services, the war in Ukraine, while still ongoing, has already demonstrated the role of space in cross-domain warfare, the vulnerability of space-based infrastructure to cyberattacks, and the probability that space cyberattacks will occur in future wars.[208] Space-cyber threats are thus reshaping the nature of national defense and economic resilience, and nations are only starting to respond to the looming risks posed by the space-cyber nexus.[209]

III. NATIONAL RESPONSES TO THE SPACE-CYBER NEXUS

This Section reviews the responses of the leading powers to the rise of the space-cyber nexus. Since space-cyber threats entered the high-level agenda only after the Viasat attack on the eve of the Russian invasion of Ukraine, only two countries to date have introduced policies or standards specifically targeting space-cyber threats.[210]

---

[207] *See* @Netblocks, X (June 29, 2023, 12:01 PM), https://x.com/netblocks/status/1674447946689986561 [https://perma.cc/BKN9-QU4P] ("Confirmed: Metrics show a disruption to satellite internet provider Dozor-Teleport which supplies Russia's FSB, Gazprom, Rosatom and military installations; the incident comes amid a wave of cyberattacks by a group claiming affiliation with Wagner PMC[.]").

[208] *See* Juliana Suess, *Jamming and Cyber Attacks: How Space Is Being Targeted in Ukraine*, ROYAL UNITED SERVS. INST. (Apr. 5, 2022), https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine [https://perma.cc/3JCK-2CSF] ("As the war in Ukraine rages on, satellite communications providers are facing cyber attacks and disruption of their services. . . . Given the auxiliary role that space assets hold for militaries—think communications, positioning, timing and so on—it naturally follows that these assets become targets themselves.").

[209] *See* Ulpia-Elena Botezatu & Adrian-Victor Vevera, *Cyber Orbits: The Digital Revolution of Space Security*, *in* NATIONAL SECURITY IN THE DIGITAL AND INFORMATION AGE 110 (Sally Burt ed., 2024) ("This evolution reflects the growing recognition that cybersecurity threats pose a significant risk to national infrastructure, undermining a nation's economic, social, and political stability without a single physical incursion."); *see also Cybersecurity*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/topics/cybersecurity (Oct. 25, 2024) (noting that President Biden has recently made cybersecurity a top priority of the Department of Homeland Security).

[210] *See* Anna Ribeiro, *US Releases Framework for Space Diplomacy, Focuses on Critical Infrastructure and Cybersecurity of Space*, INDUS. CYBER (May 31, 2023),

A. RUSSIA

We are not aware of any official Russian policy or guidelines on cybersecurity of space systems, but the issue is on the agenda following the war in Ukraine. The cyberattack that Russia launched on Viasat presumably made the country aware of the cyber vulnerabilities of its own space systems. Moreover, during the early days of the war, hacktivists threatened to launch cyberattacks on Russian satellites, and the head of the Russian Space Agency Roscosmos warned that such attacks would be *casus belli*—justification for war.[211] Additionally, Russian officials have asserted that the use of satellite Internet provided by civilian operators on the battlefield is a violation of the Outer Space Treaty, potentially making them legitimate targets for retaliatory strikes.[212] Yet, while Russia cautions other nations against leveraging commercial infrastructure in space for military ends, Russia itself employs both civilian and commercial remote-sensing satellites to bolster its

---

https://industrialcyber.co/regulation-standards-and-compliance/us-releases-framework-for-space-diplomacy-focuses-on-critical-infrastructure-and-cybersecurity-of-space/ [https://perma.cc/QX7L-B3GJ] ("The [U.S. Department of State] is set to work with U.S. cybersecurity agencies and entities to promote a secure environment with cybersecurity interoperability to strengthen space asset resiliency against adversarial offensive operations."); Daryna Antoniuk, *Germany to Launch Cyber Military Branch to Combat Russian Threats*, THE RECORD (Apr. 5, 2024), https://therecord.media/germany-to-launch-cyber-military-unit-russia [https://perma.cc/VVC5-XCL4] ("Germany is set to introduce a dedicated cyber branch as part of its military restructuring . . . with an aim to combat increasing cyber aggression from Russia toward NATO members.").

[211] *See* Bryan Bender, *Russia's Space Chief Says Hacking Satellites 'A Cause for War,'* POLITICO (Mar. 2, 2022, 12:46 PM), https://www.politico.com/news/2022/03/02/russia-space-chief-hacking-satellites-war-00013211 ("A top Russian space official said any cyber attacks on the country's satellites would be considered 'a cause for war,' while denying that a control center had been taken down by hackers.").

[212] *See Zakharova Zaı̈avila, Chto SShA Ispol'zuiūt Grazhdanskie Sputniki Dlı̈a Boevoĭ Podderzhki VSU* [*Zakharova Stated that the US Uses Civilian Satellites for Combat Support of the Ukrainian Armed Forces*], TASS (Dec. 29, 2022), https://tass.ru/politika/16712831 [https://perma.cc/X9Z4-GBCQ] (describing how the United States and its NATO allies are allegedly violating the 1967 Outer Space Treaty by using civilian commercial satellites for combat support of Ukraine); *see also MID Dopustil Udary po "Kvazigrazhdanskim" Sputnikam* [*MFA Admits Strikes on "Quasi-Civilian" Satellites*], RBC (Oct. 16, 2023, 11:56 AM), https://www.rbc.ru/politics/16/10/2023/652cf3659a79475034af8ee0 [https://perma.cc/3VYY-WFNE] (reporting that Russian officials have questioned the United States' use of civilian satellites as potential treaty violations).

military capabilities.[213] An interesting case is Russian military's alleged practice of conducting airstrikes based on satellite imagery acquired through third-party, Western commercial space companies.[214]

Russian experts acknowledge the risk of cyberattacks on space systems, including the risk of spoofing or jamming of signals of GLONASS, the Russian equivalent of the GPS system.[215] Accordingly, officials from Roscosmos play an important role in the administration of the Russian cybersecurity system.[216] It is also interesting to note that Russia's perception of cybersecurity is part of the more general issue of information. For instance, the term "cybersecurity" is not widely used in Russia; instead, Russia uses

---

[213] OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 17 (2024) ("Moscow employs its civil commercial remote-sensing satellites to supplement military-dedicated capabilities and has warned that other countries' commercial infrastructure in outer space used for military purposes can become a legitimate target.").

[214] *See* Graeme Wood, *A Suspicious Pattern Alarming the Ukrainian Military*, THE ATLANTIC (Mar. 18, 2024), https://www.theatlantic.com/international/archive/2024/03/american-satellites-russia-ukraine-war/677775/ [https://perma.cc/5MGR-LJ5J] ("[Ukrainian] experts suspect that Russia 'purchases satellite imagery through third-party companies' that do business with Western satellite-imagery companies, and that these images 'could be used in armed aggression against Ukraine.'").

[215] *See* Boris Torgashev & Kristina Elagina, *The Growing Need for Cybersecurity in Global Navigation Satellite Systems*, EKONOMIKA I KACHESTVO SISTEM SVIĀZI [ECON. & QUALITY COMMC'N SYS.], Mar. 2022, at 54, 57, https://journal-ekss.ru/wp-content/uploads/2022/10/54-60.pdf [https://perma.cc/RZC7-M9WF] (arguing for more robust cybersecurity measures following recent cyberattacks on the Russian GLONASS).

[216] *See Ukaz Prezidenta RF ot 14 Aprelia 2022 g. N 203 "O Mezhvedomstvennoĭ Komissii Soveta Bezopasnosti Rossiĭskoĭ Federatsii po Voprosam Obespecheniia Tekhnologicheskogo Suvereniteta Gosudarstva v Sfere Razvitiia Kriticheskoĭ Informatsionnoĭ Infrastruktury Rossiĭskoĭ Federatsii"* [*Decree of the President of the Russian Federation of April 14, 2022 No. 203 "On the Interdepartmental Commission of the Security Council of the Russian Federation on Issues of Ensuring the Technological Sovereignty of the State in the Sphere of Development of the Critical Information Infrastructure of the Russian Federation"*], GARANT, https://base.garant.ru/404483518/ [https://perma.cc/NLH2-G63F] (Sept. 30, 2024) (noting that the head of Roscosmos is tasked with analyzing the technological independence of critical information infrastructure facilities from foreign technologies and identifying and assessing internal and external threats to national security).

the broader term "information security,"[217] which includes what we call cybersecurity.

B. CHINA

The Gulf War was a wake-up call for China and its People's Liberation Army (PLA) and served as a catalyst for a new focus on the space-cyber domain.[218] The "local wars under modern, high-tech conditions" model, which became key to the PLA's doctrine after the Gulf War, was refined under Hu Jintao to the current "local wars under informationized conditions" model.[219] Rooted in the PLA's response to the innovations of the Gulf War, the "absorption of cyber warfare, electronic warfare, satellite communications and reconnaissance, and psychological operations units" by China's Strategic Support Force (SSF) in 2015 represented the PLA's acknowledgement of the future importance of the space-cyber domain.[220] "China is also increasingly relying on space and cyber assets" that present new potential vulnerabilities[221]—a reality of which Chinese President Xi Jinping is keenly aware. In a speech to PLA soldiers stationed in Shaanxi province, Xi emphasized that

---

[217] *See Ukaz Prezidenta RF ot 5 Dekabriā 2016 g. N 646 "Ob Utverzhdenii Doktriny Informatsionnoĭ Bezopasnosti Rossiĭskoĭ Federatsii"* [*Decree of the President of the Russian Federation of December 5, 2016 No. 646 "On Approval of the Doctrine of Information Security of the Russian Federation"*], GARANT (Dec. 6, 2016), https://www.garant.ru/products/ipo/prime/doc/71456224/ [https://perma.cc/9MMB-R29H] (defining "information security" as "the state of protection of the individual, society and the state from internal and external information threats"); *see also Osnovy Gosudarstvennoĭ Politiki Rossiĭskoĭ Federatsii v Oblasti Mezhdunarodnoĭ Informatsionnoĭ Bezopasnosti na Period do 2020 Goda* [*Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security for the Period up to 2020*], GARANT (Apr. 22, 2014), https://www.garant.ru/products/ipo/prime/doc/70541072/ [https://perma.cc/3V7F-FWJP] (stating that the main threat in the field of international information security is the use of information and communication technologies).

[218] *See* Dean Cheng, *Space and National Security: China's Great Leap Upward*, *in* THE PLA BEYOND BORDERS: CHINA MILITARY OPERATIONS IN REGIONAL AND GLOBAL CONTEXT 311, 317 (Joel Wuthnow, Arthur S. Ding, Philip C. Saunders, Andrew Scobell & Andrew N.D. Yang eds., 2021) [hereinafter THE PLA BEYOND BORDERS] (referencing the Gulf War's expansive reach as a reason to focus on coordinating joint operations from space).

[219] *Id.* at 318.

[220] John Chen, Joe McReynolds & Kieran Green, *The PLA Strategic Support Force: A Joint Force for Information Operations*, *in* THE PLA BEYOND BORDERS, *supra* note 218, at 151, 151.

[221] Joel Wuthnow, *Introduction*, *in* THE PLA BEYOND BORDERS, *supra* note 218, at 1, 4.

space assets "should be well managed, well used, and well protected."[222] Xi further stated that the PLA must strengthen information protection capabilities in space.[223] A 2022 white paper echoes this sentiment and states that China will work toward this policy in the next five years.[224] To that end, China had previously integrated cyberspace, space, and electronic warfare into joint military operations through its Strategic Support Force (SSF) as part of its military reforms,[225] and by April 2023, U.S. Chief of Space Operations General Chance Saltzman stated, "We are seeing an incredibly sophisticated array of threats including the traditional SATCOM jammers and GPS jammers to more destabilizing . . . directed energy weapons (and) cyber-attacks."[226] Although researchers in the PRC have already independently developed a framework for addressing cyber threats,[227] we do not know of any

---

[222] *Xi Jinping: Taikong Zichan Shi Guoji Zhanlue Zichan, Yao Guan Hao Yong Hao, Geng Yao Baohu Hao* (习近平：太空资产是国家战略资产，要管好用好，更要保护好) [*Xi Jinping: Space Assets Are National Strategic Assets. We Must Manage and Use Them Well, and We Must Protect Them Well*], PENGPAI XINWEN (澎湃新闻) [SURGE NEWS] (Sept. 17, 2021, 11:20 AM), https://m.thepaper.cn/newsDetail_forward_14545244; *Xi Urges China's Strategic Space Assets to Be Well Managed, Well Used, Well Protected*, GLOB. TIMES, https://www.globaltimes.cn/page/202109/1234491.shtml [https://perma.cc/BM9W-2D8M] (Sept. 16, 2021, 11:39 PM).

[223] *See* GLOB. TIMES, *supra* note 222 ("Xi stressed . . . that more efforts should be put in safeguarding space assets by enhancing the abilities in emergency backup and survival systems, and information protection.").

[224] 2021 ZHONGGUO DE HANGTIAN (2021中国的航天) [CHINA'S SPACE PROGRAM IN 2021], ZHONGGUO GUOWUYUAN XINWEN BANGONGSHI (中国国务院新闻办公室) [CHINA STATE COUNCIL INFO. OFF.] (Jan. 28, 2021, 10:16 AM), https://www.gov.cn/zhengce/2022-01/28/content_5670920.htm [https://perma.cc/U63R-YC3R] (outlining China's plan to create a space environment governance system in the next five years).

[225] DEF. INTEL. AGENCY, 2022 CHALLENGES TO SECURITY IN SPACE 10 (2022), https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf [https://perma.cc/VQN8-7G6C].

[226] Ireland Degges, *Gen. Chance Saltzman Calls for Shifts in Mindsets and Methods to Keep Pace with Space Domain*, EXECUTIVEGOV (Apr. 20, 2023), https://executivegov.com/2023/04/gen-chance-saltzman-calls-for-pivots-to-keep-pace-with-space-challenges/ [https://perma.cc/EB3X-8XN6].

[227] *See generally* Bin Liu (刘斌) et al., *Mianxiang Taikong Weixie de Taishi Ganzhi Benti Jianmo* (面向太空网络战威胁的态势感知本体建模) [*Situational Awareness Ontology Modeling for Threat from Space Cyber Operations*], 45 JITONGGONGCHENG YU DIANZIJISHU (系统工程与电子技术[J]) [J. SYS. ENG'G & ELECS.] 745 (2023) (discussing a proposed analysis framework for satellite cyberspace threat awareness); Ferreira et al., *supra* note 183 (describing such a framework for stopping cyberattacks).

policies China has adopted thus far specifically addressing cyberthreats to space assets.

C. INDIA

India has not yet implemented specific policies to address cyberthreats to its space infrastructure, but it seems that the issue is on the Indian government's radar for future policy advancements.[228]

D. FRANCE

France's 2019 Space Defense Strategy acknowledges that cyberattacks are the most likely threats to space security, noting also the difficulties in their attribution.[229] While there is yet to be a more comprehensive response, France, as a European leader in space, may position itself as a leader also on Earth, as it hosts the largest annual European conference dedicated to space cybersecurity.[230]

---

[228] *See* AJEY LELE, CYBER THREATS TO SPACE DOMAIN: RISKS AND RESPONSES 57 (2023) ("[M]uch needs to be done domestically in the combined domain of space and cyber. The National Cyber Security Strategy, which connects with the Data Security Council of India, does not reference space infrastructure."); *see also* Tobby Simon, *Cyberproofing India's Space Assets*, CTR. FOR INT'L GOVERNANCE INNOVATION (Jan. 29, 2023), https://www.cigionline.org/articles/cyberproofing-indias-space-assets/ [https://perma.cc/Z7MQ-T3EA] ("While the latest National Cyber Security Strategy conceptualized by the Data Security Council of India does not mention space infrastructure, it does recognize the importance of cyber diplomacy.").

[229] *See* ARMED FORCES MINISTRY, SPACE DEFENCE STRATEGY 23 (2019), https://cd-geneve.delegfrance.org/IMG/pdf/space_defence_strategy_2019_france.pdf [https://perma.cc/3XVU-CQHW] ("Difficult to attribute, [cyberattacks] may have reversible or irreversible effects . . . .").

[230] *See About*, CYSAT, https://cysat.eu/about/ [https://perma.cc/3UN2-AJ2J] (describing the "biggest European event exclusively dedicated to safeguarding space assets and data," which takes place in Paris in 2025).

E. GERMANY

Shortly after the Russian invasion of Ukraine, Germany introduced policies and standards on space cybersecurity.[231] These documents, published by the German Federal Office for Information Security, in collaboration with Airbus, include a policy statement, IT baseline protection profile for space infrastructures, and technical guidelines for information security for space systems.[232]

F. JAPAN

The Russian-Ukrainian war significantly influenced the revision process of key Japanese security-related strategic documents.[233] One pivotal aspect was the inclusion of active cyber defense strategies within the cyber domain.[234] Additionally, these documents emphasize the enhancement of cooperation and interoperability in cross-domain operations, encompassing "space, cyber, and electromagnetic domains, to further strengthen the joint integrated deterrence capability of Japan and the United States."[235]

Furthermore, in summer 2022, Japan's Ministry of Economy, Trade and Industry published *Guidelines on Cybersecurity*

---

[231] *See* 2 INT'L INST. FOR STRATEGIC STUD., CYBER CAPABILITIES AND NATIONAL POWER 48 (2023) ("The Russian aggression against Ukraine in 2022 produced a sharp reaction in Germany, and the government introduced a raft of new measures thereafter.").

[232] *See generally, e.g.*, *Cyber Security for Air and Space Applications*, FED. OFF. INFO. SEC., https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/IT-Sicherheit-in-Luft-und-Raumfahrt/it-sicherheit-in-luft-und-raumfahrt.html [https://perma.cc/LFU8-T4VP] (policy statement); *IT-Grundschutz Profile for Space Infrastructures*, FED. OFF. INFO. SEC. (June 30, 2022), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=5 (IT baseline protection profile); *Technical Guideline BSI TR-03184: Information Security for Space Systems, Part 1: Space Segment*, FED. OFF. INFO. SEC. (July 28, 2023), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03184/BSI-TR-03184_part1.pdf?__blob=publicationFile&v=2 (technical guidelines).

[233] Jun Osawa, *How Japan Is Modernizing Its Cybersecurity Policy*, STIMSON (Feb. 2, 2023), https://www.stimson.org/2023/japan-cybersecurity-policy/ [https://perma.cc/J3K5-TNED].

[234] *See id.* ("There are two significant changes in the cyber area of this new [National Security Strategy]: the development of a posture for information warfare and the introduction of active cyber defense in cybersecurity.").

[235] *Id.*

Measures for Commercial Space Systems.[236] These guidelines advise important risk scenarios and outline necessary attack mitigation measures, with the purpose of encouraging businesses to take voluntary cybersecurity measures; however, they are informative in nature and fall short of providing concrete governance and technical standards.[237]

G. UNITED STATES

The United States leads in the number and breadth of instruments addressing space cybersecurity.[238] These include Space Policy Directive-5 (SPD-5), issued by President Donald Trump on September 4, 2020, which serves as the foundation of U.S. space-cyber policy.[239] The Biden Administration also saw priority in addressing the exposure to space cyberthreats. A high-level discussion held at the White House in 2023, with participants including the Office of the National Cyber Director (ONCD) and the National Space Council, explored ways government agencies should address these threats.[240] In May 2024, the ONCD released the *2024 Report on the Cybersecurity Posture of the United States*, which

---

[236] *See generally* MINISTRY OF ECON., TRADE & INDUS., GUIDELINES ON CYBERSECURITY MEASURES FOR COMMERCIAL SPACE SYSTEMS VER 1.0. SUMMARY (Jul. 21, 2022), https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/20220721_3.pdf [https://perma.cc/MA35-UYUL] (describing Japan's general rules on cybersecurity for particularly sensitive commercial space systems).

[237] *See id.* at 6 ("Operators of the commercial space systems use these guidelines *as a reference* for the cybersecurity measures of their companies. Governments, municipalities, and companies use these guidelines when procuring space systems *to confirm* whether the operators have taken basic cybersecurity measures." (emphasis added)).

[238] *See, e.g.*, 1 INT'L INST. FOR STRATEGIC STUD., CYBER CAPABILITIES AND NATIONAL POWER: A NET ASSESSMENT 15 (2021) ("[The United States] is the only country with a heavy global footprint in both civil and military uses of cyberspace . . . .").

[239] *President Signs Space Cybersecurity Policy Directive*, OFF. OF SPACE COM. (Sept. 4, 2020), https://www.space.commerce.gov/president-signs-space-cybersecurity-policy-directive/ [https://perma.cc/3722-QJX2].

[240] *See* Press Release, The White House, Readout of Space Systems Cybersecurity Executive Forum Hosted by the Office of the National Cyber Director and the National Space Council (Mar. 28, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/28/readout-of-space-systems-cybersecurity-executive-forum-hosted-by-the-office-of-the-national-cyber-director-and-the-national-space-council/ [https://perma.cc/QU6Q-CGUU] (highlighting a forum hosted by the ONCD and the National Space Council "focused on bolstering cybersecurity in the space systems ecosystem").

noted the increased reliance on space systems for the maintenance of critical infrastructure.[241] The ONCD report went on to state that "[a]s the space ecosystem continues to evolve and integrate new commercial participants, the cybersecurity of space systems will be a shared responsibility"—citing the spillover effects on U.S. and European partners after the 2022 cyberattack that ostensibly targeted Ukraine's telecommunications.[242]

Other U.S. agencies have released similar policies and reports. For instance, the Department of Homeland Security has published a "space policy."[243] Together with the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), which is part of the Department of Homeland Security, also published a joint Cybersecurity Advisory on Strengthening Cybersecurity of SATCOM Network Providers and Customers.[244] The FBI, the National Counterintelligence and Security Center (NCSC), and the Air Force Office of Special Investigations (AFOSI) published a joint advisory in August 2023 as well.[245] Additionally, the National Institute of Standards and Technology (NIST) have published several documents addressing cybersecurity.[246] Moreover, the State

---

[241] *See* OFF. OF THE NAT'L CYBER DIRECTOR, 2024 REPORT ON THE CYBERSECURITY POSTURE OF THE UNITED STATES 4 (2024) ("A growing number of critical infrastructure assets rely upon space-based systems for communications, sensing, navigation, and timing.").

[242] *Id.*

[243] Memorandum from the Sec'y of the U.S. Dep't of Homeland Sec. on the DHS Space Policy (Apr. 14, 2022), https://www.dhs.gov/sites/default/files/2022-06/DHS%20Policy%20Statement%20063-01%20Revision%2001%20-%20DHS%20Space%20Policy.pdf [https://perma.cc/J9JY-QRWZ].

[244] *Strengthening Cybersecurity of SATCOM Network Providers and Customers*, CYBERSEC. & INFRASTR. SEC. AGENCY, https://www.cisa.gov/sites/default/files/publications/AA22-076_Strengthening_Cybersecurity_of_SATCOM_Network_Providers_and_Customers.pdf [https://perma.cc/5MUL-BP4N] (May 10, 2022).

[245] *See* Keith Cowing, *NCSC/FBI/USAF Bulletin: Safeguarding the US Space Industry*, SPACEREF (Aug. 18, 2023), https://spaceref.com/space-commerce/ncsc-fbi-usaf-bulletin-safeguarding-the-u-s-space-industry/ [https://perma.cc/X5WJ-MCTY] (containing a link to the original DNI memorandum).

[246] *E.g.*, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST IR 8323, FOUNDATIONAL PNT PROFILE: APPLYING THE CYBERSECURITY FRAMEWORK FOR THE RESPONSIBLE USE OF POSITIONING (2021), https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8323.pdf; NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST IR 8401, SATELLITE GROUND SEGMENT: APPLYING THE CYBERSECURITY FRAMEWORK TO SATELLITE COMMAND AND CONTROL (2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf; NAT'L INST. OF STANDARDS &

Department has even incorporated space-cyber security into its recently published guidelines.[247] Finally, Congress has introduced two bills dedicated to space cybersecurity.[248] Indeed, the United States is leading in the introduction of both policy papers and technical standards on space cybersecurity.

The next Section reviews the rules of international law that apply warfare in the new domains of space, cyberspace, and the space-cyber nexus.

IV. THE LAWS OF WAR IN THE NEW WARFARE DOMAINS: SPACE, CYBER, AND THE SPACE-CYBER NEXUS

This Section presents the international law applicable to military operations in space, cyberspace, and the space-cyber nexus. As this Section demonstrates, compared to the traditional warfighting domains of land, sea, and air, which are fairly well regulated, these new domains are subject to a much thinner layer of regulation, if any.[249] While some legally binding rules were adopted to regulate space warfare,[250] no such rules have been adopted regarding cyberspace.[251] Indeed, most of the existing rules and norms for the

---

TECH., U.S. DEP'T OF COM., NIST IR 8270, INTRODUCTION TO CYBERSECURITY FOR COMMERCIAL SATELLITE OPERATIONS (2023), https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf; NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., NIST IR 8441, CYBERSECURITY FRAMEWORK PROFILE FOR HYBRID SATELLITE NETWORKS (HSN) (2023), https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8441.pdf.

[247] *See* Craig Bamford, *US State Department Releases Strategic Framework on Space Diplomacy*, SPACEREF (June 21, 2023), https://spaceref.com/space-commerce/us-state-department-releases-strategic-framework-space-diplomacy/ [https://perma.cc/G37D-JYQU] (discussing and providing a link to the U.S. State Department space policy document).

[248] *See* S. 1425, 118th Cong. (2023) (requiring reports on the federal support of cybersecurity measures in commercial satellite systems); H.R. 5017, 118th Cong. (2023), (directing the Secretary of Homeland Security to issue guidance reports on space systems and other critical infrastructure).

[249] *See* JEFFREY L. CATON, THE LAND, SPACE, AND CYBERSPACE NEXUS: EVOLUTION OF THE OLDEST MILITARY OPERATIONS IN THE NEWEST MILITARY DOMAINS 26 tbl.4 (2018) ("The lack of international laws and regulations governing the environment complicates responses to actions in this domain.").

[250] *See infra* Section IV.A.

[251] *See* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 603, 661–62 (2011) ("At present, the international community lacks consistency regarding even the most basic aspects of cyber

space and cyberspace domains are *non*-legally binding.[252] The space-cyber nexus is the newest domain and similarly lacks any dedicated regulation in international law; the separate rules on space and cyberspace may apply, but they were not adapted to this new domain and may contradict each other.[253]

A. THE LAWS OF SPACE WARFARE

History shows us that often a single event can become the starting point of global processes that touch the interests of many individuals and even countries; the regulation of space warfare is no exception. The launch of *Sputnik-1* was such an event. Against the backdrop of the Cold War and fears of a nuclear war, "the launch of *Sputnik* served to intensify the arms race and raise Cold War tensions" between the United States and the USSR, especially after the "Soviet Union also tested the first intercontinental ballistic missile" that same year.[254] The international community needed to react to the opening of a new frontier that raised many concerns, including the placement of nuclear weapons in orbit by the rival superpower.[255] Just one month after the Soviet launch of *Sputnik-1*, in November 1957, the UNGA adopted perhaps the first resolution mentioning space, and the first in the context of space warfare.[256] With this resolution, the UNGA urged a concerned United States to reach a disarmament agreement that would "provide for . . . [t]he joint study of an inspection system designed to ensure that the sending of objects through outer space shall be exclusively for peaceful and scientific purposes."[257] A year later, on December 13,

---

warfare . . . . This inability to achieve international consensus on even the most fundamental aspects of cyber warfare underscores the fact that such uncertainty invites cyber warfare operations during the intermediate flux of legal uncertainty and lack of enforcement against such attacks by the international community.").

[252] *See* Tepper, *supra* note 15, at 460 (noting that lawmaking in space warfare tends to lend itself to nonbinding agreements).

[253] See *infra* Section IV.C.4 for a discussion of the application of the laws of space warfare and cyber warfare to the space-cyber nexus.

[254] *Sputnik, 1957*, OFF. OF THE HISTORIAN, https://history.state.gov/milestones/1953-1960/sputnik [https://perma.cc/D2U7-KMB9].

[255] *See id.* (describing the impact of *Sputnik-1*'s launch on U.S. weapons strategy).

[256] G.A. Res. 1148 (XII) (Nov. 14, 1957).

[257] *Id.* ¶ 1(f).

1958, the UNGA adopted the first resolution dedicated to space exploration.[258] The resolution recognized "that it is the common aim that outer space should be used for peaceful purposes only" and expressed the wish "to avoid the extension of present national rivalries into this new field."[259]

To date, five legally binding treaties and seven key UN declarations dedicated to space activities have been adopted,[260] the most important of which was the 1967 Outer Space Treaty, which foresaw the issues and principles specified later in the other international treaties on space activities.[261] The 1967 Treaty provides the basic rules applicable to human space activities and may be considered the "constitution of space," as it is widely accepted and provides vague norms that no one disputes—although their interpretation is debated.[262] This Treaty is the source of all legally binding rules on space warfare[263] and applies not only to signatory states but also to nonstate actors under jurisdiction of these states.[264] In addition, the Treaty's provisions have likely been crystallized in customary international law and therefore apply to all states, regardless of whether they ratified it.[265]

---

[258] David Kuan-Wei Chen, *New Ways and Means to Strengthen the Responsible and Peaceful Use of Outer Space*, 48 GA. J. INT'L & COMPAR. L. 661, 664 (2020).

[259] G.A. Res. 1348 (XIII) (Dec. 13, 1958).

[260] *See generally* UNITED NATIONS OFF. FOR OUTER SPACE AFFS., INTERNATIONAL SPACE LAW: UNITED NATIONS INSTRUMENTS (2017) (containing a compilation of all relevant UN treaties and declarations dedicated to space activities).

[261] *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty] ("The exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries irrespective of their degree of economic or scientific development, and shall be the province of all mankind.").

[262] *See* Tepper, *supra* note 15, at 480–81 (noting the importance of the Outer Space Treaty while acknowledging certain debates regarding its interpretation).

[263] *See id.* at 480 ("Over the next several years, the UN considered proposals for prohibiting the use of space for military purposes and the placement of weapons of mass destruction in space, which resulted in several limited but *binding agreements*, most prominently the Outer Space Treaty." (emphasis added)).

[264] *See* Outer Space Treaty, *supra* note 261, art. VII ("[E]ach State Party from whose territory or facility an object is launched[] is internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons . . . .").

[265] *See* Ram S. Jakhu & Steven Freeland, *The Relationship Between the Outer Space Treaty and Customary International Law*, 59 PROC. INT'L INST. SPACE L. 183, 194 (2016) ("An

1. The (General) Laws of War Applied to Space. Article III of the Outer Space Treaty provides that, "States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, in accordance with international law."[266] By applying international law, the Outer Space Treaty imports the extensive body of international law, including its laws of war.[267]

The laws of war are traditionally divided into two main categories concerning the rules of war[268]: (1) *jus ad bellum*, the rules providing when it is lawful for a state to resort to the use of armed force in general; and (2) *jus in bello,* the laws of armed conflict, also known as international humanitarian law (IHL), which comprises the rules regulating behavior *during* an armed conflict.

There was major codification of the laws of war at the end of the nineteenth century and beginning of the twentieth century with the adoption of the Hague Conventions of 1899 and 1907.[269] The aftermath of World War II saw another wave of laws of war, influenced by the horrors of that war,[270] with the adoption of the UN Charter in 1945 and the four Geneva Conventions in 1949,[271] as well

---

important implication of this is that *all* states, whether or not parties to the Outer Space Treaty, can be held responsible, and even liable, for space related acts or omissions of their respective public/private entities . . . .").

[266] Outer Space Treaty, *supra* note 261, art. III.

[267] *See* Frans G. von der Dunk, *Armed Conflicts in Outer Space: Which Law Applies?*, 97 INT'L L. STUD. 188, 198–91 (asserting that international law has become applicable to outer space due to the language contained in the Outer Space Treaty).

[268] *See, e.g.*, *Jus Ad Bellum and Jus In Bello*, INT'L COMM. OF THE RED CROSS (Oct. 29, 2010), https://www.icrc.org/en/document/jus-ad-bellum-jus-in-bello [https://perma.cc/8SSQ-UZ6A] (explaining the difference between the terms).

[269] *See generally* CARNEGIE ENDOWMENT FOR INT'L PEACE, THE HAGUE CONVENTIONS OF 1899 (II) AND 1907 (IV) RESPECTING THE LAWS AND CUSTOMS OF WAR ON LAND (1915) (presenting both the Hague Conventions of 1899 and 1907 side by side for comparison and clarity).

[270] *See* Geoffrey Best, *World War Two and the Law of War*, 7 REV. INT'L STUD. 67, 77 (1981) ("[O]ne thing is clear; the experience of the Second World War directly and dramatically revolutionized the law on military occupation and resistance, and made it what it still is. No other branch of the law of war has been so much changed since 1907, and this is because of the strength of feeling among Germany's victims that it had been unfair to them. . . . The 1949 Geneva Conventions may equally be called victims' legislation.").

[271] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of Armed

as their Additional Protocols in 1977[272] and 2005.[273] These treaties operate within large categories and build the system of regulations depending on the various theaters of war: land, sea, and air.[274]

The UN Charter established a new international order and relations between nations[275] and provided the most basic rules of war, including the prohibition on the "threat or use of force" and the self-defense exception to this prohibition, which permits responses to "armed attack[s]."[276] Because what constitutes a use of force or an armed attack is not defined by the UN,[277] the question becomes: What test should be employed to define potential cyberattacks on space systems? There are two primary approaches for determining if an act constitutes a use of force: The first is the target-based

---

Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

[272] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609.

[273] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem (Protocol III), Dec. 8, 2005, 2404 U.N.T.S. 261.

[274] The Second Geneva Convention, for example, focuses specifically on maritime warfare. *See* Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea, *supra* note 271, art. 58 ("The present Convention replaces the Xth Hague Convention of October 18, 1907, for the adaptation to Maritime Warfare of the principles of the Geneva Convention of 1906 . . . .").

[275] *See* U.N. Charter art. 1, ¶ 2 ("The Purposes of the United Nations are . . . [t]o develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace . . . .").

[276] *See id.* art. 2, ¶ 4 ("All Members shall refrain in their international relations from the *threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." (emphasis added)); *id.* art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." (emphasis added)).

[277] *See* Bace et al., *supra* note 175, at 5 ("[T]he U.N. Charter does not define 'use of force,' or offer any criteria . . . ."); *see also* U.N. Charter art. 51 (providing that an "armed attack" triggers the right to exercise "individual or collective self-defense," but failing to define what constitutes such an attack).

approach,[278] which focuses on the criticality of a target to a state's security, and the "scale and effects" test, which developed from the *Nicaragua v. United States* case in the International Court of Justice.[279] However there remains no consensus on the subject, with each approach drawing critique.[280]

2. Regulation of Space Warfare by the Outer Space Treaty. In addition to importing international law and the laws of war to the domain of space, the Outer Space Treaty also includes a single article, Article IV, that provides specific rules on space warfare and prohibits the placement of weapons of mass destruction anywhere in space.[281] In addition, Article IV reserves "[t]he moon and other celestial bodies [to] be used by all States Parties to the Treaty *exclusively* for peaceful purposes."[282] Article IV further prohibits "[t]he establishment of military bases . . . and the conduct of military maneuvers on celestial bodies."[283] The full Article reads:

> States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.
>
> The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful

---

[278] *See* Bace et al., *supra* note 175, at 5 ("The target-based approach posits that the critically of a cyber operation's target plays a decisive role in determining whether it qualifies as an armed attack.").

[279] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27) ("[I]n customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its *scale and effects*, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces." (emphasis added)).

[280] *See* Bace et al., *supra* note 175, at 5–6 (stating that the target-based approach "has faced widespread criticism from various angles," with little evidence to suggest it "has evolved into customary international law").

[281] Outer Space Treaty, *supra* note 261, art. IV.

[282] *Id.* (emphasis added).

[283] *Id.*

> purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited.[284]

However, the formulation of Article IV leaves room for several interpretations and leaves out some military uses that are not prohibited. First, while it prohibits the placement of the most harmful types of weapons in space, Article IV does not prohibit the placement of *conventional* weapons.[285] Second, while the Article prescribes that celestial bodies shall be used *exclusively* for "peaceful purposes," it does not prescribe the same for Earth orbits and void space.[286] Third, some countries have adopted a narrow interpretation of "peaceful purposes," such as the U.S. government, which has interpreted "peaceful" to mean "nonaggressive," but not "nonmilitary,"[287] thus making *nonaggressive* military uses of outer space lawful.[288] Nevertheless, the U.S. interpretation leaves a

---

[284] *Id.*

[285] *See* Sa'id Mosteshar, *Space Law and Weapons in Space*, OXFORD RSCH. ENCYC. OF PLANETARY SCI. (May 23, 2019), https://oxfordre.com/planetaryscience/display/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-74 [https://perma.cc/24CY-R3YH] ("[Nuclear weapons] may not be placed in Earth's orbit or otherwise stationed in space. However, there is no restriction on conventional weapons." (citation omitted)).

[286] *See id.* ("In contrast to void space, the use of celestial bodies is reserved exclusively for peaceful purposes.").

[287] *See id.* ("[T]he United States has gone to great lengths to promote the interpretation of 'peaceful' as 'nonaggressive' rather than nonmilitary or civilian.").

[288] *See* U.N. GAOR, 20th Sess., 1422d mtg. at 429, U.N. Doc. A/C.1/SR.1422 (Dec. 20, 1965) ("[T]he United States had constantly endorsed the principle that outer space should be used for peaceful purposes. In that context, 'peaceful' meant non-aggressive rather than non-military. . . . The question of military activities in space could not be divorced from the question of military activities on earth. The test of any space activity must therefore be not whether it was military or non-military but whether it was consistent with the Charter and other obligations of international law."); *see also* Carl Q. Christol, *The Common Interest in the Exploration, Use and Exploitation of Outer Space for Peaceful Purposes: The Soviet-*

backdoor in the "peaceful purposes" principle, and indeed, many nations—including all major superpowers—de-facto use outer space for various military purposes.[289] Therefore, even though the Outer Space Treaty demilitarizes celestial bodies and prohibits the usage of most harmful weapons in the space domain, it does not prevent a space arms race, and the quest to prevent such a race was and still is an ongoing, and so far only partially successful, effort for the international community.[290]

3. Regulation of Space Warfare by Other Space Treaties. Four treaties followed the 1967 Outer Space Treaty, further elaborating on the latter's issues and principles. In the period from 1968 to 1979, four treaties were adopted: the Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space (1968); the Convention on International Liability for Damage Caused by Space Objects (1972); the Convention on Registration of Objects Launched into Outer Space (commonly known as the Registration Convention) (1975); and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979).[291] These treaties are commonly

---

American Dilemma, 18 AKRON L. REV. 193, 197 (1984) ("The prevailing, but not unanimous, view is that only aggressive conduct violates the norm of peaceful uses and purposes. . . . This approach adopts the view set out in Article 4, paragraph 2 of the Principles Treaty, that the use of military personnel, when their activities are peaceful in nature, is permissible.").

[289] *See* Steven Freeland, *Peaceful Purposes? Governing the Military Uses of Outer Space*, 18 EUR. J. L. REFORM 35, 47 (2016) ("Following the attacks of 11 September 2001, the United States Administration embarked on a policy designed to dominate the space dimension of military operations. . . . The European Union has also identified outer space as 'a key component for its European Defense and Security Policy' and China and Russia also regard space as a vital part of their military infrastructure." (footnote omitted)); *id.* at 37 ("[I]t is clear that outer space has been and is being used for military purposes . . . .").

[290] *See id.* at 49–50 ("The Outer Space Treaty, as well as the other United Nations Space Treaties, do not currently provide stringent rules or incentives to prevent an arms race in outer space, let alone a conflict involving (and perhaps 'in') space.").

[291] Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Apr. 22, 1968, 19 U.S.T. 7570, 672 U.N.T.S. 190 [hereinafter Rescue Agreement]; Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention]; Convention on the Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention]; Agreement Governing the Activities of States on the Moon and other Celestial Bodies, Dec. 18, 1979, 1363 U.N.T.S. 22 [hereinafter Moon Agreement].

referred to as the Rescue Agreement, the Liability Convention, the Registration Convention, and the Moon Agreement, respectively.[292]

The Liability Convention is widely recognized and may have implications as to space warfare.[293] It first expands on Article VII of the Outer Space Treaty, which provides that a launching state is "internationally liable for damage to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space, including the moon and other celestial bodies."[294] It is important to note that this is strict attribution, while the general rules of international law on attribution—notably the International Law Commission's Articles on State Responsibility—pose conditions to the recognition of such responsibility.[295]

The Liability Convention also imposes liability for the damage[296] caused by the launching state,[297] defines the types of such liability

---

[292] *Space Law Treaties and Principles*, UNITED NATIONS OFF. FOR OUTER SPACE AFFS., https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html [https://perma.cc/9P3F-F3V7].

[293] *See, e.g.*, Trevor Kehrer, Comment, *Closing the Liability Loophole: The Liability Convention and the Future of Conflict in Space*, 20 CHI. J. INT'L L. 178, 191 (2019) ("Space may well be the site of the next arms race, akin to the nuclear arms race of the Cold War. And similar to the deterrent and de-escalation effect of the Cold War treaties on the U.S. and Soviet Union, even those nations that might have the potential to protect themselves in the future may end up needing to rely on provisions of international law if things go wrong. In that event, the Liability Convention must be workable and sensible.").

[294] Outer Space Treaty, *supra* note 261, art. VII.

[295] *See* Int'l L. Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 124, 125 (2001) (referencing the Liability Convention when discussing situations "where there is a plurality of responsible States in respect of the same wrongful act"). For further discussion on attribution in wider international law, see generally 5 THOMAS WEATHERALL, THEORY AND PRACTICE OF PUBLIC INTERNATIONAL LAW: DUALITY OF RESPONSIBILITY IN INTERNATIONAL LAW 133–77 (Vincent Chetail ed., 2022).

[296] *See* Liability Convention, *supra* note 291, art. I(a) ("The term 'damage' means loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations[.]").

[297] *See id.* art. I(c) ("The term 'launching State' means: a State which launches or procures the launching of a space object; [or a] State from whose territory or facility a space object is launched[.]").

(i.e., joint and several liability),[298] and offers the terms[299] and measures of resolving disputes about space accidents.[300] Though the convention envisioned civil liability and not for acts of war, it may also apply to the latter.

The Moon Agreement applies to the Moon as well as to "other celestial bodies within the solar system."[301] Like the Outer Space Treaty, it reserves celestial bodies *exclusively* for peaceful purposes and bans the establishment of military bases on them as well as testing any type of weapons and conducting military maneuvers on celestial bodies.[302] Articles 1 and 3 of the Agreement read:

> 1. The moon shall be used by all States Parties exclusively for peaceful purposes.
>
> . . . .
>
> 3. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manœuvres on the moon shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes

---

[298] *See id.* art. IV ("In the event of damage being caused elsewhere than on the surface of the earth to a space object of one launching State or to persons or property on board such a space object by a space object of another launching State, and of damage thereby being caused to a third State or to its natural or juridical persons, the first two States shall be *jointly and severally liable* to the third State . . . ." (emphasis added)).

[299] *See id.* art. X ("A claim for compensation for damage may be presented to the launching State not later than one year following the date of the occurrence of the damage or the identification of the launching State which is liable.").

[300] *See id.* art. XIV ("If no settlement of a claim is arrived at through diplomatic negotiations as provided for in Article IX, within one year from the date on which the claimant State notifies the launching State that it has submitted the documentation of its claim, the parties concerned shall establish a Claims Commission at the request of either party.").

[301] Moon Agreement, *supra* note 291, art. 1.

[302] *Compare id.* art. 3 ("The moon shall be used by all States Parties exclusively for peaceful purposes. . . . The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manœuvres [sic] on the moon shall be forbidden."), *with* Outer Space Treaty, *supra* note 261, art. IV ("The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manœuvres on celestial bodies shall be forbidden.").

> shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration and use of the moon shall also not be prohibited.[303]

However, the Moon Agreement failed to gain any meaningful support, with only a handful of ratifying countries and none of the leading spacefaring nations.[304] But since the Agreement does not add much to the Outer Space Treaty in the context of space warfare, its failure is of no great significance.[305]

4. Efforts to Prevent a Space Arms Race. Efforts to prevent a space arms race have been on the agenda of the UN since 1981, when the UNGA adopted resolution 36/97C, entitled Prevention of an Arms Race in Outer Space (PAROS).[306] This agenda item has since been repeatedly discussed,[307] with subsequent similar resolutions reemerging but not gaining significant traction. For example, the 2018 iteration of the resolution reaffirmed the importance and urgency of preventing an arms race in outer space,[308] acknowledging that the current legal regime applicable to

---

[303] Moon Agreement, *supra* note 291, art. 1, 3.

[304] *See Status of Treaties: Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, U.N. TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XXIV-2&chapter=24&clang=_en [https://perma.cc/75D9-67N4] (showing that only 18 states have ratified the Moon Agreement).

[305] The purpose of the Moon Agreement was to provide a framework for the utilization of space resources, and in this context, it included a significant regime; however, this regime may have been the reason why it failed. *See* Eytan Tepper, *Structuring the Discourse on the Exploitation of Space Resources: Between Economic and Legal Commons*, 49 SPACE POL'Y 1, 6 (2019) ("Article 11 of the Moon Agreement is perceived as the main reason most states have chosen not to ratify [it] as they may not wish to introduce the CHM principle which adds a layer of rules and limitations on top of those included in the notion of global commons.").

[306] G.A. RES. 36/97C, Prevention of an Arms Race in Outer Space (Dec. 9, 1981).

[307] *See, e.g.*, G.A. RES. 63/40 (Dec. 2, 2008); G.A. RES. 64/28 (Dec. 2, 2009); G.A. RES. 65/44 (Dec. 8, 2010); G.A. RES. 66/27 (Dec. 2, 2011); G.A. RES. 67/30 (Dec. 3, 2012); G.A. RES. 68/29 (Dec. 5, 2013); G.A. RES. 70/26 (Dec. 7, 2015); G.A. RES. 71/31 (Dec. 5, 2016); G.A. RES. 72/26 (Dec. 4, 2017); G.A. RES. 73/30 (Dec. 5, 2018) (collectively and consistently reaffirming the international goal of preventing an arms race).

[308] *See* G.A. RES. 73/30, *supra* note 307 ("The General Assembly . . . [e]mphasizes the necessity of further measures with appropriate and effective provisions for verification to prevent an arms race in outer space[.]").

outer space did not guarantee such a result and needed to be enhanced to this effect.[309]

Having failed to produce a treaty, the UN established small working groups to report back to it. Thus, it created a Group of Governmental Experts (GGE) that issued a report on Transparency and Confidence-Building Measures in Outer Space Activities (TCBMs),[310] and later an open-ended working group (OEWG) on "[r]educing space threats through norms, rules and principles of responsible behaviour."[311] These working groups do not aim to introduce legally binding rules but rather to achieve consensus on nonbinding principles.[312] However, while the GGE resulted in the introduction of TCBM norms, the OEWG has not reached any consensus so far.[313]

---

[309] *See* Tepper, *supra* note 15 at 514 ("Decentralized governance in global affairs is inherent and inevitable, and it also has advantages, notably in the continuous evolution of governance under anarchic conditions. . . . [F]or the laws of space warfare to continue to evolve productively, governance-building efforts should focus more on expanding the existing elemental regimes and introducing new elemental regimes, and less on futile attempts at introducing a comprehensive multilateral regime or treaty.").

[310] Rep. of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, transmitted by Note by the Secretary-General, U.N. Doc. A/68/189 (July 29, 2013); *see also* U.N. Secretary-General, *Transparency and Confidence-Building Measures in Outer Space Activities*, ¶ 12, U.N. Doc. A/72/65 (Feb. 16, 2017) ("The present report highlights both the existing capabilities and gaps regarding the implementation of transparency and confidence-building measures. . . . It is hoped that the report will bring into focus those areas in which further efforts are needed to promote the practical implementation of transparency and confidence-building measures in outer space activities, with the goal of preventing an arms race in outer space.").

[311] G.A. Res. 76/231, Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviors, ¶ 5 (Dec. 24, 2021); *see also Open-Ended Working Group on Reducing Space Threats*, UNITED NATIONS OFF. FOR DISARMAMENT AFFS., https://meetings.unoda.org/meeting/57866/documents [https://perma.cc/4TG2-8GWW] (hosting a repository of documents authored by the Open-Ended Working Group on Reducing Space Threats).

[312] *See* G.A. Res. 76/231, *supra* note 311, ¶ 5(c) (convening the open-ended working group "to make recommendations on possible norms, rules and principles of responsible behaviours" that could "*contribute to the negotiation of* legally binding instruments" (emphasis added)).

[313] *See* Tepper, *supra* note 15, at 490–91 (explaining that the OEWG was established to recommend possible norms and principles but ended without any such agreement); Jessica West, *Missed Opportunity to Curb Security Threats in Space Leaves All More Vulnerable*, CTR. FOR INT'L GOVERNANCE INNOVATION (Sept. 29, 2023), https://www.cigionline.org/articles/missed-opportunity-to-curb-security-threats-in-space-leaves-all-more-vulnerable/ [https://perma.cc/XU7Q-JB24] ("After several worthwhile

In 2008, Russia and China proposed a legally binding treaty banning the placement of weapons in outer space.[314] The draft treaty, entitled the Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT), was heavily criticized, and the two states submitted a revised draft of the PPWT in 2014,[315] though this too failed to garner broad international support and was neglected.[316] In 2008, the European Union (EU) launched another initiative to strengthen security in space, by putting forward a proposal for a non-legally binding instrument: the International

---

sessions dedicated to developing norms, principles and rules for responsible behaviour in outer space, the Open-Ended Working Group (OWEG) concluded its last session without reaching agreement even on the most basic procedural description of the meetings."); *see also* GGE on TCBMs, *supra* note 310 ("The present report contains the study on outer space transparency and confidence-building measures conducted by the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, which was established by the Secretary-General of the United Nations. The study was adopted by consensus.").

[314] *See PAROS Treaty*, NUCLEAR THREAT INITIATIVE, https://www.nti.org/education-center/treaties-and-regimes/proposed-prevention-arms-race-space-paros-treaty/ (describing the development of the Proposed Prevention of an Arms Race in Space Treaty and providing a link to the 2008 draft proposal by China and Russia).

[315] *See* Jinyuan Su, *The "Peaceful Purposes" Principle in Outer Space and the Russia–China PPWT Proposal*, 26 SPACE POL'Y 81, 85–89 (2010) (highlighting issues with the 2008 draft treaty attempt, including definitional issues, open questions on the right of self-defense, and disagreement on inclusion of a verification regime); *see also* Permanent Reps. of the Russian Federation and China to the Conference on Disarmament, Letter dated June 10, 2014 from the Permanent Rep. of the Russian Federation and the Permanent Rep. of China to the Conference of Disarmament addressed to the Acting Secretary-General of the Conference transmitting the Updated Russian and Chinese Texts of the Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT) introduced by the Russian Federation and China, U.N. Doc. CD/1985 (June 12, 2014) (introducing an updated version of the 2008 PPWT to be circulated at the Conference of Disarmament).

[316] *See* Brian Britt, *The PPWT and Ongoing Challenges to Arms Control in Space*, 113 JOINT FORCE Q. 80, 81 (2024) ("The original draft treaty and its 2014 successor are rife with loopholes, failing to effectively define a weapon, what constitutes its use, and how accidents could be separated from intentional acts of aggression. PPWT drafts have loitered in purgatory in the face of staunch opposition led by the United States and key allies such as the United Kingdom (UK)." (footnote omitted)).

Code of Conduct for Outer Space Activities (ICoC).[317] This effort also failed and was later abandoned.[318]

The UNGA did succeed in endorsing two resolutions calling for political commitment of member states. The first such resolution reflected the Russo-Chinese position (i.e., their jointly suggested PPWT), and the United States submitted the other. First, in 2014, the UNGA adopted a resolution encouraging "all States, especially space-faring nations, to consider the possibility of upholding as appropriate a political commitment not to be the first to place weapons in outer space."[319] But while numerous states undertook the commitment, some Western countries opposed it and refrained from making such commitments themselves.[320] Then, in 2022, the UNGA adopted a resolution initiated by the United States calling for states to pledge not to conduct destructive direct-ascent antisatellite missile testing.[321] While this resolution was supported by 155 countries, 9 voted against, and 9 abstained.[322] Significantly, Russia and China voted against, and India abstained.[323] Thus, of the four countries with ASAT capabilities, only the United States, which had completed such tests long ago, made the pledge.[324]

---

[317] Council of the European Union, Council Conclusions and Draft Code of Conduct for Outer Space Activities, annex II, No. 17175/08.

[318] *See* Britt, *supra* note 316, at 81 ("In 2014, for instance, the European Union's International Code of Conduct for Outer Space Activities failed to reach a consensus and was pronounced dead after 6 years of repeated revisions and negotiations, despite a voluntary, nonbinding nature that explicitly permits the use of kinetic ASATs for safety and debris-reduction considerations.").

[319] G.A. Res. 69/32, No First Placement of Weapons in Outer Space (Dec. 2, 2014).

[320] *See Vote on Draft Resolution on Weapons of Mass Destruction in Outer Space*, SEC. COUNCIL REP. (Apr. 23, 2024), https://www.securitycouncilreport.org/whatsinblue/2024/04/vote-on-draft-resolution-on-weapons-of-mass-destruction-in-outer-space.php [https://perma.cc/9KXJ-M4LW] (explaining that, while some states felt a legal agreement was necessary to prevent an arms race in space, some Western members objected and others have felt that such an international agreement was unnecessary).

[321] *See* Marcia Smith, *U.N. Approves Resolution Not to Conduct Destructive ASAT Tests*, SPACEPOLICYONLINE.COM, https://spacepolicyonline.com/news/u-n-approves-resolution-not-to-conduct-destructive-asat-tests [https://perma.cc/Q2ZR-VX4P] (Dec. 7, 2022, 10:41 PM) (reporting that the UNGA voted in favor of the U.S.-initiated resolution to stop countries from conducting ASAT tests in a manner that creates space debris).

[322] *Id.*

[323] *Id.*

[324] *Id.*

Leaks in Washington in February 2024 that Russia had developed a nuclear space weapon—a space-based antisatellite nuclear weapon[325]—led to a discussion at the UN Security Council on its first ever draft resolution on space issues. Put forward by the United States and Japan, the resolution reaffirmed state parties' obligations under Article IV of the Outer Space Treaty, which banned the placement of nuclear weapons in space.[326] Russia and China suggested an amendment to the draft resolution so that it would call for a ban on the placement of *any* weapons in space, but the proposed amendment was rejected.[327] The result of the vote at the Security Council was thirteen in favor, one abstention (China), and one against (Russia); in effect, Russia vetoed the resolution.[328] In doing so, Russia noted that, while it opposed the placement of nuclear weapons in space, the draft resolution was a provocation intended to portray it in a negative light and was thus illegitimate.[329] A second vote a month later failed again.[330]

---

[325] *See* Theresa Hitchens, *From Russia with Nukes? Sifting Facts from Speculation About Space Weapon Threat*, BREAKING DEF. (Feb. 15, 2024, 4:09 PM), https://breakingdefense.com/2024/02/russia-nuclear-weapon-space-mike-turner-threat-white-house/ [https://perma.cc/CM4P-2YF9] ("The New York Times today quoted officials 'briefed on the matter' as saying that the Biden administration has 'informed Congress and its allies in Europe about Russian advances on a new, space-based nuclear weapon designed to threaten America's extensive satellite network.'").

[326] *See* Joint Statement on Behalf of the United States and Japan on the Draft Security Council Resolution on Weapons of Mass Destruction in Outer Space (Apr. 19, 2024), https://usun.usmission.gov/joint-statement-on-behalf-of-the-united-states-and-japan-on-the-draft-security-council-resolution-on-weapons-of-mass-destruction-in-outer-space/ [https://perma.cc/ANF5-7RCJ] ("[T]he resolution affirms our shared goal of preventing an arms race in outer space and the obligations of all States Parties to comply with the Outer Space Treaty, including not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of WMD.").

[327] *See* Press Release, Security Council, Security Council Fails to Adopt First-Ever Resolution on Arms Race in Outer Space, Due to Negative Vote by Russian Federation, U.N. Press Release SC/15678 (Apr. 24, 2024) ("The addition of the operative paragraph proposed by the Russian Federation and China does not delete from the draft resolution a call not to develop weapons of mass destruction and not to place them in outer space . . . . China's representative said the draft amendment provides for *the inclusion of all types of weapons* . . . ." (emphasis added)).

[328] *Id.*

[329] *Id.*

[330] *See* Press Release, Security Council, For Second Time Since Late April Security Council Fails to Adopt First-Ever Resolution on Preventing Arms Race in Outer Space, U.N. Press Release SC/15700 (May 20, 2024) ("The Security Council again failed to adopt a resolution on

5. The McGill Manual *and* Woomera Manual. There are several well-known sources summarizing and interpreting international law applicable to different warfare domains: the *San Remo Manual on International Law Applicable to Armed Conflict at Sea*,[331] the *HPCR Manual on International Law Applicable to Air and Missile Warfare*,[332] and the *Tallinn Manual on International Law Applicable to Cyber Warfare*.[333] Some authors even call such types of sources "the manual approach" and argue that it manifests the unique development of international law.[334] Recently, an international project led by the McGill Institute of Air and Space Law resulted in the publication of the *McGill Manual on International Law Applicable to Military Uses of Outer Space* (the MILAMOS).[335] A separate group worked on and published the

---

outer space today—following the Russian Federation's veto of a similar text on 24 April—with members voting in the same manner that saw the defeat of a proposed amendment to that text . . . .").

[331] SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Dowswald-Beck ed. 1995).

[332] HPCR: MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2013).

[333] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

[334] *See, e.g.*, Jean-Marie Henckaerts, *Customary International Humanitarian Law: A Response to US Comments*, 89 INT'L REV. RED CROSS 473, 489 (2007) ("[M]ilitary manuals and teaching manuals may put forward propositions that are based on law, but may also contain instructions based on policy or military considerations that go beyond the law . . . . [I]t was considered that teaching manuals authorized for use in training represent a form of state practice. . . . As a result, training manuals, instructor handbooks and pocket cards for soldiers were considered as reflecting state practice."). *But see* Bruno Demeyere, Editorial, *The Power of Asking "How"—A Key to Understanding the Development of IHL?*, 104 INT'L REV. RED CROSS 1507, 1508 (2022) ("While governments may task representatives with participating in such efforts in their personal capacity, or contribute to the drafting process through informal consultations (the 'manual' approach, e.g. in the field of cyber warfare, among others), they almost always retain plausible deniability in terms of who said what, and who is bound by which rules.").

[335] 1 MCGILL MANUAL ON INTERNATIONAL LAW APPLICABLE TO MILITARY USES OF OUTER SPACE (Ram S. Jakhu & Steven Freeland eds., 2022) [hereinafter MILAMOS]; *see also Manual on International Law Applicable to Military Activities in Outer Space*, MCGILL U., https://www.mcgill.ca/milamos [https://perma.cc/MUK2-QJ6P] ("[T]he . . . [p]roject aims to develop a widely-accepted manual clarifying the fundamental rules applicable to the military use of outer space in time of peace, including challenges to peace.").

Woomera Manual on the International Law of Military Space Operations.[336]

A manual approach seeks to capture and define the body of international law in a way that is accessible, comprehensive, and objective—to identify more common norms and practices but, significantly, *not* to create new rules.[337] Rather, these manuals seek to identify the *existing* international law that applies to the relevant warfare domain and suggest how it may apply in that context.[338] Indeed, the stated aim of the MILAMOS is the clarification of "the fundamental rules applicable to military uses of outer space by both States and non-state actors in time of peace and in periods of tension that pose challenges to peace."[339] By comparison, the *Woomera Manual* provides a "comprehensive, objective, and universal examination of the application of international law to military space activities and operations."[340]

The manuals are not legally binding, but the rationale behind them is that they will serve as an important reference for policymakers and their legal advisers and provide an internationally agreed-upon benchmark to which adherence would prevent international condemnation.[341]

B. THE LAWS OF CYBER WARFARE

There are no dedicated treaties or treaty articles regulating military operations in cyberspace.[342] However, the international community now widely recognizes that existing international law

---

[336] THE WOOMERA MANUAL ON THE INTERNATIONAL LAW OF MILITARY SPACE ACTIVITIES AND OPERATIONS (Jack Beard, Dale Stephens & David Koplow eds., 2024) [hereinafter WOOMERA].

[337] *See* TODD HARRISON, CTR. FOR STRATEGIC & INT'L STUD., INTERNATIONAL PERSPECTIVES ON SPACE WEAPONS v–vi (2020), https://aerospace.csis.org/wp-content/uploads/2020/05/Harrison_IntlPerspectivesSpaceWeapons-compressed.pdf [https://perma.cc/8MEE-M8RU] (providing examples of such manuals and clarifying their purpose in international law).

[338] *Id.* at vi.

[339] MILAMOS, *supra* note 335, at 5.

[340] *Compare* WOOMERA, *supra* note 336, at 2, *with* text accompanying *supra* note 339.

[341] *See* WOOMERA, *supra* note 336, at viii ("With its foundational emphasis on State practice and the rule of law, this *Manual* seeks to advance peaceful cooperation in space and provide a safer and more predictable framework for military space activities and operations.").

[342] *See supra* note 251 and accompanying text.

extends to cyberspace and cyberwarfare.[343] Further, several forums have developed nonbinding norms and rules.[344]

The first step is to consider whether international law applies to cyberspace. In the case of outer space, it was a treaty—the Outer Space Treaty—that applied international law to outer space;[345] there is no such equivalent in scope with regards to warfare in cyberspace.[346] However, the UN has established a series of GGEs, and their non-legally binding reports established that existing norms of international law apply to outer space.[347] It is important to note in this context that all major superpowers were represented in those GGEs, so their reports—adopted unanimously—represent a wide consensus.[348] The report of the third GGE, submitted in 2013, stated that "the application of norms derived from existing international law relevant to the use of [Information and Communication Technologies (ICTs)] by States is essential to reduce risks to international peace, security and stability." [349] The

---

[343] *See* Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note by the Secretary-General, ¶ 11, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter GGE, A/70/174] ("Previous reports of the Group reflect an emerging consensus on responsible State behaviour in the security and use of [cyberspace] derived from existing international norms and commitments. The task before the present Group was to continue to study, with a view to promoting common understandings, norms of responsible State behaviour, . . . and identify where additional norms that take into account the complexity and unique attributes of [cyberspace] may need to be developed."). *But see* Raboin, *supra* note 251, at 624 ("At present, international law has yet to fully comprehend the legal ramifications of cyber warfare. As such, international law typically only applies to cyber warfare activities by analogy.").

[344] *See* Tepper, *supra* note 15, at 460 ("This reality of international lawmaking on space warfare supports the observations of . . . scholars that international lawmaking is broadly tilting toward non-binding agreements.").

[345] *See supra* Section IV.A.2.

[346] *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 3 (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN 2.0] ("There are very few treaties that directly deal with cyber operations and those that have been adopted are of limited scope.").

[347] *See* Tepper, *supra* note 15, at 496–97 (describing this series of GGEs and the reports suggesting that international law should apply to cyberspace); *see also* discussion *supra* note 343.

[348] *See* Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note by the Secretary-General, U.N. Doc. A/68/98 (June 24, 2013) (listing the countries represented in the GGEs, which includes the five permanent members of the UN).

[349] *Id.*

report of the fourth GGE, submitted in 2015, built on the previous report and "examined *how* international law applies to the use of [information and communication technologies] by States."[350] The 2015 report also "emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by States."[351] These two reports therefore established the wide recognition that international law applies to cyberspace, and with that application, the laws of war were thus applied to warfare in the cyberspace.

1. Cyberattacks as an "Armed Attack." Through the application of international law to cyberspace came the application of the UN Charter, with its prohibition on the threat and use of force—though with an exception in case of "armed attack."[352] But does a cyberattack amount to an armed attack? Oona Hathaway notes that:

> [S]ome have suggested that cyber-attacks should be treated as acts of war. Yet the attacks look little like the armed attacks that the law of war has traditionally regulated. . . . [E]xisting law effectively addresses only a small fraction of potential cyber-attacks. The law of war, for example, provides a useful framework for only the very small number of cyber-attacks that amount to an armed attack or that take place in the context of an ongoing armed conflict.[353]

A series of declarations by the leading superpowers and NATO further seem to suggest that a cyberattack can, depending on the

---

[350] GGE, A/70/174, *supra* note 343 (emphasis added).

[351] *Id.*

[352] *See* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security." (emphasis added)).

[353] Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 817 (2012).

circumstances, amount to an armed attack in the meaning of the UN Charter.[354]

2. The Rome Statute and the ICC. An interesting development is the recently announced position and actions of the International Criminal Court (ICC) on cybercrimes. In September 2023, Karim Khan, the third prosecutor of the ICC, expressed a commitment to prosecuting cybercrimes that potentially violated the Rome Statute.[355] In June 2024, it was then revealed that the ICC was investigating alleged Russian cyberattacks on Ukrainian civilian infrastructure.[356] The ICC subsequently issued arrest warrants for former Russian Minister of Defense Sergei Shoigu and Chief of General Staff Valery Gerasimov, both of whom were suspected of committing war crimes and crimes against humanity.[357] While the ICC did not directly link the issuance of the warrants to Russian

---

[354] *See* Tepper, *supra* note 15, at 495 (explaining that, under certain circumstances, a cyberattack can constitute an illegal use of force giving rise to a right to self-defense (quoting Harold Hongju Koh, Remarks, *Twenty-First-Century International Lawmaking*, 101 GEO. L.J. 725, 742 (2013)); *see also* Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, 67 JOINT FORCE Q. 40, 41 (2012) (discussing the "Schmitt Analysis," which suggests that the seven factors contributing to whether something is an armed attack include "severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility").

[355] *See* Karim A.A. Khan KC, *Technology Will Not Exceed Our Humanity*, DIGIT. FRONT LINES (Aug. 20, 2023), https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity [https://perma.cc/FY3N-ZPZR] ("While no provision of the Rome Statute is dedicated to cybercrimes, such conduct may potentially fulfill the elements of many core international crimes as already defined."); *see also* Andy Greenberg, *The International Criminal Court Will Now Prosecute Cyberwar Crimes*, WIRED (Sept. 7, 2023, 12:19 PM), https://www.wired.com/story/icc-cyberwar-crimes ("[A] spokesperson for the office of the prosecutor confirmed that this is now the office's official stance. 'The Office considers that, in appropriate circumstances, conduct in cyberspace may potentially amount to war crimes, crimes against humanity, genocide, and/or the crime of aggression,' the spokesperson writes, 'and that such conduct may potentially be prosecuted before the Court where the case is sufficiently grave.'").

[356] Anthony Deutsch, Stephanie van den Berg & James Pearson, *Exclusive: ICC Probes Cyberattacks in Ukraine as Possible War Crimes, Sources Say*, REUTERS (June 14, 2024, 11:56 AM), https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14.

[357] Laura Gozzi, *War Crimes Arrest Warrants Issued for Top Russian Officials*, BBC (June 25, 2024), https://www.bbc.com/news/articles/c988qjje02eo [https://perma.cc/R2FY-RA94].

cybercrimes in Ukraine, these may be part of the alleged war crimes.

This expansion of the ICC's jurisdiction to include cybercrimes faces several difficulties. First, the ICC can prosecute individuals but not states or organizations.[358] Second, major spacefaring nations, including China, Russia, India, and the United States, either did not sign the Rome Statute or withdrew their signatures.[359] Third, it is unclear whether the jurisdiction of the ICC will cover cyberattacks launched during peacetime.[360] Nevertheless, this important development requires attention and monitoring, as this new interpretation of the Rome Statute may portray cyberattacks on space-based infrastructure, including civilian-use infrastructure, as war crimes.

3. International Communication Law. International communication law represents, in many ways, the most direct analogue to cybersecurity. The Constitution of the International Telecommunication Union (ITU Constitution) prohibits "harmful interference," defined in the document's Annex as that which "endangers . . . safety services, or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service."[361] The definition of safety services can then be interpreted broadly to include all critical national infrastructure (CNI) that is vulnerable to cyberattacks as well.

The ITU Constitution also gives governments wide discretion in regulating private activity, including acts to stop or cut off telecommunications "contrary to . . . public order, or to decency."[362]

---

[358] INT'L CRIM. CT., UNDERSTANDING THE INTERNATIONAL CRIMINAL COURT 14 (2020), https://www.icc-cpi.int/sites/default/files/Publications/understanding-the-icc.pdf.

[359] *See The States Parties to the Rome Statute*, INT'L CRIM. CT., https://asp.icc-cpi.int/states-parties [https://perma.cc/LKK9-X3EY] (not listing China, Russia, India, and the United States as parties to the Rome Statute); *see also Russia Withdraws from International Criminal Court Treaty*, BBC (Nov. 16, 2016), https://www.bbc.com/news/world-europe-38005282 [https://perma.cc/M9S7-2QTY] (discussing Russia and the United States' withdrawals from the Rome Statute).

[360] *See* Rome Statute of the International Criminal Court arts. 7–8, July 17, 1998, 2187 U.N.T.S. 91 (establishing jurisdictional bases for war crimes under Article 8 and for crimes against humanity during peacetime under Article 7, with no indication as to which bases would apply to cyberattacks).

[361] Constitution of the International Telecommunication Union annex ¶ 1003, Dec. 22, 1992, S. TREATY DOC. No. 104-34.

[362] *Id.* art. 34.

However, the drawback of these regulations is that the ITU (1) offers limited guidance in crafting a comprehensive legal framework to hold attackers more accountable and (2) transfers the duty to deal with cyber attackers to the national level.[363]

4. The Budapest Convention on Cybercrime. There have been some attempts to create a system that can impose legal liability on cyberattackers at the regional level. The most well-known is the Convention on Cybercrime signed in Budapest in 2001 (the Budapest Convention).[364] Introduced by the Council of Europe, the Budapest Convention defines nine categories of criminal offenses and calls on signatory states to adopt domestic laws to criminalize these offenses; the Budapest Convention also establishes a regime to enhance international cooperation on combating cybercrime.[365] So far, seventy-six nations have joined as parties to the Budapest Convention.[366] Similarly, in 2003, Asia-Pacific Economic Cooperation (APEC) leaders issued a joint statement undertaking to enact their own domestic legislation to combat cybercrime.[367]

5. The Forthcoming UN Convention on Cybercrime. In addition to the Budapest Convention, another legally binding treaty on

---

[363] *See* Kristen Cordell, *The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 14, 2020), https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard [https://perma.cc/9SHG-5DH8] ("The study groups write *recommendations*, which roll up to inform *resolutions* that are sent up to the larger body to vote on as *decisions*. . . . ITU decisions and outcomes are [then] implemented through national-level rules and regulations.").

[364] *See* Convention on Cybercrime pmbl., Nov. 23, 2001, 2296 U.N.T.S. 167 ("Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation[.]").

[365] *See id*. arts. 2–10 (defining categories of criminal offenses under the Budapest Convention); *id*. art. 22 (directing signatories to establish jurisdiction over the defined offenses); *id*. ch. III (setting forth principles of international cooperation related to the defined offenses).

[366] *See The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols*, COUNCIL OF EUR., https://www.coe.int/en/web/cybercrime/the-budapest-convention [https://perma.cc/4M3P-Y6AR] (listing the current parties to the Budapest Convention).

[367] *See* David Legard, *APEC Furthers Plans to Combat Cybercrime*, NETWORK WORLD (Jul. 29, 2003), https://www.networkworld.com/article/2335534/apec-furthers-plans-to-combat-cybercrime.html [https://perma.cc/W5D2-BKLT] ("Countries that want to be able to tackle cybercrime need to pass wide-ranging laws and be prepared to openly cooperate with other countries . . . . The statement came at the end of a conference organized by the APEC e-

cybercrimes is rapidly hurtling toward its end. Prepared by a dedicated UN Ad Hoc Committee, the efforts have already passed the stages of sharing ideas and proposals and the introduction of a preliminary draft.[368] Indeed, the committee was set to adopt a final draft to be submitted to the UNGA for adoption but could not secure the consensus needed; consequently, this final stage was postponed.[369]

The main feature of the proposed convention is an extended list of thirty-four cybercrime offenses that have not been previously implemented at an international level.[370] However, a half-dozen of those offenses focus on content, giving rise to concerns about freedom of speech and freedom of information.[371] Nevertheless, the

---

Security Task Group in Bangkok last week which sought ways to develop comprehensive legal frameworks to combat cybercrime and to build law enforcement units capable of investigating cybercrime.").

[368] *See Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, UNITED NATIONS OFF. ON DRUG & CRIME, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home [https://perma.cc/P3DU-P92X] ("[T]he Committee approved a draft General Assembly resolution to which the approved draft text of the Convention will be annexed, for adoption by the General Assembly.").

[369] *See No Consensus for the UN Cybercrime Treaty: The Concluding Session of the Ad Hoc Committee on Cybercrime 2024*, DIGIT. WATCH (Feb. 10, 2024), https://dig.watch/updates/no-consensus-for-the-un-cybercrime-treaty-the-concluding-session-of-the-ad-hoc-committee-on-cybercrime-2024 [https://perma.cc/4C3A-87AM] ("The concluding session of the Ad Hoc Committee on Cybercrime ended, but an additional session awaits as consensus has not been reached.").

[370] Tim Starks, *The Perilous Path to a New Cybercrime Treaty*, WASH. POST: THE CYBERSECURITY 202, (Apr. 28, 2023, 7:07 AM), https://www.washingtonpost.com/politics/2023/04/28/perilous-path-new-cybercrime-treaty/.

[371] *See id.* (discussing free speech concerns pertaining to offenses that are content-dependent rather than cyber-dependent); *ARTICLE 19's Comments on the Consolidated Negotiating Document on the Elaboration of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, UNITED NATIONS OFF. ON DRUG & CRIME 2–3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/ARTICLE_19_submission_Negotiating_Document_January_2023.pdf [https://perma.cc/NPX8-C9EM] (contending that the proposed content-based restrictions would conflict with international human rights obligations and foreclose alternative mechanisms of redress); *UN: Draft Cybercrime Treaty Threatens Rights*, HUMAN RTS. WATCH (Jan. 23, 2024, 9:00 AM), https://www.hrw.org/news/2024/01/23/un-draft-cybercrime-treaty-threatens-rights ("The draft convention contains over broad criminal provisions, weak—and

draft convention has the potential to be adopted because of its support by various nations, including Russia and the United States.[372]

6. The Tallinn Manual. Similar to the MILAMOS, the *Tallinn Manual* is a study on the rules of international law applicable to cyber conflicts and cyber warfare.[373] The first version of the manual was published in 2013, and the updated *Tallinn Manual 2.0* was released in 2017;[374] work is currently underway on the *Tallinn Manual 3.0*.[375] There are notable differences between the two current manuals. First, the title of the manual changed from *Applicable to Cyber Warfare* in the original version to *Applicable to Cyber Operations* in the second.[376] Additionally, *Tallinn 2.0* discusses cyber activities like cyber espionage, cyber terrorism, and

---

in some places nonexistent—human rights safeguards, and provides for excessive cross-border information sharing and cooperation requirements, which could facilitate intrusive surveillance.").

[372] *See* Jason Pielemeier, *Rethinking the United Nations Cybercrime Treaty*, JUST SECURITY (Sept. 23, 2024), https://www.justsecurity.org/100333/rethinking-united-nations-cybercrime-treaty/ [https://perma.cc/6K4B-7NR2] (noting that the treaty was initiated by Russia and has since won the support of the United States).

[373] *See* Tepper, *supra* note 15, at 499 ("The *Tallinn Manual* . . . is a NATO-initiated and supported academic study on the rules of international law applicable to cyber conflicts and cyber warfare published in 2013.").

[374] *See id.* ("The *Tallinn Manual 2.0*, released in 2017, expands the scope of the first edition to cyber operations during peacetime.").

[375] *See CCDCOE to Hose the Tallinn Manual 3.0 Process*, THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/ [https://perma.cc/PT4R-T8KQ] ("The envisioned five-year project will involve updating all chapters of the *Tallinn Manual 2.0* to address the evolving nature of cyber operations and State responses, as well as adding new topics of importance to States.").

[376] *See* Kalev Leetaru, *What Tallinn Manual 2.0 Teaches Us About the New Cyber Order*, FORBES (Feb. 9, 2017), https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/ [https://perma.cc/3BR7-P3S4] (observing that the *Tallinn Manual*'s title change reflects an acknowledgement that the majority of cyberattacks do not rise to the level of a formal act of war as recognized in international law).

the "use of cyber weapons and equipment in the fight against cybercrime and terrorism."[377]

C. THE LAWS OF SPACE-CYBER WARFARE

There has yet to be any multilateral instrument—hard or soft law,[378] treaty or guideline—to regulate the space-cyber nexus directly. Since the nexus involves both space and cyberspace and, at this stage, lacks dedicated regulation, we can only apply both the laws of space warfare and the laws of cyber warfare to the new nexus. These may provide a viable interim solution, but they are insufficient and could potentially be contradicting on certain issues.

1. Application of International Law. While no instrument declares so, since international law applies to both outer space and cyberspace in a limited capacity,[379] it is safe to assume that the application of international law will also apply to the space-cyber nexus.[380] With this application comes the application of the laws of war.[381] This is also provided by the *McGill Manual* reviewed below.[382]

2. No UN Channel Dedicated to Space-Cyber Warfare. The space-cyber nexus has only recently emerged as a warfighting domain. It

---

[377] Ensar Seker, *Tallinn Manual—International Law to Cyberspace*, MEDIUM: DIGIT. DIPL. (Aug. 10, 2020), https://medium.com/digital-diplomacy/tallinn-manual-international-law-to-cyberspace-fc2304ebcd93 [https://perma.cc/4LFV-7JKJ]; *see also* TALLINN 2.0, *supra* note 346, at 192–93 (discussing application of international human rights law to cyber espionage); *id.* at 199 (noting the use of the Internet by terrorist organizations); *id.* at 452 (defining cyber weapons); *id.* at 75 (defining cybercrime and mutual assistance methods and technologies).

[378] *See* Teresa Fajardo, *Soft Law*, OXFORD BIBLIOS., https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0040.xml (Jan. 30, 2014) ("The generic term *soft law* covers a wide range of instruments of different nature and functions that make it very difficult to contain it within a single formula. Its only common feature is that it is in written form . . . . Moreover, it covers those weak provisions of international agreements not entailing obligations.").

[379] *See* discussion *supra* Sections III.A.1, III.B.1.

[380] See *supra* Section II.C.4 for a discussion of the recent emergence of the space-cyber domain as a distinct military domain.

[381] *See, e.g.*, *The Laws of War in a Nutshell*, INT'L COMM. OF THE RED CROSS (Oct. 19, 2016), https://www.icrc.org/en/document/what-are-rules-of-war-Geneva-Conventions [https://perma.cc/R3R5-HDD6] ("The rules of war, or international humanitarian law (as it is known formally) are a set of international rules that set out what can and cannot be done during an armed conflict.").

[382] *See infra* Section IV.C.3.

is therefore not surprising that there is an undersupply of rules for space-cyber operations due to the at times reactive nature of international law generation.[383] The UN still works in two separate channels: one working on developing the laws of space warfare, and another on the laws of cyber warfare and crimes.[384] Thus, there has yet to be a dedicated channel for the space-cyber nexus. The UN-mandated GGEs on space are separate from those on cybersecurity and so are the OEWGs;[385] in 2021, the OEWG on cybersecurity submitted its final report, which does not mention space even once.[386] And while cybersecurity was invoked by the OEWG on reducing space threats, the issue was rejected for inclusion on the OEWG's agenda.[387]

3. The McGill *and* Tallinn Manual *Applied to Space-Cyber Warfare.* The *McGill Manual* includes one rule on cyber operations and the *Tallinn Manual* includes a chapter on space law. However, it is important to note that work is ongoing on a third version of the *Tallinn Manual*, which will likely include an updated chapter on space.

The McGill Manual reads:

> Rule 112 – Cyber Activities that Constitute Space Activities

---

[383] *See* Michal Saliternik & Sivan Shlomo Agon, *Proactive International Law*, 75 U.C. L.J. 661, 668 (2024) ("In line with this reactive, event-based approach of international law, international norms and institutions have often been created with the aim of devising solutions to the specific crises and problems encountered . . . . In this way, past events have become a constitutive element of the international legal order and an integral 'part of international law's evolutionary narratives.'").

[384] See *supra* Sections IV.A–B for a discussion of each channel of international lawmaking.

[385] *See, e.g.*, BEYZA UNAL, THE ROYAL INST. OF INT'L AFFS., CYBERSECURITY OF NATO'S SPACE-BASED STRATEGIC ASSETS 28 (2019) ("The United Nations has appointed GGEs on cyber and space developments. . . . It is imperative to create ongoing efforts and synergy between the cyber GGE and space GGE. Establishing norms of secure cyberspace would also improve security.").

[386] *See generally* Final Substantive Rep. of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc A/AC.290/2021/CRP.2 (Mar. 10, 2021).

[387] *See* JESSICA WEST, THE OPEN-ENDED WORKING GROUP ON REDUCING SPACE THREATS: RECAP OF THE THIRD SESSION JANUARY 30 TO FEBRUARY 3, 2023, at 5 (2023) (including a number of topics on outer space with the exception of cybersecurity issues).

> Cyber activities that constitute space activities, including military space activities, are governed by international space law, as well as the applicable rules of general international law.[388]

This rule, which represents a wide consensus of experts on *existing* international law, applies international law—and hence also the laws of war—to space-cyber activities.[389] It further applies space law to space-cyber activities, which is of particular importance considering the strict liability rules provided by the Outer Space Treaty and Liability Convention.[390]

Chapter 10 of *Tallinn Manual 2.0* is titled "Space Law" and addresses cyber activities "in, from, or through outer space."[391] The chapter notes the importance of outer space regarding cyber activities "ranging from civilian communications and navigation to military operations."[392] It also notes that "cyber operations could be directed against, or utilise, space-related cyber infrastructure."[393] The chapter further reviews cyber operations' uses and misuses of "space-related cyber infrastructure," including satellites.[394] Significantly, the chapter distinguishes between space-enabled cyber operations and cyber-enabled space operations:

> [W]hen considering the relationship between cyber operations and outer space, it can be useful to distinguish between space-enabled cyber operations and cyber-enabled space operations. The former, such as satellite-to-earth and satellite-to-satellite cyber communications, have little to do with outer space beyond being enabled by cyber infrastructure based on space assets. Space law generally applies to these types of cyber operations in a limited fashion. . . . In contrast, cyber-enabled space operations involve the actual

---

[388] MILAMOS, *supra* note 335, at 11.

[389] *See supra* Sections III.A.1, III.B.1.

[390] See *supra* Section IV.A.3 for a discussion of the Liability Convention.

[391] TALLINN 2.0, *supra* note 346, at 270.

[392] *Id.*

[393] *Id.*

[394] *Id.*

> operation of space assets or the conduct of space operations by cyber means. Examples include the employment of telemetry, tracking, and command systems for communications between ground stations and spacecraft and using cyber means to affect the functionality of a space asset or its payload. As an example, if cyber operations are used to take control of a satellite or its payload, the cyber operations are enabling an activity in outer space, whether they are fully or partially carried out therein.[395]

Space law applies mainly to space activities,[396] and in discussing space-cyber activities, most of which are launched from Earth,[397] a preliminary question would be if they qualify as "space activities." Chapter 10 again indicates that they are:

> Activities on the earth also qualify as space activities when they involve activities, or otherwise achieve effects, in outer space, such as the control of space objects. This is especially relevant with respect to cyber operations, as most cyber operations affecting or utilising space assets are initiated from the earth. To the extent space law applies to a particular circumstance involving cyber operations, it may, as *lex specialis*, prevail over contrary rules found elsewhere in this Manual.[398]

The Manual also notes the application and importance of the ITU rules to space-cyber operations, notably the prohibition of causing "harmful interference."[399] Notably, the chapter includes three rules that are discussed in detail below.

---

[395] *Id.* at 270–71.

[396] *See* Skip Smith, *A Space Law Primer for Colorado Lawyers, Part 1: International Space Law*, COLO. LAW., Mar. 2018, at 48, 49 ("Space law is the collection of international national laws governing space-related activities.").

[397] *See* TALLINN 2.0, *supra* note 346, at 272 ("[M]ost cyber operations affecting or utilizing space assets are initiated from the earth.").

[398] *Id.*

[399] *Id.* at 273 ("The Experts took note of the importance of international telecommunication law with respect to certain space activities, since particular aspects of satellite

> Rule 58 – Peaceful purposes and uses of force
>
> (a) Cyber operations on the moon and other celestial bodies may be conducted only for peaceful purposes.
>
> (b) Cyber operations in outer space are subject to international law limitations on the use of force.[400]

Rule 58(a) reflects Article IV of the Outer Space Treaty in reserving the Moon and other celestial bodies *exclusively* for peaceful purposes.[401] Rule 58(b) provides, in application of UN Charter Article 2(4), that space-cyber activities may not involve the unlawful use of force—in other words, that "any cyber operation that originates in, transits, or terminates in outer space and rises to the level of an unlawful threat or use of force is barred."[402] However, the *Manual* notes, based on the UN Charter and space law treaties, that "it is lawful to exercise the right of self-defence in outer space or to employ space-based assets to defend against armed attacks occurring on the earth."[403]

> Rule 59 – Respect for space activities
>
> (a) A State must respect the right of States of registry to exercise jurisdiction and control over space objects appearing on their registries.
>
> (b) A State must conduct its cyber operations involving outer space with due regard for the need to avoid

---

communications and their protection are governed by that body of law . . . ."); *see also supra* Section IV.B.

[400] TALLINN 2.0, *supra* note 346, at 273.

[401] *See id.* ("[Rule 58(a)] reflects Article IV of the Outer Space Treaty, which places specific restrictions on certain military activities in outer space. In particular, it provides that the earth's moon and other celestial bodies shall be used *exclusively* for peaceful purposes . . . ." (emphasis added)).

[402] *Id.* at 274; *see also id.* ("The reference to the UN Charter confirms that Article 2(4)'s prohibition of the threat or use of force applies fully to activities in outer space.").

[403] *Id.*

> interference with the peaceful space activities of other States.[404]

Applying Article VIII of the Outer Space Treaty, Rule 59(a) mandates that states respect the jurisdictional prerogatives of the state where a space object is registered to regulate their use and enforce the said regulations.[405] Yet, this prerogative includes a duty to exert continuous supervision and control over the use of satellites registered with the state and, inter alia, ensure conformity with international law.[406] Rule 59(b) applies Article IX of the Outer Space Treaty to the case of space-cyber operations,[407] suggesting that a cyberattack on space assets would be considered a prohibited interference.[408]

> Rule 60 – Supervision, responsibility, and liability
>
> (a) A State must authorise and supervise the cyber 'activities in outer space' of its non-governmental entities.
>
> (b) Cyber operations involving space objects are subject to the responsibility and liability regime of space law.[409]

Rule 60(a) applies Article VI of the Outer Space Treaty to the case of space-cyber activities by ensuring that nonstate actors also comply with the rules of international law, including those on space-

---

[404] *Id.* at 277.

[405] *See id.* ("[Rule 59(a)] applies the general requirement that a State must respect the jurisdictional prerogatives of other States . . . . As set forth in Article VIII of the Outer Space Treaty, a space object is subject to the 'jurisdiction and control' of the State on whose national registry the object is carried.").

[406] *Cf. id.* at 279 ("[D]ue regard . . . is generally understood as requiring States to act in a manner that does not impede the exercise by other States of the rights they enjoy in outer space.").

[407] *Id.* at 278.

[408] *See id.* ("[T]his obligation is customary in nature. It is of particular relevance to cyber operations that might result in physical damage or optical interference or the creation of space debris that may be expected to affect the space activities of other States.").

[409] *Id.* at 279–80.

cyber activities.[410] Rule 60(b) then applies the liability regime of space law to space-cyber activities.[411] This is meaningful, considering the higher standard of responsibility and liability provided in space law compared to the one provided in general international law.[412]

Finally, it is important to note that, while the *Tallinn Manual 2.0* is not legally binding,[413] it is the opinion of the experts behind it that "the Rules in this Chapter generally reflect customary law."[414] To the extent that this is correct, these rules are binding on all states, whether or not that state ratified any of the space law treaties—or any other international treaty for that matter—including the UN Charter.

4. The Need for an Integrated Approach. While the *McGill Manual* and *Tallinn Manual 2.0* provide important basic principles, there may still be a need for an integrated approach to this space governance dilemma, one that is understanding of the space-cyber nexus. As noted in a previous article:

> Whereas a combined space-cyber theatre has already emerged and manifested itself, the governance responses remain disjointed at the international level and inadequate at the national level.

---

[410] *See id*. at 280 ("[Rule 60(a)] is drawn from Article VI of the Outer Space Treaty, which provides that States are responsible for assuring that their 'national activities in outer space,' including those of non-governmental entities, 'are carried out in conformity with the provisions' of the Outer Space Treaty. . . . [A] State is generally responsible for, and must authorise and on a continuing basis supervise, the cyber activities in outer space . . . of its non-governmental entities . . . .").

[411] *See id*. at 281 ("[Rule 60(b)] acknowledges that space activities, including those involving cyber operations, are subject to the space law regime of responsibility and liability.").

[412] *Compare* Liability Convention, *supra* note 291, art. II ("A launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft in flight."), *with* RESTATEMENT (THIRD) OF FOREIGN RELS. L. § 451 (AM. L. INST. 1987) ("Under international law, a state or state instrumentality is immune from the jurisdiction of the courts of another state, except with respect to claims arising out of activities of the kind that may be carried on by private persons.").

[413] *See* TALLINN 2.0, *supra* note 346, at 2 ("It is essential to understand that *Tallinn Manual 2.0* is not an official document, but rather the product of two separate endeavors undertaken by groups of independent experts acting solely in their personal capacity.").

[414] *Id*. at 272.

. . . .

> [The] separate efforts [in the UN] and manuals on space and cyber warfare, respectively, are, however, only a starting point. There is a need for an integrated approach and focus to develop and then adopt policy through the prism of the space-cyber security nexus that responds to the complexities of the nexus.[415]

Several Chatham House studies have likewise concluded that there is an "escalatory cycle" of militarization in the space-cyber domain that has been met with a patchwork of insufficient national and international policies; a multilateral regime with requisite flexibility is therefore "urgently required."[416] This may even take the form of another manual. In any case, the increasing difficulty in adopting new legally binding international treaties[417] present persistent problems for space governance; a more feasible route to introducing new rules on space-cyber operations should be through nonbinding instruments. In response, the first step must be to identify shared norms that may later be incorporated into legally binding instruments and how *existing* international law applies to the space-cyber nexus.

---

[415] Tepper, *supra* note 4, at 3, 4.

[416] *See* CAROLINE BAYLON, THE ROYAL INST. OF INT'L AFFS., CHALLENGES AT THE INTERSECTION OF CYBER SECURITY AND SPACE SECURITY: COUNTRY AND INTERNATIONAL INSTITUTION PERSPECTIVES 14 (2014) ("There is growing concern within the cyber and space communities that both sectors are heading not only towards increasing militarization but a step beyond, towards increasing *weaponization*. It is therefore vital to take steps to break the escalatory cycle now, before it is too late."); DAVID LIVINGSTONE & PATRICIA LEWIS, THE ROYAL INST. OF INT'L AFFS., SPACE, THE FINAL FRONTIER FOR CYBERSECURITY? 2 (2016) ("Development of a flexible, multilateral space and cybersecurity regime is urgently required. . . . An international 'community of the willing'—made up of able states and other critical stakeholders within the international space supply chain and insurance industry—is likely to provide the best opportunity to develop a space cybersecurity regime competent to match the range of threats."); *see also* UNAL, *supra* note 385, and accompanying text.

[417] *See* Jack Goldsmith & Eric A. Posner, The Limits of International Law *Fifteen Years Later*, 22 CHI. J. INT'L L. 110, 123 (2021) ("The post-Cold War enthusiasm for international law has now collapsed . . . . [There has been] a deepening popular unhappiness with globalization and international governance, which in turn generated domestic political upheavals as nationalist, nativist, and populist movements made inroads on popular opinion.").

V. MULTI-TRACK INTERNATIONAL LAWMAKING FOR THE SPACE-CYBER NEXUS

This Section reviews the rise of nonbinding international agreements and how they transform international lawmaking. It then presents multi-track diplomacy and polycentric governance. Finally, it connects the dots by suggesting that the feasible path for introducing the laws of space-cyber warfare is by multi-track diplomacy, leading to the introduction of an array of nonbinding international agreements by multiple forums in a polycentric system of governance.

A. NONBINDING INTERNATIONAL AGREEMENTS ON SPACE-CYBER WARFARE?

Recent literature demonstrates how international lawmaking has transformed and is increasingly made by way of nonbinding international agreements.[418] This is a result of both global and domestic factors. Globally, it is increasingly harder to adopt legally binding international rules.[419] Domestically, with growing divisions, it is often difficult and very lengthy to approve binding international agreements.[420] The result is that the bulk of new international agreements are nonbinding, which also changes the nature of

---

[418] *See, e.g.*, Bradley et al., *supra* note 27, at 1281 ("Not only have nonbinding agreements become more prevalent, but many of the most consequential (and often controversial) U.S. international agreements in recent years have been concluded in whole or in significant parts as nonbinding agreements."); *see also* Harold Hongju Koh, Remarks, *Twenty-First-Century International Lawmaking*, 101 GEO. L.J. 725, 740–42 (2013) (noting examples of U.S. nonbinding international agreements).

[419] *See* Tepper, *supra* note 15, at 501–02 ("Legally binding international lawmaking is an ever-harder task. The basic nature of global affairs—the lack of a global political authority—is joined by growing power diffusion. There are more State actors—the number of UN Member States grew from 51 in 1945 to the current 193 in 2023—and they are joined by non-State actors, particularly in space, where commercial companies are almost taking the lead from national space agencies." (footnote omitted)).

[420] *See id.* at 502–03 ("[T]he U.S. domestic process of adopting legally binding international agreements, like Article II treaties and executive agreements, is ever more complicated bureaucratically and politically and is an increasingly inadequate solution for the U.S. needs for global engagement."); *see also* Koh, *supra* note 418, at 728 ("[A] particular nontreaty route might be legally available to the Executive for entering into certain kinds of international agreements but may not be *politically* advisable as a matter of comity to Congress.").

international law.[421] Considering this, we can expect that the development of rules for the space-cyber nexus will, at least in the beginning, be comprised mainly of nonbinding agreements or guidelines.[422]

Nonbinding international agreements can take a diversity of forms in a multiplicity of institutional settings. From "joint statements and communiques" to more formal papers, these subtle agreements form an important part of international relations and appear to be the trend in international governance.[423] These agreements do not retain the full legal weight of treaties or bilateral agreements, which are governed by international law,[424] but rather combine elements of "soft law" or "informal law" from governmental actors who have traditionally developed "hard law," such as diplomats or UN organizations.[425]

Nonbinding international agreements may be suitable for the space-cyber nexus, not just because they may be more feasible under current global politics but also due to the "pacing problem."[426] The

---

[421] *See* Bradley et al., *supra* note 27, at 1288 ("Nonbinding agreements . . . are not just an important part of the international agreement landscape; they are, increasingly, the *dominant* part.").

[422] *See* Tepper, *supra* note 15, at 503 ("Either way, polycentric governance and non-binding agreements are the response to the increasing difficulty, and diminished desirability, of introducing legally binding international treaties and agreements. Indeed, space governance as a whole is already on track to become polycentric.").

[423] *See* Bradley et al., *supra* note 27, at 1303 ("Nonbinding agreements can include all manner of informal diplomatic communication, including emails, phone calls, and everyday cables that foster relatively trivial forms of international cooperation and coordination.").

[424] *See* Vienna Convention on the Law of Treaties art. 2(1)(a), *opened for signature* May 23, 1969, 1155 U.N.T.S. 331 ("'Treaty' means an international agreement concluded between States in written form and governed by international law . . . .").

[425] *See* CHARLES B. ROGER, THE ORIGINS OF INFORMALITY: WHY THE LEGAL FOUNDATIONS OF GLOBAL GOVERNANCE ARE SHIFTING, AND WHY IT MATTERS 1 (2020) ("Nonbinding international agreements, often known as 'soft law,' proliferated across many issue areas. Even more notably, a growing variety of informal international organizations . . . have come to dominate governance of some of the most pressing challenges the world faces." (footnote omitted)).

[426] *Cf.* COMMITMENT AND COMPLIANCE: THE ROLE OF NON-BINDING NORMS IN THE INTERNATIONAL LEGAL SYSTEM 13 (Dinah Shelton ed., 2000) [hereinafter COMMITMENT AND COMPLIANCE] ("Legally binding norms may be inappropriate when the issue or the effective response is not yet clearly identified, due to scientific uncertainty or other causes, but there is an urgent requirement to take some action. Similarly, it may be necessary where diverse

pacing problem refers to the inability of legal or regulatory regimes to keep adjusting to the intensifying pace of technological change[427]: "New technologies that used to have two-year cycle times now can become obsolete in six months, and the pace of change is not slowing."[428] Nonbinding and narrowly focused regimes are quicker to be introduced and amended.[429] Thus, where hard law is rigid, nonbinding agreements are more flexible.[430] As a result, it is often the case that industry players prefer to avoid state control, as would occur under a treaty framework, preferring instead to develop soft law mechanisms through industry-led, bottom-up processes.[431] But while nonbinding agreements cannot be enforced, states that engage in processes leading to them—and undertake a political obligation in joining them—are likely to comply, as nonbinding agreements also represent state interests both in the introduction of negotiated rules and in avoiding reputational damage.[432]

---

legal systems preclude legally binding norms. Thus, soft law may be increasingly utilized because it responds to the needs of the new international system.").

[427] *See* Ryan Hagemann, Jennifer Huddleston Skees & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 59 (2018) ("[The] accelerated rate of market penetration, coupled with the introduction of fast-developing technologies, gives rise to what philosophers and social scientists refer to as the pacing problem . . . .").

[428] SHRUPTI SHAH, RACHEL BRODY & NICK OLSON, THE REGULATOR OF TOMORROW: RULEMAKING AND ENFORCEMENT IN AN ERA OF EXPONENTIAL CHANGE 3 (2015).

[429] *See* COMMITMENT AND COMPLIANCE, *supra* note 426, at 13 ("Soft law generally can be adopted more rapidly because it is non-binding. It can also be quickly amended or replaced if it fails to meet current challenges.").

[430] *Id.*

[431] *Cf.* SHAH ET AL., *supra* note 428, at 9 ("Some forward-thinking regulators have navigated similar challenges by providing industry innovators with a clear set of guidelines for developing new offerings. In other cases, industry entities have come up with their own set of standards and principles, which could be adopted by a regulator as the base standard.").

[432] *See* Bradley et al., *supra* note 27, at 1312 ("Compliance with both [binding and nonbinding] agreements frequently depends on some combination of self-interest, reciprocity, reputation, and informal sanctions."). *But cf. id.* ("Even when this is true, binding agreements often create what are regarded as stickier obligations. . . . [T]he perceived reputational harm done by violating a binding agreement may be greater than that for violating a nonbinding one.").

B. MULTI-TRACK DIPLOMACY FOR THE SPACE-CYBER NEXUS

International and multilateral agreements are achieved by way of diplomacy, and there is more than one track of diplomatic negotiations.[433] Even when focusing on multilateral agreements, the UN channel is not the only one. *Encyclopedia Britannica* defines diplomacy as "the established method of influencing the decisions and behavior of foreign governments and peoples through dialogue, negotiation, and other measures short of war or violence."[434] Nowadays, some scholars define at least nine tracks of diplomacy.[435] However, by prioritizing none of them, the same scholars emphasize that all of the tracks are linked, though each has its own "resources, values, and approaches."[436] For clarity and practical purposes, we will discuss here only the three main diplomacy tracks: Track One (Official Diplomacy), Track Two (Nongovernmental Diplomacy), and Track 1.5.

1. The Rise of Multi-Track Diplomacy. In 1981, U.S. Department of State employee Joseph V. Montville coined the terms "track one

---

[433] *See Diplomacy*, ENCYC. BRITANNICA, https://www.britannica.com/topic/diplomacy [https://perma.cc/P724-9PAX] (Nov. 26, 2024) ("Historically, diplomacy meant the conduct of official (usually bilateral) relations between sovereign states. By the 20th century, however, . . . diplomacy had expanded to cover summit meetings and other international conferences, parliamentary diplomacy, the international activities of supranational and subnational entities, unofficial diplomacy by nongovernmental elements, and the work of international civil servants.").

[434] *Id.*

[435] *See* John W. McDonald, Profile, *The Institute for Multi-Track Diplomacy*, 3 J. CONFLICTOLOGY 66, 67–68 (2012) (listing and describing the nine tracks of diplomacy: (1) government, or peacemaking through diplomacy; (2) nongovernment/professional, or peacemaking through conflict resolution; (3) business or peacemaking through commerce; (4) private citizen, or peacemaking through personal involvement; (5) research, training, and education, or peacemaking through learning; (6) activism, or peacemaking through advocacy; (7) religion, or peacemaking through faith in action; (8) funding, or peacemaking through providing resources; and (9) communications and the media, or peacemaking through information).

[436] *See What Is Multi-Track Diplomacy?*, INST. FOR MULTI-TRACK DIPL., https://imtdsite.wordpress.com/about/what-is-multi-track-diplomacy/ [https://perma.cc/RC6M-42DL] ("No one track is more important than the other, and no one track is independent from the others. Each track has its own resources, values, and approaches, but since they are all linked, they can operate more powerfully when they are coordinated.").

and track two diplomacy."[437] Track One Diplomacy, or Official Diplomacy, is "an instrument of foreign policy for the establishment and development of contacts between the governments of different states through the use of intermediaries mutually recognized by the respective parties."[438] Most negotiations will fall under this category.[439]

Track Two Diplomacy is the "unofficial, informal interaction between members of adversary groups or nations that aims to develop strategies, influence public opinion, and organize human and material resources in ways that might help resolve their conflict."[440] The 1993 Oslo Accords between representatives of Israel and the Palestine Liberation Organization, for instance, grew out of unofficial Track Two discussions before transitioning into Track One negotiations.[441]

Track 1.5 is a hybrid type of diplomacy that may be defined as "conversations that include a mix of government officials—who participate in an unofficial capacity—and non-governmental experts, all sitting around the same table."[442] Some scholars also distinguish Track 1.5 Diplomacy in that the facilitators of such conversations are unofficial bodies or citizens.[443] The China–U.S. Strategic Nuclear Dynamics Dialogue is a vivid example of Track

---

[437] William D. Davidson & Joseph V. Montville, *Foreign Policy According to Freud*, 45 FOREIGN POL'Y 145, 157 (1981).

[438] Jeffrey Mapendere, *Track One and a Half Diplomacy and the Complementarity of Tracks*, 2 CULTURE PEACE ONLINE J. 66, 67 (2000) (citation omitted).

[439] Lia Sokol, *Multi-Track Diplomacy Explained*, NUCLEAR THREAT INITIATIVE (Apr. 19, 2022), https://www.nti.org/atomic-pulse/multi-track-diplomacy-explained/.

[440] Joseph V. Montville, *The Arrow and the Olive Branch: A Case for Track Two Diplomacy*, *in* THE PSYCHODYNAMICS OF INTERNATIONAL RELATIONS 161, 162 (Vamik D. Volkan, Joseph V. Montville & Demetrios A. Julius eds., 1991).

[441] *See* Mapendere, *supra* note 438, at 75 ("The Oslo Accord signed by Israel and the Palestine Liberation Organization was the result of joint efforts between Track Two institutions that facilitated and enhanced Track One initiatives." (citation omitted)).

[442] Jennifer Staats, Johnny Walsh & Rosarie Tucci, *A Primer on Multi-Track Diplomacy: How Does It Work?*, U.S. INST. OF PEACE (Jul. 31, 2019), https://www.usip.org/publications/2019/07/primer-multi-track-diplomacy-how-does-it-work.

[443] *See* Susan Allen Nan, *Track One-and-a-Half Diplomacy: Contributions to Georgian-South Ossetian Peacemaking*, *in* PAVING THE WAY: CONTRIBUTIONS OF INTERACTIVE CONFLICT RESOLUTION TO PEACEMAKING 161, 165 (Ronald J. Fisher ed., 2005) ("In the conflict resolution context, Track-One-and-a-Half Diplomacy is defined as diplomatic initiatives that are facilitated by unofficial bodies, but directly involve officials from the conflict in question.").

1.5 Diplomacy: from 2004 to 2019, the nonprofit Center for Strategic and International Studies and, later, the Pacific Forum used Track 1.5 Diplomacy to help create "an epistemic community between US and Chinese strategists" and to foster "frank and candid" discussions with Chinese counterparts on nuclear issues.[444]

But while the terminology itself only dates back to the 1980s, it should be noted that informal dialogue leading to official actions goes back much longer.[445] For instance, the compromise between the U.S. and Soviet delegations on the Nuclear Non-Proliferation Treaty was made during an unofficial hike in the mountains above Lake Geneva in the 1960s.[446] Nevertheless, track classification has helped us understand resources, values, and approaches necessary for each type of diplomacy.

2. Multi-Track Diplomacy for the Space-Cyber Nexus. Since 2011, when the Office of the Coordinator for Cyber Issues at the U.S. State Department was created, more than twenty-five countries have established similar institutions in their foreign ministries to deal with cybersecurity matters[447]—demonstrating the general recognition by nations that cyberattacks are global challenges and diplomacy must play a pivotal role in responding to them. This official track, as well as the work within the UN on space warfare and cyberwarfare, should be complemented by all types of multi-track diplomacy in order to achieve optimal results. Track 1.5 and Track Two Diplomacy, in particular, would help broaden the scope of the discourse, facilitate more open and frank communication, provide more in-depth understanding of the policy and governance challenges, and offer additional and alternative forums to explore

---

[444] David Santoro & Robert Gromoll, *On the Value of Nuclear Dialogue with China: A Review and Assessment of the Track 1.5 "China–US Strategic Nuclear Dynamics Dialogue,"* 20 PAC. F. (SPECIAL REP.) 1, 2, 27 (2020).

[445] Sokol, *supra* note 439.

[446] *See* Roland Timerbaev, *In Memoriam: George Bunn (1925-2013)*, ARMS CONTROL ASS'N, https://www.armscontrol.org/act/2013-06/memoriam-george-bunn-1925-2013 [https://perma.cc/469X-ZFPK] ("The creative process of finding the middle-ground formula began on a hike in the mountains, continued as we wrote down our agreed ideas on the text while riding the cable car back down, and eventually brought about results endorsed by both sides.").

[447] Chris Painter, *Diplomacy in Cyberspace: The Rise of the Internet and Cyber Technologies Constitutes One of the Central Foreign Policy Issues of the 21st Century*, FOREIGN SERV. J., June 2018, at 26, 27.

new ideas that can potentially fold into Track One dialogues or even create a venue for engagement.

C. POLYCENTRIC GOVERNANCE OF SPACE-CYBER ACTIVITIES

1. Polycentric Governance of the Commons. Polycentric (or multicentered) governance is a multilevel, multipurpose, multifunctional, and multisectoral model.[448] The study and theory of polycentric governance was developed by Vincent and Elinor Ostrom and other scholars at the Workshop in Political Theory and Policy Analysis; it came to be known as the Bloomington School of Political Economy,[449] and Elinor Ostrom was awarded the Nobel Prize "for her analysis of economic governance, especially the commons," focusing on polycentric governance.[450] According to Michael McGinnis, "The basic idea [of polycentric governance] is that any group of individuals facing some collective problem should be able to address that problem in whatever way they best see fit."[451] Polycentricity underscores the benefits of self-organization, along with coordinating regulations, norms, and market forces "at multiple levels."[452] The theory also underscores the notion that no

---

[448] *See* Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 169, 171–72 (2011) (describing the typical characteristics of polycentric governance systems).

[449] *See generally* 1 ELINOR OSTROM AND THE BLOOMINGTON SCHOOL OF POLITICAL ECONOMY: A COMPENDIUM OF KEY STATEMENTS, COLLABORATIONS, AND REACTIONS (Daniel H. Cole & Michael D. McGinnis eds., 2015) (offering a guide to Elinor Ostrom's research, the Bloomington School of Political Economy, and competing approaches to polycentricity).

[450] *Illustrated Presentation*, THE NOBEL PRIZE, https://www.nobelprize.org/prizes/economic-sciences/2009/illustrated-information/ [https://perma.cc/7GCC-2WMX].

[451] Michael D. McGinnis, Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care 1 (May 2, 2011) (unpublished manuscript prepared for presentation at the Conference on Self-Governance, Polycentricity, and Development, Renmin University of China, Beijing), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2206980 [https://perma.cc/5NNH-TC2Y].

[452] Elinor Ostrom, *Polycentric Systems as One Approach for Solving Collective-Action Problems* 1 (Ind. Univ. Workshop in Pol. Theory and Pol'y Analysis, Working Paper No. 08-6, 2008), http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/4417/W08-6_Ostrom_DLC.pdf [https://perma.cc/56MT-G3TD].

single entity can address global collective action challenges, including at the space-cyber nexus.

However, polycentric networks can also be, to a certain degree, inefficient and fragmentary, and they still must "meet standards of coherence, accountability, determinacy, [and] sustainability."[453] This fragmentation and gridlock was on display in the struggling attempts both to regulate space resource utilization and space debris and to prevent an arms race in outer space.[454] Thus, the benefits and drawbacks of polycentric governance should be critically assessed in the space-cyber context. Instead of attempting simple solutions to complex problems, a polycentric approach is multifaceted. In short, polycentric governance is:

> [A] case of decentralized governance in which there are multiple independent centers of decision-making ("governance centers"), with at least partial overlap in jurisdictions. The governance centers interact and collaborate to a certain extent, or take each other into account, in complex and ever-changing ways. Out of these seemingly uncoordinated processes of mutual adjustment, emerges the repertoire of norms and rules that guide the behavior of actors within the entire realm.[455]

In addition to states, commercial companies are gradually taking the lead in space activities and have an important role in polycentric governance systems, as do epistemic communities. The case of SpaceX demonstrates both the need to consider extending commercial companies a seat at the table when discussing space governance and the need to bring them into compliance with adopted rules. On the one hand, in response to concerns about the potential environmental challenges of Starlink satellites, SpaceX has committed to fostering "a safe orbital environment, protecting human spaceflight, and ensuring the environment is kept

---

[453] Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSPS. ON POLS. 7, 8 (2011).

[454] *See* discussion *supra* Section II.A.

[455] Eytan Tepper, *The Big Bang of Space Governance: Towards Polycentric Governance of Space Activities*, 54 N.Y.U J. INT'L L. & POL. 485, 533 (2022).

sustainable for future missions to Earth orbit and beyond" through such measures as in-space collision avoidance systems and data sharing with other firms and space agencies.[456] The company is taking the added steps of ensuring no enduring contribution to orbital debris by ensuring that their satellites are low enough to burn up in the case of failure.[457] However, the firm has previously been criticized for its cavalier treatment of international space law, going so far as to state in its Starlink Terms of Service that it will adhere to "self-governing principles" for its eventual Martian settlement.[458] As of 2024, the terms still state that "the parties recognize Mars as a free planet and that no Earth-based government has authority or sovereignty over Martian activities."[459]

SpaceX highlights the challenges of relying too heavily on private actors to practice effective self-regulation as part of a polycentric approach to tackling collective action challenges arising at the space-cyber nexus. Success often requires active engagement by all stakeholders "who must share a sense of responsibility to the customers and mutual trust in one another."[460] This is not easy to build in any community, but governments can play a helpful coordinating function, as is explored further below.

---

[456] Elizabeth Howell, *SpaceX Promises Sustainability and Safety for Starlink Constellation*, SPACE.COM (Mar. 2, 2022), https://www.space.com/spacex-sustainability-safety-starlink-satellite-megaconstellation [https://perma.cc/HFF7-ZLVE].

[457] *See id*. (listing among the key practices for Space X's Starlink "[o]perating at low altitudes . . . to ensure no persistent debris, even in the unlikely event a satellite fails on orbit").

[458] *See Starlink Terms of Service*, STARLINK, https://www.starlink.com/legal/documents/DOC-1020-91087-64 [https://perma.cc/9F6J-Y7VA] ("For Services provided on Mars, or in transit to Mars via Starship or other spacecraft, the parties recognize Mars as a free planet and that no Earth-based government has authority or sovereignty over Martian activities. Accordingly, [d]isputes will be settled through self-governing principles, established in good faith, at the time of Martian settlement."); *see also* Anthony Cuthbertson, *Elon Musk's SpaceX Will 'Make its Own Laws on Mars,'* THE INDEPENDENT (Oct. 28, 2020, 11:34 PM), https://www.independent.co.uk/space/elon-musk-spacex-mars-laws-starlink-b1396023.html [https://perma.cc/F494-B986] (interpreting the relevant language in Starlink's Terms of Service to mean that SpaceX will not recognize international law on Mars).

[459] STARLINK, *supra* note 458.

[460] Scott Shackelford, *Companies' Self-Regulation Doesn't Have to be Bad for the Public*, THE CONVERSATION (June 12, 2019, 7:30 AM), https://theconversation.com/companies-self-regulation-doesnt-have-to-be-bad-for-the-public-117565 [https://perma.cc/6635-HVQE].

2. Polycentric Governance of Space-Cyber Activities. The space lawmaking process in the UN has proven to be inefficient and non-optimized for the rapidly growing space and space-cyber domains. Under normal circumstances, proposed space-centric resolutions originate in the UN Committee on the Peaceful Uses of Outer Space (COPUOS), where they must achieve consensus in order to be escalated to the UNGA for a vote.[461] While this somewhat tedious process has nevertheless led to the introduction of the five space law treaties we have today, adopted between 1967 and 1979, no new treaty has been adopted since,[462] and COPUOS, now one of the largest UN committees, struggles to achieve consensus amongst its 102 members.[463] The custom to adopt decisions within COPUOS by consensus is key for ensuring wide acceptance of the adopted rules, but over time it "has become something of a straitjacket."[464]

As space activities and actors soared in scope and variety, and the legal framework struggled to keep up to date with the developments, today's space lawmaking is increasingly introduced by various off-UN forums and by national, bilateral and minilateral[465] efforts. In fact, it was an inter-agency committee that developed the Space Debris Mitigation Guidelines that were later adopted by COPUOS and the UNGA, and university research centers initiate and lead groups of experts that introduce important instruments on key topics—from the utilization of space resources

---

[461] *See* SCOTT J. SHACKELFORD, GOVERNING NEW FRONTIERS IN THE INFORMATION AGE 328 (2020) (explaining the "cumbersome" consensus requirements needed for COPUOS resolutions to be brought to the UNGA for a vote); *see also* Tepper, *supra* note 455, at 488–89, 491 (further discussing the difficulties in the lawmaking process within COPUOS).

[462] See *supra* Section IV.A.3 for a discussion of the five existing space treaties.

[463] *See Members of the Committee on the Peaceful Uses of Outer Space*, UNITED NATIONS OFF. FOR OUTER SPACE AFFS., https://www.unoosa.org/oosa/en/members/index.html [https://perma.cc/M6YG-5WFP] (indicating that COPUOS has 102 member states).

[464] SHACKELFORD, *supra* note 461, at 328.

[465] *See* Nickolay Mladenov, *Minilateralism: A Concept That Is Changing the World Order*, THE WASH. INST. FOR NEAR E. POL'Y (Apr. 14, 2023), https://www.washingtoninstitute.org/policy-analysis/minilateralism-concept-changing-world-order [https://perma.cc/U57J-N9FN] ("'Minilateralism' [is] an international relations concept that involves small groups of nations collaborating to tackle problems or pursue mutual goals.").

to military uses of outer space.[466] Indeed, space governance has already transitioned from a monocentric to a polycentric system.[467]

From a massive empirical database, Elinor Ostrom distilled eight design principles that correlate with robust governance systems,[468] and a selection of these may be adapted to the governance of the space-cyber nexus. Accordingly, the following features of polycentric systems are important to consider for the long-term sustainability of the final frontier.

First, nonbinding agreements and instruments may be reinforced by multiple regulatory scales.[469] This allows for greater flexibility under certain circumstances while promoting overall adherence—as opposed to inflexible standards. Additionally, such instruments would have the benefit of applying to a diversity of actors rather than just to states under a more traditional treaty framework.

Second, clarifying legal ambiguities and formalizing norms of behavior serve to better define graduated sanctions for potential rule violators, along with ensuring the efficacy of dispute resolution.[470]

---

[466] *See* Tepper, *supra* note 455, at 504, 512, 514 (explaining the inter-agency foundations of the Space Debris Mitigation Guidelines, noting resolutions adapted by COPUOS and the U.N. General Assembly, and discussing the university research centers involved in developing awareness of space, generally, and military uses of space, specifically); *see also* UNITED NATIONS OFF. FOR OUTER SPACE AFFS., SPACE DEBRIS MITIGATION GUIDELINES OF THE COMMITTEE ON THE PEACEFUL USES OF OUTER SPACE iii–iv (2010) (explaining the foundations of peaceful approaches to using and sharing space resources); *The Hague International Space Resources Governance Working Group*, UNIVERSITEIT LEIDEN, https://www.universiteitleiden.nl/en/law/institute-of-public-law/institute-of-air-space-law/the-hague-space-resources-governance-working-group [https://perma.cc/UL9M-8R2U] (noting the university research centers involved in developing plans for using space resources).

[467] *Cf.* Tepper, *supra* note 455, at 491 ("Comprehensive monocentric governance is simply no longer feasible.").

[468] Ostrom, *supra* note 30, at 652–53 (outlining the eight design principles associated with successful government institutions).

[469] *See, e.g.*, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) (setting forth the policy of President Obama's Administration to work collaboratively with private owners of cyber infrastructure to achieve enhanced cybersecurity and resilience).

[470] *See* Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES IN BUILDING GOVERNANCE MECHANISMS 105, 121–22 (Eric Brousseau, Tom

Third, nested enterprises are central to the success of these institutions according to Elinor Ostrom, who posited that larger institutions are important for "govern[ing] the interdependencies among smaller [governance] units,"[471] thereby emphasizing the necessity of efficient multi-stakeholder governance with higher coordination rather than coercion. Specifically, COPUOS and the UN Office of Outer Space Affairs are well positioned to serve as higher-order coordinators. Already, many regulatory initiatives prepared by off-UN forums are subsequently presented at COPUOS. The Hague International Space Resources Governance Working Group was such an off-UN forum whose results were presented at COPUOS.[472]

3. Bottom-Up Regulation of the Space-Cyber Nexus. The space-cyber nexus gained high-level attention only recently, pursuant to the attack on Viasat. It is therefore unsurprising that governance efforts to address it are in their infancy. This also applies to bottom-up efforts, but those efforts that have started would still provide key parts of the puzzle in the governance of the space-cyber nexus.

One project, launched before the invasion of Ukraine, brought together global stakeholders to discuss governance responses to the emerging space-cyber nexus, with the aim of identifying shared norms and the international law applicable to space-cyber warfare.[473] Although progress was stalled by rising global conflicts, this project would address the new nexus with an integrated approach of a single domain instead of a space approach to cybersecurity or vice versa.

The International Organization for Standardization (ISO)—a nongovernmental, industry-focused creator of widely accepted

---

Dedeurwaerdere, Pierre-André Jouvet & Marc Willinger eds., 2012) (examining graduated sanctions and dispute resolution as design principles of polycentric governance).

[471] *Id*. at 122.

[472] UNIVERSITEIT LEIDEN, *supra* note 466.

[473] *See Space-Cyber Governance*, CAN. RSCH. CHAIR IN INT'L POL. ECON., https://www.chaire-epi.ulaval.ca/en/space-cyber [https://perma.cc/KDQ2-F3TE] ("[W]ith the aim of identifying the international law applicable to space-cyber warfare and principles . . . for responsible space-cyber behavior that will represent[] a broad consensus, this project brings together a cohort of scholars, experts, and practitioners from around the world to discuss governance responses to the merging nexus of space-cyber.").

cybersecurity frameworks[474]—has also begun the development of voluntary guidelines for mitigating and responding to space cybersecurity incidents.[475] Although the standard has not yet been finalized, the success of other ISO frameworks suggests that it would play an influential, bottom-up role in space-cyber governance. After all, ISO/IEC 27001, an ISO-developed cybersecurity framework, has already become one of the most influential cybersecurity frameworks in the world, experiencing sustained growth in its adoption since its initial publication.[476] Although unclear whether the ISO space-cyber guidelines will highlight the new risk of conflict-based space-cyber attacks, the guidelines will undoubtedly still influence how organizations and industries adjust to new threat scenarios in space, just as ISO/IEC 27001 has inherently influenced cybersecurity norms through its widespread adoption.[477]

Another potential source for bottom-up space cyber governance is the Institute of Electrical and Electronics Engineers (IEEE), an international professional association that, like the ISO, develops industry standards but, unlike the ISO, focuses on electronic systems.[478] The IEEE recently established an international working group to tackle space cybersecurity issues[479] and is in the process of developing a standard that will "define[] cybersecurity controls for space systems including modules for the ground system, space

---

[474] *See, e.g.*, ISO/IEC 27001, INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION—INFORMATION SECURITY MANAGEMENT SYSTEMS—REQUIREMENTS iv (3d ed. 2022) (describing and providing background on the ISO).

[475] ISO/TS 20517, SPACE SYSTEMS—CYBERSECURITY MANAGEMENT REQUIREMENTS AND RECOMMENDATIONS (1st ed. 2024).

[476] MONA MIRTSCH, JAKOB POHLISCH & KNUT BLIND, ASS'N FOR INFO. SYS., INTERNATIONAL DIFFUSION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD ISO/IEC 27001: EXPLORING THE ROLE OF CULTURE (2020).

[477] *See id.* at 2 (explaining the popularity and growth rate of the standard).

[478] *See Developing Standards*, IEEE STANDARDS ASS'N, https://standards.ieee.org/develop/ [https://perma.cc/G82C-4ETU] ("As a global standards development organization, IEEE supports and advocates a set of standards development principles, executed by the IEEE Standards Association (IEEE SA). These principles provide a community for voluntary cooperation among interested parties and stakeholders, enable technical excellence, global interoperability, and innovation to foster economic growth and society prosperity.").

[479] *See P3349 – Space System Cybersecurity Working Group*, IEEE STANDARDS ASS'N, https://sagroups.ieee.org/3349/the-project/ [https://perma.cc/PXZ3-YWWC] (detailing the five subcommittees tasked with developing a standard).

vehicle, link segment, and the integration layer."[480] The IEEE standard is expected to play a critical role in the bottom-up promotion of space-cyber governance.

Albeit in a less comprehensive way than the standards developed by the ISO and the IEEE, other nongovernmental organizations also have the potential to influence the governance of the space-cyber nexus. One organization, the European Cooperation for Space Standardization (ECSS), was established "to develop a coherent, single set of user-friendly standards for use in all European space activities."[481] While the ECSS has not yet introduced a standard for cybersecurity of space systems, it is a potential future source for such a standard that, regardless of its legally binding nature, would have an effect across the European space sector. Similarly, the Consultative Committee for Space Data Systems (CCSDS), a collaboration between governmental space agencies, has provided limited cybersecurity standardization recommendations for a variety of critical space systems.[482] Thus, although ECSS and CCSDS have not yet developed fully comprehensive standards like those currently proposed by ISO and IEEE, their contributions may nevertheless play an important role in bottom-up governance of the space-cyber nexus. Overall, given the forthcoming comprehensive space-cybersecurity frameworks and already extant noncomprehensive standards developed by nongovernmental organizations, it seems apparent that such organizations have the

---

[480] *P3349 – Standard for Space System Cybersecurity*, IEEE STANDARDS ASS'N, https://standards.ieee.org/ieee/3349/11182/ [https://perma.cc/WYX7-SEJD]; *see also* GREGORY FALCO ET AL., IEEE STANDARDS ASS'N, AN INTERNATIONAL TECHNICAL STANDARD FOR COMMERCIAL SPACE SYSTEM CYBERSECURITY – A CALL TO ACTION 3 (2022) ("Given the current market and threat landscape, a strategic, systematic effort is necessary to address new mission cybersecurity challenges in a rigorous, technical manner. . . . This paper is a call for action to the space systems community to formulate a technical standards committee that will define cybersecurity technical requirements . . . encompassing the ground segment, space segment, user segment, link segment and the integration layer across the system of systems.").

[481] EUR. COOP. FOR SPACE STANDARDIZATION, https://ecss.nl/ [https://perma.cc/Y6AA-X4QL].

[482] *See* FALCO ET AL., *supra* note 480, at 4–5 (discussing the role of the CCSDS and the need for additional security); *see also* CONSULTATIVE COMM. FOR SPACE DATA SYS., RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS: SPACE DATA LINK SECURITY PROTOCOL iv, 1–2 (2022) (listing the CCSDS agencies and detailing the purpose, scope, applicability, and rationale of the standard).

potential to promote governance of the space-cyber nexus from the bottom up. In the aggregate, these bottom-up initiatives, as well as other nonbinding agreements and instruments to be negotiated and adopted by other forums, are all part of the in-the-making array of instruments that could provide the governance of the space-cyber nexus.

VI. Conclusion

The new warfare domains of space and cyberspace have merged into the space-cyber nexus, which poses risks to space-based infrastructure and are critical to security and the economy. The cyberattack on Viasat on the eve of the Russian invasion of Ukraine demonstrated the benefits and temptation of launching cyberattacks on space systems, and such attacks will be part of future armed conflict.

States have only just begun to respond to these new challenges at the national level, and at the international level, governance responses and the laws of space-cyber warfare have also yet to be developed. It is therefore necessary to identify common norms and introduce widely agreed-upon rules to apply to space-cyber warfare, just as such rules are needed for the other warfare domains.

Considering the inherent and increasing difficulties in introducing new legally binding international treaties, there is a need for pathways that complement the work of long-standing multilateral institutions. This Article has suggested a polycentric approach to the gradual development of the laws of space-cyber warfare that will produce an array of nonbinding instruments put forward by multiple forums, including informal forums and Track 1.5 and Track Two Diplomacy. Such a polycentric approach is a feasible way to progressively develop the laws of space-cyber warfare that one day may be codified into legally binding instruments.