Centre for International
Governance Innovation

CIGI Papers No. 287 — November 2023

Clearing the Fog
The Grey Zones of Space Governance

Jessica West and Jordan Miller

Centre for International
Governance Innovation

CIGI Papers No. 287 — November 2023

Clearing the Fog
The Grey Zones of Space Governance

Jessica West and Jordan Miller

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Program Manager Jenny Thiel
Senior Publications Editor Jennifer Goyder
Publications Editor Susan Bubak
Graphic Designer Abhilasha Dewan

For publications enquiries, please contact publications@cigionline.org.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Jessica West is a CIGI senior fellow and a senior researcher at Project Ploughshares, a Canadian peace and security research institute, where she focuses on technology, security and governance in outer space. She has held this position since 2015 and previously worked there on space security and nuclear disarmament issues (2006–2009). As part of her work at Project Ploughshares, Jessica served for seven years as the program manager of the international research consortia responsible for the Space Security Index project, and as managing editor for the 2007–2009 and 2016–2019 publications. She interacts regularly with key UN bodies tasked with space security and sustainability issues. Jessica is also a research fellow at the Kindred Credit Union Centre for Peace Advancement at Conrad Grebel University College at the University of Waterloo, a member of the North American and Arctic Defense Research Network, and a member of the Canadian Pugwash Group.

Jordan Miller is a Ph.D. student at the Royal Military College of Canada, where he is studying the role of information operations in international politics, war and in competition below the threshold of armed conflict. He is also the director of marketing and brand strategy with Calian Group, and is the vice-chair of the Public Policy and Advocacy Committee for Space Canada, where he has authored policy position papers and spoken on panels about the role of space capabilities for defence and national security.

Acronyms and Abbreviations

AI	artificial intelligence
ASAT	anti-satellite
GGE	Group of Governmental Experts
IHL	international humanitarian law
IoT	Internet of Things
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
OEWG	Open-Ended Working Group
OST	Outer Space Treaty
RCM	RADARSAT Constellation Mission
RPO	rendezvous-and-proximity operations
SSA	space situational awareness

Executive Summary

The term "grey zone" is frequently invoked in military and national security contexts to refer to a perceived blurring of conventional notions of war and peace illustrated by harmful activities that fall below the threshold of armed conflict. In space, such activities include non-kinetic sources of interference with space systems such as cyber. Yet, while the concept clearly resonates with contemporary experiences of competition and conflict, its growing use has been followed by criticism from some academics and analysts who question its novelty, precision and utility. The objective here is to develop a more nuanced understanding of the grey zone that takes into consideration its multiple sources, dangers and harms.

The authors begin by shifting focus from the grey zone as a description of tactics to a problem of governance. Specifically, grey zones are approached as spaces in which the *rules of governance and conduct* are not clear or are contested. While there is a body of well-established international space law that provides aspirations, principles and parameters to guide human activity in outer space that are rooted in the 1967 Outer Space Treaty (OST), a sense of governance gaps, unsettled questions and vagueness is pervasive. These uncertainties are particularly pronounced in the context of rapidly changing activities and technical capabilities in outer space. Identifying these lacunae as the source of greyness in space governance, the authors argue that grey zone conflict in outer space is part of a persistent failure to adequately govern peaceful space activities in outer space.

The implications of these grey zones in space governance extend far beyond space. Peeling back the layers of opacity that shroud the grey zone, the paper explores three entangled governance challenges that reveal the complexity of its sources, scope and harms.

Stronger governance measures are needed. The paper concludes by outlining opportunities for providing some colour in the grey zones of space governance by clarifying the parameters and rules of peaceful uses of outer space, making space activities and their potential harms more visible, and pursuing cross-domain governance discussions. Such efforts must be broad and layered, incorporating a variety of means, mechanisms and actors. At a time when the global governance of outer space is pulling in different directions, engagement across perspectives and initiatives is essential to avoid fragmented governance that would exacerbate rather than clarify the grey and potentially stifle the innovative uses of space that are driving our current era of human activity.

Introduction

Outer space is everywhere. No longer confined to the vastness beyond Earth, outer space has been integrated by humans into our homes, travel, education, work and human connections. Today, space is — literally as well as figuratively — in our pockets.

The global commercial space industry is growing at a breathtaking rate. In dollar value, forecasts peg it at just under US$1 trillion by 2040 and up to US$2.7 trillion by 2045 (Crane et al. 2020). But space has more than a dollar value. New ways to utilize outer space are allowing us to accumulate and analyze unprecedented amounts of data, increase connectivity around the globe, acquire new knowledge about our galaxy and initiate a nascent off-planet economy. Space is now at the core of human innovation.

Good global governance is needed to sustain this ability to use and benefit from outer space. While space is not a lawless "frontier," neither is it a sanctuary from political conflict.[1] As has been said perhaps too often, space is "congested, contested, and competitive" (Department of Defense and Office of the Director of National Intelligence 2011). In recent years, these features have been linked to an increased prominence in defence, military and foreign policy discussions with "grey zones" and "hybrid warfare."[2] These terms denote activities that are deemed aggressive, competitive and even harmful, but fall short of armed violence or the use of force; included are information, cyber, economic and political actions intended to maximize national benefit but stop short of war.

1 See Kenney (2021) and Dickey (2020).

2 See Department of National Defence (2017), Robinson (2022) and Bilal (2021).

The term "grey zone" is used by militaries to indicate the absence of boundaries between conventional notions of war and peace, and the use of non-kinetic and innovative tactics that fall between these two thresholds (Morris et al. 2019, 8). Because it is so broad, this concept can obscure more than it illuminates (Arquilla 2018). Yet the authors believe that the term retains value, not least because it reflects an experience of competition and conflict that clearly resonates with many. Obscurity — or fogginess — is part of that experience. The task here is to help bring about a more nuanced understanding of the sources, dangers and harms that lurk unseen in the greyness.

The paper begins by shifting the focus on the grey zone from a matter of tactics to a problem of governance. Specifically, grey zones are approached as spaces in which the rules of governance and conduct are not clear or are contested. The implication is that the associated challenges will not likely be addressed only with military tools but will also require stronger governance measures that illuminate the features of grey zones and reduce uncertainty.

Building on earlier research published by CIGI on the space-cyber nexus, the authors find that there is not one grey zone, but a cluster of nebulous governance challenges that are set to grow as our use of outer space not only expands but evolves in unexpected ways (Shull, Wark and West 2023). The ultimate challenge, then, is to colour in governance frameworks so that less grey — less ambiguity — remains.

In this paper, the authors peel back the layers of opacity that shroud the grey zone to reveal some of these unsettled governance issues that give rise to it, expand its scope and result in hidden harms. The analysis flows from the military concept of grey zone tactics to an identification of three entangled governance challenges:

- the intermingling of space with terrestrial domains and capabilities;
- the blending of war and peace in outer space, which the authors refer to as the "fog of peace"; and
- the human elements of space systems.

The paper concludes by discussing governance approaches to reduce the scope and harmful effects of grey zones in outer space by better defining the contours of peaceful and non-peaceful uses of outer space, making space activities and their potential harms more visible, and pursuing cross-domain governance discussions that include efforts to put humans at the forefront of security. Like the grey zone itself, the answer is not singular, but requires multiple and overlapping initiatives across numerous institutions and actors.

Now is the time to unpack the greyness. We are entering a new era of governance, as evidenced by diplomatic initiatives such as the UN Open-Ended Working Group (OEWG) on reducing space threats and the upcoming UN Group of Governmental Experts (GGE) on Further Practical Measures for the Prevention of an Arms Race in Outer Space, bilateral initiatives such as the Artemis Accords, technical processes to set standards at the International Organization for Standardization (ISO) and the unprecedented expansion of commercial and government activities and capabilities in space. Stronger governance is necessary not only to maintain outer space as a domain that can remain peaceful for all to use, but also to facilitate the innovative uses of space that are driving this new era of human activity.

Grey Zones as a Governance Challenge

Much about grey zones is familiar. The concept reminds us of the Cold War standoff between the United States and the Soviet Union, when direct confrontation risked escalation to the use of nuclear weapons (Stoker and Whiteside 2020, 26). Moreover, competition between states has long integrated all elements of national power — military, economic, alliances — to either deter an enemy from aggressive action or compel them to stop aggressive action once it starts (Echevarria 2016, 1–11). The term has been applied to many types of activities and interactions across various domains. Some claim that it is overused, an example of "academic fashion" that is superficial, vague and fading quickly (Libiseller 2023). While it might be fashionable, the idea of a grey zone retains its usefulness, particularly from the vantage point of governance.

Since the end of the Cold War, the term has gained prominence in both policy and academic circles. Among practitioners, the emphasis is on tactics and strategy of conflict. The 1999 book *Unrestricted Warfare*, written by two Chinese army colonels, argues that the concepts of peace and war are no longer useful in defining how great powers interact — competition is the constant, whether military power is involved or not (Liang and Xiangsui 2015; translated from the original). The 2010 US *Quadrennial Defense Review* is one of the first Western political documents to invoke the concept of a grey zone, which it defines as an ambiguous area of contemporary conflict that is "neither fully war nor fully peace" (Department of Defense 2010, 73). In Canada's defence policy, *Strong, Secure, Engaged,* discussion of the grey zone refers to the use of coordinated diplomatic, informational, cyber, military and economic interests to achieve strategic objectives, often through the use of information operations to create confusion and ambiguity and maintain deniability over direct or sponsored actions (Department of National Defence 2017, 53).

This focus on tactics means that the grey zone is often linked with hybrid warfare — the use of unconventional tactics and irregular modes of force. Because such tactics often fall short of armed violence, they can enable grey zone conflict, but the two concepts are not synonymous (Dowse and Bachmann 2019). Yet such conceptual confusion points to the pitfalls of approaching the grey zone narrowly as only a matter of the means and methods of warfare.

Additionally, a focus on tactics often involves invoking the grey zone as an accusation to describe the activities of others, in particular Russia and China. Such accusations flow both ways. For example, the so-called Gerasimov doctrine was viewed by the West as a Russian perspective on combining the application of military power with an international communications and information operations campaign. In fact, Gerasimov was describing what he saw as American military operations in the 1990s that leveraged information campaigns and UN resolutions to justify US political and military interventions in Somalia, Haiti and the Balkans (Fridman 2018).

Moving beyond tactics, academic and think tank literature has focused on teasing out the qualities of the grey zone as a distinct mode of contemporary conflict. Core concepts include notions of extreme competition (Hernández-García 2022), and coercion (Brands 2016; Wirtz 2017; Azad, Haider and Sadiq 2023; Jordan 2020), as well as objectives such as "provocation without escalation" (Luo 2022), which point to challenges with traditional understandings of deterrence. Such conceptual work emphasizes the grey zone as a new problem space for militaries. Yet critics rightfully push back against what they see as a trend to label everything short of conventional warfare "grey zone warfare" (Brands 2016).

The authors' own approach views the grey zone not as a singular construct or challenge, but as a feature of governance. This sense of the grey zone as an outcome of governance — or lack thereof — is present in both prominent uses and critiques of the term. For example, a white paper from the United States Special Operations Command (2015, 1) highlights "uncertainty about the relevant policy and legal frameworks." Similarly, Canada's current defence policy refers to a "fog" that "exists just below the threshold of armed conflict" (Department of National Defence 2017, 53). Analysts who criticize the use of the term have likewise described it as a "fuzzy domain" where the rules are unclear (Scott 2022) and have accused Western states in particular of giving rise to the grey zone by lacking resolve to enforce existing rules (Jonsson 2022). In wider global governance literature, the grey zone speaks to areas where international rules can be bent, ignored or remade (Drache and Jacobs 2018).

An emphasis on governance also underlies descriptions of the objectives of activities said to take place in the grey zone, namely undermining rules or making new ones. Analysts often epitomize grey zone aggression as having revisionist intentions (Hernández-García 2022) and exploiting uncertainty to "eat away at the status quo one nibble at a time" (Brands 2016). Often described as "prodding" (Layton 2023), grey zone tactics are said to "impose quandaries on custodians of an existing order" (Holmes and Yoshihara 2017, 323). For this reason, grey zones are described as features of an era marked by "great power rivalry" (Mazarr 2022) offering a welcome outlet for competition that does not involve direct military confrontation (Monaghan 2021).

The authors view grey zones as both a problem of and problem for governance. As a problem of governance, they flow from ambiguity of law, rules, technology and even the nature of activities themselves. Although falling short of armed

conflict, the potential effects of activities that seek to exploit ambiguity can be far from benign. Uncertainty of rules and thresholds in the grey zone can allow conflict to escalate in unpredictable ways, "due to unclear norms of behaviour and escalation thresholds, complex domain interactions, and new capabilities" (Department of Defense 2022, 6). Amid such uncertainty, states may have different interpretations of what constitutes a proportional response; such differences could lead to misunderstandings and misinterpretations of intention and actions.

Legitimate military responses are limited. The US *National Defense Strategy* raises this challenge when it identifies a lack of consensus on what constitutes a proportional response to non-kinetic attacks on cyber and space infrastructure as the source of a risk of inadvertent crisis escalation. Insights from the cyber domain, where attacks remain persistent, suggest that not only is deterrence not working (Soesanto and Smeets 2021), but that such binary concepts are ill suited for more complex operating environments such as cyberspace, which the authors would argue also applies to outer space (Iasiello 2013; Smeets and Soesanto 2020; McKenzie 2017). This is particularly dangerous in an era when nuclear-armed states increasingly rely on nuclear arsenals to extend deterrence to non-nuclear threats.

Importantly, as the analysis in this paper makes clear, grey zone actions can cause harm, even if there is no armed conflict. Not only can "below threshold" actions escalate to nuclear confrontation, but so-called non-violent activities can themselves inflict damage, not least because they often take place in civilian spaces. Thus, minimizing the scope and effects of such competition is worthwhile. This makes grey zones a problem for governance, and a problem for everyone.

Grey Zones in Space Governance

As in other domains, invocations of the grey zone concept to outer space are often used to describe actions other than the use of kinetic military power, including cyber operations, information warfare, electronic interference with satellite signals and the use of directed energy to dazzle or temporarily blind satellite sensors (Steer 2023). These activities do not result in physical destruction of objects but can have a significant effect on the space systems being targeted and the security of the data flowing through them. For example, the North Atlantic Treaty Organization's (NATO's) space policy notes that potential adversaries have the capability to hold space assets at risk, deny or degrade critical space-based capabilities, and negatively impact public use of space systems, yet this capability "fall[s] below the thresholds of threat of force, use of force, armed attack or aggression" (NATO 2022). Nonetheless, such activities are increasingly described to the public in terms of "attacks" or a state of "siege" (Trevithick 2021).

While such statements might be attributed to the general escalation of warfighting rhetoric associated with military activities in outer space, they also point to a fundamental source of insecurity. For example, interference with space systems can have wide-reaching ramifications, including on critical infrastructure, such as electricity grids, that is dependent on such systems. Yet a focus on tactical activities means that the specifics of space governance that enable such actions, as well as their broader consequences, are rarely questioned. Instead, hostile actions and persistent insecurity become normalized.

Existing Space Governance

Challenges related to space governance are not due to a lack of laws or treaties that apply to outer space per se. There is a body of well-established international space law that provides aspirations, principles and parameters to guide human activity in outer space. At the heart of this framework is the 1967 OST.

Among the clearest stipulation of the OST is that international law, including the UN Charter, applies to outer space. Other principles declare that all states share an equal right to use and explore outer space; such activities should be for the benefit of humanity; and states should exercise due regard for others and avoid harmful interference when conducting space activities. The placement or orbiting of nuclear or other weapons of mass destruction is prohibited, as are military activities or installations on the Moon or other celestial bodies. And states bear responsibility

and liability for their own actions and those of national non-state entities in outer space.

The OST thus provides the foundation for effective governance. Some pieces of this foundation have been further developed in subsequent agreements, including the Agreement on the Rescue of Astronauts, the Registration Convention and the Liability Convention (the Moon Agreement lacks significant state ratification).

Nonetheless, the sense of governance gaps in outer space is pervasive. One challenge is a lack of detail: numerous core principles in the OST regarding the use of space, such as due regard, have never been clarified in practice. Others point to tensions between core principles. Both Melanie K. Saunders (2021) and Cristian van Eijk (2022) have described the principles of freedom and equality as conflicting and even opposing principles that limit the realization of the latter. The notion of sovereignty is another source of tension. Outer space is not subject to claims of national appropriation, but states maintain national jurisdiction over their activities and objects in outer space (von der Dunk 2002). Peaceful use is also a conflicted concept, said to be "agreed upon in principle" but "disputed in substance" (Su 2022).

Legal uncertainty also arises from the overlap between space and other governance jurisdictions. Space systems operate across domains that reach from Earth to space through digital and cyber connections and are thus subject to space law, international law and international humanitarian law (IHL), which are sometimes at odds (von der Dunk 2021).

Domestic laws also apply, serving as the primary mode by which the principles of the OST are implemented. But the laws of different states can offer competing interpretations and inconsistent applications. For example, various approaches to domestic licensing and regulation of private sector resource extraction activities have unfolded despite lack of international consensus on the meaning of the OST's ban on "national appropriation" in this context (DePagter 2022). And more states are signing on to the Artemis Accords to enable new multinational and commercial activities on the Moon. Likewise, national frameworks are emerging to regulate the use of emerging technologies in outer space, such as satellite servicing capabilities. These developments further demonstrate the growing commercial reality of the grey zone.

There is thus a growing sense that the nature of space activity today is outpacing existing governance. In their new book *Who Owns Outer Space? International Law, Astrophysics, and the Sustainable Development of Space*, Michael Byers and Aaron Boley (2023) raise a series of unsettled governance questions that have produced fundamentally different answers.

Returning to the concept of the grey zone, scholarship has also attributed this to changes in technology that have outpaced the governance of war. Although not specific to space, Dale Stephens (2020) points to the physicality of legal understandings of armed conflict and attacks on the one hand, and the proliferation of non-physical capabilities and targets and non-lethal means of inflicting harm on the other. For example, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* indicates that most states view harmful cyber operations as "attacks" only when they result in physical injury, death, damage or destruction (Schmitt 2017).

Each of these lacunae provide sources of greyness in space governance. Importantly, rather than a problem with the governance of war or armed conflict, they point to gaps in the governance of peace.

And this is the crux of the paper's argument: that grey zone conflict in outer space is closely linked to a persistent failure to adequately govern peaceful space activities. But the scope of the challenge is wider than this. Beginning with the connectedness of outer space to earthly domains, these linkages are explored as both an accelerator of uncertainty and ambiguity and an exacerbator of the potential resulting harms. Finally, attention is turned to the human elements of space systems that too often are lost in the fog, which demand a new understanding of the nature of space systems, their vulnerabilities and the implications of their use and harm.

Earth-Space Continuum

Space is not a vacuum. Analyst Robin Dickey (2020) calls the persistent belief in the separateness and specialness of space as an isolated environment the "myth of sanctuary." Indeed, space systems themselves are not only in space. Satellites depend on a global array of ground infrastructure and computer systems to operate and end-user terminals to provide service. The connections are not only physical. A constant stream of data

from satellites to Earth animates television, radio and telecommunications; enables cyberspace; provides intelligence collection to inform national security and defence decision making; and makes military force deployment around the world possible. And just as space affects many activities on Earth, Earth activities also affect space.

This overlap with earthly domains expands the scope of the grey zone in space governance and exacerbates the effects. Although the overlaps are many, three sources of interaction — cyber, data, and nuclear warning and command and control — are illustrative.

Cyber

Although military planning and global governance policy treat outer space and cyber as separate domains, they are intimately linked. Cyber is enabled by foundational capabilities for global timing and synchronization provided by satellite-based systems such as GPS. At the same time, space systems — networks of satellites, ground stations, computer systems, software, end users — are increasingly digital and rely on cyber connectivity to function. The cyber domain is involved in everything related to the flow of data between computer systems and networks. But that same domain also contains threatening cyber intrusions that target the systems that collect, transmit, use and control the flow of data, as well as the data itself.

Although satellites can be hacked, with grave effect across the space system, ground stations, which transmit and receive satellite data, and end-user terminals, are also vulnerable and an easier target of interference (Hadley 2023). Indeed, Russia interfered with the Viasat system in Ukraine by targeting a vulnerability in end-user ground-based modems to distribute a massive denial of service attack throughout the network (Burgess 2022). The Viasat example shows that a successful attack on a single node can provide the attacker with access to a much broader network, and therefore the ability to generate significant, rippling effects. In another example from August 2022, researchers successfully hacked into the Starlink network from a terminal on land, bypassing security features to upload malicious code (Wouters 2022).

Such vulnerability to cyber interference is significant. Tracking by the Center for Strategic and International Studies shows the number of incidents among Western states growing in number and intensity.[3]

Yet governance of space and cyber capabilities and activities remains siloed (Shull and Aganaba 2023). Recent efforts to clarify the applicability of existing law to cyberspace through the *Tallinn Manual* and the *McGill Manual* of the military uses of outer space barely reference the other domain. This gap both contributes to grey zone activities in space and is exploited to resist additional governance measures. For example, China insisted that efforts to discuss cyberthreats to space systems at the UN OEWG were misplaced, claiming that as a terrestrial domain, cyber is regulated by other legal frameworks (West 2023a).

Not only is the overlap of space and cyber activities poorly reflected in global governance, but there are also gaps remaining between principles adopted across these domains. For example, while the United Nations has agreed to a voluntary norm against cyber interference with critical infrastructure (Hogeveen 2022, 13), states have been slow to recognize a similar link to protection for critical infrastructure and space systems (see below).

Data

Data, among the core raison d'être of space systems, provides another important connection between space and Earth. Although by no means limited to military uses, data and the ability to transmit it are increasingly the life blood of military operations on Earth, predicated on situational awareness, precision navigation and instantaneous global communications to deliver effective force more precisely than ever before (Barnett 2004, 194; Echevarria 2021, 199–200). As Laetitia Cessari (2023) has written, today's battlefield is digital, requiring constant flows of, and command over, data. This emphasis on data is likewise reflected in China's concept of "informationalized" battlefields that integrate space and information technologies (Yuan 2023; State Council Information Office of the People's Republic of China 2019).

This emphasis on data is not only a military phenomenon. The small satellite revolution has helped to spur the big data revolution — a dizzying array of new applications that employ artificial

3 See www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

intelligence (AI) and machine learning — that is described as "pervasive global surveillance and high-speed, high-volume analytics" (Pekkanen, Aoki and Mittleman 2022). Satellites provide us with the data (almost all commercial) that allows us to detect, attribute and classify almost all human activities on Earth (Pekkanen 2022). How data is used and by whom is nebulous: "satellite imagery is non-discriminatory — it sees a civilian school bus the same way it sees a tank" (ibid.).

Data is also vulnerable and fragile. It can be stolen. It can be damaged. It can be manipulated. And it can be misused.

In the past, spoofing of GPS signals directed ships off course; more recently, data manipulation has concealed those ships (Goward 2020). Today, Earth-imaging data can be manipulated to create "fake geography" that can be used in disinformation campaigns (Zhao et al. 2021). Manipulated data has the potential to be inserted into the countless applications that draw on space data for automated systems or AI, including future weapons systems.

While we are beginning to have a global discussion on the governance of internet data (Kuzio et al. 2022; Medhora 2018), issues related to how space data is used and accessed, and by whom, are not yet on the public radar. Ripple effects of the confluence of space, cyber and data are bound to become more widespread and common with the rise of the Internet of Things (IoT), which creates complex webs of connected computing devices, machines, data, objects and people. Space systems are a central IoT component.

Strategic Early Warning and Nuclear Weapons

Today Earth is home to more than 12,000 nuclear warheads. Most are kept on high alert for rapid launch, ready to respond to perceived or imminent nuclear attack, as well as kinetic attacks or cyberattacks on key assets in space.

Critically, a significant portion of the infrastructure that supports command, control, communications, computers, intelligence, surveillance and reconnaissance (known as C4ISR) — which include real-time monitoring and early warning of missile launches and possible nuclear attacks — run through space and present a vector for cyber or data attacks (United States Government Accountability Office 2021). The magnitude of the potential consequences of perceived interference with nuclear capabilities is significant: whether intentional or not, interference with these systems could cause confusion and inadvertent conflict escalation, because such interference is commonly viewed as a prelude to nuclear war (Acton and MacDonald 2021).

Current nuclear deterrence strategies risk further escalation. Both the United States and Russia claim to be willing to use nuclear weapons in response to "significant" non-nuclear threats, including a cyberattack (United States Office of the Secretary of Defense 2018; Bugos 2020). While the thresholds for such a response are intentionally unclear, a perceived attack on early warning and command-and-control capabilities could be interpreted as a prelude to a first strike. When combined with differing understandings of the dynamics of conflict escalation, the result is a real danger that seemingly minor incidents could produce horrific conflict escalation (Lonergan and Yarhi-Milo 2022).

Although such nuclear scenarios represent a worst-case outcome for interactions in the entanglement of Earth-space capabilities, interference with less strategic satellite systems can also have unintended but grave physical effects on Earth, including to critical infrastructure (see below), which could likewise incur unpredictable responses and escalate conflict. This risk of war, however, is deeply rooted in a persistent failure to adequately govern peace.

The Fog of Peace

A clear concept of peace is essential when defining any governance model, but especially for outer space, where it provides a raison d'être of the OST. But the concept remains murky; this murkiness allows a grey zone within space governance and activities therein to flourish.

What constitutes the peaceful use of outer space has been kept deliberately vague. As noted above, the only explicit restrictions in the OST are found in article IV related to weapons of mass destruction and activities on the Moon. Nowhere in the treaty is "peace" or "peaceful" use or purposes defined. Although at the time of drafting, many states, including those in the Non-Aligned Movement, were eager to limit space activities to exclusively peaceful purposes, in practice such

purposes have long included "non-aggressive" and "beneficial" military activities (Saunders 2021).[4]

This association of peace with military use is intentional. The mantra "space for peace" first emerged in 1955 in the context of emerging military space launch and satellite projects. Yumi Tabuchi (2020) argues that peace justified the principle of freedom in space — including the freedom to launch military satellites. A right to the peaceful use of outer space has been used to justify near absolute freedom. The resulting challenge is that few rules have been adopted to clarify and constrain undesirable and even harmful actions below the threshold of armed conflict.

In effect, peace in outer space has been construed in terms of ends not means, functioning as a form of productive ambiguity that has allowed non-peaceful activities, including the development and testing of weapons, through what Jessica West (2023b) has described as a "fog of peace."

A particularly prominent example is the use of the language of peaceful purposes to mask weapons capabilities and tests. For two decades, the Soviet Union referred to co-orbital anti-satellite (ASAT) test capabilities as satellites that "carry scientific equipment to continue research in outer space" (Leitenberg 1984, 31); this claim was repeated following a suspected test in 2020 (West 2020). US President Ronald Reagan presented the US "Star Wars" ballistic missile defence system, which was based on a layer of interceptors in space, as "purely defensive, peaceful technology" that would help to free the world of nuclear weapons (Weinraub 1986). China's first kinetic ASAT demonstration in 2007 was described as a "scientific experiment"; China claimed that it "all along upholds the peaceful use of outer space and opposes weaponization and arms race in outer space" (Space War 2007). India issued an official statement after its 2019 kinetic ASAT test, stating that "India has no intention of entering an arms race in outer space" and that "space must only be used for peaceful purposes" (Government of India 2019).

This fog has also shrouded most military activities from effective governance. Few rules restrict military or even "non-peaceful" uses of space (Grunert 2021). For this reason, efforts to fill in what is viewed by many states as an arms control gap in space governance has been a part of the UN agenda for more than 40 years. But this gap rests on broader omissions in the governance of peaceful uses of outer space. Military activities and capabilities have historically been accepted as peaceful while also beyond the scope of rules that govern peaceful use. For example, the International Telecommunication Union (ITU) coordinates international radio-communication services and use of the shared radio frequency spectrum by non-military operators. However, article 48 of the ITU constitution gives states complete freedom over military radio use. Similarly, the 1972 Registration Convention, which is intended to create transparency in space by identifying and maintaining an international register of launched objects, in accord with article VIII of the OST, is not well applied to military activities in practice.

Few satellites are registered as having a military function; information on the few that are reveals little about actual uses and capabilities (Jakhu, Jasani and McDowell 2018). A narrow definition of "peaceful" at the UN Committee on the Peaceful Uses of Outer Space keeps any discussion of specific military activities or potential non-peaceful uses of space off limits in that forum (Froehlich, Seffinga and Qiu 2020). Also taboo are efforts to govern civilian capabilities that might also have military uses, or be used for such purposes.

The resulting lack of governance provides significant scope for harmful applications of space technology and activities to flourish within the bounds of legal or acceptable uses of space. Two additional qualities add to the challenge: the blending of military and civilian uses of space, and ambiguity about the peaceful nature and uses of space technology.

Blending Military and Civilian Uses of Space

The broad application of peaceful use in outer space means that space systems often defy classification based on use: known as dual use, space systems often have both military and civilian uses and users (Azcárate Ortega 2022). The American GPS is perhaps the best-known example. Developed and operated by the US Department of Defense, GPS was initiated in 1973 as a joint civil/military program composed of a constellation of satellites that broadcast positioning, navigation and timing signals to Earth. A backbone of military capabilities for navigation, tracking and weapons guidance, GPS also

4 *International co-operation in the peaceful uses of outer space*, UNGAOR, 17th Sess, Supp No 17, UN Doc A/RES/1802(XVII) (1962).

supports a growing number of civilian functions: timing and synchronization for cellphones, traffic lights, power grids, the internet, air traffic control, mining, farming, construction, search and rescue, supply chain management, global communication and transportation, and mapping.

In Canada, the RADARSAT Constellation Mission (RCM) of synthetic aperture radar satellites provides whole-of-government services including surveillance of the maritime approaches to Canada (supporting the Canadian Coast Guard and the North American Aerospace Defence Command), as well as early warning for natural disasters and ecosystem monitoring of wetlands, forestry and agricultural land.[5] Indeed, much critical civilian infrastructure is linked to military space systems. As well, many commercial space capabilities, such as satellite communications, were developed with some military assistance and have long served military customers (Slotten 2002). During the so-called first space war in the Persian Gulf in 1990–1991, the US military relied on both military and commercial space systems (Anson and Cummings 1991).

However, the current blending of military and civilian capabilities and activities, with the more recent addition of commercial, is unprecedented in intensity and reach, challenging current boundaries between peaceful and warlike operations of objects in space. A broad range of services, including direct support for combat, is now provided by commercial vendors of dual-use capabilities to Western militaries. No longer serving only national governments, commercial actors are increasingly providing capabilities to third parties, including those involved in conflict.

In Ukraine, commercial space capabilities supplied by Western allies are described as providing direct combat support on the front lines (Massa 2022). Starlink — a commercially operated broadband service provider owned by SpaceX — provides satellite-based voice and broadband connectivity to both civilian and military users in Ukraine, especially in areas where land-based telecommunications infrastructure has been either destroyed or disrupted by cyberattacks (Tucker 2023). There is some evidence that Starlink data was used without authorization to operate armed drones, further blurring the boundaries (Roulette 2023). Commercial satellite imagery, including RCM data, has also provided the Ukrainian government with near-real-time intelligence, improving situational awareness and supporting decision making (Wark 2022). As well, public statements by the United States at the United Nations indicate that China has provided commercial satellite services to aid Russia.

Why does such a growing integration of civilian and military space systems and services matter? Because the blending of systems and services introduces additional risks by potentially making dual-use capabilities valid targets under the laws of armed conflict. Objects with civilian functions are not exempt from the application of force in an armed conflict, if used for military purposes. At the United Nations, Russia has been vocal about the legitimacy of such targets (Reuters 2022). Incidents of dual-use targeting include cyber and electronic interference, including the AcidRain cyberattack against commercial operator Viasat (O'Neill 2023), and persistent efforts to jam Starlink satellites (Horton 2023). Cyberattacks of the computer systems of satellite operators are also believed to be widespread.

We know that in armed conflict, civilians are often not well protected. In grey zone activities, civilians might not be considered at all. The result can be unintended harm to civilians, including those in states not party to the original conflict. Once again, Ukraine offers a glimpse at possible unintended effects. The Viasat hack affected services across Europe; for example, it took thousands of German wind turbines offline (Burgess 2022). This, in turn, can escalate conflict further.

The prevalence of dual-use technology in space also poses a policy conundrum at the national level: to what extent are governments willing to protect civilian or commercial systems from harm (Hitchens 2022)? And, since states are responsible for the regulation and supervision of all national space activities, including those of commercial operators, to what extent might non-military actors implicate states in armed conflict? China asked this exact question recently at the United Nations (West 2023c, 10).

Creeping militarism and further expansion of governance grey zones in space is yet another risk, including on the Moon. The OST bars military activities and installations on the Moon, but it allows the use of military personnel for peaceful

5 See www.asc-csa.gc.ca/eng/satellites/radarsat/what-is-rcm.asp.

purposes. In the first race to the Moon, NASA recruited military officers and pilots for astronaut positions.[6] But now, military organizations such as the US Space Force are expanding their mission beyond Earth's orbit and support for terrestrial military capabilities to include activities focused on — if not physically on — the Moon, as part of a whole-of-government cislunar strategy (Executive Office of the President of the United States 2022). The military is also assuming a growing role in support of civilian and commercial lunar activities such as intelligence (lunaspatial intelligence or LUNINT). A concept for a Cislunar Highway Patrol System to protect civil and commercial activities is also under development (Perkins 2022).

Such activities, while "peaceful," risk escalating geopolitical tensions at a time when great powers seek a technological advantage in space over their rivals. Against a backdrop of competition below the threshold of armed conflict, ambiguity and continued stretching of the boundaries of peace may make inadvertent military confrontation more likely and erode some of the few restrictions on military activities that are in place.

Ambiguity of "Peaceful Purposes"

Much space technology is not only dual use, but inherently dual purpose, capable of performing both civilian and military functions, or of being repurposed for a different use altogether (Azcárate Ortega 2022). In practice, the line between "peaceful" and "non-peaceful" capabilities almost disappears. Although it is not the case that anything in outer space can be turned into a tool for malicious activities, it is certainly true that the capabilities and intended uses of objects on orbit are not always clear. Sometimes, as noted above regarding the testing of weapons, the ambiguity is deliberate.

Such ambiguity adds to the potential scope of harmful activities in outer space. Determining the function or intended use of dual-purpose technology is becoming more challenging as advanced on-orbit capabilities develop, including services linked to rendezvous-and-proximity operations (RPO). Such capabilities enable activities such as satellite servicing and debris removal, as well as military surveillance and inspection efforts, and could also be used to support weapons platforms in space. The ability to repurpose such commercial capabilities for "active defence" in outer space has been offered as a key benefit in policy discussions led by the US-based Center for Strategic and International Studies (Harrison, Johnson and Young 2021).

Such uncertainty is frequently on display. For example, suggestions are made that China's robotic arm — not unlike the Canadarm used on the International Space Station — could be used as a weapon against foreign satellites (Rogin 2021). China has, in turn, called the US Mission Extension Vehicle for satellite servicing a weapon (West 2023c, 16). Not only does this ambiguity expand the scope of potential grey zone activities while contributing to geopolitical tensions, but it also ensnares civilian and commercial uses of space in the resulting uncertainty.

Humans in the Loop

Humans have a deep relationship with space. For thousands of years, the sky above us has been a source of human culture and knowledge. When the OST emphasizes "benefits for all" in article I, it signals awareness of the basic human right to access and use outer space, and the role that space plays in the lives of all people and communities (Freeland 2022). In combination with the important and recurring theme of "the needs of developing countries" throughout relevant UN instruments, this focus suggests that the impacts of space activities on individuals and communities are important considerations when regulating humankind's adventures in outer space.

Yet humans are seldom considered in discussions of space governance, particularly in relation to security. The common definition of a space system — a satellite, a ground station and a communication link — excludes human operators and users. The human-free focus of states on space governance and prevailing notions of grey zone competition are then combined with what Carol Cohn (1987) describes as technostrategic language that unlinks weapons and tactics from real-world effects. The true connections between human security/insecurity and space security/insecurity remain undeveloped.

Beyond Humanity

Astronauts are the rare human element in space, diplomatic extensions of the state and "envoys" of

6 See www.usafa.edu/astronauts/.

humankind (according to the OST). But space is not just about the extraordinary: it is about people's everyday lives. The breadth of the impact of outer space capabilities on human well-being is reflected in the underlying role of space to achieve the UN Sustainable Development Goals. Of the 169 targets, 65 (almost 40 percent) rely on space-based geolocation and Earth observation (Di Pippo 2019).

Platitudes about the benefits of space to humanity fail to indicate the uneven ways in which benefits (and harms) are distributed. For example, the deployment of mega constellations of satellites are touted as the means to reach humanitarian objectives by providing broadband internet access to underserved communities (Frąckiewicz 2023). But commercial imperatives that influence geographic coverage and cost mean that the internet still will not be universally accessible (Patel 2021). At the same time, the launch of so many thousands of satellites obscures a clear and complete view of the night sky that is critical to the work of astronomers and the preservation of Indigenous culture and knowledge (Lawler, Boley and Rein 2022). Yet satellite communications are undoubtedly essential lifelines in remote areas such as Canada's Arctic.

The framing of actions that cause non-kinetic disruptions to space systems as part of grey zone conflict neglects salient factors about the unequal global distribution of both benefits and harms. Those with access to fewer resources feel the impact of disruptions more acutely (Concepcion 2022).

There is growing awareness that the human cost of any war in space would be devastating, on many levels (International Committee of the Red Cross 2021). But seemingly minor disruptions to space systems could also result in crippling harm to human infrastructure and daily lives. The hacking of GPS and navigation capabilities, which serve billions of people across all sectors of society, has already had an impact on critical civilian infrastructure such as commercial airline service.

We also need to ask about the effects of grey zone violence on gendered and other social groups. We already know that women are disproportionately affected by disruption or loss of access to critical infrastructure (Morgan et al. 2020). The gendered impacts of cybersecurity and digital security have also been documented (Brown and Pytlak 2020; Pourmalek 2023). But more research is needed to understand and address the unequal dynamics of space-related technology and the disproportionate impacts related to gender, race and socio-economic status. States are increasingly aware of the value of equity, diversity and inclusions in space policies,[7] although policy choices tend to focus on diversity in space missions, not Earth impacts.

The Human-Protection Gap

Thinking needs to shift from protections for space systems to humanitarian protection and include grey zone activities as well as out-and-out armed conflict. The prevalence of dual-use space systems and growing participation by commercial space operators in military activities mean that more and more civilian users of outer space could be affected by grey zone attacks. And civilian infrastructure needs greater protection as it becomes a more frequent and deliberate target of non-kinetic interference, as we have seen in the context of cyberattacks on health-care facilities (Kumar 2021). Space-related infrastructure is not likely to be an exception to this rule.

Yet there remains a significant gap between governance that protects civilians during times of war — the laws of armed conflict — and the reality of civilian harm from activities below this threshold (Lattimer and Sands 2018). While the international human rights regime applies during peacetime, little attention has been paid to relate human rights to the use of outer space (Freeland and Ireland-Piper 2022), let alone protections during peacetime. More focus is needed on who and what is deserving of protection, and who is being overlooked.

The Human-in-Security Gap

Humans are not only recipients of the benefits and harms linked to space systems, but active participants. The global space enterprise requires human participation at all stages. Maintaining cybersecurity and data security requires technical and scientific processes that are driven by human beings. Because humans are fallible and flawed, they can threaten the space enterprise in a variety of ways.

Space systems are resource and input intensive. Advanced manufactured components are necessary to produce everything from the satellites to the servers that store data on Earth. With tens of thousands of vendors around the world manufacturing and selling components, there are

7 See www.mbie.govt.nz/science-and-technology/space/national-space-policy/.

an almost infinite number of access points and opportunities for hackers to compromise hardware or software (Shadbolt 2021). To this number add service providers that are linked to space systems, with each link a potential access point (Lewis, Moloney and Ussery 2021). Add to this government and private sector actors and the attack surface is immense and attribution challenging.

Inconsistency in the application of human-related security protocols, or insufficient or weak implementation of them, presents countless vulnerabilities to the space enterprise (Gallant and Miller 2023). Whether through error or malign intent, the immensity of the attack surface for the space enterprise means that even minor vulnerabilities or breaches could be disastrous.

Colouring the Grey

Operators in the grey zone often use coercive or aggressive tactics, especially if they fall below the threshold of physical force or are deniable or semi-deniable. But focusing on such behaviour misses the broader view of the core conditions that create the grey zone, which relates to inadequate conceptualizations of peaceful uses and purposes and insufficient governance. The authors' analysis also points to key gaps in governance between overlapping domains, and between different uses and users of outer space. The effects of these gaps are exacerbated by rapid changes in space technology, by the uses and users of space, and by the integration of outer space with other domains of human activity.

The existence of grey space can satisfy certain needs. For example, fuzzy language in high-level agreements can facilitate buy-in by allowing for variations in interpretations that enable diplomatic creativity and face-saving, and so diminish the possibility of major military confrontation. Flexible rules can be re-interpreted in the face of new activities and circumstances, facilitating evolution in governance. Sean Monaghan (2021) thus argues for the tolerance and management of grey zones.

But any decision to manage such spaces must acknowledge the various harms that they can produce. Intentionally unresolved grey zones create opportunity for ongoing and future actions in those zones. Efforts to reveal the many layers of opacity of a grey zone show that it envelops all users and uses of outer space. Persistent harmful interference and poor governance detract from the ability of those users to access and use outer space in a way that is safe, secure and sustainable. States with fewer space capabilities and less redundancy are even more vulnerable. The role and impact of humans in this picture is almost entirely overlooked.

Viewing grey zone conflict as tolerable may encourage unwarranted complacency. The risk of misperception and misinterpretation — core drivers of violent conflict — is high when there is ambiguity about boundaries and rules. Such a risk is particularly dangerous in a domain that is essential to strategic nuclear early warning and command and control, and where ambiguity is viewed as a means of strategic flexibility.

Short of a doomsday scenario, there is evidence that the proliferation of grey zone activities is both causing civilian harm and inspiring a "defence race" in outer space as states pursue protective capabilities, including "bodyguard" satellites and drones (Mowthorpe 2022). This race is further evidence of the instability of the current governance framework.

Finally, competing interpretations of vague rules can result in fragmented governance as states implement different approaches to national space activities. As states pursue their own goals, the result can be a "race to the bottom," with harmful practices incentivized.

There is no single governance solution to this challenge, nor is the onus only on states. To reduce the harm from grey zone activities, discussion on governance should focus on reducing the scope, opacity and harmful effects of activities and governance structures that are currently unclear or grey by adding detailed colouring.

The remainder of this paper will discuss three core harm-reduction strategies: clarifying the peaceful use of space, illuminating the grey zone and pursuing cross-domain discussions.

Clarifying the Peaceful Use of Space

An unclear definition of "peaceful use" encourages the expansion of grey zone space activities. While a strict definition of what counts as

peaceful — and what does not — may be elusive and even counterproductive in a time of technological revolution, efforts can be made to clarify elements of space governance.

Rules for Peaceful Use

Better rules for non-harmful uses of outer space by all actors, particularly for dual-purpose capabilities such as RPO and advanced robotics, can help to clarify the definition of peaceful use.

A legal framework already exists for outer space. What is needed is the communication of clear rules to demonstrate what peaceful and non-harmful use means in practice. Such rules are already an accepted standard in other domains in which dual-use technology is used. Rules permit access and use of nuclear capabilities for peaceful purposes; for example, the Chemical Weapons Convention also mandates rules for commercial activities related to toxic and dangerous chemicals.[8] Aircraft are a relevant example: once the most lethal weapon on Earth, civilian uses were differentiated and governed via the Chicago Convention, which allowed industry to flourish.[9]

An effort at such rulemaking was undertaken at the OEWG — set to be renewed in 2025 — under the headline of responsible behaviour; while the focus of the working group is on military activities, the applicability of such rules extends beyond them (West 2023d). Examples of responsible behaviour include the communication and prior notification of activities, sharing information about the parameters of orbital operations and orbital data, better use of the Registration Convention, and consulting and coordinating with other operators.

The Consortium for Execution of Rendezvous and Servicing Operations (2022) is currently unfolding an industry-wide initiative "that identifies and leverages best practices from government and industry." The ISO is also engaged in ongoing efforts to establish voluntary technical standards for space systems and operations. The establishment of consistent practices can define a standard of peaceful use while mitigating potential harms.

Rules that help to demonstrate the peaceful nature of technology do not stifle innovation but instead help the industry flourish by bringing clarity to the regulatory and operating environments. While a voluntary approach to industry self-governance is likely to fall short of long-term needs, it is a step in the right direction.

Identifying Threatening and Non-peaceful Space Activities

Military activities in outer space are likely to remain largely a grey area of governance. States have historically been unwilling to accept restrictions on their use of space, particularly in relation to national security. But clarity is needed on the boundaries of peaceful use, as well as restrictions on the most egregious capabilities and activities, including those below the threshold of armed conflict.

In addition to the existing ban on weapons of mass destruction in outer space, discussions at the UN OEWG on reducing space threats included suggestions for voluntary restrictions on activities that could damage or disrupt critical civilian infrastructure or strategic early warning and weapons command and control (West 2023d); such restrictions should be supported. A voluntary moratorium on the testing of direct-ascent ASAT missiles should expand to include all destructive weapons tests and become universal (West 2022a).

States should also consider additional restrictions that distinguish between peaceful and non-peaceful uses of technology; such a discussion could be taken up at the upcoming session of the GGE on the Further Practical Measures for the Prevention of an Arms Race in Outer Space, in coordination with the discussion on norms of responsible behaviour at the OEWG.

Although the OEWG did not arrive at a consensus outcome, other worthy suggestions from the discussion include efforts to make all space activities safer, including space launches, the release of secondary space objects, technology demonstrations, military exercises and non-cooperative close approaches, through requirements such as pre-notification.

8 *Treaty on the Non-Proliferation of Nuclear Weapons*, 1 July 1968, 729 UNTS 161 (entered into force 5 March 1970); *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction*, 13 January 1993, 1974 UNTS 45 (entered into force 29 April 1997, effective 7 June 2020, pursuant to Depositary Notification C.N.86.2020.TREATIES-XXVI.3, issued on 23 April 2020).

9 Details on this distinction were presented by Charles Stotler at the first meeting of the UN OEWG on reducing space threats on May 12, 2022. The presentation is not yet available online.

Humanitarian considerations should be imposed on all space activities. Although the legal obligation to implement IHL requirements for civilian protection applies to activities associated with the use of force and armed conflict, the International Committee of the Red Cross (2023) has declared that measures to minimize civilian harm in outer space should be implemented during peacetime. Cassandra Steer (2023) notes that such limits are often applied during times of peace precisely to prevent potential military escalation.

Adopt Stronger Domestic Governance

According to article VI of the OST, states bear responsibility for the actions in space of organizations domiciled within their borders. States can further limit grey zone activities by enhancing domestic governance through policies and laws that set out clear behavioural expectations and requirements and enforce standards.

Such standards can exceed those enshrined in international law. For example, the US Federal Communications Commission has created a new five-year de-orbiting rule.[10] Such rules, in turn, can influence global governance. The enhancement of domestic governance structures would certainly benefit Canada, which has no overarching national space policy. New Zealand's newly adopted National Space Policy could serve as a model.[11]

Improving Visibility of Space Activities

Space activities take place far from Earth and are not readily seen, making them difficult to regulate. The ambiguity of grey zone activities makes governance even more challenging. Efforts that make all space activities more visible and observable can help to illuminate grey zone activities and make harmful actions more readily apparent (West and Doucet 2022, 35–45). The following measures could help make all activities in space more visible, and thus more easily included in other discussions about governance.

Norms of Behaviours

The UN OEWG effort to develop norms of behaviour can help to differentiate between helpful and harmful, and threatening and non-threatening activities. Such behaviours — which are also easier to observe than the capabilities of satellites in space — can help to make visible sources of security and insecurity. Over time, such activities can help to establish clear patterns of behaviour that are adopted by most space actors. These norms illustrate what peaceful uses and activities look like.

Likewise, transparency and confidence-building measures that are specifically designed to clarify space activities, policies and doctrines should be implemented. Actions recommended in the 2013 GGE consensus report on transparency and confidence-building measures include routine pre-notifications; more ambitious registration practices, information exchanges and national reporting; and better efforts to publish national policies, priorities and doctrines to aid in interpreting space activities.[12]

Mechanisms for Communication and Data Sharing

Dedicated institutional means, mechanisms and tools are needed to facilitate, regularize and depoliticize space governance (Dorn and Scott 2000). Especially needed are means to communicate and clarify peaceful uses of space, including mechanisms to facilitate pre-notification, enhanced registration and disclosure of capabilities, information exchange, data sharing and consultations, and direct means of communication between operators (West 2022b).

To date, there has been poor institutional development to support such governance. The OST does not provide for a secretariat or a schedule of meetings of states parties, limiting the ability to formalize discussions on governance that fall under the treaty (Meyer 2020).

10 See www.fcc.gov/document/fcc-adopts-new-5-year-rule-deorbiting-satellites.

11 See New Zealand Space Agency and Ministry of Business, Innovation & Employment (2023).

12 *Report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities*, UNGAOR, 68th Sess, UN Doc A/68/189 (2013), online: <https://digitallibrary.un.org/record/755155>.

Enhanced Cooperation for Space Situational Awareness

Space situational awareness (SSA) is "keeping track of objects in orbit and predicting where they will be at any given time."[13] SSA is needed to understand where objects are and how they are behaving, and to anticipate what they might do in the future. Improving SSA means improving observations of space activities and therefore detecting abnormal and potentially threatening objects and behaviours.

The OEWG discussed the need for greater sharing and accessibility of SSA data, and to facilitate such sharing through standardization (West 2023c). Protocols for civil aviation and commercial shipping already exist, providing a shared picture of where aircraft and vessels are, where they are going and what they are doing.

The discussion of the grey zone in space makes clear that SSA must involve more than locating satellites in orbit. Efforts are also needed to standardize data to make sharing more feasible. Measures to identify non-physical sources of harm, such as the radio frequency spectrum that satellites use for data transmission and cyber activities conducted by satellites, are also needed. Mechanisms for reporting and data sharing could help.

Voluntary measures could also help to make space activities more visible and reduce uncertainty. In addition to norms of behaviour, satellites for peaceful or benign purposes should incorporate design features that make them easier to identify and track and safer to operate.[14] All operators should forgo stealth materials.

Pursue Cross-Domain Governance Discussions

Outer space governance has long been stove-piped. For example, diplomats persist in separating discussions on limiting weapons in space from discussions that limit weapons on Earth that are aimed at space; as well, OEWG discussions display efforts to disregard cyber or other terrestrial activities that affect space. This approach has stymied more robust security and arms control measures that could shrink the grey zone and created governance gaps.

Stove-piping raises legal and other questions: How does space law fit with the many pieces of international law? How are capabilities from different domains of activity entangled with space capabilities? How is such entanglement approached by different states?

Work is needed to disentangle governance of the space-nuclear nexus; the space-cyber nexus; and linkages among space, data and critical infrastructure. The integration of space and AI is likely to create yet more governance challenges. Growing cross-domain cooperation among allies — such as that between the United States and Australia on both space and cybersecurity (Sevastopulo 2022) — suggests that opportunities for bilateral discussion may offer a feasible path forward.

At a more practical and less political level, such considerations might take place in intergovernmental organizations such as the International Committee on Global Navigation Satellite Systems.

States can close gaps at the national level by more thoroughly considering the implications of space and space technology across critical infrastructure sectors.

Impacts on Humans

Outer space is a deeply human domain, even if largely occupied by hardware so far. Satellites are in orbit to support human activities on Earth. Space exploration is for the purpose of helping humans better understand the universe. For those reasons, consideration of present and potential harms and benefits to humans must be considered.

Recognition of the linkages between space systems and critical infrastructure on Earth is growing, but a deeper understanding is needed of the unequal effects of space on the differentiated impacts on people based on gender, race and socio-economics. An effort to populate outer space requires a critical assessment of the unequal ways in which the benefits, impacts and harms of space technology are distributed (Litfin 1997).

Any discussion on governance for space must consider how to provide equal access to and protection for the critical uses of space for all people, including considerations for human rights in outer space

13 See www.spacefoundation.org/space_brief/space-situational-awareness/.

14 See, for example, NASA (2023, chapter 12).

Conclusion

Enhanced governance initiatives will not eliminate the grey zone. And that is fine. While there may be benefits in maintaining some aspects of it, there are also incentives to mitigate it. For example, no one wants to increase the risk of armed conflict in outer space; this common desire acts to preserve some grey zone activities below the threshold of war.

There is resistance to new forms of restraint in outer space. At the OEWG, states including Russia and China objected to efforts to develop norms of responsible behaviour, relying only on narrowly interpreted laws to preserve order while maintaining strategic freedom. Champions of norms including the United States are unwilling to agree to new legal restrictions or obligations. Emerging spacefaring states — many of which feel discriminated against by existing rules — are suspicious of any new restrictions (Rajagopalan 2023). Commercial actors, too, have incentives to exploit fuzziness in the rules. But too much uncertainty is bad for both peace and bottom lines.

Efforts to illuminate the grey zone are also limited by the high — some say excessively high — level of secrecy accorded information related to outer space (Carberry 2022). The degree of secrecy is said to hinder cooperation among allies, even within established alliances. Yet sharing some data more widely would bring greater visibility to the space domain and encourage confidence in the good behaviours of other space actors.

But the biggest obstacle to casting light into any grey zone activities rests on the fact that the grey zone is not only an effect of governance, but a site of governance. A growing focus on great power competition — including competition to set (or change) the rules in line with strategic interests, makes new top-down governance efforts challenging, particularly in international bodies such as the United Nations. And competition can make the application of rules even more complex and unpredictable. But this does not make governance impossible.

Unlike the Cold War era, when many discrete security initiatives were mutually agreed between the United States and Soviet Union, the grey zone in outer space is multi-domain, multi-issue, multinational and highly commercial, as well as strategically competitive. Herein lies the value of adopting a governance focus: it is not restricted to a single rule set, institution, actor, approach or even domain.

Like the grey zone itself, governance efforts to mitigate the negative effects of the grey zone must be broad and layered, incorporating many different initiatives from laws and norms to rules of behaviour, institutions, design features, communication mechanisms, data sharing and standardization. Under the umbrella of principles provided by the OST, the impetus for such initiatives can be many: unilateral, bilateral, intergovernmental or non-governmental (including commercial and civil society actors).

How do we maintain coherence amid such a flurry of activity? Engagement is key. Engagement will not lead to consensus on all grey issues. However, a lack of engagement promotes fragmented governance and exacerbates gaps in the rules, and across actors and domains. UN and other multilateral fora thus remain essential, but they are not the sole site of global governance.

The biggest question for the future of space governance is not who sets the rules, but what are the aspirations and outcomes we hope to achieve?

Works Cited

Acton, James M. and Thomas MacDonald. 2021. "Nuclear Command-and-Control Satellites Should Be Off Limits." Defense One, December 10. www.defenseone.com/ideas/2021/12/nuclear-command-and-control-satellites-should-be-limits/187472/.

Anson, Peter and Dennis Cummings. 1991. "The first space war: The contribution of satellites to the gulf war." *The RUSI Journal* 136 (4): 45–53. https://doi.org/10.1080/03071849108445553.

Arquilla, John. 2018. "Perils of the Gray Zone: Paradigms Lost, Paradoxes Regained." *PRISM: The Journal of Complex Operations* 7 (3): 118–28. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_7-3/prism_7-3.pdf.

Azad, Tahir Mahmood, Muhammad Waqas Haider and Muhammad Sadiq. 2023. "Understanding Gray Zone Warfare from Multiple Perspectives." *World Affairs* 186 (1): 81–104. https://doi.org/10.1177/00438200221141101.

Azcárate Ortega, Almudena. 2022. "Dual-use and dual-purpose objects." Topic 3: Current and future space-to-space threats by States to space systems. Open-Ended Working Group on Reducing space threats through norms, rules and principles of responsible behaviours. United Nations Institute for Disarmament Research presentation. https://documents.unoda.org/wp-content/uploads/2022/09/OEWG-dual-use-presentation-FINAL.pdfBarnett, Thomas P. M. 2004. *The Pentagon's New Map: War and Peace in the Twenty-First Century*. New York, NY: Berkley Books.

Bilal, Arsalan. 2021. "Hybrid Warfare — New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review*, November 30.

Brands, Hal. 2016. "Paradoxes of the Gray Zone." Foreign Policy Research Institute. February 5. www.fpri.org/article/2016/02/paradoxes-gray-zone/.

Brown, Deborah and Allison Pytlak. 2020. *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom and the Association for Progressive Communications. https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf.

Bugos, Shannon. 2020. "Russia Releases Nuclear Deterrence Policy." Arms Control Association, July/August. www.armscontrol.org/act/2020-07/news/russia-releases-nuclear-deterrence-policy.

Burgess, Matt. 2022. "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine." *Wired*, March 23. www.wired.com/story/viasat-internet-hack-ukraine-russia/.

Byers, Michael and Aaron Boley. 2023. *Who Owns Outer Space? International Law, Astrophysics, and the Sustainable Development of Space*. Cambridge, UK: Cambridge University Press.

Carberry, Sean. 2022. "Over-Classification, Lack of Standards Stymies Allied Space Forces." *National Defense Magazine*, June 24. www.nationaldefensemagazine.org/articles/2022/6/24/over-classification-lack-of-standards-stymies-allied-space-forces.

Cesari, Laetitia. 2023. "Commercial Operators on the Digital Battlefield." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/commercial-space-operators-on-the-digital-battlefield/.

Cohn, Carol. 1987. "Sex and Death in the Rational World of Defense Intellectuals." *Signs: Journal of Women in Culture and Society* 12 (4): 687–718. https://doi.org/10.1086/494362.

Concepcion, Giovani. 2022. "Statement Delivered by Mr. Giovani Concepcion, Chief of Space Policy and Legal Affairs, Philippine Space Agency." Statement delivered on behalf of the Philippines, United Nations General Assembly, Open-Ended Working Group on Reducing Space Threats through Norms, Rules, and Principles of Responsible behavior, Geneva, Switzerland, September 12. https://documents.unoda.org/wp-content/uploads/2022/09/TOPIC-2-PHL-STATEMENT.pdf.

Consortium for Execution of Rendezvous and Servicing Operations. 2022. "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)." October. https://satelliteconfers.org/wp-content/uploads/2022/10/CONFERS-Guiding-Principles_Rev3_Oct2022.pdf.

Crane, Keith W., Evan Linck, Bhavya Lal and Rachel Y. Wei. 2020. "Projections of the Future Size of the Space Economy." In *Measuring the Space Economy: Estimating the Value of Economic Activities in and for Space*. Washington, DC: Institute for Defense Analyses. www.ida.org/-/media/feature/publications/m/me/measuring-the-space-economy-estimating-the-value-of-economic-activities-in-and-for-space/d-10814.ashx.

DePagter, Morgan M. 2022. "Comment: 'Who Dares, Wins:' How Property Rights in Space Could Be Dictated by the Countries Willing to Make the First Move." *Chicago Journal of International Law Online* 1.2 (summer). https://cjil.uchicago.edu/online-archive/who-dares-wins-how-property-rights-space-could-be-dictated-countries-willing-make.

Department of Defense. 2010. *Quadrennial Homeland Security Review Report*. February. Washington, DC: Department of Defense. https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf.

———. 2022. *2022 National Defense Strategy of The United States of America*. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

Department of Defense and Office of the Director of National Intelligence. 2011. *National Security Space Strategy (Unclassified Summary)*. January.

Department of National Defence. 2017. *Strong, Secure, Engaged: Canada's Defence Policy*. www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf.

Di Pippo, Simonetta. 2019. "Space for the Sustainable Development Goals." Presentation at the United Nations/China Forum on Space Solutions: Realizing the Sustainable Development Goals, Changsha, China, April 24–27. www.unoosa.org/documents/pdf/psa/activities/2019/UNChinaSymSDGs/Presentations/Simonetta_Di_Pippo_-_Keynote-_Space_for_the_SDGs_v_FINAL.pdf.

Dickey, Robin. 2020. "The Rise and Fall of Space Sanctuary in U.S. Space Policy." Center for Space Policy and Strategy, September. https://aerospace.org/sites/default/files/2020-09/Updated_Dickey_SpaceSanctuary_20200901_0.pdf.

Dorn, A. Walter and Douglas S. Scott. 2000. "Compliance Mechanisms for Disarmament Treaties." In *Verification Yearbook 2000*, edited by Trevor Findlay, 229–47. London, UK: Verification Research, Training and Information Centre.

Dowse, Andrew and Sascha-Dominik (Dov) Bachmann. 2019. "Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?" The Conversation, June 17. http://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841.

Drache, Daniel and Lesley A. Jacobs. 2018. "Introduction: Grey Zones in International Economic Law and Global Governance." In *Grey Zones in International Economic Law and Global Governance*, edited by Daniel Drache and Lesley A. Jacobs, 3–20. Vancouver, BC: UBC Press.

Echevarria, Antulio J., II. 2016. *Operating in the Gray Zone: An Alternative Paradigm for US Military Strategy*. Carlisle, PA: US Army War College Press.

———. 2021. *War's Logic: Strategic Thought and the American Way of War*. New York, NY: Cambridge University Press. 2021.

Executive Office of the President of the United States. 2022. "National Cislunar Science & Technology Strategy." A Product of the Cislunar Technology Interagency Working Group of the National Science & Technology Council. November. www.whitehouse.gov/wp-content/uploads/2022/11/11-2022-NSTC-National-Cislunar-ST-Strategy.pdf.

Frąckiewicz, Marcin. 2023. "The Role of Starlink in Empowering Developing Countries." TS2 Space, February 24. https://ts2.space/en/the-role-of-starlink-in-empowering-developing-countries/.

Freeland, Steven. 2022. "The Regulation of Space Activities: A Human Rights Perspective." In *Liber Amicorum Sergio Marchisio: Il Diritto della Comunità Internazionale tra Caratteristiche Strutturali e Tendenze Innovative*, 1057–71. Naples, Italy: Editoriale Scientifica. https://researchdirect.westernsydney.edu.au/islandora/object/uws%3A68165/.

Freeland, Steven and Danielle Ireland-Piper. 2022. "Space Law, Human Rights and Corporate Accountability." *UCLA Journal of International Law and Foreign Affairs* 26 (1). https://escholarship.org/uc/item/3636p0sp.

Fridman, Ofer. 2018. *Russian Hybrid Warfare: Resurgence and Politicisation*. New York, NY: Oxford University Press.

Froehlich, Annette, Vincent Seffinga and Ruiyan Qiu. 2020. *The United Nations and Space Security: Conflicting Mandates between UN COPUOS and the CD*. Studies in Space Policy, vol. 21. Cham, Switzerland: Springer International Publishing. https://doi.org/10.1007/978-3-030-06025-1_1.

Gallant, Brian and Jordan Miller. 2023. "Growth of the Space Economy and New Cyber Vulnerabilities." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/the-growth-of-the-space-economy-and-new-cyber-vulnerabilities/.

Government of India. 2019. "Frequently Asked Questions on Mission Shakti, India's Anti-Satellite Missile Test Conducted on 27 March, 2019." Press Release, March 27. www.mea.gov.in/press-releases.htm?dtl/31179/Frequently_Asked_Questions_on_Mission_Shakti_Indias_AntiSatellite_Missile_test_conducted_on_27_March_2019.

Goward, Dana. 2020. "New GPS 'circle spoofing' moves ship locations thousands of miles." GPS World, May 26. www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/.

Grunert, Jeremy. 2021. "The 'Peaceful Use' of Outer Space?" War on the Rocks, June 22. https://warontherocks.com/2021/06/outer-space-the-peaceful-use-of-a-warfighting-domain/.

Hadley, Greg. 2023. "'Backdoor' to Attack Satellites: CSO Sees Cyber Risks in Space Force Ground Systems." *Air & Space Forces Magazine*, February 1. www.airandspaceforces.com/backdoor-to-attack-satellites-cso-highlights-ground-networks/.

Harrison, Todd, Kaitlyn Johnson and Makena Young. 2021. *Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons*. Aerospace Security Project, Center for Strategic and International Studies.

Hernández-García, Luis A. 2022. "The grey zone: a conceptual approach from the Armed Forces." IEEE Opinion Paper 34/2022.

Hitchens, Theresa. 2022. "To protect and maybe defend: NRO, SPACECOM ponder commercial satellite defense options." Breaking Defense, September 1. https://breakingdefense.com/2022/09/to-protect-and-maybe-defend-nro-spacecom-ponder-commercial-satellite-defense-options/.

Hogeveen, Bart. 2022. *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN*. Australian Strategic Policy Institute International Cyber Policy Centre. March. https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

Holmes, James R. and Toshi Yoshihara. 2017. "Deterring China in the 'Gray Zone': Lessons of the South China Sea for U.S. Alliances" *Orbis* 61 (3): 322–39. https://doi.org/10.1016/j.orbis.2017.05.002.

Horton, Alex. 2023. "Russia tests secretive weapon to target SpaceX's Starlink in Ukraine." *The Washington Post*, April 19. www.washingtonpost.com/national-security/2023/04/18/discord-leaks-starlink-ukraine/.

Iasiello, Emilio. 2013. "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7 (1): 54–67.

International Committee of the Red Cross. 2021. "The Potential Human Cost of the Use of Weapons in Outer Space and the Protection Afforded by International Humanitarian Law." Position paper submitted by the International Committee of the Red Cross to the Secretary-General of the United Nations on the issues outlined in General Assembly Resolution 75/36. April. https://front.un-arm.org/wp-content/uploads/2021/04/icrc-position-paper-unsg-on-resolution-A-75-36-final-eng.pdf.

———. 2023. "Preliminary recommendations on possible norms, rules and principles of behaviours relating to threats to space systems." Working paper submitted by the International Committee of the Red Cross to the open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours. January 27. www.icrc.org/en/download/file/260782/icrc_working_paper_on_preliminary_recommendations_on_possible_normative_development_final.pdf.

Jakhu, Ram S., Bhupendra Jasani and Jonathan C. McDowell. 2018. "Critical Issues Related to Registration of Space Objects and Transparency of Space Activities." *Acta Astronautica* 143 (February): 406–20. https://doi.org/10.1016/j.actaastro.2017.11.042.

Jonsson, Oscar. 2022. "Myth 1: 'Russia is waging "grey-zone" warfare.'" Chatham House. July 14. www.chathamhouse.org/2022/06/myths-and-misconceptions-around-russian-military-intent/myth-1-russia-waging-grey-zone.

Jordan, Javier. 2020. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict." *Journal of Strategic Security* 14 (1): 1–24.

Kenney, Caitlin M. 2021. "Space Force general wants rules for space." Stars and Stripes, March 3. www.stripes.com/theaters/us/space-force-general-wants-rules-for-space-1.664278.

Kumar, Sheetal. 2021. "The missing piece in human-centric approaches to cybernorms implementation: the role of civil society." *Journal of Cyber Policy* 6 (3): 375–93. https://doi.org/10.1080/23738871.2021.1909090.

Kuzio, Jacqueline, Mohammad Ahmadi, Kyoung-Cheol Kim, Michael R. Migaud, Yi-Fan Wang and Justin Bullock. 2022. "Building Better Global Data Governance." *Data & Policy* 4: e25. https://doi.org/10.1017/dap.2022.17.

Lattimer, Mark and Philippe Sands, eds. 2018. *The Grey Zone: Civilian Protection between Human Rights and the Laws of War*. New York, NY: Hart.

Lawler, Samantha M., Aaron C. Boley and Hanno Rein. 2022. "Visibility Predictions for Near-Future Satellite Megaconstellations: Latitudes near 50° Will Experience the Worst Light Pollution." *The Astronomical Journal* 163 (21). https://doi.org/10.3847/1538-3881/ac341b.

Layton, Peter. 2023. "Responding to China's Unending Grey-Zone Prodding." RUSI, April 21. www.rusi.org/explore-our-research/publications/commentary/responding-chinas-unending-grey-zone-prodding.

Leitenberg, Milton. 1984. "Studies of Military R&D and Weapons Development." Center for International and Security Studies, University of Maryland. https://man.fas.org/eprint/leitenberg/index.html.

Lewis, Dan, Megan Moloney and Nicole Ussery. 2021. "SOS Space: Why cybersecurity and supply chain risk management must go hand in hand." SpaceNews, November 16. https://spacenews.com/op-ed-sos-space-why-cybersecurity-and-supply-chain-risk-management-must-go-hand-in-hand/.

Liang, Qiao and Wang Xiangsui. 2015. *Unrestricted Warfare.* Translated from the Original People's Liberation Army Documents. Brattleboro, VT: Echo Point Books & Media.

Libiseller, Chiara. 2023. "'Hybrid Warfare' as an academic fashion." *Journal of Strategic Studies* 46 (44): 858–80. https://doi.org/10.1080/01402390.2023.2177987.

Litfin, Karen T. 1997. "The Gendered Eye in the Sky: A Feminist Perspective on Earth Observation Satellites." *Frontiers* 18 (2): 26–47. https://doi.org/10.2307/3346964.

Lonergan, Erica and Keren Yarhi-Milo. 2022. "Cyber Signaling and Nuclear Deterrence: Implications for the Ukraine Crisis." War on the Rocks, April 21. https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/.

Luo, Shuxian. 2022. "Provocation without escalation: coping with a darker gray zone." Brookings Commentary, June 20. www.brookings.edu/opinions/provocation-without-escalation-coping-with-a-darker-gray-zone/.

Massa, Mark. 2022. "Commercial satellites are on the front lines of war today. Here's what this means for the future of warfare." Airpower after Ukraine essay series. Atlantic Council, August 30. www.atlanticcouncil.org/content-series/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/.

Mazarr, Michael J. 2022. *Understanding Competition: Great Power Rivalry in a Changing International Order — Concepts and Theories.*" Santa Monica, CA: RAND Corporation.

McKenzie, Timothy. 2017. "Is Cyber Deterrence Possible?" Air Force Research Institute Papers, Air University Press. January.

Medhora, Rohinton P., ed. 2018. *Data Governance in the Digital Age.* CIGI Essay Series. Waterloo, ON: CIGI. www.cigionline.org/publications/data-governance-digital-age/.

Meyer, Paul. 2020. "Arms Control in Outer Space: Mission Impossible or Unrealized Potential?" Policy Perspective. Canadian Global Affairs Institute. October. www.cgai.ca/arms_control_in_outer_space_mission_impossible_or_unrealized_potential.

Monaghan, Sean. 2021. "Bad Idea: Winning the Gray Zone." Center for Strategic and International Studies, Defense360. December 17. https://defense360.csis.org/bad-idea-winning-the-gray-zone/.

Morgan, G., A. Bajpai, P. Ceppi, A. Al-Hinai, T. Christensen, S. Kumar, S. Crosskey and N. O'Regan. 2020. *Infrastructure for Gender Equality and the Empowerment of Women.* Copenhagen, Denmark: United Nations Office for Project Services. https://content.unops.org/publications/UNOPS-Infrastructure-for-Gender-Equality-and-the-Empowerment-of-women.pdf.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk and Marta Keep. 2019. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.* Santa Monica, CA: RAND Corporation. www.rand.org/pubs/research_reports/RR2942.html.

Mowthorpe, Matthew. 2022. "The Russian space threat and a defense against it with guardian satellites." *The Space Review* (blog), June 13. www.thespacereview.com/article/4401/1.

NASA. 2023. "Identification and Tracking Systems." In *State-of-the-Art Small Spacecraft Technology*, 335–45. NASA Ames Research Centre, January. www.nasa.gov/smallsat-institute/sst-soa/.

NATO. 2022. "NATO's overarching Space Policy." January 17. www.nato.int/cps/en/natohq/official_texts_190862.htm.

New Zealand Space Agency and Ministry of Business, Innovation & Employment. 2023. "National Space Policy." May 31. www.mbie.govt.nz/dmsdocument/26656-national-space-policy.

O'Neill, Patrick Howell. 2023. "Russia hacked an American satellite company one hour before the Ukraine invasion." *MIT Technology Review*, May 10. www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/. .

Patel, Neel V. 2021. "Who Is Starlink Really For?" *MIT Technology Review*, September 6. www.technologyreview.com/2021/09/06/1034373/starlink-rural-fcc-satellite-internet/.

Pekkanen, Saadia M. 2022. "Zooming in on the Promise and Peril of Satellite Imagery." *Seattle Times*, August 26. www.seattletimes.com/opinion/zooming-in-on-the-promise-and-peril-of-satellite-imagery/.

Pekkanen, Saadia M., Setsuko Aoki and John Mittleman. 2022. "Small Satellites, Big Data: Uncovering the Invisible in Maritime Security." *International Security* 47 (2): 177–216.

Perkins, Joanne. 2022. "AFRL's Cislunar Highway Patrol System seeks industry collaboration." Air Force Research Laboratory, March 21. www.afrl.af.mil/News/Article/2972971/afrls-cislunar-highway-patrol-system-seeks-industry-collaboration/.

Pourmalek, Panthea. 2023. "The Dialogue Around Digital Security Must Account for Gendered Risks." Opinion, Centre for International Governance Innovation, May 31. www.cigionline.org/articles/the-dialogue-around-digital-security-must-account-for-gendered-risks/.

Rajagopalan, Rajeswari Pillai. 2023. "Space and Cyber Global Governance: A View from the Global South." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/space-and-cyber-global-governance-a-view-from-the-global-south/.

Reuters. 2022. "Russia warns West: We can target your commercial satellites." Reuters, October 27. www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27/.

Robinson, Anthony. 2022. "What is Grey Zone confrontation and why is it important?" The Cove, July 18.

Rogin, Josh. 2021. "A shadow war in space is heating up fast." *The Washington Post*, November 30. www.washingtonpost.com/opinions/2021/11/30/space-race-china-david-thompson/.

Roulette, Joey. 2023. "SpaceX curbed Ukraine's use of Starlink internet for drones — company president." Reuters, February 9. www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/.

Saunders, Melanie K. 2021. "Conference Diplomacy as the Machinery for Manufacturing Consent: Pax Americana and the Case of the Outer Space Treaty and the World Trade Organization." *Melbourne Journal of International Law* 22 (1).

Schmitt, Michael N., ed. 2017. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Prepared for the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge, UK: Cambridge University Press.

Scott, Ben. 2022. "We Need to Stop Talking about the Grey Zone." The Interpreter, March 17. www.lowyinstitute.org/the-interpreter/we-need-stop-talking-about-grey-zone.

Sevastopulo, Demetri. 2022. "US and Australia Boost Space and Cyber Co-Operation to Counter China." *Financial Times*, March 28. www.ft.com/content/a6efecd9-8f7f-4072-ba86-f405c03bc005.

Shadbolt, Luke. 2021. "Technical Study: Satellite Cyberattacks and Security." White Paper. June 30. London, UK: HDI Global Specialty SE. www.hdi.global/infocenter/insights/specialty/technical-study/.

Shull, Aaron and Timiebi Aganaba. 2023. "Formulating, Interpreting and Applying International Law in Space." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/formulating-interpreting-and-applying-international-law-in-space/.

Shull, Aaron, Wesley Wark and Jessica West, eds. 2023. "Securing the New Space Domain: An Introduction." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/securing-the-new-space-domain-an-introduction/.

Slotten, Hugh R. 2002. "Satellite Communications, Globalization, and the Cold War." *Technology and Culture* 43 (2): 315–50.

Smeets, Max and Stefan Soesanto. 2020. "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!" *Council on Foreign Relations* (blog), February 18. www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence.

Soesanto, Stefan and Max Smeets. 2021. "Cyber Deterrence: The Past, Present, and Future." In *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century — Insights from Theory and Practice*, edited by Frans Osinga and Tim Sweijs, 385–400. The Hague, The Netherlands: T. M. C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_20.

Space War. 2007. "China Says Anti Satellite Test Did Not Break Rules." Space War, February 12. www.spacewar.com/reports/China_Says_Anti_Satellite_Test_Did_Not_Break_Rules_999.html.

State Council Information Office of the People's Republic of China. 2019. "China's National Defense in the New Era." White Paper. July 24. Beijing, China: Foreign Languages Press. https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

Steer, Cassandra. 2023. "International Humanitarian Law in the 'Grey Zone' of Space and Cyber." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/.

Stephens, Dale. 2020. "Influence Operations & International Law." *Journal of Information Warfare* 19 (4): 1–16.

Stoker, Donald and Craig Whiteside. 2020. "Blurred Lines: Gray-Zone Conflict and Hybrid War — Two Failures of American Strategic Thinking." *Naval War College Review* 73 (1).

Su, Jinuyan. 2010. "The 'Peaceful Purposes' Principle in Outer Space and the Russia-China PPWT Proposal." *Space Policy* 26 (2): 81–90.

Tabuchi, Yumi. 2020. "Project Vanguard and Ike's 'Space for Peace.'" *Nanzan Review of American Studies* 42: 23–42.

Trevithick, Joseph. 2021. "U.S. Satellites Are Being Attacked Every Day According To Space Force General." The Drive, November 30. www.thedrive.com/the-war-zone/43328/u-s-satellites-are-being-attacked-everyday-according-to-space-force-general.

Tucker, Patrick. 2023. "Decrying Starlink's 'Weaponization,' SpaceX Cuts Support for Ukrainian Military.' Defense One, February 9. www.defenseone.com/technology/2023/02/spacex-now-says-they-dont-want-starlink-be-weaponized-ukraine/382797/.

United States Government Accountability Office. 2021. *Weapon Systems Cybersecurity: Guidance Would Help DOD Programs Better Communicate Requirements to Contractors.* Washington, DC: United States Government Accountability Office. March. www.gao.gov/assets/gao-21-179.pdf.

United States Office of the Secretary of Defense. 2018. *Nuclear Posture Review*. February. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

United States Special Operations Command. 2015. "The Gray Zone." White Paper. September 9. https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

van Eijk, Cristian. 2022. "Unstealing the Sky: Third World Equity in the Orbital Commons." *Air and Space Law* 47 (1): 25-44.

von der Dunk, Frans. 2002. "Sovereignty and Space: When and Where Shall the Twain Meet?" In *State, Sovereignty, and International Governance*, edited by Gerard Kreijen, Marcel Brus, Jorris Duursma, Elizabeth De Vos and John Dugard, 462–81. Oxford, UK: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199245383.003.0020.

———. 2021. "Armed Conflicts in Outer Space: Which Law Applies?" *International Law Studies* 97 (1). https://digital-commons.usnwc.edu/ils/vol97/iss1/17.

Wark, Wesley. 2022. "Commercial Satellite Deployed in Ukraine's Defence." Opinion, Centre for International Governance Innovation, March 31. www.cigionline.org/articles/commercial-satellites-deployed-in-ukraines-defence/.

Weinraub, Bernard. 1986. "Reagan Terms 'Star Wars' Peaceful Project like Radar." *The New York Times*, October 18. www.nytimes.com/1986/10/18/world/reagan-terms-star-wars-peaceful-project-like-radar.html.

West, Jessica. 2020. "Did Russia test a weapon in space?" July 30. Waterloo, ON: Project Ploughshares. https://ploughshares.ca/pl_publications/did-russia-test-a-weapon-in-space/.

———. 2022a. "Ready for lift-off? A commitment to restrain anti-satellite weapons testing." *Ploughshares Monitor* 43 (4). www.ploughshares.ca/publications/ready-for-lift-off-a-commitment-to-restrain-anti-satellite-weapons-testing.

———. 2022b. *Developing norms for enhanced security in outer space: Process and priorities.* May. Waterloo, ON: Project Ploughshares. www.ploughshares.ca/reports/developing-norms-for-enhanced-security-in-outer-space-process-and-priorities.

———. 2023a. *The Open-Ended Working Group on Space Threats: Recap of the Second Meeting, September 2022*. January. Waterloo, ON: Project Ploughshares. www.ploughshares.ca/reports/the-open-ended-working-group-on-space-threats-recap-of-the-second-meeting-september-2022.

———. 2023b. "Arms Control and the Myth of Peaceful Use of Outer Space." In *Oxford Handbook of Space Security*, edited by Saadia M. Pekkanen and P. J. Blount. New York, NY: Oxford University Press.

———. 2023c. *The Open-Ended Working Group on Reducing Space Threats: Recap of the Third Session January 30 to February 3 ,2023*. June. Waterloo, ON: Project Ploughshares. www.ploughshares.ca/reports/the-open-ended-working-group-on-reducing-space-threats-recap-of-the-third-session.

———. 2023d. *Recommendations by states from the Third Session of the United Nations Open-Ended Working Group on Reducing Space Threats*. June. Waterloo, ON: Project Ploughshares. www.ploughshares.ca/reports/recommendations-by-states-from-the-third-session-of-the-un-oewg-on-reducing-space-threats.

West, Jessica and Gilles Doucet. 2022. *A Security Regime for Outer Space: Lessons from Arms Control.* Ploughshares Special Report. October. Waterloo, ON: Ploughshares. www.ploughshares.ca/reports/a-security-regime-for-outer-space-lessons-from-arms-control.

Wirtz, James J. 2017. "Life in the 'Gray Zone': observations for contemporary strategists." *Defense & Security Analysis* 33 (2): 106–14. https://doi.org/10.1080/14751798.2017.1310702.

Wouters, Lennert. 2022. "Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal." Black

Hat USA 2022 conference, August 6–11, Las Vegas, NV. www.blackhat.com/us-22/briefings/schedule/ndex.html#glitched-on-earth-by-humans-a-black-box-security-evaluation-of-the-spacex-starlink-user-terminal-26982.

Yuan, Yue. 2023. "Chinese Thinking on the Space-Cyber Nexus." Cybersecurity and Outer Space Essay Series, Centre for International Governance Innovation, January 29. www.cigionline.org/articles/chinese-thinking-on-the-space-cyber-nexus/.

Zhao, Bo, Shaozeng Zhang, Chunxue Xu, Yifan Sun and Chengbin Deng. 2021. "Deep fake geography? When geospatial data encounter Artificial Intelligence." *Cartography and Geographic Information Science* 48 (4): 338–52. https://doi.org/10.1080/15230406.2021.1910075.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline