CENTER FOR SPACE POLICY AND STRATEGY

AUGUST 2022

COMMERCIAL NORMENTUM: SPACE SECURITY CHALLENGES, COMMERCIAL ACTORS, AND NORMS OF BEHAVIOR

ROBIN DICKEY
THE AEROSPACE CORPORATION

AEROSPACE

ROBIN DICKEY

Robin Dickey is a space policy and strategy analyst at The Aerospace Corporation's Center for Space Policy and Strategy, focusing on national security space. Her prior experience includes risk analysis, legislative affairs, and international development. She earned her bachelor's and master's degrees in international studies at Johns Hopkins University.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

Contact us at www.aerospace.org/policy or policy@aero.org

Summary

Concerns about the potential for conflict in space are not limited to traditional security actors such as states and militaries. Commercial actors also have a stake in security-related space norms, and this stakeholder relationship may translate to new forms of commercial participation in the norm development process. This paper seeks to find potential norms that would serve both commercial and military actors' interests and evaluates how commercial actors may contribute to their development and implementation. Scenarios in which commercial actors may be threatened in space and cases from other domains help to explore both the potential threats and normative responses. Commercial actors and policymakers could consider which potential norms may reduce the risk and threat to commercial actors, which norms are heavily impacted by commercial behavior, and which norms are costly for commercial compliance. Policymakers and business leaders alike will need to evaluate how commercial participation could proceed, with options including engagement with relevant government stakeholders, participation in international forums and working groups, and industry consortia and public advocacy. Proactive commercial contribution to security-related space norm discussions will be a crucial step in helping commercial actors navigate and mitigate potential threats with less disruption to the capabilities and services they provide their customers and the world.

Introduction

Commercial actors have steadily increased the size and significance of their roles in international space activities. Companies operate the majority of satellites in orbit and provide crucial services for both civilians and militaries around the world, ranging from launch services to satellite communications to Earth observation data. As a result, governments, international organizations, and companies have expressed increasing interest in commercial participation in the development, codification, and adoption of norms of behavior for space.

Commercial involvement in the development of norms of behavior in space has mostly been limited to issues of space safety and sustainability in peacetime. However, peacetime may not always be the context for commercial space activities. Commercial activities in space will continue in times of tension, and commercial systems and activities will face risks and threats during conflict. Policymakers and commercial leaders alike must consider these situations when forming a complete picture of commercial participation in space norms.

This paper demonstrates the expanded possibilities for commercial stakeholders to participate in the development of space norms beyond safety and sustainability in peacetime, including into situations involving hostile action.

The paper references three non-space examples of norm efforts aimed at mitigating threats to commercial actors during crisis or conflict: responses to collateral damage to civilians caused from indiscriminate weapons like landmines, attempts to prevent shootdowns of commercial aircraft, and efforts to deter deliberate targeting of commercial maritime shipping. All three examples help to explore how commercial actors would be impacted by a wide range of potential security-related norms for space activities. Then, the options for commercial participation in norm development are considered and analyzed in terms of factors that may drive a need for commercial participation. Commercial actors possess more options and motivations for getting involved in space norm development than have often been discussed. This paper explores these options.

Current Status of Commercial Participation in Space Norms

Although there is no universally agreed-upon definition for "norms of behavior," this analysis adopts the definition of norms as *generally accepted standards of appropriate behavior*.[1] This broad definition encompasses a range of agreements and diplomatic mechanisms such as voluntary guidelines, proliferated best practices, entrenched customs, technical standards, and even binding treaties. Each of these mechanisms has its own definition. "Standards," for example, are commonly defined as sets of codified rules describing requirements, specifications, or characteristics that can be used consistently to ensure that materials, products, processes, and services are interoperable while "best practices" are defined as techniques or methodologies that have been proven to reliably lead to a desired result through experience and research.[2] Not all examples of these mechanisms are norms. The key common element that determines whether a specific example of a mechanism is also a norm is broad agreement among a relevant community that certain behaviors are acceptable or unacceptable. So, a standard adopted by a group of commercial satellite operators for interoperable systems to use during rendezvous and proximity operations (RPOs) would become a norm if the vast majority of operators conducting RPOs started following the same standards and criticized operators who did not follow along. This last element of criticizing or imposing costs on those who do not comply with a norm is crucial to the norm's degree of development and acceptance. A norm may still exist if certain actors violate it, but only if the rest of the community is willing to call out the unacceptable behavior and impose costs.[3]

International debate on space norms of behavior tends to fall into two categories: (1) safety and sustainability issues and (2) security issues. These categories are typically discussed in different international fora, often involving different terminology and different actors. Within the United Nations (UN) framework, member states typically discuss safety and sustainability issues in the Committee on the Peaceful Uses of Outer Space (COPUOS) and reserve security issues for the Conference on Disarmament, the Institute for Disarmament Research (UNIDIR), and the UN First Committee. Commercial actors have long been more welcome in discussions on safety and sustainability norms than security norms.

Commercial space actors have demonstrated mixed interest in participating in the development of norms outside of a peacetime safety and sustainability context. A 2018 survey of "Commercial Companies' Perceptions of Security Space" received written and verbal input from over 100 commercial experts. The researchers concluded

that, with some exceptions stemming from companies that provide direct services to the U.S. military, most respondents saw security issues as having low relevance to day-to-day commercial operations and deferred to the government for maintaining security.[4] In a 2021 workshop for the space industry hosted by the United Nations Institute for Disarmament Research (UNIDIR), some discussants indicated that they had witnessed hostility towards industry participation in security-related discussions for both geopolitical and technical reasons.[5] The report concluded that "some companies may exercise caution in engaging because of concerns over alienating their customers."[6] As a result, commercial actors tend not to participate in discussions related to security issues in outer space.

However, with major powers talking more explicitly about an era of militarized competition, commercial actors will likely have to operate in times that are not so peaceful, and commercial companies will not be exempt if conflict breaks out. In those situations, norms could help to mitigate some of the risks and threats for commercial operators. There are already signs indicating some commercial actors may be paying increased attention to space security-related norms. Numerous companies have started publicly criticizing behaviors by militaries that cause disruptions or hazards in the space environment. Inmarsat, for example, recently published a space sustainability report commenting on a number of security-related topics, including anti-satellite (ASAT) missile testing and hybrid warfare in space.[7] In the report, Inmarsat proposed normative and policy efforts such as promoting kinetic ASAT testing moratoriums, lower thresholds for calling out nefarious or reckless activities in orbit by other governments, and formal mechanisms for governments and commercial satellite operators to share intelligence.[8]

As concerns about conflict in space increase, policymakers and business leaders will need to explore the stake that commercial actors have in security-related space norms. This stakeholder relationship may translate to new forms of commercial participation in the development process for norms of behavior in space.

The Intersection of Commercial Actors, Norms of Behavior, and Space Security

This analysis uses three cases of possible threats to commercial satellites and space activities to derive potential security-related norms that could benefit from commercial involvement. The three cases vary in the directness of the threat to commercial actors by states. In order of increasing intentionality of threats, commercial systems could face:

- Collateral damage from attacks on military objectives
- Attacks due to misidentification or misinterpretation of a commercial activity
- Deliberate targeting—either kinetic or non-kinetic—in war

In the absence of public evidence of overtly hostile, physical attacks on adversaries' satellites,[*] examples from other domains can contribute to analysis on the possibilities for the intersection of security and commercial actors in space. First, the issue of collateral damage to civilians, civilian property, and commercial actors is examined through the efforts to prevent indiscriminate casualties from landmines. To explore what happens

[*]There have been cases of deliberate frequency jamming, cyberattacks or interference with satellites, and destructive demonstrations of anti-satellite (ASAT) weapons against a country's own satellite. For more, see the counter-space threat assessments produced by the Defense Intelligence Agency, Center for Strategic and International Studies, and Secure World Foundation.

when commercial actors are misidentified or mistakenly perceived to be undertaking hostile military action, the analysis considers shoot-downs of commercial airliners. Finally, to investigate the issues arising when commercial systems become a target of war, the analysis considers intentional attacks on maritime commercial shipping. Table 1 summarizes the seven potential norms discussed across the three scenarios

Commercial/Civilian Collateral Damage

Civilians and their property have been unintentional victims of crises and conflicts throughout the history of war. In this case, the term "collateral damage" refers to incidental harm to civilians or their property caused by attacks or the use of weapons targeted at military objectives. This can happen in conflict due to the proximity of civilians to military objectives or due to the use of weapons with indiscriminate effects. The case of antipersonnel (AP) landmines and their use in the 20th century provides an example of how international norms can be developed in response to collateral damage. This parallels the challenges of indiscriminate systems in space—like debris-producing anti-satellite weapons and other, both physical and non-physical, forms of collateral damage.

Land Domain Threat Example: Antipersonnel (AP) Landmines

Combatants used landmines in almost every conflict around the world in the 20th century. In 1996, the International Committee of the Red Cross (ICRC) released a report reviewing 26 conflicts in which mines were used between 1940 and 1995, concluding that in most cases AP mines in particular posed a significant threat to civilians long after conflicts had concluded because their locations were poorly marked and mines are much more difficult to remove than they are to plant.[9] A 1994 U.S. State Department report to Congress had reached similar conclusions, reporting that "these mines remain active and deadly long after conflicts cease, killing and maiming an estimated 26,000 people, mostly innocent civilians, every year."[10] Lingering landmines, especially the smaller AP landmines that are easier for individuals to accidentally trigger, have affected economics and commerce beyond the direct effects on civilians. For example, landmines killed 9,000 cattle and an unknown number of other livestock in Zimbabwe between 1980 and 1995, devastating incomes of peasant farmers in the area.[11]

Table 1: List of Potential Norms with Security Implications and a Commercial Stake

Collateral Damage	Misidentification and Misperception	Deliberate Targeting During Conflict
Bans or limits on kinetic anti-satellite tests or deliberate debris production	Effective practices and means of deconflicting/adjudicating SSA data	Standards and best practices to make commercial satellites a harder target
Further implementation and enforcement of existing norms related to indiscriminate acts such as nuclear detonations or radiofrequency interference	Crisis or emergency lines of communication	Designation of "off-limits" commercial satellites
	Common definitions of threatening behavior	

Although not a perfect analogy, the landmine example shares several characteristics with the issue of indiscriminate, particularly debris-related, threats and hazards in space: landmines can cause a persistent threat over decades after a conflict; are more expensive to remove than to create; can prevent commercial and civilian activity in an area by creating serious risks and costs; and are often difficult to locate, map, and track. The physics of space provide the potential for indiscriminate damage to civilian and commercial property but have some unique complicating attributes. If an airplane is destroyed, it crashes. If a ship at sea is destroyed, it sinks. If a satellite is destroyed, it breaks up into hundreds, thousands, or hundreds of thousands of missiles that travel thousands of miles per hour, intersecting the paths of other satellites, over and over again potentially for decades, depending on the altitude. This means that the destruction of a satellite in a conflict could result in the destruction of a commercial satellite on the other side of the world months or years later, a similar dynamic to the persistent threat of landmines for decades after they were deployed.

Potential Norm Against Destructive ASAT Testing

A norm development effort is brewing in response to debris-producing anti-satellite (ASAT) weapons tests in space. China, the United States, India, and Russia have each destroyed at least one of their own satellites using a direct-ascent missile in the last 15 years. The indiscriminate debris from ASAT tests can pose a threat to military, civil, and commercial space actors alike, and so commercial actors would have a stake in norms minimizing the threat. Commercial actors have become more vocal protesting debris-producing ASAT tests. When China conducted a debris-generating ASAT test in 2007, the condemnation mainly came from governments. When Russia, in 2021, tested a kinetic ASAT weapon by destroying one of its own satellites above 400 kilometers in altitude, condemnations came from numerous commercial space actors as well. Criticism of the test came from leaders from SpaceX, SES, Airbus, Astroscale, United Launch Alliance, Axiom Space, Planet, Virgin Orbit, the Space Data Association, the Secure World Foundation, the American Institute of Aeronautics and Astronautics, and the Satellite Industry Association. When Vice President Kamala Harris announced a unilateral commitment not to conduct destructive direct-ascent ASAT missile tests as part of an effort to build an international norm, several of those commercial entities (such as Planet, Astroscale, and the Space Data Association) publicly applauded the announcement.[12] These responses indicate that commercial actors are increasingly paying attention to space security issues out of recognition that debris threatens everyone in space. Therefore, commercial actors have a stake in influencing or promoting the development of international norms that deter kinetic ASAT tests and the deliberate production of debris.

To some extent, this new focus represents commercial companies' growing interest in space safety and sustainability. Nevertheless, the inclusion of ASATs in the international space norms discussion tips commercial companies' participation into the security field.

Potential Norms for Other Indiscriminate Attacks and Interference

Other security-focused activities in space can also have indiscriminate effects, creating some crossover between security, safety, and sustainability issues. Nuclear detonations and radio frequency interference (RFI) could also significantly affect satellites or activities that were not the target of an attack. There are norms, laws, and international organizations intended specifically to prevent the testing, placement, or use of nuclear weapons in

outer space and to minimize RFI by regulating usage of the radiofrequency spectrum. The maintenance and implementation of these norms, however, will likely involve increasing interest and participation by commercial actors.

RFI is particularly challenging because it can happen both intentionally and unintentionally, and the difficulty of determining intent in a case of RFI can further blur the lines between safety, sustainability, and security. The prevention of RFI is a key objective of the International Telecommunication Union (ITU), which creates new legally binding provisions related to international spectrum sharing at the World Radio Conference every four years. From a norm perspective, most of the challenges will revolve around establishing distinction between accidental RFI, targeted RFI, and collateral (not targeted at the systems that are affected) RFI. Because RFI can happen so frequently, some satellite operators like Eutelsat seek to participate in the space security discussions on the future of electromagnetic interference more than any other security issue.[13] As commercial use of spectrum increases, inputs and cooperation from commercial actors in norm development will become more significant in distinguishing between RFI from day-to-day operations and RFI driven by crisis, conflict, or competition.

The issue of nuclear detonations, on the other hand, is much less entangled with commercial actors. Nuclear tests in space, like STARFISH PRIME in 1962, proved that nuclear detonations and the resulting electromagnetic pulse and radiation have devastating effects on space activities: one third of satellites in orbit at the time were damaged or destroyed.[14] Since the 1963 signing of the Limited Test Ban Treaty prohibiting such detonations in space and the 1967 Outer Space Treaty's prohibition on placing nuclear weapons in orbit or stationing them in space at all, the space security norms related to nuclear weapons have been some of the strongest in the domain. Because these norms are enshrined into international law, commercial and noncommercial actors do not need to relitigate the issue. However, there are gaps and ambiguities in the international legal regime that could pose challenges for implementation and enforcement of the norms in the future, such as the lack of a universal definition of space and whether there should be specific norms against interfering with nuclear-powered satellites. Commercial actors may not need to be involved directly in some of these discussions related exclusively to state nuclear capabilities, but it is worth recognizing that they, too, would be affected were nuclear norms violated in space.

Table 2 summarizes some of the potential security-related norms, discussed above, in which commercial actors have a stake in the discussion from the perspective of preventing collateral damage. These potential norms (such as a ban on

Table 2: Potential Norms with Commercial Stake to Prevent Collateral Damage

Norm	Commercial Stake
Ban or limit kinetic anti-satellite (ASAT) tests or deliberate debris production.	Reduce likelihood of debris proliferation in a crisis/conflict, which would threaten commercial satellites indiscriminately.
Further implementation and enforcement of existing norms limiting indiscriminate acts.	Support deterrence/regulation of use of systems that can have indiscriminate effects on commercial operations, such as nuclear detonations or RFI.

kinetic ASAT testing, prevention of nuclear detonations, or limits on indiscriminate RFI in space) all focus on state behaviors and capabilities, so a commercial role in norm development may have been previously overlooked. But commercial actors can face significant costs in loss of satellites or disruption of services, so these actors do have a stake in the success or failure of these norms.

Misidentification and Suspicion in Crisis and Conflict

In crises and conflicts, commercial space actors also risk getting caught in the middle of a tense and escalatory environment. Commercial systems may be targeted or attacked in these situations, whether intentionally or accidentally. The attack could occur either because a commercial system is misidentified as a military system or because that commercial system is suspected of acting aggressively or threateningly.[†] Although this scenario is still hypothetical in space, examples pulled from the air domain and shoot-downs of commercial airliners can help explore the risk posed to commercial spacecraft during times of crisis. This in turn aids the identification of potential space norms with a security nexus and a commercial stake.

Lessons from norm development following commercial airline shoot-downs can be applied to space. A comparison of the air and space domains indicates several potential security-related space norms that could involve a commercial stake or participation despite the differences between the domains.

There are several mitigating factors when translating from air to space that might help limit the likelihood of similar attacks on commercial spacecraft. In the air domain, the shooting state often had minutes or seconds to determine whether an aircraft was a genuine threat and attack it. In space, timelines for identifying and responding to a concern can span hours or days due to the vast distances involved in space and relative predictability of satellite trajectories. This may reduce the tension and pressure to assume the worst seen in the air domain, especially if coupled with trusted space situational awareness capabilities. The

Air Domain Threat Example: Commercial Aircraft Shoot-Downs

Since the early 1950s, there have been at least 11 cases of states shooting down commercial aircraft. Most of the incidents began with states perceiving a commercial aircraft as a threat and trying to determine a response under speed, distance, and time pressure exacerbated by the context of crisis or conflict. In some cases, like the 1988 U.S. shoot-down of Iran Air Flight 655 and the 2020 Iranian shoot-down of a Ukraine International Airlines plane, the shooting state misidentified the aircraft as a missile or fighter aircraft of an adversary.[15] In other cases, states did not immediately misidentify the aircraft but were unsure and determined that the behavior of the aircraft or proximity to sensitive airspace justified an intercept. When Korean Airlines Flight (KAL) 007 entered Soviet airspace after deviating from its planned route, the Soviet Union shot it down. Soviet officials claimed that the pilot of Flight 007 had not responded to the visual signals of the intercepting aircraft and that they were therefore justified in shooting it down because they suspected the aircraft was on a reconnaissance mission.[16] Shooting states demonstrated varying behaviors in the aftermath of cases similar to KAL 007: some apologized and undertook compensation for the victims despite claiming justification, others refused to admit wrongdoing at all.

[†]This is not to say that perceptions of commercial behavior as threatening are always mistaken. Especially as commercial actors provide an increasing range of services to militaries, commercial satellites could become viable military targets under the Law of Armed Conflict. This discussion instead focuses on cases in which commercial behavior, like a close approach or incident of radio interference, was not intended by the commercial actor and not a deliberate threat but is perceived as such by a military or state actor.

form of "attack" in space also might not be as kinetic as the air domain shoot-downs and may involve nonkinetic or reversible interference, such as jamming or cyberattacks. Another characteristic of space that may mitigate the threat is, as established in Article II of the Outer Space Treaty, states cannot claim sovereignty over any part of space.[17] Many of the attacked commercial aircraft had entered or were approaching the sovereign airspace of the shooting state, heightening the state's perception of a direct threat or violation. Since there is no "territory" belonging to states that can be violated in space, there may be fewer sensitivities over a commercial satellite's location. Similarly, there have been at most only 19 humans in space at a time as of December 2021, so satellite proximity issues will typically not involve a perceived direct threat to human life.[18] If commercial satellites are not infringing on sovereign territory or posing a risk to humans, this might lower the intensity of potential crises and reduce the likelihood of states attacking commercial satellites out of fear.

On the other hand, there are several factors that may heighten the costs or risks of escalation against commercial systems in space. The lack of direct threat to human life in space may be counteracted by the *indirect* threat to human life on Earth that would be posed by disruption to vital infrastructure supported by space—such as communication, navigation, and situational awareness for emergency responders.[19] Although large numbers of humans have not ventured to space thus far, this may gradually increase in the future through the expansion of space tourism and commercial and national space stations in low Earth orbit. States have already demonstrated quick and sometimes harsh responses to space activities perceived to threaten the safety of astronauts in orbit. The increasing role that commercial satellites play in providing services such as communication and remote sensing to militaries could also contribute to heightened perceptions of commercial satellites as potential threats.

Furthermore, commercial satellites do not need to have weapons capabilities *or* hostile intent in order to pose a risk to other space systems. When objects are traveling as fast as 5 miles per second (the speed of the International Space Station), a completely unintentional collision can be just as destructive as a targeted attack.[20] Even if causing a collision using an operational satellite is perhaps not the most likely form of attack in space, the pressures to assume the worst of an approaching satellite might outweigh such unlikelihood in the minds of military decisionmakers. And commercial satellites are far from immune to the software errors, technical navigation challenges, or maneuvering malfunctions that could send a satellite speeding toward another country's sensitive satellite the way KAL 007 sped towards a military base on Sakhalin Island. This complicates the space application of norms that were developed to prevent hasty shoot-downs of commercial aircraft by lowering the threshold for what could be perceived as a threat in space.

Role of Space Situational Awareness in Preventing Misperception and Escalation

Commercial airliner shoot-downs and potential threats to commercial satellites do, however, share limits and failures in navigation, situational awareness, and communications. The aircraft shoot-downs demonstrated how significantly a lack of situational awareness can exacerbate misunderstandings. The vast dimensions of space and typically robotic nature of its occupants means that there is rarely an opportunity for a concerned state to look visually at a satellite and recognize whether it is commercial or military. Instead, satellite operators rely on complex sensors and trackers—often not even their own—to determine from afar what an object is and where it is going. Space situational awareness (SSA) capabilities are improving significantly, but there are still plenty of errors and disagreements. For example, a rocket body originally identified as the second stage of a

SpaceX Falcon 9 was projected to crash into the moon in March 2022. Observers determined, in February 2022, that the object had been likely misidentified and was probably from China's Chang'e 5-T1 mission.[21] Even this identification was not made with 100 percent confidence because all attempts to identify the rocket were based on "circumstantial evidence" and China has claimed that the Chinese rocket body in question had already reentered Earth's atmosphere.[22]

Even for objects closer to Earth, different SSA providers determine different likelihoods of collision between objects because they use different models and assumptions, which is further exacerbated by different notions of how close is "too close." This was exemplified by China's complaint that several Starlink satellites had passed too close to their Tianhe space station, forcing it to maneuver out of the way. The United States responded that their own SSA system had assessed that the Starlink satellites were not passing close enough to Tianhe to merit a conjunction warning.[23] At least for the near future, misidentifications, accusations, and conflicting threat perceptions in space could lead to potentially escalatory concerns and disagreements.

One normative and policy approach in response to commercial aircraft shoot-downs was to improve commercial pilots' awareness of where they were relative to sensitive airspace. Flight KAL 007—and others before it—had likely wandered off course due to instrument error. In response, President Ronald Reagan decided to make the signals from the next generation of Global Positioning System (GPS) available for free to civilians, which came into full effect in the mid-1990s.[24] None of the major shoot-downs of commercial airliners after 1995 occurred because the commercial aircraft was significantly off course. Similarly, norms aimed at providing clearer data to satellite operators of where they are relative to others in space could help reduce the risk of misidentification or escalatory close approach incidents.

Norms related to SSA data sharing often involve issues of space safety and sustainability. However, having a grasp on where space objects are and what they are doing also plays a significant role in space security considerations, and the application of norms can change significantly based on whether there is a context of crisis or conflict. This is especially the case when states rely on SSA data to identify threats and investigate intent. The more that different actors operate using incomplete or contradictory pictures of the space environment, the more possibilities there are for miscalculations, misperceptions, and escalatory disputes. One report written for the Strategic Multi-layer Assessment (SMA) argued that transparency in space communications "can be an important tool for mitigating or avoiding conflict spirals that can occur based on misperception" and that agreement on key space terms used in SSA communication is an important aspect of maintaining space security.[25] Commercial actors would also benefit from the security applications of these norms through opportunities to provide evidence and demonstrate that they are not a threat to a concerned state. In a paper titled "Safety Norms for Space Security," Daniel Porras and Letitia Zarkan proposed a norm for the "sharing of mission data among government agencies, companies, and organizations, as a means of creating trust among all space actors."[26] Commercial actors with this knowledge and trust can better convey to other countries their intentions and activities to deescalate misunderstandings. Some data sharing efforts involving commercial actors are already under way, such as through the Space Data Association's promotion of best practices and operational data sharing between both commercial and state participants.[27] However, the development of an information-sharing norm involving commercial actors may also face obstacles, such as the desire of commercial actors to maintain a competitive advantage or to protect intellectual property—issues that might need to be balanced and considered in order to gain commercial support.

Potential Norms for Communication and Coordination

Related to the issues of common standards for SSA and norms of sharing SSA data, norms can also help to facilitate lines of communication that could be used to de-escalate issues between commercial and state actors. In the Starlink-Tianhe case, Chinese officials claim to have tried to reach out to SpaceX to try to resolve the conjunctions while American officials claim that neither the United States nor SpaceX received any attempts at contact.[28] Similar communication issues came to light in 2015 when a Russian military satellite maneuvered to sit between two satellites belonging to the company Intelsat. Intelsat reportedly tried to contact the owners of the Russian satellite both directly and through the Department of Defense and did not receive a response, leaving Intelsat concerned about whether their satellites were under threat.[29]

Missed connections in communications were the most common factor in the shoot-down incidents of commercial aircraft. In many cases, the commercial aircraft did not receive military attempts to communicate because they were listening to the wrong radio frequencies or could not perceive visual or sound cues due to the weather or time of night.[30] Due to the tense context of crisis or conflict and speed of the aircraft relative to sensitive areas, states had only minutes to make decisions and assumed the worst of unresponsive aircraft. The International Civil Aviation Organization (ICAO) attempted to remedy the issue through a clearer step-by-step process as the norm for how to intercept unidentified aircraft, including visual and radio signals that should be used.[31] The absence of common practices and procedures for establishing contact between satellite operators of different countries could be a sign of risk to come in space. Norms could help to clarify efficient and reliable processes for establishing rapport before the situation escalates to violence. Norms could be developed to answer questions such as whether operators in companies and foreign states should contact each other directly or if communications should be facilitated by the states to which the commercial operators belong or the states that registered the space objects in question. Common expectations for using certain methods to convey concerns would also make it easier to determine whether an attempt to communicate was accidentally missed or deliberately ignored.

Using Norms to Express Threat Perceptions

Finally, norms can establish common understanding of which behaviors will be interpreted by states as a threat, which can in turn inform commercial actors on which actions to avoid. In the air domain, the ICAO weighed in on the normative dispute over threat perceptions in 1984 by amending the Convention on International Civil Aviation to indicate "every State must refrain from resorting to the use of weapons against civil aircraft in flight."[32] After this point, the norm solidified to placing the burden on states to correctly identify aircraft and established a higher threshold for what behavior by a civilian aircraft constitutes a threat. As implied by Porras, Zarkan, and the SMA report on clarifying space language and behavioral norms, shared definitions of "threatening behavior" will also solidify the state perspectives on when it is acceptable or not acceptable to attack a commercial or unidentified satellite.[33] How close can a satellite get or what actions can it take before a state is allowed to use force against it? What measures are states expected to take to identify and communicate with satellites before they can be categorized as a threat? Is the burden to prove that a satellite is not a threat on the state, the commercial operator, or some combination of the two? Answering any of these questions could help to prevent misperceptions and miscalculations.

There are many similarities, differences, exacerbating factors, and mitigating factors in comparing commercial aircraft shoot-downs to the potential threats to commercial satellites. This

comparison illustrates several potential space norms with security applications in which commercial actors may have a stake. Table 3 summarizes the stake that commercial space actors could have in three of these potential norms.

Deliberate Targeting During Conflict

In war, commercial actors can become strategic targets of combatants. This scenario applies to both commercial actors that are providing support to militaries, which could be valid military targets under the Law of Armed Conflict, and to those that are not. Although commercial actors are less protected by international law and more likely to be targeted if they are directly supporting military missions and objectives, commercial systems have become targets even when they do not support military missions at all. In space as on Earth, there is no guarantee that all combatants will distinguish between commercial actors directly involved or not in a conflict. Commercial actors could especially come under threat if a combatant sees strategic value in disrupting economic and infrastructure functions in space to weaken the societies of their opponents. A key example of this dynamic comes from the maritime domain, in which commercial shipping has frequently been a subject of attack in wars and conflicts.

Maritime Domain Threat Example: Attacks on Commercial Maritime Shipping

Commercial maritime shipping has frequently been the subject of deliberate campaigns of targeting and destruction during wars. In World War I and the Iran-Iraq War, for example, one or more combatants took repeated actions to commandeer or sink commercial ships belonging either to opposing combatants or to ostensibly neutral countries supporting the opponents. These attacks were often not limited to commercial actors providing direct support to the military, such as weapons shipments or troop transports. In some cases, like Germany in World War I, the strategy was to economically cripple their opponent, Great Britain.[34] In others, like with Iranian attacks on Kuwaiti oil shipping during the Iran-Iraq war, the attacker attempted to deter noncombatant states from supporting the attacker's opponents, trying to convince the Gulf States to pressure Iraq to stop its own attacks on Iranian oil.[35] Whatever the reason, commercial shipping often faces high risk in the vicinity of conflicts, sometimes regardless of its nexus to supporting the combatants directly and despite international laws of armed conflict intended to prevent attacks on civilians.

Table 3: Potential Norms with Commercial Stake to Prevent Crisis Escalation

Security Norm	Commercial Stake
Effective practices and means of deconflicting/ adjudicating SSA data.	Easier state identification and characterization of commercial activities, improve commercial awareness of potential high-risk situations or close approaches with sensitive satellites.
Crisis or emergency lines of communication.	More efficient and reliable means of de-escalating commercial-military security concerns. Prevent misinterpretation of intent caused by lack of communications.
Common definitions of threatening behavior.	Improve commercial understanding of which behaviors could result in threat or attack by state actors to avoid those behaviors or have preemptive conversations when unavoidable.

This example of threats to commercial actors demonstrates more the risks that commercial systems could face in a space conflict than it shows any specific normative actions commercial actors can take. However, an understanding of the potential threat can help to identify challenges and mitigating factors of which commercial actors may need to be aware.

There is increasing discussion that the risk to commercial space actors might not be as small as once thought. Leaders of companies such as COMSPOC, which is focused on space situational awareness, have raised concerns that commercial satellites could be the first targets in a conflict.[36] In 2019, then-nominee for Secretary of Defense, Mark Esper, indicated that adversaries were unlikely to discriminate between U.S. military satellites and commercial satellites providing military services.[37] Another DOD official took the concern a step further by arguing "it would actually be surprising if China made any distinction in its war planning, given the fact that China does not differentiate between military, civil and commercial space activities or entities."[38] Were conflict to significantly escalate in space, the potential lack of distinction between military and commercial satellites could result in targeting of even commercial satellites that do not provide military services.

Several characteristics of space could limit the likelihood of direct attacks on commercial satellites. As frequently as deliberate constriction of trade and infrastructure has been utilized in war through sieges or blockades, there is not yet a clear understanding of the effects of a "space blockade" on a state's ability to pursue a conflict. If an aggressor is not confident of a military justification for an attack on a particular commercial operator, it may not decide that such an action is worth the military or diplomatic costs. The other mitigating factor is that those costs on the aggressor could be higher for targets in space than in other domains because of the previously discussed indiscriminate nature of several possible types of attacks. Just as a kinetic attack on a military target in space could result in debris threats for commercial satellites, a kinetic attack on another country's commercial satellites could create debris that in turn threatens the aggressor's satellites. This could lead to a lower likelihood of commercial satellites being attacked than terrestrial targets. An aggressor may instead target a ground station or opt for more limited means of attack, such as reversible or temporary interference through jamming or cyber intrusions.

On the other hand, in a conflict spanning both Earth and space, commercial satellites may be attractive targets for two reasons: (1) the vast majority of satellites are uncrewed, so attacking satellites may be seen as less escalatory because it does not directly harm or kill humans, (2) satellites are very difficult to defend and therefore may be seen as easy targets. Policymakers and strategists often repeat the mantra that "satellites don't have mothers," which raises the question of whether a state would willingly escalate a conflict to retaliate against an attack with no direct human casualties.[39] Congressman Jim Cooper, chairman of the U.S. House of Representatives Subcommittee on Strategic Forces, echoed this sentiment in July 2021 by arguing that "no one should die for a robot."[40] Satellites are also vulnerable to attack because they travel in predictable orbits, are slow to maneuver, and many potential defenses are prohibitively expensive or infeasible given the constraints of physics in space.[‡]

[‡] It is also not clear yet what a "protector" satellite could or should do if responsive systems were possible. For more on the physics-based limitations on potential maneuvers or engagements in space, see Rebecca Reesman and James R. Wilson, "The Physics of Space War: How Orbital Dynamics Constrain Space-to-Space Engagements," The Aerospace Corporation Center for Space Policy and Strategy (October 2020), https://csps.aerospace.org/sites/default/files/2021-08/Reesman_PhysicsWarSpace_20201001.pdf

The range of potential nonkinetic threats—such as RFI, directed-energy disruption of sensors, or cyberattacks—also indicates that an attacker may use less provocative or destructive options to undermine commercial actors. Commercial satellites are particularly vulnerable because they do not require military-level security and protection standards for hardware or software design and implementation. While this is not necessarily an issue for larger space companies that have invested in significant cyber protections, it is a limitation on companies with fewer resources. As one commercial satellite operator indicated, "We just don't as a small company have the money to really put into practice cyber security controls."[41] All of this is compounded by the difficulty in attributing nonkinetic attacks and activities in space, which can make it more difficult to respond.

These nonkinetic, temporary, and reversible forms of interference and attack have been perceived by some commercial actors as the most likely threat, a perception that has been reinforced by events during the 2022 Russian invasion of Ukraine.[42] Around the beginning of the invasion in February, SpaceX reported jamming of Starlink satellite communications in Ukraine, and a cyberattack on the Viasat KA-SAT satellite internet network disabled modems serving tens of thousands of customers in Ukraine and around the region.[43] In March 2022, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued an alert about possible cyber threats to satellite communication networks "given the current geopolitical situation" and provided a list of recommendations for how to mitigate the threat.[44] This uptick in threats to commercial satellite operators in and around a terrestrial conflict could signal a recurring trend in future conflicts.

Potential Norms or Standards for Commercial Security Measures

One potential avenue for norms to help mitigate this issue is to develop standards, practices, and support systems to help commercial actors protect themselves. For example, commercial actors have been integral to the development of norms for maritime security and protection against nonstate, criminal piracy in West Africa. The 2021 Gulf of Guinea Declaration on Suppression of Piracy was signed by over 400 maritime industry stakeholders, including a mix of states, ship owners, and shipping associations.[45] The Declaration promoted international collaboration norms and implementation of the Best Management Practices West Africa, which established a series of practices "to help ships plan their voyage and to detect, avoid, deter, delay and report attacks."[46] Although the threat of nonstate, criminal attacks differs significantly from the types of attacks conducted by state actors, this case demonstrates that commercial actors have previously taken a collaborative, normative approach to attempt to deter attacks. Similar space efforts may not have any effect on state actors determined to destroy a commercial satellite but could have a marginal impact on the effectiveness of more limited or reversible attempts at interference.

Protections against limited or reversible means of attack, such as electromagnetic interference or cyberattacks, could be regulated by establishing minimum cybersecurity standards, especially if there is a public safety or critical infrastructure concern. Protections could also be promoted voluntarily through promulgation of best practices or programs that provide funding and training to improve security. Some efforts of this type are already underway. For example, the National Institute of Standards and Technology (NIST) has been developing a report providing background and risk management concepts for cybersecurity for commercial space actors.[47] Organizations like the Space Information Sharing and Analysis Center (Space ISAC) aim to improve security and resilience against threats in the space sector by sharing intelligence on threats and vulnerabilities and by providing educational resources.[48] Frank

Backes, Senior Vice President of Kratos Space and the Board Chair of Space ISAC, argued that "without question, there are security standards that any company in the space sector can be deploying within their organizations."[49] Wider application of these standards could provide the foundation for a norm promoting commercial protection from threats.

It is up for debate whether these measures would actually constitute potential norms or if the possibilities are so dependent on the activities, interests, and resources of each individual commercial actor that community-wide consensus and normative pressure would not be possible. Following this paper's definition of a norm, the turning point between individual best practices and a broader norm for security standards would be a trend of criticizing or imposing social costs on commercial actors who notably fail to follow the common standard. This point may never be reached, or it may appear among specific subsets of commercial actors, such as among telecommunications providers or among companies providing direct services to militaries. Commercial and government leaders alike will need to consider whether there are benefits for developing a common approach or if the most practical option is for each actor to define its own security practices.

Norms and Deterrence: Can Commercial Satellites Be Declared "Off-Limits"?

A final possible normative approach to protect commercial space actors is to establish that it is unacceptable behavior to target civilian commercial satellites and systems even during wartime. A key aim of International Humanitarian Law (IHL) and the Law of Armed Conflict (LOAC) has been to protect civilians and their property wherever they are, including space. Some relevant clauses can be found in Articles 52 and 57 of the Additional Protocols to the 1949 Geneva Conventions, paraphrased as:

- Civilian objects shall not be the object of attacks; attacks should be limited to objects that would provide a definite military advantage if they were neutralized, captured, or destroyed
- Attackers must take precautions to avoid causing incidental harm to civilians or their property
- Any harm that does occur for civilians must be proportionate to the military advantage gained.[50]

These principles and the Geneva Conventions in general are widely considered to be customary international law for all state actors, and entities ranging from the International Court of Justice to the U.S. Department of Defense *Law of War Manual* have confirmed that IHL applies to space.[51]

However, from a normative standpoint, experts disagree on how the application of IHL would actually function in space. Does temporary interference that does not cause physical damage count as an attack? Are commercial satellites that sell services to militaries viable military objectives? Several efforts are underway to interpret and apply IHL and LOAC to space, such as the *Woomera Manual* and the *McGill Manual on International Law Applicable to Military Uses of Outer Space* (MILAMOS).[52] Legal experts such as Dr. Wen Zhou of the International Committee of the Red Cross (ICRC) and Georgetown Law professor David Koplow argue that inclusion of both military and civilian payloads on the same satellite bus or extensive use of commercial satellite services for military purposes would make those satellites legitimate military targets.[53] In the May 2022 session of the Open-Ended Working Group on Reducing Space Threats, Koplow and other international experts debated the issue of protecting commercial and civilian satellites from armed attack and the nuances of dual-use satellites. Australian expert Dr. Cassandra Steer disagreed with Koplow on the grounds that many kinds of interferences and

attacks would have "disproportionate effects on the civilian population when a dual use satellite is the target."[54] The disproportionate effects would make such attacks illegitimate even if there was some military benefit from targeting the commercial satellite.

With these debates in mind, there are several options for developing norms that increase protections on commercial satellites by declaring what kinds of attacks or targets are legally "off-limits," as shown in Figure 1. In response to the call in UN Resolution 75/36 for states to submit their views on responsible, irresponsible, and threatening behavior in space, Germany, France, Canada, Japan, Sweden, and the United Kingdom all proposed norms against disrupting civilian objects, space infrastructure, or interfering in space services in a way that poses a threat to the public.[55] One option would be to attempt to create a norm protecting all commercial satellites, including those providing some military services, on the grounds of Steer's argument that attacks would disproportionately affect civilians unless the attacks could somehow be limited to only disrupting military payloads or signals. This approach would help to simplify some of the arguments over which satellites qualify for IHL protection but might face objections or be ignored by states that perceive a strong strategic need to disrupt any services flowing to the military of an adversary. A politically easier option may be to clarify protections for satellites that provide essential services to civilian society. The ICRC argues that states could consider segregating military and civilian uses of space objects and identify objects "indispensable to the survival of the civilian population," such as those providing services to hospitals, emergency responders, and irrigation networks.[56] This essential services approach would exclude numerous commercial satellites from the highest degree of normative protection but could be closer to consideration as legal and political common ground. Commercial companies that do not provide services to militaries may also see benefit in norms clarifying that their satellites are not viable targets because they are purely "civilian objects," leaving other commercial

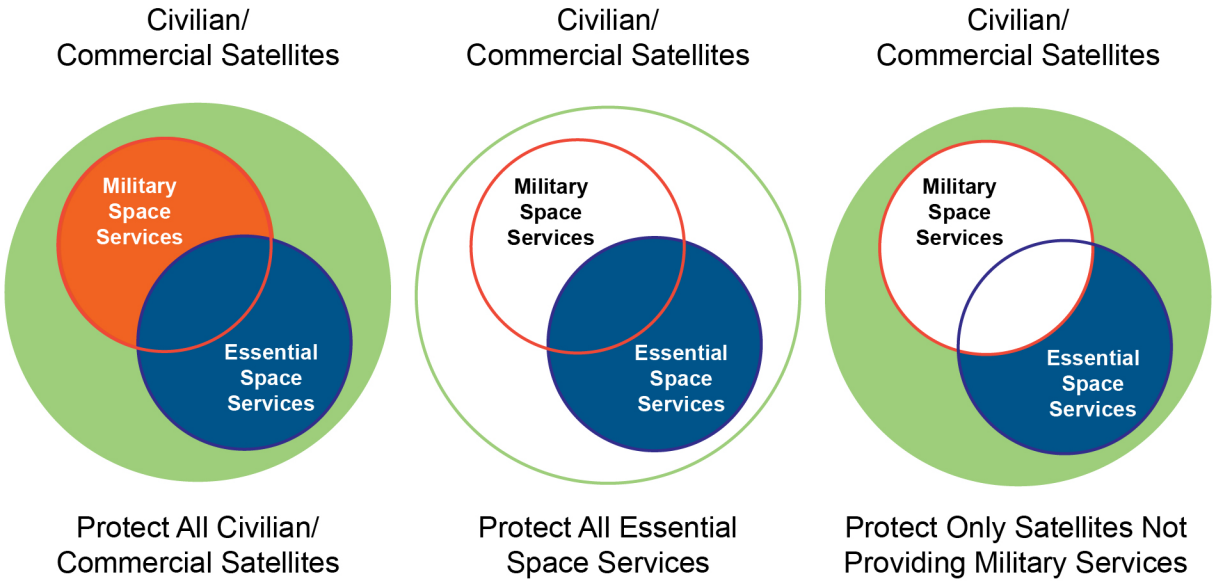

Figure 1: Options for norms declaring subsets of civilian/commercial satellites "off-limits" to attack.

Table 4: Potential Norms with Commercial Stake to Mitigate Deliberate Attacks	
Norm	**Commercial Stake**
Standards and practices to make commercial systems and services a harder target.	Make commercial systems less attractive as targets or reduce harm to commercial actor if an attack occurs.
Designation of "off-limits" commercial satellites.	Clarification/application of IHL/LOAC in the space domain can help deter attacks or coordinate responses for protected classes of commercial space assets.

operators to focus on sources of protection other than the Law of Armed Conflict.

Norms against attacking any or a subset of commercial satellites clearly will not deter all potential threats. In the maritime domain, Iranian forces targeted the Kuwaiti oil tankers despite the prohibitions in the Geneva Convention Additional Protocols that declared civilians and neutral states "off-limits" for deliberate attacks. In some cases, these norms may be more effective for justifying or coordinating responses to violations, providing a legal or political point around which other space actors can rally if a state goes rogue. International responses may coalesce more quickly and with more political will for harsh consequences for norms that are strongly adopted by the international community and clear enough that it is easy to detect violations. The Russian invasion of Ukraine, violating a core international norm of state territorial sovereignty, triggered a severe response from nations around the world, including sanctions on Russia, security assistance to Ukraine, and votes by 141 countries in the UN to condemn the invasion.[57] The responses were not limited to countries; by June 2022, almost 1,000 companies publicly announced that they were "voluntarily curtailing operations in Russia to some degree beyond the bare minimum legally required by international sanctions," demonstrating the role companies can choose to play in international enforcement of norms.[58]

However, even norms with credible enforcement or responses will likely face violations or be undermined in conflict. When the United States reflagged Kuwaiti tankers and began protecting them in convoys, Iran continued to attack the commercial shipping until the United States mistakenly shot down Iran Air Flight 655 in July 1988.[59] These limitations on the effectiveness of norms and responses to their violation indicate that the normative efforts to protect commercial satellites should not be the only approach to mitigating potential threats. However, they can be an important piece of the larger puzzle. Table 4 summarizes the stake that commercial space actors could have in two of these potential norms.

What to Make of the Commercial Stake in Norms Related to Space Security

The above analysis and examples demonstrate how commercial space actors have a stake in certain potential norms related to security issues because there are situations in which commercial actors can be threatened or attacked. The next question is how commercial actors could or should participate in norm development.

The commercial stake in space security norms does not by itself mean that commercial actors need to participate directly in norm development. Norms can be (and often are) developed and adopted by

states and then proliferated to commercial actors either through voluntary participation or through state regulations and policies for commercial actors. Furthermore, there are many possible cases in which companies may not *want* to participate in norm development for financial, proprietary, publicity, or other reasons. This indicates that commercial actors will have to navigate a number of challenges and balance sometimes conflicting interests and concerns in order to identify and pursue an appropriate role in security-related norm development. This section reviews criteria that commercial actors could consider when deciding whether to participate in development of a particular norm and explores strengths and weaknesses of approaches companies could take to help shape selected norm efforts.

Conditions and Questions for Commercial Participation

Although states have been the public leaders on diplomacy and security—and commercial influences are often concealed by being informal, indirect, or unreported in state decisionmaking—there have been numerous cases in which commercial actors have made notable contributions to the development of security-related norms of behavior. The writings of a businessman, Henry Durant, helped to inspire both the International Committee of the Red Cross and the first Geneva Convention in 1864, both of which were instrumental in the development of international humanitarian law.[60] Commercial actors also actively participated in the discussion of the 1994 amended version of the UN Convention on the Law of the Sea (UNCLOS) by giving testimony on both economic *and* national security implications of the treaty at U.S. Congressional hearings in 2007 and 2012.[61] The recent cases of the 2021 Gulf of Guinea Declaration on Suppression of Piracy and the Best Management Practices West Africa both featured heavy commercial involvement in development and adoption.

These examples demonstrate that commercial participation in security-related norms of behavior is not unheard of in other domains. But the inclusion of a broader range of stakeholders, including commercial actors, may be even more important for the space domain. In some cases, the behavior of any single actor in space has the potential to affect other actors in space through phenomena like debris or spectrum interference, and this interconnectedness raises the stakes on norm development. In other domains, norms were able to develop over years of trial and error, and oftentimes tragedies occurred before actors managed to solidify common understandings of responsible and irresponsible behavior. For example, in the analyzed commercial aircraft shootdown cases, six commercial airliners were destroyed by states before clearer norms were developed on how to deal with those situations. As tragic as each of those incidents was, the consequences of similar failures in space could be farther reaching and longer lasting. The physics of debris propagation in space make it much harder to limit the effects of any single accident or conflict. The destruction of commercial satellites could disrupt entire infrastructures of communication, information collection, or navigation through the proliferation of dangerous debris. This in turn means that space can feature an entangled mix of deliberate threats, unintended hazards, and long-term challenges to minimizing risk in the domain. Despite having different venues for discussion, safety and security issues are intertwined in space. Another issue is that at the moment satellites cannot be repaired, refueled, or repurposed with anything approaching the flexibility of most systems in other domains.[§] So, policymakers will often have to live

[§]Commercial and government actors are driving significant progress in technology development and initial capability demonstrations, so this challenge may shift in the future. For examples of advances in in-space servicing and manufacturing, see Alec J. Cavaciuti, Joseph H. Heying, and Joshua Davis, "Game Changer: In-Space

with the effects of space-related operation, regulation, and design decisions for decades.

Due to the combination of safety-security entanglement and long-term effects of certain actions, if policymakers wait to see the effects of norms developed without contributions from all the relevant stakeholders, there could be significant costs down the line. The space domain is uniquely interconnected, so space norm efforts, even those related to security issues, may need to be similarly interconnected across all space actors, not just the states that traditionally take leadership in diplomacy and norm development.

What are the cases in which the commercial stake in space norms related to security issues could translate to more direct commercial participation? Table 5 summarizes the seven norms with a commercial stake derived from the non-space examples and analyses of threats to commercial actors. With these norms, there are several factors beyond the fact that commercial actors have a stake in their adoption and acceptance that could indicate the value of commercial participation in norm development. First, some of the norms require commercial action in order to be implemented. Not all security-related norms rely solely on state behaviors, and a norm establishing lines of communication between states and commercial actors would clearly require the commercial actors to "pick up the phone" in order to function. Therefore, at a minimum, commercial actors in these cases would need to understand the norm and be capable of implementing it, and consultation with the actors establishing the norm could help to ease the process.

Another consideration for the value of commercial participation in security-related space norm development is the need to navigate the costs that norm compliance may impose on commercial actors. Norm compliance could involve changes to technologies or procedures that cost companies time, money, or effort to implement. If costs of norm implementation are high, there is a risk of the norm failing to be adopted unless sufficient incentives or enforcement mechanisms exist to ensure the commercial actors follow along. Therefore, in norm cases like commercial space or cyber security standards, laws or policies developed without consideration for commercial capabilities to implement could have negative effects, like driving out smaller space companies who cannot afford to meet the standards. Commercial actors may need to communicate in advance any obstacles to implementation so that the norm developers can include those considerations in the search for a workable solution.

Table 5: List of Potential Norms with Security Implications and a Commercial Stake

Collateral Damage	Misidentification and Misperception	Deliberate Targeting During Conflict
Bans or limits on kinetic anti-satellite tests or deliberate debris production	Effective practices and means of deconflicting/adjudicating SSA data	Standards and best practices to make commercial satellites a harder target
Further implementation and enforcement of existing norms related to indiscriminate acts such as nuclear detonations or radiofrequency interference	Crisis or emergency lines of communication	Designation of "off-limits" commercial satellites
	Common definitions of threatening behavior	

This leads to three questions that commercial actors and policymakers could consider when examining the potential for commercial participation in space norm development:

- **Commercial Stake:** Does the norm help to reduce risk or threat to commercial actors in space?
- **Commercial Impact:** Does the successful adoption and implementation of the norm rely on commercial actors' behavior?
- **Commercial Costs:** Are there significant costs or constraints that will be imposed on commercial actors with the implementation of the norm?

Answering "yes" to any one of these questions may not necessitate commercial participation in the development of a norm, but the greater the commercial stake, impact, and costs are, the more likely commercial participation in its development would be mutually beneficial.

How Commercial Actors Could Be Involved

Following the above consideration of *if* or *when* commercial actors should be involved in the development of norms related to space security, the final piece of the puzzle is *how* commercial participation should proceed. There are several possible lenses for viewing commercial participation: interaction between commercial actors and national governments; commercial contribution to international efforts at venues for norm development; and intra-industry discussions and advocacy for norms. The approaches seen through these lenses have different strengths and weaknesses for various norm efforts based on the three factors effecting the appropriate degree of commercial participation. The following discussion aims to explore these different possibilities and demonstrate the variety of approaches that could be taken, highlighting some of the potential opportunities and challenges along the way.

Interaction with National Governments

Commercial participation in norm development through direct discussions with national governments could have the benefit of leveraging existing platforms and relationships instead of creating new international bodies or procedures. However, the approach can be complicated by the timing and inclusiveness or exclusiveness of different participation options as well as the often indirect relationship between public-private cooperation and international norm development.

Commercial perspectives on norms can be considered through cooperation and conversation with specific government organizations. In the United States, for example, there are expanding space partnerships between government agencies and commercial companies, such as NASA's Collaborations for Commercial Space Capabilities and the U.S. Space Command Commercial Integration Cell.[62] Commercial-government relationships can also play out in the legislative branch, as demonstrated by the long history of companies and industry groups lobbying Congress on their various interests and needs. These interactions need not be explicitly focused on norms. Relationships or patterns of communication between governments, militaries, and commercial companies provide opportunities for all sides to express ideas and concerns relevant to space activities that could later flow into policies or international norm proposals. This is an indirect way to incorporate commercial perspectives into norm development, but the potential synergy it lends to commercial and government space activities could increase government awareness of commercial concerns when discussing space norms internationally.

Another approach is to create more formal advisory paths from commercial representatives to national leadership, as exemplified by the National Space Council User's Advisory Group (NSpC UAG). The purpose of the advisory group is "to ensure the interests of industry, other non-Federal entities and other institutions…are represented in a balanced fashion at the national level."[63] Membership includes representatives from companies such as Boeing, United Launch Alliance, Aerojet Rocketdyne, Relativity Space, Sierra Nevada Corporation, SpaceX, Blue Origin, Lockheed Martin, VOX Space, and Northrop Grumman.[64] In the UAG's most recent meeting in July 2020, the Space Policy & International Engagement Subcommittee reported on discussions about norms of behavior, highlighting that the existing main norm efforts featured heavy overlap between national security and civil and commercial aspects.[65] Notably, even though this group focuses on industry and nongovernmental perspectives, there is a National Security Subcommittee that also brought up norms of behavior.[66] This example highlights commercial interest in space norms of behavior, including those related to security issues. Furthermore, the advisory approach, as a whole, has the advantage of convening senior-level industry and government representatives across a broad range of issues and stakeholders.

One downside to these approaches is that specific commercial actors need contracts or invitations to participate in these venues, so it may be harder for smaller companies or start-ups to contribute. An alternative potential feedback loop is through the public requests for comment and feedback included in the regulatory process for many space issues. The National Oceanic and Atmospheric Administration (NOAA) and Federal Communications Commission (FCC) frequently open requests for comment and information for topics like remote sensing regulations, orbital debris, and commercial space situational awareness data.[67] While many of these efforts tie more into space safety and sustainability issues, there is also a nexus to national security concerns. Security issues are raised in, for example, remote sensing licenses and increasing awareness of space and cyber security issues for space infrastructure in the Department of Homeland Security.[68] Because the opportunities for public comment are often tied to new policies and regulations, this angle of potential commercial participation could apply at several stages of norm development. Comments could contribute to early norm brainstorming if the rulemaking is part of national unilateral efforts to demonstrate or propose norms. Or the solicitation of feedback could occur at a late stage of norm development if the rulemaking is part of national implementation of an agreed-upon international norm. This dynamic means that the opportunities for commercial influence on overall development could vary greatly depending on the timing and purpose of the rulemaking.

Commercial conversations with national governments can look very different for different kinds of commercial actors. Companies conduct a range of space activities of widely varying function and scope, and many companies are multinational. Due to the 1967 Outer Space Treaty, every commercial satellite can be traced to a state responsible for its authorization and supervision, but the commercial actors themselves can have complex organizational structures spanning various companies, leadership nationalities, facilities locations, and regulatory jurisdictions.[69] This means that companies will need to consider, on a case-by-case basis, whether participation in norm development is best pursued through domestic discussion and regulation (and for which state) or through international bodies and processes that are less reliant on a relationship to a single state.

International Opportunities for Commercial Norm Participation

Commercial actors face several opportunities for participating in norm development on the world

stage. Some venues for norm discussion are entirely state-led, some allow for commercial observers or contributors, and some are comprised entirely of commercial, instead of state, actors. Therefore, the capacity of a given forum to include commercial actors could be a contributing factor for policymakers trying to decide where to introduce a norm proposal.

Many fora where security-related space norms are discussed, like the UN Conference on Disarmament and First Committee, reserve full membership for states alone. So, commercial companies may have to look for somewhat indirect means of contributing to the conversation. This could include participation by individuals with commercial experience in national delegations as private sector experts or advisors. The U.S. Department of State has solicited commercial participants for both domestic and international events related to space safety and sustainability best practices and could consider ways of expanding this practice to other space issues.[70] Another approach is to identify which potential security norms truly have minimal to no need for commercial involvement in development and discuss those norm proposals via state-dominated processes while addressing other proposals in more inclusive fora.

There are several examples of organizations in which states still take the lead on creating norms, regulations, or laws but in which commercial actors have opportunities to contribute. Policymakers could consider fitting norm proposals to suit one of these venues or by adapting new venues along these models to suit security-related space norms.

The International Telecommunication Union (ITU) provides a valuable example for strong commercial contribution to state-led negotiations, with lessons that could be applied to security contexts as well. Commercial and other nonstate actors have status at the ITU as the approximately 900 nonvoting "Sector Members." Every four years, the ITU convenes the World Radiocommunication Conference (WRC) to create new legally binding regulations for spectrum usage, which impacts the activities of all space operators. Although all WRC decisions are ultimately made by consensus of the member states, the private sector participates significantly in the years-long preparatory process at the working level by submitting papers, providing expertise, and chairing groups that shape the inputs for the WRC.[71] At the WRC itself, commercial actors can attend either as observers or on national delegations, illustrating a wide range of opportunities for commercial companies to participate in the development of legal norms and regulations for spectrum usage.[72] This example serves as a reminder that even when based on negotiated agreements, norm development does not always begin and end with state representatives sitting at the negotiating table. Commercial actors can make substantial contributions to norm development without overtaking the diplomatic role of states.

What Can Commercial Actors Do Themselves: Consortia, Common Standards, and Public Advocacy

In some specific cases, there may be opportunities for commercial actors to participate in security related norm-development without going through state governments or intergovernmental organizations. These opportunities may be limited in scope, scale, nexus to security issues, or may not be directly tied to the state negotiations and development of the norm. However, in certain areas commercial actors may be able to leverage common interests and needs across industry or public visibility in order to directly contribute to the norm conversation.

In some cases, commercial actors may prefer the industry-led approach, especially if they perceive that attempts to mitigate irresponsible or threatening behavior through government channels are not working. For example, when the Russian satellite

known as Luch or Olymp made a close approach to two Intelsat satellites in GEO, the company ultimately decided to go public in criticizing Russia's behavior after attempts to communicate directly to the Russian government and through DOD failed. Kay Sears, the president of Intelsat General, said in an interview with *SpaceNews* that, "This is not normal behavior and we're concerned."[73] Because commercial actors operate so many satellites and sometimes have significant public visibility, either informal or structured approaches to demonstrating good behaviors or criticizing threatening behaviors may be seen as one of the most straightforward methods of contributing to norm development.

One example approach to commercial leadership in norm development is the international Consortium for the Execution of Rendezvous and Proximity Operations (CONFERS), an industry-led forum of 36 sustaining and contributing member companies and 13 observer members.[74] CONFERS aims to develop standards, international policies, and norms of behavior for satellite servicing.[75] Although this consortium explicitly focuses on the safety and sustainability aspects of norm development, it demonstrates the value of commercial actors pooling experience, technical expertise, and best practices in order to make proposals for space norms. A more security- and resilience- focused example of this approach would be the Space Information Sharing and Analysis Center (Space ISAC). Like CONFERS, Space ISAC was initially stood up under U.S. government guidance but is led by a group of companies, federally funded research and development centers, and universities.[76] Space ISAC does not currently focus on norm development as a primary goal. However, Vice Chair of the Space ISAC and technical fellow at MITRE Sam Visner has argued that participating companies have demonstrated the desire to share best practices as well as the more direct sharing of information on potential threats.[77] There are also industry associations (such as the Aerospace Industries Association, Satellite Industry Association, and Commercial Spaceflight Federation) with missions that include sharing best practices and discussing the needs and concerns of their members.[78]

There are clear limitations on the company-led approach due to its relative de-emphasis on state actors, especially for norms related to security issues. From the list of potential security- or conflict-related norms explored in this paper, the collective commercial proposal approach could best be applied to the cases of standards for commercial security and conflict-related insurance. In these cases, the companies themselves would need to be able and willing to comply with the norms. Company-led discussions could help to overcome the current challenge that companies have thus far taken very different approaches to satellite and cyber security and insurance, leading to more consistent collective practices. Discussion among these actors could help identify areas for improvement or cooperation before bringing the discussion to the broader space community.

Commercial participation in norm development can also occur outside of discussions and debates on norm content. This is especially relevant for the security-related norms in which commercial actors have a stake in norm success but do not play a direct role in implementation, such as banning kinetic ASAT tests or defining "threatening behavior." In these cases, commercial actors may choose to publicly support the norm proposal without being involved in the proposal negotiations. Public advocacy could take on forms such as publicly released white papers, press releases, social media posts, and events. This approach is already developing among commercial space actors on the ASAT test ban issue through the series of tweets, posts, and public statements made by commercial companies to condemn Russia's 2021 kinetic ASAT test. These statements are not directly integrated into international negotiations that could result in a ban

or norm against kinetic ASAT testing. Instead, they show how commercial actors can identify and express their thoughts on when space security issues impact commercial activities and in doing so contribute to public pressure to develop a norm.

Figure 2 demonstrates the range of possible paths commercial actors could take to help influence or shape the development of space norms of behavior.

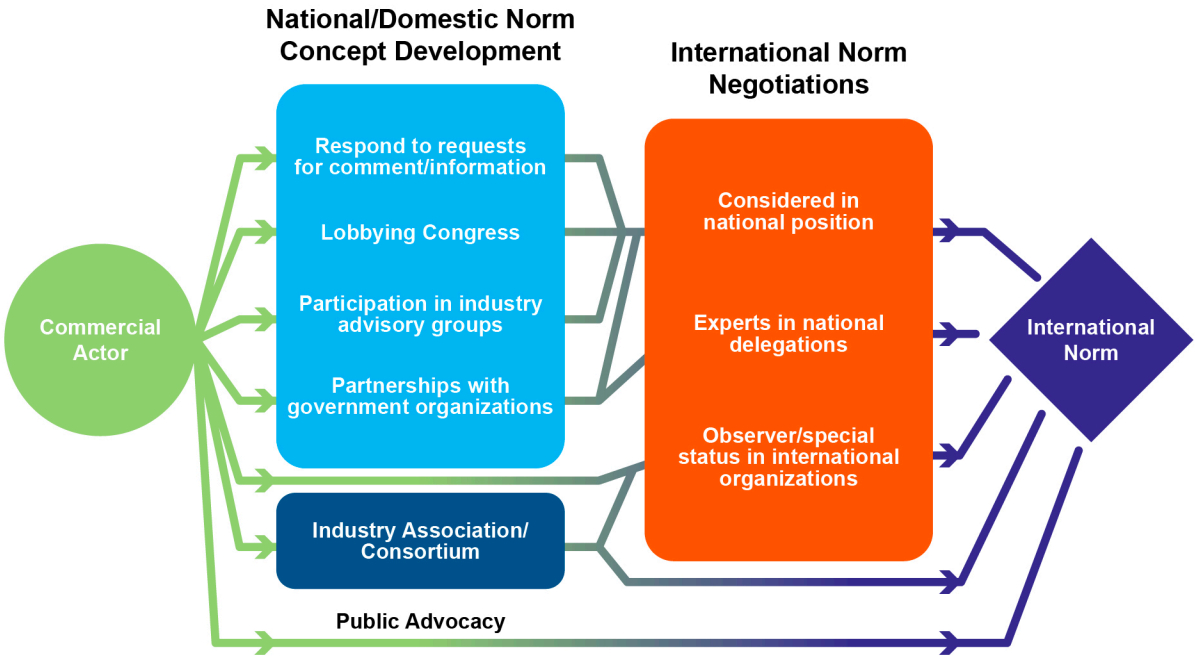

Figure 2: Paths for commercial contributions to norm development.

Conclusion

As with all broad discussions on the development of norms of behavior for space, there is no one-size-fits-all solution. Options have been identified here through the exploration of potential norms with security implications and a commercial stake, the application of a framework to consider the appropriate degree of commercial participation, and the description of potential approaches to substantive commercial contributions to space norm development. Commercial participation could range from public promotion of norms that were proposed or negotiated by states to more substantive contributions of expertise or descriptions of commercial concerns. Ultimately, the degree of commercial participation in norm development will depend on both the willingness of state actors to set the table and the interest and efforts of commercial actors to take a seat at the table.

Despite the aspirations of the international community to pursue the peaceful uses of outer space, there may come a time, if it has not come already, when space actors will have to operate in a context of crisis or conflict. As space services become ever more integrated with life and society on Earth, the international community will have to consider how commercial actors affect and are affected by crisis and conflict in space. Disruption in space will increasingly cause disruption on the ground, and vice versa. Commercial actors should not be left out of the discussion. Proactive contribution to space norm discussions, including those that touch on security issues or explore the application of norms in crisis and conflict, will be a crucial step in helping commercial actors navigate and mitigate potential threats with less disruption to the capabilities and services they provide their customers and the world.

Acknowledgments

The author would like to thank the following individuals for contributing their expertise in discussions, interviews, or reviews for the paper: Rebecca Cowen-Hirsch, Carissa Christensen, Mike Dickey, and Moriba Jah. Thanks also to colleagues across the Aerospace Corporation and to CSPS colleagues Sam Wilson, Vicky Woodburn, Jamie Morin, Dave Eccles, Mick Gleason, Audrey Allison, and Russell Rumbaugh for their contributions. Thank you to Mary Mills, Nina Isaia, and Jacob Bain for their editorial and graphics support.

References

[1] This definition was proposed and discussed in the author's previous paper, "Building Normentum" but this analysis expands from looking just at state behavior to a broader range of space actors to include commercial perspectives: Robin Dickey, "Building Normentum: A Framework for Space Norm Development," The Aerospace Corporation Center for Space Policy and Strategy (July 2021), https://csps.aerospace.org/sites/default/files/2021-07/Dickey_BuildingNormentum_20210706.pdf

[2] Michael Gleason and Travis Cottom, "U.S. Space Traffic Management: Best Practices, Guidelines, Standards, and International Considerations," The Aerospace Corporation Center for Space Policy and Strategy (August 2018), https://csps.aerospace.org/sites/default/files/2021-08/Cottom-Gleason_U.S.%20Space%20Traffic%20Management_08272018.pdf

[3] For a space-focused examination of this issue, see Michael Gleason, "No Haven for Misbehavin': A Framework for Verifying Space Norms," The Aerospace Corporation Center for Space Policy and Strategy (March 29, 2022), https://csps.aerospace.org/papers/no-haven-misbehavin-framework-verifying-space-norms

[4] Nicole Peterson, "Commercial Companies' Perceptions of Security Space," NSI, Inc. (March 2018), https://nsiteam.com/commercial-companies-perceptions-of-security-in-space/

[5] Almudena Azcárate Ortega and James Revill, "Space Industry Workshop Report," United Nations Institute for Disarmament Research (October 2021), https://www.unidir.org/spaceindustry.

[6] Ibid.

[7] "Space Sustainability Report," Inmarsat (2022), https://www.inmarsat.com/en/insights/corporate/2022/space-sustainability.html

[8] Ibid.

[9] "Anti-personnel Landmines: Friend or Foe?," International Committee of the Red Cross (1996), https://www.icrc.org/en/doc/assets/files/other/icrc_002_0654.pdf

[10] "Hidden Killers 1994: The Global Landmine Crisis," Report to U.S. Congress by Department of State, (January 1994), https://1997-2001.state.gov/global/arms/rpt_9401_demine_toc.html

[11] "Anti-personnel Landmines: Friend or Foe?," International Committee of the Red Cross (1996): 30-31, https://www.icrc.org/en/doc/assets/files/other/icrc_002_0654.pdf

[12] Planet called for a norm against all use of debris-creating ASATs a week before the Vice President's announcement and afterwards called the U.S. commitment "a critical first step."
"A Call For the United States Government To Lead International Efforts to Prohibit the Use of Debris-Creating Anti-Satellite Weapons (ASATs), Planet Labs PBC (April 11, 2022), https://www.planet.com/pulse/a-call-for-the-united-states-government-to-lead-international-efforts-to-prohibit-the-use-of-debris-creating-anti-satellite-weapons-asats/
"Astroscale U.S. Statement on the United States DA-ASAT Test Ban," Astroscale U.S. (April 19, 2022), https://astroscale-us.com/da-asat-test-ban/;
"New U.S. Commitment on Destructive Direct-Ascent Anti-Satellite Missile Testing," Space Data Association (April 2022), https://www.space-data.org/sda/news/new-u-s-commitment-on-destructive-direct-ascent-anti-satellite-missile-testing/

[13] Sandra Erwin, "Satellite operators want a seat at the table in space security discussions," SpaceNews (March 16, 2021), https://spacenews.com/satellite-operators-want-a-seat-at-the-table-in-space-security-discussions/

[14] "9 July 1962, 'Starfish Prime,' Outer Space," Comprehensive Nuclear-Test-Ban Treaty Organization," (Accessed June 3, 2022), https://www.ctbto.org/specials/testing-times/9-july-1962starfish-prime-outer-space

[15] Brad Lendon, "In 1988, a US Navy warship shot down an Iranian passenger plane in the heat of battle," CNN (January 10, 2020), https://www.cnn.com/2020/01/10/middleeast/iran-air-flight-655-us-military-intl-hnk/index.html;
Matthew Schwartz, "Iranian Report Details Chain of Mistakes in Shooting Down Ukrainian Passenger Plane," National Public Radio (July 12, 2020), https://www.npr.org/2020/07/12/890194877/iranian-report-details-chain-of-mistakes-in-shooting-down-ukrainian-passenger-pl

[16] Thom Patterson, "The downing of Flight 007: 30 years later, a Cold War tragedy still seems surreal," *CNN* (August 31, 2013), https://www.cnn.com/2013/08/31/us/kal-fight-007-anniversary/index.html;
Craig A Morgan, "Incident: The Downing of Korean Air Lines Flight 007," *Yale Journal of International Law* 11, no. 231 (1985): 240,

https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1477&context=yjil

[17] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," United Nations Office for Outer Space Affairs (December 19, 1966), https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

[18] "NASA Space Station On-Orbit Status 6 December, 2021 – Three New Visitors Arriving Wednesday," Spaceref.com (December 7, 2021), http://spaceref.com/international-space-station/nasa-space-station-on-orbit-status-6-december-2021---three-new-visitors-arriving-wednesday.html
"A new crew docks at China's first permanent space station," National Public Radio (October 16, 2021), https://www.npr.org/2021/10/16/1046742793/china-space-station-docking-astronauts
Tariq Malik and Elizabeth Howell, "Michael Strahan's Blue Origin Launch on New Shepard: Mission updates and recap," Space.com (December 12, 2021), https://www.space.com/news/live/blue-origin-michael-strahan-launch-updates

[19] Robert Wilson, Mick Gleason, and Sophia Jones, "Value of Space for Emergency Response and Disaster Relief," 72nd International Astronautical Congress (October 2021).

[20] "International Space Station Facts and Figures," National Aeronautics and Space Administration (November 4, 2021), https://www.nasa.gov/feature/facts-and-figures

[21] Deepa Shivaram, "Space junk piece set to hit the moon is likely from a Chinese rocket, not SpaceX," National Public Radio (February 15, 2022), https://www.npr.org/2022/02/15/1080827033/rocket-moon-crash-spacex-china

[22] Deepa Shivaram, "Space junk piece set to hit the moon is likely from a Chinese rocket, not SpaceX," National Public Radio (February 15, 2022), https://www.npr.org/2022/02/15/1080827033/rocket-moon-crash-spacex-china;
Andrew Jones, "China claims rocket stage destined for lunar impact is not from 2014 moon mission," Space News (February 21, 2022), https://spacenews.com/china-claims-rocket-stage-destined-for-lunar-impact-is-not-from-its-2014-moon-mission/

[23] "A/AC.105/1262: Information furnished in conformity with the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," United Nations Office for Outer Space Affairs (December 6, 2021), https://www.unoosa.org/res/oosadoc/data/documents/2021/aac_105/aac_1051262_0_html/AAC105_1262E.pdf;
"A/AC.105/1265: Notification by the United States of America concerning the notification by China (A/AC.105/1262) on preventive collision avoidance between the China Space Station (international designation 2021-035A) and United States' Starlink-1095 (international designation 2020-001BK) and Starlink-2305 (international designation 2021-024N) satellites," United Nations Office for Outer Space Affairs (February 3, 2022), https://www.unoosa.org/oosa/en/oosadoc/data/documents/2022/aac.105/aac.1051265_0.html

[24] Sarah Laskow, "The Plane Crash That Gave Americans GPS," The Atlantic (November 3, 2014), https://www.theatlantic.com/technology/archive/2014/11/the-plane-crash-that-gave-americans-gps/382204/

[25] Sabrina Pagano and John A. Stevenson, "NSI Concept Paper: How Disagreement Over Space Terms Can Create Barriers to Transparency in the Space Domain," NSI (2018): 1-2, https://apps.dtic.mil/sti/pdfs/AD1066723.pdf

[26] Daniel Porras and Laetitia Zarkan, "Safety Norms for Space Security: How the Development of STM Norms Can Strengthen Security in Space," Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) (2021), https://amostech.com/TechnicalPapers/2021/SSA-SDA/Porras.pdf

[27] "Participants," Space Data Association (Accessed April 25, 2022), https://www.space-data.org/sda/participants/

[28] "A/AC.105/1262: Information furnished in conformity with the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," United Nations Office for Outer Space Affairs (December 6, 2021), https://www.unoosa.org/res/oosadoc/data/documents/2021/aac_105/aac_1051262_0_html/AAC105_1262E.pdf;
"A/AC.105/1265: Notification by the United States of America concerning the notification by China (A/AC.105/1262) on preventive collision avoidance between the China Space Station (international designation 2021-035A) and United States' Starlink-1095 (international designation 2020-001BK) and Starlink-2305 (international designation 2021-024N) satellites," United Nations Office for Outer Space Affairs (February 3, 2022),

https://www.unoosa.org/oosa/en/oosadoc/data/documents/2022/aac.105/aac.1051265_0.html

[29] Mike Gruss, "Russian Satellite Maneuvers, Silence Worry Intelsat," *SpaceNews* (October 9, 2015), https://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/

[30] Brad Lendon, "In 1988, a US Navy warship shot down an Iranian passenger plane in the heat of battle," CNN (January 10, 2020), https://www.cnn.com/2020/01/10/middleeast/iran-air-flight-655-us-military-intl-hnk/index.html

[31] "Annex 2 to the Convention on International Civil Aviation: Rules of the Air," International Civil Aviation Organization (10th Ed, July 2005), https://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf

[32] "Annex 2 to the Convention on International Civil Aviation: Rules of the Air," International Civil Aviation Organization (10th Ed, July 2005), https://www.icao.int/Meetings/anconf12/Document%20Archive/an02_cons%5B1%5D.pdf

[33] Daniel Porras and Laetitia Zarkan, "Safety Norms for Space Security: How the Development of STM Norms Can Strengthen Security in Space," Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS) (2021), https://amostech.com/TechnicalPapers/2021/SSA-SDA/Porras.pdf;
Sabrina Pagano and John A. Stevenson, "NSI Concept Paper: How Disagreement Over Space Terms Can Create Barriers to Transparency in the Space Domain," NSI (2018): 1-2, https://apps.dtic.mil/sti/pdfs/AD1066723.pdf

[34] "Unrestricted U-Boat Warfare: The German Naval Tactic of WWI," The National WWI Museum and Memorial, https://www.theworldwar.org/learn/wwi/unrestricted-u-boat-warfare#:~:text=The%20formidable%20U%2Dboats%20(unterseeboots,the%20British%20blockade%20defeated%20Germany.

[35] Stephen Andrew Kelley, "Better Lucky than Good: Operation Earnest Will as Gunboat Diplomacy," Naval Postgraduate School Archive (June 2007), https://calhoun.nps.edu/bitstream/handle/10945/3463/07Jun_Kelley.pdf?sequence=1&isAllowed=y

[36] Sandra Erwin, "U.S. generals planning for a space war they see as all but inevitable," SpaceNews (September 17, 2021), https://spacenews.com/u-s-generals-planning-for-a-space-war-they-see-as-all-but-inevitable/

[37] Theresa Hitchens & Colin Clark, "Commercial Satellites: Will They Be Military Targets?" Breaking Defense (July 16, 2019), https://breakingdefense.com/2019/07/commercial-satellites-will-they-be-military-targets/

[38] Theresa Hitchens & Colin Clark, "Commercial Satellites: Will They Be Military Targets?" Breaking Defense (July 16, 2019), https://breakingdefense.com/2019/07/commercial-satellites-will-they-be-military-targets/

[39] Charles Pope, "Raymond and Space Force enter new, ambitious phase as U.S. Space Command changes leaders," United States Space Force (August 24, 2020), https://www.spaceforce.mil/News/Article/2322445/raymond-and-space-force-enter-new-ambitious-phase-as-us-space-command-changes-l/

[40] Jim Cooper, "Updating Space Doctrine: How to Avoid World War III," War on the Rocks (July 23, 2021), https://warontherocks.com/2021/07/updating-space-doctrine-how-to-avoid-world-war-iii/

[41] Nicole Peterson, "Commercial Companies' Perceptions of Security Space," NSI, Inc. (March 2018): 11, https://nsiteam.com/commercial-companies-perceptions-of-security-in-space/

[42] Nicole Peterson, "Commercial Companies' Perceptions of Security Space," NSI, Inc. (March 2018): 11, https://nsiteam.com/commercial-companies-perceptions-of-security-in-space/

[43] Debra Werner, "Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites," SpaceNews (April 14, 2022), https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/

[44] "Alert (AA22-076A): Strengthening Cybersecurity of SATCOM Network Providers and Customers," Cybersecurity and Infrastructure Agency (March 17, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-076a

[45] "The Gulf of Guinea Declaration on Suppression of Piracy," BIMCO (September 14, 2021), https://www.bimco.org/ships-ports-and-voyage-planning/security/gulf-of-guinea-declaration-on-suppression-of-piracy

[46] "BMP West Africa: Best Management Practices to Deter Piracy and Enhance Maritime Security off the Coast of West Africa including the Gulf of Guinea," Westpandi (March 2020), https://www.westpandi.com/getmedia/e913f6ec-61ef-40da-b40f-1adeafee3c6c/BMP-West-Africa.pdf

[47] Matthew Scholl "Draft NISTIR 8270: Introduction to Cybersecurity for Commercial Satellite Operations," National Institute of Standards and Technology (June 30, 2021),

https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8270-draft.pdf

[48] "Space ISAC: Collaborating to Protect Our Space Systems," Space Information Sharing and Analysis Center (August 17, 2021), https://s07f21n96ry3bgacl3z1pdi9-wpengine.netdna-ssl.com/wp-content/uploads/2021/08/SISAC_Membership_Flyer_08172021.pdf

[49] "How Is The Space Sector Reacting To And Mitigating Against the Effects of Russia's War?" The Downlink Podcast (March 6, 2022)https://defaeroreport.com/2022/03/07/the-downlink-mar-06-22-how-is-the-space-sector-reacting-to-and-mitigating-against-the-effects-of-russias-war/

[50] "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)," International Committee of the Red Cross (June 7, 1977), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=D9E6B6264D7723C3C12563CD002D6CE4&action=openDocument

[51] Michael Schmitt and Kieran Tinkler, "War in Space: How International Humanitarian Law May Apply," Just Security, The Woomera Manual Project – Part 3 (March 9, 2020), https://www.justsecurity.org/68906/war-in-space-how-international-humanitarian-law-might-apply/

[52] "The Woomera Manual," The University of Adelaide (Accessed June 13, 2022), https://law.adelaide.edu.au/woomera/; "What is the MILAMOS Project?" McGill University (Accessed June 13, 2022), https://www.mcgill.ca/milamos/

[53] Wen Zhou, "Protection of civilians, civilian objects and the natural environment in relation to threats arising from State behaviours with respect to outer space," United Nations Office for Disarmament Affairs (May 11, 2022), https://documents.unoda.org/wp-content/uploads/2022/05/Presentation-by-Wen-Zhou-under-topic-3-at-the-first-session-of-OEWG-on-reducing-space-threats_11-May-2022.pdf; David A. Koplow, "Reverse Distinction: A U.S. Violation of the Law of Armed Conflict in Space," *Harvard National Security Journal* 13, no. 25 (2022): pp 79-80, https://harvardnsj.org/wp-content/uploads/sites/13/2022/01/HNSJ-Vol-13-Koplow-ReverseDistinction.pdf

[54] Cassandra Steer, "Application of International Humanitarian Law/ Laws of Armed Conflict in Space: Civilians and Neutral States," United Nations Office for Disarmament Affairs (May 11, 2022), https://documents.unoda.org/wp-content/uploads/2022/05/Steer_UN-OEWG-11-May-2022.pdf

[55] "Report of the Secretary-General on reducing space threats through norms, rules and principles of responsible behaviors," United Nations Office for Disarmament Affairs (July 2021), https://www.un.org/disarmament/topics/outerspace-sg-report-outer-space-2021/

[56] International Committee of the Red Cross, "Constraints under International Law on Military Operations in, or in Relation to, Outer Space During Armed Conflicts," United Nations Office for Disarmament Affairs (May 3, 2022), https://documents.unoda.org/wp-content/uploads/2022/05/ICRC-working-paper-on-the-constraints-under-international-law-on-military-space-operations_final_en.pdf

[57] "Russia's Invasion of Ukraine: Overview of U.S. Sanctions and Other Responses," Congressional Research Service (April 22, 2022), https://crsreports.congress.gov/product/pdf/IN/IN11869

[58] "Almost 1,000 Companies Have Curtailed Operations in Russia—But Some Remain," Yale School of Management (June 13, 2022), https://som.yale.edu/story/2022/almost-1000-companies-have-curtailed-operations-russia-some-remain

[59] Andrew R. Marvin, "Operation Earnest Will—The U.S. Foreign Policy behind U.S. Operations in the Persian Gulf 1987-89; A Curious Case," Naval War College Review 73, no. 2 (Spring 2020), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8115&context=nwc-review

[60] "Henry Dunant (1828-1910)," International Committee of the Red Cross (1998), https://www.icrc.org/en/doc/resources/documents/misc/57jnvq.htm

[61] "The Law of the Sea Convention (Treaty Doc. 103-39): Perspectives from Business and Industry," U.S. Senate Committee on Foreign Relations (June 28, 2012), https://www.govinfo.gov/content/pkg/CHRG-112shrg77375/html/CHRG-112shrg77375.htm

[62] "Collaborations for Commercial Space Capabilities (CCSC)," National Aeronautics and Space Administration (2019), https://www.nasa.gov/content/collaborations-for-commercial-space-capabilities-ccsc;

"Commercial Integration Cell Fact Sheet," United States Space Force (February 2021), https://www.vandenberg.spaceforce.mil/Portals/18/documents/CFSCC/CIC-FactSheet-Feb21.pdf?ver=ch0p0vC3F2c1CUBVlT9E7A%3d%3d

[63] "National Space Council Users' Advisory Group (NSpC UAG)," National Aeronautics and Space Administration, https://www.nasa.gov/content/national-space-council-users-advisory-group

[64] "UAG Member Roster and Biographies," National Aeronautics and Space Administration (June 8, 2020), https://www.nasa.gov/content/national-space-council-users-advisory-group/membership_roster

[65] "Meeting Minutes: National Space Council User's Advisory Group 5th Meeting (Virtual)," National Aeronautics and Space Administration (July 30, 2020): 21-23, https://www.nasa.gov/sites/default/files/atoms/files/uag-5_meeting_minutes_ver5_2020-09-03_signed.pdf

[66] "Meeting Minutes: National Space Council User's Advisory Group 5th Meeting (Virtual)," National Aeronautics and Space Administration (July 30, 2020): 32, https://www.nasa.gov/sites/default/files/atoms/files/uag-5_meeting_minutes_ver5_2020-09-03_signed.pdf

[67] "NOAA Seeks Commercial Sources of SSA Data," National Oceanic and Atmospheric Administration Office of Space Commerce (February 16, 2022), https://www.space.commerce.gov/noaa-seeks-commercial-sources-of-ssa-data/
Orbital Debris in the New Space Age, Report and Order and Further Notice of Proposed Rulemaking, US Federal Communications Commission, FCC-20-54 (April 24, 2020), paragraph 62.

[68] "Commercial Remote Sensing Regulatory Affairs," NOAA Satellite and Information Services, https://www.nesdis.noaa.gov/about/our-offices/commercial-remote-sensing-regulatory-affairs;
"Trump Administration Launches First Cybersecurity Principles for Space Technologies," Department of Homeland Security (September 4, 2020), https://www.dhs.gov/news/2020/09/04/trump-administration-launches-first-cybersecurity-principles-space-technologies

[69] "Treaty on principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies," U.S. Department of State Archive 2009-2017, https://2009-2017.state.gov/t/isn/5181.htm

[70] "Commercial Participation in Domestic and International Events on Safety, Sustainability, and Emerging Markets in Outer Space," U.S. Department of Space (February 25, 2020), https://www.federalregister.gov/documents/2020/02/25/2020-03684/commercial-participation-in-domestic-and-international-events-on-safety-sustainability-and-emerging

[71] Audrey Allison, Diane Howard, David Kendall, Mark Skinner, "A Modern Model of Space Law Creation: What Can COPUOS Learn from the ITU," 72nd International Astronautical Congress IAC-21-E3.4.6 (October 2021).

[72] Audrey Allison, "New Space Law Created to Enable Space Innovation While Preserving the RF Environment in Space; Notable Outcomes of the ITU's 2019 World Radio Conference," International Astronautical Congress IAC-20-E7-7.9 (October 2020).

[73] Mike Gruss, "Russian Satellite Maneuvers, Silence Worry Intelsat," *SpaceNews* (October 9, 2015), https://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/

[74] "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)," The Consortium for Execution of Rendezvous and Proximity Operations (October 2021), https://www.satelliteconfers.org/wp-content/uploads/2021/11/CONFERS-Guiding-Principles_Revised-Oct-21.pdf

[75] "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)," The Consortium for Execution of Rendezvous and Proximity Operations (October 2021), https://www.satelliteconfers.org/wp-content/uploads/2021/11/CONFERS-Guiding-Principles_Revised-Oct-21.pdf

[76] "About Space ISAC," Space Information Sharing and Analysis Center, Accessed March 16 2022, https://s-isac.org/about-us/

[77] "How Is The Space Sector Reacting To And Mitigating Against the Effects of Russia's War?" *The Downlink Podcast* (March 6, 2022) https://defaeroreport.com/2022/03/07/the-downlink-mar-06-22-how-is-the-space-sector-reacting-to-and-mitigating-against-the-effects-of-russias-war/

[78] "About AIA," Aerospace Industries Association (Accessed May 31, 2022), https://www.aia-aerospace.org/about-aia/
"About SIA," Satellite Industry Association (Accessed May 31, 2022), https://sia.org/about-sia/

"About Us," Commercial Spaceflight Federation (Accessed May 31, 2022), http://www.commercialspaceflight.org/about-us/