Centre for International Governance Innovation

CIGI Papers No. 267 — July 2022

Rudiments of a Space Security Policy Framework

Richard J. Chasdi

Centre for International
Governance Innovation

CIGI Papers No. 267 — July 2022

Rudiments of a Space Security Policy Framework

Richard J. Chasdi

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
Publications Editor Susan Bubak
Publications Editor Lynn Schellenberg
Graphic Designer Brooklynn Schwartz

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

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

Table of Contents

About the Author

Richard J. Chasdi is a professorial lecturer in the Department of Political Science at The George Washington University in Washington, DC. Prior to that, he was a professor of management at Walsh College in Troy, Michigan. He is a senior fellow at the Global Peace Institute in London, England, and an adjunct senior fellow at the International Centre for Political Violence and Terrorism Research (ICPVTR) at the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. He received his B.A. in politics from Brandeis University in 1981, his M.A. in political science from Boston College in 1985 and his Ph.D. in political science from Purdue University in 1995.

Richard has published four books on terrorism and counterterrorism, and some two dozen book chapters and refereed articles. His first book, *Serenade of Suffering: A Portrait of Middle East Terrorism, 1968–1993* (Lexington Books, 1999), received *Choice* magazine's "Outstanding Academic Title" (2000) in the field of international relations. He serves on the editorial board of *Perspectives on Terrorism*, a journal of the Terrorism Research Initiative, and on the editorial board of *Armed Forces & Society*. Richard was a Fulbright Specialist at RSIS, working as a visiting fellow at ICPVTR. He has worked as a news consultant for Al-Jazeera, Sky News, Asharq TV and NPR.

Acronyms and Abbreviations

BRICS	Brazil, Russia, India, China and South Africa
ESA	European Space Agency
FDI	foreign direct investment
FTA	free trade agreement
GPS	Global Positioning Systems
GSO	geosynchronous orbit
IGO	intergovernmental organization
MEO	medium Earth orbit
NASA	National Aeronautics and Space Association
OEMs	original equipment manufacturers
R&D	research and development
UAVs	unmanned aerial vehicles

Executive Summary

This paper scopes out the broader challenges to space exploration security that have galvanized as a result of space privatization and fledgling space-based public-private partnerships. It uses complex systems analysis to define an "Earth-Moon loop system" and articulate security threats that range from terrorism, cyber terrorism, international war and intranational war, to conflict potentials on the Moon and in space. The paper underscores the critical connections between cyberspace and "new space" exploration threat formation, the stakeholders involved, and the structural earthbound systems factors that can influence space exploration security, such as the computer revolution, recession, globalization and climate change.

Introduction

The issue of space security and policy response requires more urgent attention as the commercial space industry becomes more readily accessible to the private sector with the intensification of space industry investment. In time, access to space will grow, in large part because there is demand for space activities from businesses and other consumers. Currently, the Moon is the primary focus of attention for many stakeholders because of its commercial potential and strategic value, and because a "staging orbit in cis-lunar space is an attractive option" for missions to Mars and beyond (Whitley and Martinez 2016, 1).

As a result, firms will gain experience in large-scale production of new technologies; consequently, the cost of production of space-bound goods and services should decline as internal economies of scale in production are achieved. Such trends in production are not new. Similar dynamics characterized the early aviation industry as new technologies, such as cabin pressurization systems, became more affordable and widely used.

In this context, new public-private efforts in space research abound, such as the joint ventures between the National Aeronautics and Space Association (NASA) and SpaceX, and NASA and Israel's SpaceIL company (Collins, n.d.). Those developments come on the heels of new and highly ambitious space projects such as Moon and asteroid exploration, undertaken by governments of countries with well-established space programs. Indeed, several of those countries, such as Russia, China and India, have independent space launch capabilities.

Beyond rocketry, private-sector collaborative efforts have focused on work to craft more advanced space-based infrastructure such as space stations. One example is the Starlab platform under development by Lockheed Martin, Nanoracks and Voyager Space, while another is the Orbital Reef platform proposed by Blue Origin, Boeing, Redwire Space, Sierra Space, Genesis Engineering and Arizona State University (Davenport 2021). Presumably, the underlying aim of those projects is twofold: first, to spur on space exploration development, and second, to enhance resource sustainability in space.

The growth apace in the commercial space industry, sometimes referred to as the "new space economy," issues a clarion call for security systems to protect space-related assets. After all, foreign direct investment (FDI) in space is susceptible to risk in similar ways to how FDI in earthbound "host" countries is vulnerable to risk from political instability. Thus, new security frameworks for outer space need to be developed, if only at a bare minimum, to maintain regular and predictable investment flows from the private sector at a rate high enough to sustain and grow the space industry.

In this first installment of a series of papers that delves into space security challenges and opportunities, the focus is on the articulation of pressing space security issues, the major actors or stakeholders to take into account in an assessment of space security, and certain political, economic and natural factors both on Earth and in space that may create risk to humans in space and space-bound infrastructure. The aim is to examine how some of those factors are interconnected, and what potential interconnections could emerge in a bounded space system inclusive of the Earth and its Moon.

The Conceptual Rudiments of Space Security

Intrinsic to any discussion of space security is the concept of risk. John Monahan describes two types of risk from two different perspectives. The first notion of risk is the "risk assessment" standpoint embraced by actuarial science where the likelihood or probability of victimization is calculated (Monahan 2012, 14–17, 6n7, 4; Chasdi 2013; 2018).

The second standpoint Monahan describes is "risk abatement," or "risk reduction," where emphasis is placed on the removal or curtailment of explanatory factors that help create risk either alone or in tandem with other factors (Monahan 2012, 7). Such factors might include macroeconomic policy to prevent high interest rates and recession, anticipatory efforts to bolster space debris protections, redundancy in computer and hardware systems, and improvement in weather pattern trajectory calculations to increase the safety of landings.

With Monahan's definition of "risk abatement," it is possible to apply Robert Spich and Robert Grosse's definition of "business security" to conceptualize the basic notion of space security. For Spich and Grosse, "business security can be defined as a defensive strategy and state of organizational readiness to assure and protect (but not guarantee) the functional integrity of the organization's operational systems against purposeful, willful and intentional attempts by agents (inside or outside) to disrupt, damage, dismantle or destroy them" (Spich and Grosse 2005, 468).

For a more comprehensive definition of space security, and in the author's judgment, for business security in general, the author suggests the following clause at least be taken into consideration at the tail end of Spich and Grosse's "business security" definition. That clause reads: "And anticipated or unanticipated natural events both earthbound and celestial, that amount to explanatory factors at the source of risk formation."

What is also intrinsic to this study is the use of complex systems analysis. Also known as "adaptive systems," complex systems analysis seeks to provide a more complete depiction of the sources of threat and how those sources are linked together in what amounts to a dynamic "living" system, such as an ecosystem populated by plants and animals (Henry 2013, 67).

For this paper's purposes, the Earth-Moon loop system described here is an expansive, complex system, defined as a quadrant of space. It draws on work where complex systems are often defined by country or by region, or even more narrowly, by cities or by neighbourhoods.

The goal for analysts is not to change the operational system but to influence its component parts and associated processes that help create risk. What complex systems analysis offers is an alternative to more traditional analytical approaches that are usually characterized by a narrower focus on specific events and processes in their purview of expertise.

The narrow focus of analysis that all too frequently characterizes governmental departments or agencies usually reflects the predominant political, diplomatic, legal, military or law enforcement orientation of an agency that is the hallmark of an institution's approach to combat threats. In contrast, complex systems analysis strives to offer a more complete and holistic understanding of an operational system, where the entirety of a system and the interaction of its parts reflect more than the sum of its parts.

The Earth-Moon Loop System

The operational space system demarcated is called the Earth-Moon loop system because it defines the space around and between the Earth and Moon (Qizhi 1982, 161–62; Rosenfield 1979, 138, 147; Whitley and Martinez 2016, 1).[1] Around Earth, there are several bandwidths of orbital space with particular significance for space security. Those layers are distinguished from each other based on the time it takes for a space vehicle to complete one Earth orbit. It follows the nature of different on-board functions that dovetail well

1 Whitley and Martinez describe this as the "Earth-Moon system."

with those particular rotation times and orbits (Mignon et al. 2000, 1; Stuart et al. 2017, 1, 10).[2]

For example, geosynchronous orbit (GSO) is an orbit where the length of one full orbit for a space vehicle amounts to almost one 24-hour day. It is commonplace to note GSO is particularly cost-effective for communications satellites because satellite antennas do not need to be reconfigured to adjust to time differences. In close proximity to GSO is "graveyard orbit," an orbit pattern frequently used to position older and obsolete spacecraft for up to 25 years as Earth's gravitational pull gradually leads to orbital decay (Mignon et al. 2000, 1; Stuart et al. 2017, 1; Whitley and Martinez 2016).[3]

In turn, medium Earth orbit (MEO) is an orbit where space platforms complete one Earth rotation in less than 24 hours. MEO is useful for spy satellites and armed satellites that need to move into position quickly when crisis conditions materialize. In comparison, low Earth orbit is a bandwidth of space that reaches up to 2,000 km above Earth, used primarily to realign space vehicles for safe descent to Earth (ibid.).[4]

It should be clear this Earth-Moon loop system also includes the extent of space subject to the Moon's gravitational pull, which is known as cis-lunar space (Mignon et al. 2000, 1; Stuart et al. 2017, 1, 10; Qizhi 1982; Rosenfield 1979, 138–47). Cis-lunar space is defined by John K. Strickland as "the area around the Earth extending out to just beyond the Moon's orbit" (Strickland 2012; Flewelling 2020). As in the case of Earth, there are several orbital pattern types around the Moon with different security ramifications. From highest to lowest orbit times, those orbits include distant retrograde orbit, Earth-Moon L2 halo, near rectilinear orbit, elliptical lunar orbit, lunar frozen orbit, prograde circular orbit and low lunar orbit (Whitley and Martinez 2016, 1–2).

What is significant for space security is that orbit preference helps betray target type and expose earthbound vulnerabilities associated with space platform functions. For instance, space platforms devoted to civilian communications become more easily identifiable and susceptible to kinetic attack based on orbit and trajectory. In a situation where the political goal is to send a symbolic message about a stakeholder's capacities to use force in space, an attack against an obsolete spacecraft might be the target of choice.

This Earth-Moon loop system is articulated because it is likely to be the primary arena and focus of commercial interests and nation-states for decades to come. For the private sector, profit motivation, refinement of core competencies (i.e., technological innovation), definition of key success factors and corporate social responsibility will spur on the commercial space industry. Public-private partnership opportunities will continue to expand as nation-states utilize the private sector to promote national interest in an anarchic or decentralized international political system (Waltz 1973).

The Complex Systems Theory Framework

The central idea behind this complex systems analysis is that threats to stakeholders critical for space exploration need to be isolated and identified because state-level and private sector resource allocation are critically important to space exploration and program development (Waltz 1959, 3–10, 159–86; Nye 1993, 24–34, 64–65). The discussion now turns to a more detailed description of complex systems analysis, its different dimensions and potential applications to space security.

Stakeholders

Within a complex system, stakeholders, explanatory factors and stressors each constitute a basic building block or element of the complex system under consideration. Stakeholders might include nation-states and several types of non-state actors. Those could be supranational organizations such as the European Union, or subnational organizations such as multinational corporations, other international enterprises, terrorist groups and criminal syndicalist organizations. In turn, stakeholders are connected to explanatory factors within this Earth-Moon loop system.

2 See https://en.wikipedia.org/wiki/Geosynchronous_orbit.

3 Ibid.

4 See https://en.wikipedia.org/wiki/Low_Earth_orbit.

Explanatory Factors

Explanatory factors are critical sources of threat formation that create risk within the Earth-Moon loop system. For Sheila R. Ronis (2007, 8–19), explanatory factors can be both external and internal to a particular complex system (Fuerth and Faber 2012). At a theoretical level, external factors largely correspond with systems-level factors in the neo-realist conception of "three-level analysis." Those systems-level factors, what Waltz calls "third-image" factors, affect three or more states" (Waltz 1959, 3–10, 159–86; Nye 1993, 24–34, 64–65; Reiss and Roth 1993, 291–326; Chasdi 2018, 65–66, 195n51, 205n11). In this analysis, "long-haul" variables correspond to deep structural or systems explanatory factors that affect three or more Earth-Moon loop system stakeholders.

At a functional level, external factors in this analysis are generally in play 18 months or more prior to a space security problem, or 18 months or more after its identification (Chasdi 2018, 65–66, 195n51, 205n11; Chasdi 2010). Some examples of earthbound external factors include, but are not limited to, globalization, the computer revolution, the Cold War (and its end), the global war on terrorism, failed and failing states, modernization processes, pandemics and climate change.

In contrast, Ronis's internal explanatory factors include those linked to conflict found at what neo-realists call the "nation-state level" (Ronis 2007). Those factors include, but are not limited to, regime type, tax codes and regulation favourable to space industry investment, economic market conditions, *kulturkampf* (culture struggle), and "social fissures" in societies that align to generate and sustain ethnic conflict (Waltz 1959, 3–10, 159–86; Diamond 1990; Chasdi 2018, 1, 183n1, 10, 55).

Unlike most external explanatory factors that correspond with having long-haul effects, internal explanatory factors are not associated with a particular time interval. In some cases, internal explanatory factors, such as regime type and social fissures, are characterized by long-haul effects. In other cases, internal explanatory factors, such as tax codes and economic market conditions, are characterized by middle-run and short-run effects.

At a functional level, middle-run factor effects in this analysis span from three months prior to recognition or identification of a space security problem to 18 months afterwards. In comparison, short-run factor effects run from up to three months before a space security problem materializes or is acknowledged to three months afterwards (Chasdi 2010; 2018).

Explanatory factor effects can also be broken down into first-order, second-order and third-order effects. In turn, that makes it possible to use what is called "intervention points" analysis. In an intervention points analysis, public policies are tailor-made and applied at particular nodes in the complex system network to remove or reduce explanatory risk factors or their effects at specific points in time. With that intervention points analysis, the paper comes full circle, back to Monahan's "risk abatement" approach.

The central idea is that external and internal explanatory factors in a complex system not only work to influence each other at those levels, but also work across levels to affect other explanatory factors. In response, public sector and private sector policy analysts can craft policies that take into account first-, second- and third-order factor effects.

Those factor effects can stem from one factor working alone or in conjunction with others, even across external and internal levels of explanatory factors. Ultimately, the aim is to craft proactive policies that stress anticipatory defensive measures to create a bulwark of defence systems for outer space.

Stressors

In addition to stakeholders and explanatory variables, political and economic events called "stressors," which happen and affect a complex system, need to be taken into account. Overall, political and economic shockwaves caused by stressors affect stakeholders and explanatory variables and their connections in an operational environment such as the Earth-Moon loop system.

Earth-Moon loop system stressors can be endogenous or exogenous to that system. Stressors that are endogenous to the system might include worldwide recession; war; climate change that causes weather pattern shifts; and major terrorist events, such as September 11.

In comparison, exogenous stressors to the Earth-Moon loop system could involve the interaction of two complex systems in space. For example, exogenous factors could be the direct or indirect political, economic or military events (and effects) that stem from the intersection of two space systems, such as an Earth-Moon loop system and an Earth-Moon-Mars loop system.[5]

The First Three Phases of Analysis

A complex systems analysis of an Earth-Moon loop system would have three preliminary phases. The first phase is to identify the range of stakeholders, explanatory factors and possible stressor events likely to predominate in this Earth-Moon loop system for a 32-year period from 2025 to 2057. This identification process unfolds through interviews with space industry experts who are the subject matter experts.

Those space industry experts highlight the actors, processes and potential events that constitute each of those building-block elements. They would also describe projected "new space economy" system characteristics for three specific 10-year time intervals (Ronis 2007, 17, 23–25). Those time intervals are 2025–2035, 2036–2046 and 2047–2057.

The second phase of a complex systems analysis involves work to scope out the different ways stakeholders, explanatory factors and potential stressors, as parts of this Earth-Moon loop system, are linked. Those links are characterized by direct and indirect connections or pathways. In other words, analysts craft a basic outline of the direct and indirect connections between stakeholders, explanatory factors and stressors within this Earth-Moon loop system. In some cases, pathways of effect will be characterized by feedback loops to designate interactive effects.

The next step in a complex systems analysis of this Earth-Moon loop system is to have those space industry experts craft a set of multiple scenarios, each tailor-made for the particular time intervals under consideration. In those scenarios or stories, one stakeholder, explanatory variable or stressor, or one set of each, is changed, holding the others constant (*ceteris paribus*) (Ronis 2007; Fuerth and Faber 2012; Henry 2013, 67). That capacity to help pinpoint different Earth-Moon loop system outcomes is based on projected change in the interaction of stakeholders, explanatory factors and stressors.

Work on alternate scenarios is valuable because the storytelling highlights critical relationships found in a complex system. In this way, a set of alternate outcomes for the complex system under consideration is generated that makes it possible to create a scheme about distribution of scarce and finite resources in anticipation of events deemed likely to happen by subject matter experts, and those "black swan" events deemed unlikely but still possible (Ronis 2007, 20–23).

The Frame of a Complex System

Beyond consideration of stakeholders, explanatory factors and stressors, the frame of this complex system has effects of its own. For some complex systems analysts, a complex system is like a jigsaw puzzle bounded by its frame, where that frame influences the way the puzzle pieces interact (i.e., fit together) (Sydelko 2014; Rosenfield 1979, 141–46). Still, this Earth-Moon loop is not a closed or static system; human-made objects such as satellites and natural objects such as meteors, meteor showers and asteroids can enter the system and become part of it for limited periods of time (Reich 2021).[6]

In addition to physical permeability as a characteristic of the Earth-Moon loop system frame, international law is an integral component of that frame. Even though international law remains state-centric, it works in both direct and indirect ways to influence stakeholder behaviours and threat potential. The conventions that scope out basic space law include, but are not limited to, the Outer Space Treaty (1967), the International Liability Convention (1972), the

5 In this paper, such exogenous stressors are not considered, nor are the theoretical implications associated with the interaction of two space systems.

6 While the elliptical orbit of Earth's so-called second moon, asteroid 469219 ("Kamo'oalewa"), places it outside the Earth-Moon loop system, the asteroid's relational orbit to the Earth, affected by Earth's gravitational pull, is as good an example as any of the dynamics involved.

Rescue Agreement (1968) and the Registration Treaty (1976) (Rosenfield 1979, 141–46).

Two examples of international conventions that influence space-bound behaviours directly include the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1984) and the Outer Space Treaty (1967) (ibid., 144). The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies is a resolution where article II requires that "all activities on the Moon, including its exploration and use, shall be carried out in accordance with international law, in particular the Charter of the United Nations."[7] Further, article III(1) stipulates that "the moon shall be used by all State Parties exclusively for peaceful purposes."[8]

In a broader sense, the Outer Space Treaty[9] is a convention that establishes a baseline of expectations about space use, declaring that outer space "shall be free for exploration and use by all States"[10] and "is not subject to national appropriation by claim of sovereignty."[11] Even though a celestial-based "public commons" for states helps promote egalitarianism for states in space, it also helps produce security implications for future space flight and exploration.

In large part, those security implications seem linked to the inevitable growth in astronaut numbers, state stakeholders, state-regulated business firms in space, and the growing amount of "space junk" with the potential to cause death and damage to investment infrastructure. Indeed, all of the foregoing processes and outcomes will be accelerated with increased competition and the politicization of space as a backdrop to this "new space" frontier.

It follows one threat to the Earth-Moon loop system that complex systems analysts should consider, which involves a "tragedy of the commons" economic condition. In such a condition, overuse of resources in the Earth-Moon loop system or outright abuse could lead to increased risk and threat for both space-bound and earthbound stakeholders, such as private investors (Hill and Hult 2015, 133). For example, poorly regulated resource mining operations on the Moon could result in resource depletion. Examples of abuse that could affect economic profitability could include makeshift and incomplete disposal of nuclear waste and other toxic materials in space or on the Moon.

International law can also influence the growth and trajectory of explanatory factors linked to threat in more indirect ways. For example, the Vienna Convention for the Protection of the Ozone Layer (1988) is pertinent because increased private sector use of rocketry could increase ozone layer depletion and cause important side effects, such as (sudden) weather system pattern changes, that may impact space liftoff and re-entry protocols.[12] It follows that, as the scope of rocket engine development increases with the expansion of the commercial space industry, the new space industry will require rocket engines designed to minimize environmental damage.

One aspect of space security underscored by the concept of outer space as a free domain for all not only parallels the more earthbound notion of public commons use but also highlights another earthbound notion. That notion is the time-honoured set of strains and tensions between the pursuit of individual nation-state interest and the collective interest of the community of nations found within the international political system. This condition is also linked to an anarchic or decentralized world, with no easy fixes.

What that implies is the need to think about functional thresholds or "red lines" relevant to commercial space policy. Those red lines should not be crossed by non-actors such as multinational corporations and their countries of registration because of collective interest and security concerns.

Picture a situation where "common use" in our Moon-based space system leads to resource hoarding and depletion by nation-state governments or commercial interests that, in turn, elicit the threat or use of force on Earth

7 *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, 5 December 1979 (entered into force 11 July 1984), UNGA Res 34/68 (XXXIV), 34 UNGAOR, Supp (No 46), 77 UN Doc A/34/664 /ANNEXES (1979).

8 *Ibid*, art III(1).

9 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 18 UST 2410, TIAS No 6347, 610 UNTS 205 (entered into force 10 October 1967).

10 *Ibid*, art I.

11 *Ibid*, art II.

12 *Vienna Convention for the Protection of the Ozone Layer*, 22 March 1985 (entered into force 22 September 1988), S Treaty Doc No 9, 99th Cong, 1st Sess (1985).

and in space, in both the physical and virtual worlds. Even though the specific security challenges to assets in cis-lunar orbit and on the Moon will likely differ in profound ways from the threat to assets in Earth orbit, the basic motivations to promote state or non-state interests will remain similar, if not the same.

The Threat or Use of Force in Space

The prospect of the threat or use of force in space could increase or materialize within the context of different types of stakeholder interactions. For example, the threat of force or its use could take place between nation-states, between nation-states and non-state actors, or between non-state actors such as terrorist groups that states could use as proxies (Denning 2001; Collins, n.d.; Chasdi 2018, 29, 187n32).[13]

It is probably no exaggeration to say that conflict between stakeholders over the 32-year trajectory envisioned will involve events within and between the physical world and the virtual world, perhaps, in some cases, nearly simultaneously. That is because international law remains subordinate to geopolitical considerations and because political, economic and strategic opportunities abound in space (Beres 1987, 106, xi, 2, 4, 24, 54, 150; 1988, 291–306; 1990, 133; Chasdi 1999, 23, 50nn20–22).

In terms of objectives, many non-state actors and some nation-state actors in space might work to undercut each other's technological developments and core competencies on Earth. Targets include government and private sector communication satellites, intelligence-gathering and weather-tracking satellites, other space platforms, and other space operations by means of cyber intrusions infected with malware or kinetic assaults (Ignatius 2021; Sonne, Ryan and Davenport 2021).

In time, the use of cyber intrusions and forceful physical actions might be sourced from outer space itself. At the tail end of the 2051 trajectory imagined, the threat or use of force might be directed at a competitor's orbital platforms or payloads in space, or at lunar-based private space assets in orbit or found on the lunar surface.

The Link between Space Security and Cybersecurity

For Linda Dawson, a delicate web of connections exists between cyberspace "data packet" transmission satellites, and earthbound internet-based systems that relay information almost instantaneously. At the heart of that network lie Global Positioning System (GPS) satellites that work to ensure timely and accurate provision of vital internet-based services that include, but are not limited to, air traffic control, cellphone use, online banking and automobile navigation systems.

Those GPS satellites' components are so delicate and so closely synchronized that any timing disruption that a cyberattack or a kinetic attack by anti-satellite weapons could produce would cause severe system deterioration almost instantaneously. In addition, collision or near-collisions of satellites could cause disruption, because orbit changes often happen, but communications between stakeholders about those orbit changes are sometimes makeshift and incomplete (McDowell 2022). Such disruptions would produce a cascade effect of security breakdowns across computer networks both in space and on Earth (Baldwin 1971), with calamitous results in the physical world (Dawson 2018, 2–3; Rogers 2001, 70–76).

Clearly, that condition underscores the interface and crucial connections between the fields of space security and cybersecurity. What compounds the problem even more is that computer-aided design and manufacturing processes have "dual-use" civilian-military applications. In essence, Dawson's example

13 Non-state space actors might include political protest groups, practising what Denning calls "hactivism," and terrorist groups. Terrorist assaults could be conducted with unmanned vehicles such as drones or other unmanned aerial vehicles (UAVs) against space infrastructure in Western countries, if the benefit of kinetic attacks against targets is appraised as high and outweighs projected cost. Those targets could include launching pads and research and development (R&D) facilities of private firms such as Blue Origin. In time, UAV platforms presumably now under development could venture into space and pose terrorist threats to orbital targets.

illustrates that technological developments and applications in the space industry have the potential to increase the vulnerability of computer technology systems, and vice versa.

Plainly, that highly complex and integrated condition between those industries has implications for the manufacturing and production processes associated with space infrastructure. In addition to original equipment manufacturers' (OEMs') security, first-tier, second-tier and third-tier companies, contracted to make subcomponent parts by the OEMs that make spacecraft and space stations, must be included in fledgling space security regimes.

To be sure, security coverage of subcontractors is not a new issue. The capacity of adversaries to corrupt subcomponents to be included in highly sensitive defence-related products resulted in provisions in the John S. McCain National Defense Authorization Act (2019) to increase security protections, primarily for US defence contractors. However, there are limitations intrinsic to this legislation's scope that leave some non-government firms external to the US defence industry outside its purview (Chasdi 2019, 10–14).

In a complex systems map, direct and indirect connections between firms that produce fully assembled American defence infrastructure and their American subcontractors with access to Chinese subcomponents could be traced to highlight vulnerabilities in supply-chain sources. Such tracing could augment other complex systems mapping efforts to focus on the product production flows that are vulnerable to infiltration by foreign powers, either through physical manipulation or via cyberspace.

Complex systems mapping could also monitor monetary flows to and from those generally recognizable and reputable entities identified as part of this highly interdependent system. In the process, those monitoring and oversight functions would work to tip off analysts to possible connections between those entities and other less reputable firms, groups or governments that could pose security problems (ibid.).

What all of the foregoing means is the set of production-related connections across both physical and virtual worlds must be considered as an intrinsic part of the overall space security concept. In the broader sense, it follows that space security involves the need for policy analysts to shed light on links and threshold points between four interrelated conflict modalities with the potential to disrupt space security: cyberwar, cyber terrorism, cybercrime and online political protest (Denning 2001).

Stakeholders

The discussion now turns to a presentation of broad categories of stakeholders. The scope of stakeholders ranges from those state and non-state stakeholders in the public sector, and private sector actors such as SpaceX, Blue Origin, Virgin Galactic and Israel's SpaceIL Group (Collins, n.d.). For the 32-year trajectory under consideration, nation-state stakeholders might be broken down into those with full space launch capabilities, those with some space program capabilities and those anticipated to acquire either program or launch capabilities (Kegley 2007, 134).[14]

There are some 14 states and one intergovernmental organization (IGO) with the capacity to launch spacecraft and their payloads into Earth orbit or, in some cases, beyond. In some cases, those countries acquired technology to launch vehicles into space during the Cold War, while others are new system entries, or otherwise had technology passed down to them by the former Soviet Union. Those states include Australia, Canada, China, France, India, Iran, Japan, Kazakhstan, North Korea, South Korea, the Russian Federation, Ukraine, the United Kingdom and the United States (O'Callaghan 2013; OECD 2021, chapter III).[15]

Intrinsic to a breakdown of states with full launch capability is consideration and inclusion of relevant legal and regulation activities related to space at the national, state, provincial or department levels. Those include, but are not limited to, laws and regulations that affect space launch

14 In some cases, but certainly not all, that division corresponds to the conceptual divisions between states that comprise the global "North-South divide," where Japan and highly industrialized Western states found primarily to the north of the equator are contrasted to developing states found primarily south of the equator.

15 See https://worldpopulationreview.com/country-rankings/countries-with-space-programs. In addition to those nation-states, the European Union is an IGO that has full launch capabilities in its European Space Agency (ESA).

prospects; communications protocols between states and state-regulated private sector actors about satellite orbit change, the taxation process related to private company investment and operations; and protocols linked to other related space activities (McDowell 2022; Messier 2021).

In a complex systems map, pathways of effect between stakeholders and explanatory factors within those issue areas would connect state, provisional or departmental agencies, and a separate set of connections, both direct and indirect, would connect those agencies and corresponding national agencies to ensure that issue-area protocol is standardized, without issue coverage gaps or interpretation problems due to language or culture, for example (Chasdi 2018, 87–88).

In a similar vein, weather system tracking methodologies used in individual countries or regions that have the potential to affect space-related activities, could also be included. In follow-up complex systems maps, issue areas would be connected much like a mosaic to give a more complete picture of the Earth-Moon loop system.

Other nation-states have effective and sustained space programs devoted to research and space exploration, but must rely on collaboration with nation-states such as Japan, with its robust launch capacities, to launch their space vehicles or related project payloads. For example, Luxembourg has become a financial centre for private start-up firms linked to space exploration efforts, in large part because of its past successes in the banking and financial services industries (Brennan 2019).

In the case of nation-states, it is also necessary to consider developing states with the ability to build or acquire computer technology or space orbital capacities over the next 30 years. While Brazil already has a space program, it is reasonable to assume that other equatorial states such as Colombia and Kenya, which have demonstrated interest in space, will spur on their efforts to become space stakeholders (Qizhi 1982, 160–61; Rosenfield 1979, 142). It is also reasonable to assume that very soon Brazil will join Russia, China and India as another BRICS (Brazil, Russia, India, China and South Africa) country with independent space launch capabilities.

Interestingly enough, another factor to spur on space development for developing states is the power and prestige associated with space launch capabilities. Such prestige might play the same role that nuclear weapons acquisition plays nowadays, where the idea is that the only way the West will take the political grievances of developing states seriously is if at least some developing countries acquire nuclear weapons. If new computer technology capacities and launch capabilities increase power and threat potential, making it possible for some developing states to influence political events on Earth, space exploration becomes a very attractive option.

In addition to state actors, non-state actors will likely gain a greater foothold in space. At present, the European Union's ESA is the single most dominant IGO space stakeholder, but it is possible that regional free trade area (FTA) involvement in space programs will increase.

Such regional free trade blocs might include Mercosur, itself composed of Argentina, Brazil, Paraguay and Uruguay, and might increase the number of IGOs involved in space, as monies from states within those blocs are pooled. It follows that rivalries and political tensions between free trade blocs could be exacerbated with their involvement in space exploration, contributing to overall security problems within the Earth-Moon loop system (Chasdi 2018, 3–4).

To be sure, private companies such as Space X, Blue Origin, Virgin Galactic, Boeing Company and Lockheed Martin will continue to develop spacecraft, space stations and other orbital equipment (Davenport 2021). The scope and depth of public-private ventures will continue to grow as additional companies, including those from the developing world, expand their space programs. As previously mentioned, subcontractor firms, such as Aerojet Rocketdyne, that manufacture and sometimes assemble systems for OEMs, must be considered as part of this new space security architecture.

Over time, other non-state actors such as terrorist organizations, paramilitary groups and cyber organizations are likely to become stakeholders in space. Those stakeholders will likely acquire the ability to use cyber terrorism and cybercrime against space-borne targets long before they acquire abilities to launch, because of the prospect of third-party transfer of computer technology from international patrons.

It is also possible that certain state sponsors of terrorism such as Iran might collaborate with terrorist groups directly to launch payloads with destructive capabilities. In a similar vein, political protest groups could use cyber intrusions to disseminate political protest manifestos related to climate change and pandemic concerns, in addition to their more traditional focus on political policy preferences and specific political leaders (Denning 2001).

Explanatory Factors

Efforts to scope out explanatory factors at work over the time trajectory projected is difficult because of the uncertainty involved, but some broad factors can be identified. For example, rates of public sector and private sector R&D investment help increase or decrease the influence of some economic-based explanatory factors linked to the Earth-Moon loop system.

In addition, the ability to assess economic trends, investor interest and other economic conditions is critical. For example, having the government and private sector work together to anticipate new challenges and opportunities for crowdsource funding and to support space-related public-private partnerships is critical to take advantage of broader economic trends and conditions. Effective scenario construction in this context makes it possible to distinguish between worst-case, best-case and "moderate change" economic conditions (Schwartz 1991, 3, 9, 20, 24, 168).

Legal structures and related instruments with the potential to contribute to fruitful economic conditions for space exploration include country-specific tax structures and regulations. Those factors serve to increase or decrease the attractiveness of R&D investment in space research based on potential rates of return. Legal options include tax provision structures such as tax incentives for certain space-affiliated industries (i.e., energy, aviation and computer technology), which can affect revenue levels and profit margins for space-related OEMs and, in turn, the proportion of profit siphoned off to support R&D programs (Yergin 2011).

Some specific explanatory factors linked to space security threat potential include:

- militarization of space;
- increased needs for energy sources;
- discoveries of accessible mineral deposits on the Moon and on asteroids;
- increased consumer demand for space tourism;
- increased feasibility of low-gravity health-care and hospital facilities for people afflicted with chronic diseases;
- new IGO stakeholders; and
- space colonies to relieve over-population or population dislocations caused by climate change or pandemic effects.

Linked to the politicization and militarization of space is the traditional political competition between nation-states and some non-state actors. Because space, like cyberspace, is a new security milieu or dimension to contend with, where new technologies and the full range of identifiable actors might not be fully understood, some theoretical retooling of international security theory might be necessary to promote Earth-Moon loop system stability.

Those efforts are critical because the capacity to deter aggression and promote conformance to a baseline of security expectations within the context of international law works to influence the "nation-state security dilemma" and the "spiral of insecurity," both in space and on Earth. Currently, where the international political system has been extended to include the virtual world and outer space, the impact of the nation-state security dilemma and the level of the spiral of insecurity involved are even more important than ever before.

The Role of Stressors

In the case of political stressors, while it is possible to scope out specific categories of stressors, it is obviously not possible to project into the future and detail specific stressor examples. There will be exogenous stressors to the Earth-Moon-based loop system, such as solar flares and asteroids that penetrate the system, as well as endogenous or internal stressors that affect more traditional complex systems sourced on Earth. A range of endogenous stressors will also pose or contribute to threats against Moon-based infrastructure or assets in the Earth-Moon loop system.

One type of political stressor is interstate war on Earth between countries. If sufficiently extensive, interstate war could manifest itself in space either through cyberwar or cyber-terrorism capabilities or in kinetic activities in space if countries with advanced technologies were involved. Indirectly, interstate war would reduce political and economic incentives to collaborate on space endeavours and could work to drain potential economic funds otherwise earmarked for space research and exploration.

In comparison, intranational war in countries with fledgling space programs could lead to cyber-intrusion capabilities used by governments against opponents or vice versa, in ways that would impact the economic conditions necessary for fledgling space programs to thrive in effective and sustained ways. Intranational conflict also creates conditions and incentives conducive to third-party involvement, and that raises the spectre of broader regional war, with effects as described above, where countries take one side or the other in the original conflict.

In addition to political stressors, there will be economic stressors that impact the Earth-Moon loop system. Two examples of exogenous economic stressors that could affect that system are the Great Recession (2007–2009) and the Asian economic crisis (1997–1998). While another worldwide recession would undoubtedly affect economic sectors and industries associated with space exploration, another recession like the Asian economic crisis could have indirect political or economic effects on developing countries in the context of space exploration aspirations.

What is known is the Asian economic crisis contributed to terrorist group recruitment in Indonesia and Malaysia, thus contributing to the strength of terrorist groups with the potential to threaten earthbound space assets such as launch facilities or R&D centres (Chasdi 2021). Terrorist threats or terrorist attacks against space system infrastructure are a possibility because investment in space exploration is a lucrative source of revenue and for increasing political and economic clout.

In turn, climate change and pandemic threats are other stressors with the potential to influence the Earth-Moon loop system. For example, climate change could spur on state-based R&D efforts to confront structural shifts in weather system functions on Earth, land degradation and soil erosion, and other climate change manifestations. In addition, there might be new links found between climate change and pandemics or other diseases that require additional research efforts associated with space research or related activities.

In the case of developing states, climate change and pandemics could lead to mass migration problems and subsequent conflict over scarce resources, with adverse effects on fledgling space programs. Those conditions in developing countries could have other indirect effects that complex systems mapping could chart.

Those other indirect effects might include an increase (or decrease) in intrastate conflict and an increase (or decrease) in terrorism recruitment effects. In addition to dangers posed to developing state space infrastructure, there is the potential for terrorists associated with countries hit hard by climate change to target Western space infrastructure because of the West's makeshift and incomplete response to climate change effects.

Another climate change path of effect might involve mass migrations to developed countries from countries in the developing world hit hard by climate change. Mass migrations can have a substantial impact on the capacity of developed countries to house newly arrived populations. In turn, these influxes of people might influence space-related R&D efforts or public policy agendas or reduce the amount of space program funding.

Besides political effects with the potential to reduce space exploration funding, broadly defined political events could influence space activities in a positive way. For example, if the emergent reality of pandemic waves constitutes a "new normal," that condition might well result in a new nation-state leadership mindset, which puts greater emphasis on multilateralism and collective orientation in the international political system to tackle problems (Williams 2013).

In turn, that new orientation could lead, over time, to enhanced space program effectiveness and efficiencies due to highly coordinated and integrated planning between states, IGOs such as the United Nations, and the private sector. In a complex systems map, it is possible to trace such indirect connections, complete with potential feedback loops to highlight amplification effects between those factors.

Final Reflections

This paper describes the rudiments of a complex systems analysis to illuminate potential security problems associated with an Earth-Moon loop space system. It draws on the neo-realist notion of three levels of analysis to differentiate between long-haul, middle-run and short-run explanatory factors and stressors that interact with stakeholders. In addition to discussing stakeholders, explanatory factors and stressors that are component parts of this Earth-Moon loop system, the paper describes how the frame of this bounded system can have its own set of effects.

Further, the direct and indirect ties between the three building blocks found in this Earth-Moon loop system can be characterized by feedback loops that can add or detract from the individual effects of stakeholders, explanatory factors and the stressors involved. For example, there can be amplification effects between two explanatory factors, or explanatory factor effects that work at cross-purposes with each other, essentially to cancel out the effects of each explanatory factor.

While it is beyond the scope of this paper to craft a more complete complex systems analysis that includes long-haul, middle-run and short-run explanatory factor effects, which contribute to security threats in this space system, it was still possible to scope out some of the major stakeholders, explanatory factors and stressors likely to be active and interactive over the next 30 years. It was also possible to paint some broad brush strokes about possible direct and indirect connections between them.

For example, there are and will be clear connections, both direct and indirect, between nation-states already involved with space launch operations. Also, there are and will continue to be close ties between those states and private companies inextricably bound up in the privatized space industry. In addition, there is the set of ties between government agencies responsible for nation-state space exploration and private companies contracted by government agencies to provide component parts and other related equipment.

Ties between those states and aspirant states involved in space exploration will continue to grow, and links between the private firms utilized by them will strengthen. Indeed, those private firms might have multiple clients across countries and confront conflict-of-interest situations that could pose vulnerabilities in the space security architecture envisioned.

Clearly, the potential for conflict-of-interest issues requires highly sustained and highly coordinated domestic law and international law initiatives. In the case of international law, most effects would probably be sourced in the frame of this Earth-Moon loop system. One complex systems mapping project might focus on the transnational connections between such firms to isolate and identify vulnerabilities and conflict-of-interest potential.

In comparison, the private sector exhibits similar sets of ties to various stakeholders that include some of those countries, as well as some of the same subcontractors used by those countries involved with space exploration research. In the narrower sense, those ties criss-cross across the space industry, and in the broader sense, between the space and computer technology industries, because these sectors are the twin pillars of the space industry. Another complex systems research mapping project might delve into the complex set of interconnections between the computer technology and space industries.

To recapitulate, a robust space security policy architecture that derives from complex systems analysis mapping must have the capacity to illuminate connections within and across a series of Earth-Moon loop subsystems. That requirement is essential because connections between stakeholders and explanatory factors and their interaction with stressors, in particular subsystems, produce subsystem vulnerabilities.

Clearly, those vulnerabilities can be exploited by adversaries who also understand the basics of this Earth-Moon loop system, namely, the particular subsystems under consideration. What is important to note is that in this Earth-Moon loop system, subsystem vulnerabilities and their interaction across subsystems are likely to amplify the effects of individual subsystem vulnerabilities in ways that are integrative rather than additive. In other words, threat is compounded and, in some cases, in unanticipated ways.

It follows that complex systems analysis work on a set of Earth-Moon loop subsystems will eventually lead to a complete Earth-Moon loop system mosaic. Those efforts could help provide a springboard for what is called an "interventions-based" policy, where particular vulnerabilities are illuminated and exposed through a series of complex systems analysis mapping projects. After the identification of vulnerability, informed policy prescriptions, based on the development of scenarios that demonstrate the effects of changing one variable or a set of variables, while holding others constant, can work to reduce vulnerabilities and strengthen subsystems.

In closing, the next step in this policy process is to establish the research direction desired to identify a particular Earth-Moon loop subsystem for much closer examination by means of complex systems analysis. An Earth-Moon loop subsystem could be scoped out by work to distinguish subsystems based on issue area; clusters of nation-state and private space firm connections; private firm supply chains that link OEMs and suppliers; or relationships between nation-states and non-state actors, such as terrorist groups, FTAs or criminal syndicalist organizations, likely to enter into the space system in the future. Delineations of those different research directions would also constitute worthy first steps in the process of work to craft an integrative security architecture for the Earth-Moon loop system envisioned.

Works Cited

Baldwin, David A. 1971. "The Power of Positive Sanctions." *World Politics* 24 (1): 19–38.

Beres, Louis René. 1987. *America Outside the World: The Collapse of U.S. Foreign Policy*. Lexington, MA: D.C. Heath and Company.

———. 1988. "Terrorism and International Law." *Florida International Law Journal* 3 (3): 291–306.

———. 1990. "Confronting Nuclear Terrorism." *Hastings International and Comparative Law Review* 14 (1): 129–54.

Brennan, Louis. 2019. "How Luxembourg is positioning itself to be the centre of space business." The Conversation, July 16. https://theconversation.com/how-luxembourg-is-positioning-itself-to-be-the-centre-of-space-business-120436.

Chasdi, Richard J. 1999. *Serenade of Suffering: A Portrait of Middle East Terrorism, 1968–1993*. Lanham, MD: Lexington Books.

———. 2010. *Counterterror Offensives for the Ghost War World: The Rudiments of Counterterrorism Policy*. Lanham, MD: Lexington Books.

———. 2013. "Risks of Terrorism, Homicide and Illness: A Methodological Consideration." *Perspectives on Terrorism* 7 (6): 126–36.

———. 2018. *Corporate Security Crossroads Responding to Terrorism, Cyberthreats, and Other Hazards in the Global Business Environment*. Santa Barbara, CA: Praeger.

———. 2019. "Tackling Horizontal and Vertical Supply Chain Vulnerabilities: Risks from Interstate Conflict and Terrorism." *Journal of Counterterrorism and Homeland Security International* 24 (4): 10–14.

———. 2021. "Prevention of Major Economic Disruptions Following Acts of Terrorism — The Case of the Bali Bombings of 2002 and 2005." In *Handbook of Terrorism Prevention and Preparedness*, edited by Alex P. Schmid, 985–1026. New York, NY: ICCT, The Hague.

Collins, Liz. n.d. "NASA Wasn't Prepared For What SpaceX's Ship Brought Back." Mental Flare. mentalflare.com/g/spacex-mission-snag/6/?.

Davenport, Christian. 2021. "Rockets aren't enough. Jeff Bezos and the growing commercial space industry now want to build space stations." *The Washington Post*, October 25. www.washingtonpost.com/technology/2021/10/25/private-space-stations-blue-origin-boeing/.

Dawson, Linda. 2018. *War in Space: The Science and Technology Behind Our Next Theater of Conflict.* Cham, Switzerland: Springer Praxis Books.

Denning, Dorothy E. 2001. "Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." *Computer Security Journal* XVI (3): 1–34.

Diamond, Larry. 1990. "Nigeria: Pluralism, Statism and the Struggle for Democracy." In *Politics in Developing Countries: Comparing Experiences with Democracy*, edited by Larry Diamond, Juan L. Linz and Seymour Martin Lipset, 341–409. Boulder, CO: Lynne Rienner.

Flewelling, Brian. 2020. "Securing cislunar space: A vision for U.S. leadership." *Space News*, November 9. https://spacenews.com/op-ed-securing-cislunar-space-a-vision-for-u-s-leadership/.

Fuerth, Leon S. and Evan M. H. Faber. 2012. *Anticipatory Governance Practical Upgrades: Equipping the Executive Branch to Cope with Increasing Speed and Complexity of Major Challenges.* Washington, DC: National Defense University, Center for Technology & National Security Policy. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Anticipatory-Governance.pdf.

Henry, Nicholas. 2013. *Public Administration and Public Affairs.* 12th ed. New York, NY: Pearson.

Hill, Charles W. L. and G. Tomas M. Hult. 2015. *Global Business Today*. 9th ed. New York, NY: McGraw Hill Education.

Ignatius, David. 2021. "Opinion: A great-power game is already underway in space." *The Washington Post,* November 16. www.washingtonpost.com/opinions/2021/11/15/china-russia-and-america-jockey-for-advantage-in-space/.

Kegley, Charles W. 2007. *World Politics: Trend and Transformation.* 11th ed. Boston, MA: Thomson Wadsworth.

McDowell, Jonathan. 2022. "Chinese Space Station – Starlink Encounters." Jonathan's Space Report No. 804, January 18. www.planet4589.org/space/jsr/jsr.html.

Messier, Doug. 2021. "Completion of FAA Environmental Assessment of SpaceX Boca Chica Expansion Delayed At Least Another Month." Parabolic Arc, December 22. www.parabolicarc.com/2021/12/22/completion-of-faa-environmental-assessment-delayed-at-least-another-month/.

Mignon, David, Franck Raballand, Jean-Louis Gonnaud and Sophie Jallade. 2000. "EuroStar 2000 Disposal on a Graveyard Orbit: Orbital Control Strategy and Operational Implementation." EADS Astrium. https://issfd.org/ISSFD_2004/papers/P0132.pdf.

Monahan, John. 2012. "The Individual Risk Assessment of Terrorism." *Psychology, Public Policy, and Law* 18 (2): 167–205. doi:10.1037/a0025792.

Nye, Joseph S., Jr. 1993. *Understanding International Conflicts: An Introduction to Theory and History.* New York, NY: HarperCollins College.

O'Callaghan, Jonathan. 2013. "How many countries have rockets capable of reaching space?" Space Answers, March 21. www.spaceanswers.com/space-exploration/how-many-countries-have-rockets-capable-of-reaching-space/.

Organisation for Economic Co-operation and Development. 2011. *The Space Economy at a Glance 2011.* Paris, France: OECD Publishing. doi:10.1787/9789264111790-en.

Qizhi, He. 1982. "The Problem of Definition and Delimitation of Outer Space." *Journal of Space Law* 10 (2): 157–64.

Reich, Aaron. 2021. "Asteroid the size of Disney castle may be part of Earth's Moon — study." *The Jerusalem Post,* November 12. www.jpost.com/science/asteroid-the-size-of-disney-castle-may-be-piece-of-earths-moon-study-684814.

Reiss, Albert J. and Jeffrey A. Roth, eds. 1993. *Understanding and Preventing Violence.* Washington, DC: National Academy Press.

Rogers, Paul. 2001. *Losing Control: Global Security in the Twenty-first Century.* 3rd ed. New York, NY: Pluto Press.

Ronis, Sheila R. 2007. *Timelines into the Future: Strategic Visioning Methods for Government, Business and Other Organizations.* Lanham, MD: Hamilton Books.

Rosenfield, Stanley B. 1979. "Where Air Space Ends and Outer Space Begins." *Journal of Space Law* 7 (2): 137–48.

Schwartz, Peter. 1991. *The Art of the Long View: Planning for the Future in an Uncertain World.* New York, NY: Doubleday.

Sonne, Paul, Missy Ryan and Christian Davenport. 2021. "Russian satellite strike is viewed as provocative." *The Washington Post,* November 16.

Spich, Robert and Robert Grosse. 2005. "How Does Homeland Security Affect U.S. Firms' International Competitiveness?" *Journal of International Management* 11 (4): 457–78.

Strickland, John K. 2012. "The cislunar gateway with no gate." *The Space Review*, October 1. www.thespacereview.com/article/2165/1.

Stuart, Jeffrey, Angela Dorsey, Farah Alibay and Nuno Filipe. 2017. "Formation Flying and Position Determination for a Space-Based Interferometer in GEO Graveyard Orbit." PowerPoint presentation by Jet Propulsion Laboratory, California Institute of Technology. https://trs.jpl.nasa.gov/bitstream/handle/2014/47460/CL%2317-0971.pdf.

Sydelko, Pamela J. 2014. "Crime on the Urban Edge." Workshop presented at the National Defense University, Washington, DC, September 23.

Waltz, Kenneth N. 1959. *Man, the State, and War: A Theoretical Analysis.* New York, NY: Columbia University Press.

———. 1973. "The Meaning of Anarchy." In *International Politics: Anarchy, Force, Imperialism*, edited by Robert J. Art and Robert Jervis, 10–20. Boston, MA: Little, Brown and Company.

Whitley, Ryan and Roland Martinez. 2016. "Options for Staging Orbits in Cis-Lunar Space." Annual IEEE Aerospace Conference Paper. https://ntrs.nasa.gov/api/citations/20150019648/downloads/20150019648.pdf.

Williams, Phil. 2013. "Lawlessness and Disorder: An Emerging Paradigm for the 21st Century." In *Convergence: Illicit Networks and National Security in the Age of Globalization*, edited by Michael Miklancik and Jaqueline Brewer, 15–36. Washington, DC: National Defense University Press.

Yergin, Daniel. 2011. *The Quest: Energy, Security and the Remaking of the Modern World.* New York, NY: Penguin Press.

Centre for International
Governance Innovation

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

@cigionline

RECYCLED
Paper made from recycled material
FSC® C023070
www.fsc.org