

## Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability

Sitki Egeli

**To cite this article:** Sitki Egeli (2021) Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability, Journal for Peace and Nuclear Disarmament, 4:1, 116-140, DOI: [10.1080/25751654.2021.1942681](https://doi.org/10.1080/25751654.2021.1942681)

**To link to this article:** <https://doi.org/10.1080/25751654.2021.1942681>



© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group on behalf of the Nagasaki University.



Published online: 25 Jun 2021.



[Submit your article to this journal](#)



Article views: 3431



[View related articles](#)




[View Crossmark data](#)



Citing articles: 2 [View citing articles](#)

# Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability

Sitki Egeli 

Political Science and International Relations, Izmir University of Economics, Balçova, Izmir, Turkey

## ABSTRACT

Satellites in Earth's orbit fulfill important functions in support of NC3 – nuclear command, control, and communication infrastructures of nuclear-armed states. Yet high confidence placed in those satellites' uninterrupted availability is based on shaky grounds and potentially dangerous. Ever since the placing in orbit of the first satellites, state and non-state actors have persistently pursued ways to harm them or to interrupt or compromise their services. Among the range of options to achieve such destruction or interference are kinetic and non-kinetic attacks executed by other satellites and craft that are themselves positioned in space. Recent technological advances in so-called proximity operations have rendered such space-to-space engagements more achievable, effective, and attractive. On the downside, the real-life efficiency of space-to-space engagements is subject to important limitations and unknowns. Augmenting the potential and attractiveness of space-to-space engagements in anti-satellite role though are the limitations of space situational awareness and the consequent difficulties encountered in prompt and unfailing detection and attribution of space-to-space intrusions. This dangerous and destabilizing property of space-to-space operations holds the potential of complicating nuclear-armed states' endeavor to preserve the coherence of their NC3 – a situation whose negative ramifications on strategic stability could be serious and potentially catastrophic.

## ARTICLE HISTORY

Received 03 December 2019

Accepted 07 June 2021

## KEYWORDS

Anti-satellite; command and control (nuclear); space-to-space warfare; arms control (space); strategic stability

## Introduction

Although the focus of most analysts and the fascination of the public have largely been on nuclear warheads and their delivery vehicles, such as ballistic missiles and bombers, equally if not more important is the role played by the nuclear command, control, and communication (NC3) architecture and capabilities fielded by states possessing nuclear weapons. NC3 comprises the comprehensive network of sensors, communication channels, command-and-control hardware and software, and crews operating them through which nuclear-armed states detect, transmit, and distribute warnings of an impending nuclear strike, make decisions on appropriate response, and issue orders to their own nuclear forces. Most of those elements are terrestrial; others are

**CONTACT** Sitki Egeli  [sitki.egeli@ieu.edu.tr](mailto:sitki.egeli@ieu.edu.tr)  Political Science and International Relations, Izmir University of Economics, Balçova, Izmir, Turkey

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group on behalf of the Nagasaki University. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

positioned in space. The significance of NC3 for nuclear stability and deterrence caught the attention of military planners and scholars alike, especially toward the later phases of the Cold War. It was pointed out that “weapons and strategic doctrines are meaningless unless [...] the superpowers also have the means to know what is happening in the chaos of a crisis or war [...] and have [the ability to ensure that] orders [are] carried out precisely and faithfully” (Carter 1985, 32). Meanwhile, some analysts sounded the alarm on the dangers of what they described as “nuclear Sarajevos”: “construction of fantastically complex nuclear command organizations [that] parallels the conflict institutions [of interlocking alerts and mobilizations] built in the decade before 1914, but on a far more spectacular and quick-reacting scale” (Bracken 1983, 3).

This comparatively concise study has no intention of revisiting the decades-old debate surrounding NC3. Instead, its focus will be on NC3’s space-based elements and the likely consequences for strategic stability of hampering or destroying those space-based NC3 assets. Primarily, the assets in question are various types of satellites orbiting Earth, some of which are dual use, implying their use by both nuclear and nonnuclear forces and military and civilian operators. Except for North Korea, all nuclear-armed states rely on satellites to varying degrees for NC3 functions. Those functions include – but are not limited to – early warning of missile launches, communications, geopositioning, navigation, and timing and synchronization of NC3 systems and networks. It is no secret that ever since the placing in orbit of the first satellite in 1957, techniques have been persistently pursued to harm satellites or to interrupt or compromise their services. The range of options are multiple: anti-satellite missiles, cyberattacks, electronic jamming/spoofing, and directed energy beams sent from Earth’s surface, or alternatively, kinetic and non-kinetic attacks executed by other satellites and craft that are themselves positioned in space. All those options will be briefly discussed with an eye to comparing their strong and weak points, but this study’s prime focus will be on attacks, harassment, and obstruction against satellites conducted by other satellites and spacecraft. Over the decades, several terms – for example, orbital weapons, killer satellites, space mines, co-orbital anti-satellite operations, and space-based anti-satellite weapons – have been used to refer to space-to-space hostile engagements. More recently, “space-to-space warfare” has been suggested to describe such a mode of employment (Harrison 2020, 5–8; Gleason and Hays 2020, 2). This article will borrow that taxonomy to analyze the magnitude and possible ramifications of spaceborne, human-induced threats directed at space-based elements of NC3. Although the means to achieve such space-to-space harm and interference have been actively pursued and deployed since the very beginning of the Space Age, recent technological advances surrounding the subset comprising so-called proximity operations and rendezvous and proximity operations (RPO) appear to have brought increased attention to the disruptive impact of space-to-space engagements (Damale 2020). Thus, within the larger realm of spaceborne intrusive activity directed at satellites, the particular emphasis of this study will be on proximity operations. The latter implies “a series of orbital maneuvers executed to place and maintain a spacecraft in the vicinity of another space object [...] to accomplish mission objectives” (Pfrang and Weeden 2020a). Unlike the multiplicity of works analyzing military operations in space, this study will be scrutinizing possible disruptive effects of space-to-space proximity operations on NC3 capabilities of nuclear-armed states.

## Threats to Satellites

There are over 3,300 active satellites today serving both civilian and military end users (Union of Concerned Scientists 2021). Over the years, their continued presence has come to constitute such an intrinsic and indispensable part of modern life that their uninterrupted services are taken for granted. Yet this widely held assumption of uninterrupted availability is unfounded and potentially dangerous. There is sufficient evidence of satellites' vulnerability to the natural hazards of the space environment as well as to human-induced harm and interference. In fact, soon after orbiting their satellites, Cold War rivals the Soviet Union and the United States pursued and eventually deployed means to destroy or interfere with each other's satellites. Over the years, other countries, all of which happen to be nuclear-armed states, followed in their footsteps.

The earliest and most visible form of anti-satellite activity involved shooting rockets at them. The term used to describe Earth-to-space kinetic kill weapons is Direct-Ascent Anti-Satellite (DA-ASAT). The first examples of these weapons were tested as early as 1959, and they have been deployed operationally since 1964 (Bateman 2020). Today, four spacefaring nations – the United States, Russia, China, and India – have dedicated DA-ASAT capabilities to target satellites at lower altitudes. These so-called low Earth orbit (LEO) satellites are found at altitudes up to 2,000 kilometers above Earth's surface. China is believed to have further experimented with DA-ASAT weapons capable of reaching satellites at higher medium Earth orbits (MEO) and geosynchronous Earth orbits (GEO) (Weeden 2020b). Additionally, since ballistic missile warheads travel at speeds and altitudes comparable to LEO satellites, any exoatmospheric missile defense system aimed at intercepting those warheads could be used to shoot down LEO satellites too (Grego 2012, 11). This means that by virtue of their Arrow-3 and Aegis/SM-3 missile defense systems, Israel and Japan should also be added to the list of countries capable of undertaking DA-ASAT activity.

At first glance, DA-ASAT weapons appear to be the most straightforward and effective way to destroy satellites. With flight times of less than 10 minutes to reach LEO satellites, they leave their target little time to detect and react to an attack (Reesman and Wilson 2020, 14). Yet their use entails a number of important drawbacks. The primary one is the debris cloud created by a violent, kinetic impact with the targeted satellite and the serious danger such debris causes for other satellites, including one's own satellites at the same and in adjacent orbits. Moreover, DA-ASAT weapons are like large fireworks, giving away instantly their launch point on Earth and thus the identity of the attacker. Therefore, their use would most likely trigger a response in kind. Considering the vulnerability of one's own satellites to anti-satellite activity, this is hardly a comforting and desirable situation for potential aggressors. Besides, the United States has already threatened to respond with nuclear weapons if elements of its NC3 came under attack with nonnuclear weapons (Acton 2019). Other nuclear-armed states should be expected to react similarly; the stakes are therefore very high. All those considerations transform DA-ASAT into weapons not for first use but rather for retaliation to deter possible DA-ASAT attacks by others.

The problem of debris and the ease of attribution that would normally dissuade states from using DA-ASAT weapons could be partly offset by resorting to non-kinetic options. The first among those options is electronic attack used to overwhelm satellites'

uplinks or downlinks with random radio frequency (RF) noise jamming or by corrupting the content of those links through what is called spoofing (Reesman and Wilson 2020, 15). Electronic warfare techniques developed over the decades for use in ground, naval, and air combat could be readily employed to impair satellites or even seize control of them (Atherton 2018). Following the lead of the United States and Russia, several states possess such anti-satellite electronic attack capabilities (Weeden and Samson 2020: x–xvi).

Another non-kinetic option is resorting to directed energy weapons – primarily laser beams that could dazzle or harm sensitive electro-optical sensors carried by satellites, as well as streams of high-power microwaves (HPM) to interrupt or perhaps even damage onboard electronics. On the plus side, electronic attack and directed energy options both eliminate the debris problem, complicate the task of identifying intruders, deliver attacks far faster (at the speed of light), and greatly increase the number of shots an aggressor might take (Reesman and Wilson 2020, 17). On the downside, ascertaining and judging their effectiveness beforehand or even during an attack is tricky. Their impact is temporary, meaning they will be effective as long as an electronic, laser or HPM emitter is turned on and the targeted satellite remains within range and line of sight. This also implies that the longer the duration of an attack and its emissions, the higher the chances of detection, countermeasures, counteraction, and ultimately retaliation. There also are important technical limitations to reckon with. For both electronic attack and directed energy weapons, the intensity of electronic signals and laser beams decreases with the distance from the source, and they are further weakened going through the atmosphere (Reesman and Wilson 2020, 17). A straightforward fix is moving the source closer to its target by installing electronic attack or directed energy devices on spacecraft. This attribute of electronic attack and directed energy options increases their attractiveness as the techniques of choice for space-to-space engagements – a prospect to be revisited later in this essay.

Cyberattacks constitute another equally if not more attractive non-kinetic option, along with which hardware and software weaknesses of satellites and their ground stations could be exploited to gain unauthorized access or to inject malicious codes. An intruder using the cyber domain could steal data, interrupt satellite availability and services, inflict temporary or permanent damage, or even seize control of satellites. Within the last decade, there have been several cases of satellites being hacked and even briefly hijacked by suspected state and non-state actors (Lewis and Livingstone 2016). On the downside, the success of cyberattacks is dependent on whether an adversary's network and systems can be infiltrated; thus there is no way to ascertain in advance that a cyberattack would negate space capabilities as anticipated (Bateman 2020). The strong point of cyberattacks is the difficulties encountered in detecting and attributing them. Without timely and reliable attribution, punishment is rendered difficult, and without punishment, deterrence becomes shaky. The challenges of attributing cyberattacks are magnified by the added difficulty of compiling reliable, conclusive, and, most importantly, real-time forensic evidence in space (Kallberg 2018). Furthermore, barriers to entry for cyberattack capabilities are lower than any other forms of anti-satellite activity. Those considerations appear to have convinced leading space powers to treat cyberattacks as the most probable and imminent menace to their space assets (Hitchens 2020c).

## Focus on Space-to-space Attack and Proximity Operations

In addition to Earth-to-space attacks, an obvious alternative for harassing or destroying satellites is to place another satellite, spacecraft, or device into orbit and then maneuver it closer to a targeted satellite in order to achieve a kinetic or non-kinetic effect. The United States and the Soviet Union sought to develop and deploy such space-to-space aggressive capabilities right from the beginning of the Space Age. Among earlier iterations were co-orbital anti-satellite (CO-ASAT) operations – placing into orbit an interceptor, “which then maneuvers to alter its orbit to a trajectory that brings it close to a target.” (Pfrang and Weeden 2020b) The maneuver to approach the target could take place immediately after the interceptor was placed into orbit or after it has remained dormant for an extended period – a mode of employment referred to frequently as “space mines” (Grego 2012, 8). In their earlier format, CO-ASAT weapons aimed to destroy satellites by direct collision at hypervelocities – which was rather difficult to achieve – or, more commonly, by getting close and releasing a cloud of fragments. For example, a Soviet CO-ASAT interceptor that became operational in 1973 and remained in service for two decades “is designed to approach a satellite, guided by controllers on the ground. [...] The onboard radar system guides the interceptor to within tens of meters of the target, then detonates an explosive that damages the target with shrapnel propelled by the explosion.” (Grego 2012, 3)

Hypervelocity collision and shrapnel techniques create a great deal of debris and differ little in their consequences from the disfavored DA-ASAT approach. As the Cold War moved to an end, rapidly advancing technologies rendered low-velocity controlled contact with the target, as well as packing the intruder with electronic warfare or directed energy emitters, became the more attractive options for space-to-space missions. RF jamming and spoofing was conceived as the earliest form of non-kinetic space-to-space attack. Eventually, it was supplemented by directed energy (lasers and HPM) emitters, cyberattacks launched from satellites, and the more exotic techniques such as spraying of aerosol clouds containing nanoparticles to pollute a satellite’s sensors, antennas, and solar panels (Hendrickx 2018). Besides eliminating the debris problem, non-kinetic attack added to the measure of deniability, and lessened the burden of getting in the immediate vicinity of the target (Reesman and Wilson 2020, 15). It now sufficed to maintain a stable position relative to a target at a distance of perhaps tens of kilometers away from it. The outcome is the increasing relevance in space-to-space warfare of proximity operations – “orbital maneuvers executed to place and maintain a spacecraft in the vicinity of another space object on a relative planned path for a specific time duration to accomplish mission objectives” (Pfrang and Weeden 2020a). Besides deploying non-kinetic tools, a malevolent spacecraft could also get very close to its target and seek to inflict physical damage without generating much debris. For instance, it could deploy a probe or robotic arm to damage the targeted satellite’s antennas, solar panels, or other critical systems. It could deploy a probe or use its own body mass for a controlled, low-velocity collision to inflict structural damage or push the targeted satellite off its orbit. More recently, Russia experimented with firing projectiles at very close range (Wright 2020), which may arguably have the benefit of reducing the amount of debris.

All told, there is little doubt that proximity operations offer attractive options for achieving space-to-space mission objectives ranging from eavesdropping, blinding,

jamming, and damaging of satellites to destroying or deorbiting them without necessarily creating large debris clouds. In this regard, technological advances, especially since the 1990s, provided proximity operations with a further boost by enabling deployment of smaller and lighter spacecraft that could get very close to other satellites without much assistance or guidance from the ground. Such small spacecraft could be fitted with “onboard guidance, navigation, and control systems to identify and track a targeted space object and fine-tune its trajectory for proper interception” (Pfrang and Weeden 2020b). It could then employ a number of kinetic or non-kinetic techniques. Due to its comparatively small size and autonomous mode of operation, such a craft has a better chance of avoiding detection and remaining relatively covert and inconspicuous. For instance, its presence could be disguised by launching it alongside a legitimate satellite, whereby it could evade detection by buddying with a satellite mother ship; remain within the latter’s radar, optical, or electronic shadow; or hiding itself among the larger chunks of debris created by the launch. When designed to incorporate radar and optical stealth features, such small craft can more easily evade detection by radars and telescopes constantly scanning the orbit for such unidentified and potentially hostile objects. Similarly, they could evade electronic detection by resorting to harder to detect suppressed carrier signals (Pfrang and Weeden 2020a).

The truth of the matter is that spacecraft that could potentially double as anti-satellite weapons do not have to be discreet or evade detection anymore. In recent years, the explosion of RPO saw an ever-increasing number of maneuvering spacecraft being used in Earth’s orbit to carry out a large variety of experimental, commercial, and undeniably legitimate functions, ranging from space debris removal to in-orbit inspection, repair, and refueling of satellites. In essence, all RPO-capable spacecraft are intrinsically dual use. That means their operators could readily shift them from benign commercial or scientific duties to hostile and intrusive action, whereby they could conveniently approach other objects in space without the cooperation, consent, or knowledge of the latter. They could then use a whole variety of intrusive, interruptive or destructive techniques; most of these could be low-tech, nonexplosive techniques that did not produce debris (Grego 2012, 5, 9–10). In fact, since the 1990s, not only the three leading space powers – the United States, Russia and China – but also a growing number of others have deployed state- and privately operated spacecraft to fulfill a great variety of RPO missions. With the exception of North Korea and Pakistan, all nuclear-armed states are capable of conducting proximity operations against other countries’ satellites. And as the following section explains, some of those satellites play critical roles in most nuclear-weapon states’ NC3 architectures.

Although space-to-space warfare and proximity operations appear to be offering extremely attractive, effective, and hard-to-negate means to harass, obstruct, or destroy satellites, the reality in the field is much more complex and contentious because the real-life effectiveness of space-to-space engagements is subject to a large variety of limitations and ambiguities. Hence the imperative to identify those limitations before jumping to quick and misleading conclusions.

First and foremost among these are the difficulties and peculiarities of maneuvering in space. Warfare in space takes place across vast heights, widths, and depths. Movements across those huge volumes are counterintuitive and do not analogize well with the movement on land, in the air, or at sea (Bilsborough 2020). For instance, satellites and

spacecraft move in circular or elliptical paths, meaning the most direct path between two points in space is rarely a straight line. Perhaps more significantly, satellites typically move along trajectories that are easy to track and predict, and deviating from their prescribed orbital path requires great time and effort (Reesman and Wilson 2020, 5–6). To put it differently, the extent of maneuvering in space is a function of the size of propulsion system and the amount of fuel that could be packed inside a spacecraft, and typically that is not large. Therefore, even small movements must be executed very precisely and carefully; they must be spread over time and well planned, given the limited fuel budget. This is a far cry from the Hollywood conception of the extremely agile spatial encounters in which spacecraft seek to outmaneuver each other through sudden jumps and turns. There are circumstances in which an attacker and its target could be moving at very high speeds relative to each other. But in such a flyby profile, the attacker and its target would instantly speed past each other and unless a debris-generating – and not so easy – head-on collision is targeted, such a momentary intersection of trajectories would be useful only for inspection missions in which the goal is to capture images of the target (Reesman and Wilson 2020, 8–9). Conversely, if one wishes to execute proximity operations whose value for anti-satellite missions has already been identified, then an attacking spacecraft trying to position itself near its target would be obliged to undertake a series of much slower, phased maneuvers. Since the amount of fuel carried on board would always be limited, utmost attention must be paid to using it efficiently. Sudden, steep, and energetic maneuvers must be minimized with an eye to unexpected eventualities. For example, if the targeted satellite is alerted and starts performing evasive maneuvers, then the attacker must have enough reserves to readjust its path to catch up with its target. Normally, a realistic pattern for conducting proximity operations would be for the offensive spacecraft to slowly position itself on the same orbital plane as its target in a maneuver that could take days, perhaps weeks. It would then wait for orders to execute a faster maneuver (that is, within hours) to move to an engagement trajectory and perform its mission. Because of these limitations on fuel and maneuvering, close encounters in space cannot be fast, momentary, or haphazard. Instead, slow and deliberate planning aimed at properly positioning an orbital weapon into an appropriate attack position is the more common mode of operation (Reesman and Wilson 2020, 11, 20).

Nor are the circumstances and the tactics of proximity operations invariably applicable to targets at all orbits and altitudes. At the lower LEO altitudes, the task of maneuvering an attacking spacecraft will be complicated by the very large number of satellites spread over hundreds of diverse orbital planes while circling Earth at great speeds (Reesman and Wilson 2020, 12). Consequently, a quick, spontaneous strike in LEO may necessitate significant jumps between altitudes and orbital planes, and the need for very large fuel budgets to execute such maneuvers would render them impractical. Instead, an LEO attacker would more likely be placed from the outset into the orbital plane of its target and then initiate small maneuvers over many days to move itself closer before attacking (Reesman and Wilson 2020, 12). Such a mode of action will not be fast, and it will not be inconspicuous to constant monitoring from Earth of LEO objects. Conversely, at the GEO altitude where most satellites are neatly lined up along a single orbital belt, it would be easier and faster for an attacker positioned along the same belt to approach its target. Accordingly, in order to remain stationary above a fixed point of



interest on Earth, larger and heavier GEO satellites must all stay at the exact same altitude of 35,768 kilometers above the equator. This creates an imaginary GEO belt on which hundreds of GEO satellites are in a row and separated from each other by a distance of as little as 75 kilometers (Reesman and Wilson 2020, 13). So at least in theory, it would be relatively easy for a hostile spacecraft to position itself on the GEO belt and then move forward or backward to quickly approach its target with much less effort. In fact, activities of US and Russian inspector satellites in GEO indicate that a single attacker could visit and potentially engage several satellites in succession along the GEO belt (Pfrang and Weeden 2020a, 2020c). On the downside though, commercial satellites populating the GEO belt move very little and very slowly, through maneuvers spread over weeks. Therefore, a fast-moving malevolent spacecraft is rather unlikely to have its motions go unnoticed since many operators maintain constant monitoring of their high-value GEO satellites (Reesman and Wilson 2020, 14).

This highlights the importance of space situational awareness (SSA) as a factor to consider in analyzing and judging the prospects of proximity operations and other forms of anti-satellite activity. In this regard, constant, real-time, and effective monitoring of objects in Earth's orbit is vitally important for detecting anti-satellite activity. Detection is imperative for evading, attributing and punishing – therefore deterring – hostile activity. But SSA is equally necessary for undertaking anti-satellite activity in the first place because such operations could not be carried out in the absence of accurate and timely information on the precise location and behavior of the targets. Nonetheless, when it comes to tracking objects in orbit today, many assume that everything is under control and we know exactly what is in orbit and where all objects are located all the time. That could not be further than the truth. While some objects are tracked, not all are and not all the time (Atherton 2020). SSA uses three categories of sensors to detect, track, and predict the movements of orbital objects. Those are radars, telescopes, and devices listening for electromagnetic emissions of satellites (Jah 2020). Of these, electronic listening is effective only against objects emitting electronic signals, but not all objects of concern would be actively communicating with the outside world all the time. Thus, its coverage is patchy and transient. In comparison, radars allow around-the-clock, real-time detection of all sizable objects that come within their field of view. However, they are limited in range to a few thousand kilometers and thus cannot see objects beyond LEO and lower-MEO altitudes. Consequently, for objects at the higher MEO, GEO, and HEO (highly elliptical orbit) altitudes, powerful telescopes stand out as the principal means used for space surveillance. However, telescope performance depends on favorable weather and clear skies; solar exclusion prevents observations for four to eight hours during daytime; and smaller objects or objects in the immediate vicinity of each other cannot be identified and differentiated with sufficient fidelity (Jah 2020; Hendrix 2020; Weeden 2017).

In fact, the task involves more than detecting and tracking orbital objects. Rather, SSA is an extremely complex task that requires comprehensive, real-time aggregation and processing of massive amounts of information, and this is a feat that is within reach of only the United States at the moment (Wauthier 2020). Yet even the impressive array of sensors and processing capabilities deployed by the United States provides something that is more like a series of snapshots than a live feed of space. Objects in LEO are mapped out a few times a day, while the update frequency for the higher orbits maybe

once every three days (Townsend 2020, 83; Economist 2019). Depending on the circumstances, this may become too long a delay to allow timely detection and evasion. Furthermore, with grainy surveillance, the task of reliable and timely attribution – and therefore the credibility of effective retribution and deterrence against anti-satellite action – becomes questionable. On the comforting side, though, the space around high-value satellites would most likely be under constant, more attentive watch by their operators. When alerted by suspicious movements of a potential attacker, the target could initiate evasive maneuvering. But this kind of evasive response is not without own problems: Defensive maneuvers consume fuel and reduce the total service life of the satellite. In addition, they often temporarily take the targeted satellite out of its primary mission and thus achieve the same results the attacker was seeking in the first place (Reesman and Wilson 2020, 7). Consequently, there is considerable uncertainty, and decision making is neither simple nor straightforward. In this respect, while the defender cannot be confident of always detecting objects approaching its satellites, the attacker cannot count on remaining hidden or disguised. Worse, unless initiating its final maneuver, the attacker may not have the means to determine whether its true identity and intentions have already been discovered by the defender. This strong element of ambiguity surrounding proximity operations gives rise to a complex and linked series of circumstances and variables defying shortcut generalizations and predictions about the likely prospects of hostile proximity operations in space.

In fact, those prospects are also compounded by a number of limitations and hard choices pertaining to the design and operational features of the spacecraft to undertake such missions. The first of these is an attacking craft's agility and maneuverability. Ideally, packing large quantities of fuel would do the job. But this would have the effect of increasing the size and weight of the spacecraft, thereby rendering stealth, concealment, and deception more difficult. More fuel would also mean a lighter and therefore less capable mission payload. For example non-kinetic emitters or robotic arms could no longer be carried. Launching larger and heavier objects into orbit also would make the undertaking more costly and increase the chances of detection. Thus, there are no easy answers to the problems created by the inverse relationship between size and weight on one hand and maneuverability on the other.

A second important consideration is onboard power generation and storage capacity, especially for those craft intended to fulfill non-kinetic missions. Electronic and directed energy attacks require significant amounts of power. But augmenting onboard power generation adds to size and weight and also depletes the limited supply of fuel. Batteries for power storage are heavy and their performance degrades over time. Resorting to solar panels for power generation would compromise the craft's low observability. More exotic power generation techniques, such as conventional explosives (to generate HPM) or use of a nuclear reaction to power electronic jammers, have been contemplated (Strout 2020a). But they would add considerably to the size and complexity of the spacecraft. And increased complexity results in reduced reliability.

Longevity and durability of a spacecraft's sensitive systems is another problematic domain. The brief overview of proximity operations earlier in this essay pointed out that a likely tactic would be for the attacker not to initiate threatening maneuvers immediately after launch into orbit. Instead, it would try to seem harmless while waiting for the optimal time and correct circumstances to attack. Such a "space mine" mode of employment may

entail long periods, perhaps years, of inaction. However, space is a very harsh environment and the reliability of a spacecraft and its various systems and fuel tends to degrade over time. Consequently, its owner would have decreasing confidence in its performance if the offensive spacecraft is allowed to remain dormant for too long (Grego 2012, 15).

Still another important and controversial design feature is a space weapon's degree of autonomy. The more autonomous a spacecraft is, the smaller is the need to communicate with its operators. And the more silent an attacker becomes, the more difficult it is for the defenders to detect and interfere with its operations. Autonomy also eliminates the need for maintaining a line of sight between a space weapon and its operators, who would normally be positioned at a fixed location on Earth. The advantages of such autonomy could be particularly large at the LEO, MEO, and HEO altitudes where the targets are constantly circling Earth and periodically move out of view of their ground-based controllers. Still, autonomy risks becoming a double-edged sword. Despite recent strides in artificial intelligence to assist autonomous decision making, the owners of autonomous spacecraft could place only limited confidence in their ability to cope with unforeseen circumstances. Because warfare in space remains largely unexplored and untested, there is plenty of room for technological and tactical surprises. Challenges with recalling or retasking autonomous satellite killers are likely to add to hesitations, as proximity operations are inherently slow, whereas the pace of developments in crises and confrontations back on Earth could be faster.

In summary, between the technical and technological limitations confining spacecraft on the one hand and the difficulties of maneuvering in space on the other, a perfect and impregnable space weapon that combines small size, agility, stealth, reliability, and lethality is simply unachievable. Nor are the high-value satellites totally defenseless in the face of space-to-space threats. Still, this does not mean a space weapon that manages to disguise itself long enough cannot exploit the loopholes in its target's SSA capabilities to strike a decisive blow and permanently or temporarily take its target out of action. High-value satellites in the GEO belt appear to be the most likely and lucrative targets of such space-to-space intrusion. The brief overview in the next section points out that satellites used most extensively by NC3 organizations are the ones positioned at GEO altitude.

### **Spaceborne Elements of NC3**

Several types and categories of satellites fulfill important functions that directly or indirectly serve NC3 organizations of nuclear-armed states. Among these, the role played by satellites fulfilling missile launch early-warning, strategic communications, and positioning and timing functions is more central and immediate for NC3. Therefore, our brief overview will focus on those three functions and satellites fulfilling them. This does not mean a whole variety of other satellites (for example, earth observation, electronic intelligence, meteorological forecasting, and radiation monitoring) are irrelevant. Rather, their inputs and impact on NC3 are not as time critical and direct, and therefore not as decisive or consequential for nuclear stability.

#### ***Early Warning***

Early warning of incoming missiles is a mission fulfilled by satellites fitted with heat-sensitive sensors capable of picking up the exhaust plumes of missiles against the colder

background of Earth and space. Typically, they can issue the first warning of missile launches in less than a minute after liftoff. This is much quicker and earlier than ground-based early-warning radars, which are restricted by the curvature of Earth and the limited range of radar signals. Radars can thus detect incoming missiles roughly halfway into their journey. This means that, faced with a first strike by an intercontinental ballistic missile (ICBM), early warning provided by satellites would precede detection by ground radars by roughly 15 minutes (Ramana, Rajaraman and Mian 2004). This additional 15 minutes doubles the time available to decision makers to comprehend the situation, deliberate, and choose and initiate their response. The shorter the available time, the higher the chances of hurried, misjudged, and miscalculated decisions.

The United States and the Soviet Union (and its successor Russia) are the only two states to have developed and orbited early-warning satellites. Those are large, costly, and technologically demanding assets positioned at GEO and HEO altitudes so as to attain a wider view of the surface of Earth. The United States has led the race since 1971 by maintaining a constellation of up to a dozen such satellites at any given time, providing near-global, around-the-clock coverage of all missile launches (Forden, Podvig and Postol 2000). The Soviet Union joined shortly afterward with up to nine satellites operating simultaneously. Yet after the end of Cold War, the Russian capability was gradually depleted due to negligence and budgetary constraints (Clark 2002; Podvig 2012). Since 2015, Russia has been reconstituting its early-warning constellation with the deployment of more capable and reliable HEO satellites, whose number currently stands at four (Hendrickx 2021). Recently, China begun adding an early-warning element to its NC3 architecture. Some claim that this effort, which is currently run with Russia's technical assistance (Litvinova 2019), could soon be expanded to include three GEO early-warning satellites (Global Security 2019).

Obviously, the US early-warning constellation comprising more satellites is the more resilient and redundant one in the face of hostile activity. Yet there are several other considerations to take into account. For instance, early-warning satellites have a reputation for generating false alarms – a fact that was vividly illustrated by the 1983 Petrov incident, when sunlight reflected from clouds above the continental United States led the sole Soviet satellite on watch to report a salvo of incoming ICBMs. Nuclear Armageddon was averted thanks to the good sense of the Soviet officer in charge who decided he needed to corroborate this warning. He waited for the illusory missiles to enter within the detection range of ground-based radar and thus proved them nonexistent (Forden, Podvig and Postol 2000: 33). One way to reduce the escalatory and destabilizing effect of false alarms is by comparing inputs coming from multiple satellites with overlapping fields of view (Ramana, Rajaraman and Mian 2004). Given the need for such comparison, the loss of one or more early-warning satellites operated by the United States risks compromising reliability and efficiency of space-based early warning. Loss of satellites may also open gaps in global coverage. Furthermore, it would shift the burden of authenticating an impending nuclear first strike to ground-based radars. Known as “dual phenomenology,” the practice of comparing data readings from at least two different sources is critical for preventing false alarms that could set off a dangerous spiral of actions and counteractions leading up to tragic consequences (Long 2016). As a backup to its early-warning satellites, the United States has retained six of its Cold War-era radars; their fields of view are confined to the northerly missile approach corridors from

Europe and Asia to North America (Korda and Kristensen 2019, 297). Faced with missiles closing in on the US mainland from other, primarily southerly directions, detection by radars would be limited or nonexistent and the burden of detection would fall almost exclusively on satellites. Considerable sensitivity to the loss of one or more of early-warning satellites could thus be expected.

Recognizing the vulnerability of their “big, fat, juicy” satellites built for efficiency in benign environments rather than to withstand attacks (Sankaran 2019; Hitchens 2020b), US authorities have recently been taking steps to increase the resilience of their high-value constellations. One current program seeks to supplement GEO satellites with a distributed architecture of several hundred smaller, cheaper, and easier-to-replace LEO satellites, which bring the added benefit of higher resolution and “cradle to grave” tracking of ballistic missiles and other heat-radiating targets (Strout 2019; Trimble 2020).

In comparison with the larger constellation of the United States, it stands to reason that the smaller Russian and the future Chinese constellations would be more susceptible to anti-satellite activity. Russia’s current fleet of four HEO satellites provides the minimum baseline for around-the-clock detection of missile launches from the North American continent and the Atlantic Ocean. Plans are in place to add more, perhaps up to 10 additional HEO and GEO satellites to prevent gaps in coverage that would result from the loss of even a single satellite. More satellites would also prove useful in reducing false alarms through cross-referencing by several satellites (Hendrickx 2021). However, Russia has experienced technical and budgetary difficulties in sustaining or expanding its satellite constellations (Luzin 2020). As a consequence of their insufficient numbers, satellites took a back seat in Russia’s ground-based early-warning network. Instead, in recent years Moscow managed to establish a large network of radars to provide coverage of all potential attack zones. This is a capability that was not achieved even in Soviet days (Hendrickx 2021).

### ***Satellite Communications***

Coherent communications carrying warning data from sensors to command posts and orders from command posts to nuclear forces are a basic and vital function of any NC3 architecture. Such an architecture comprises both spaceborne and terrestrial elements. With the exception of North Korea, all nuclear-armed states use satellites to varying degrees to augment their strategic communications. Positioned very high, most commonly along the GEO belt, communication satellites take advantage of their vantage point to overcome the range limitation imposed on radio waves by the curvature of Earth. In case their services are interrupted, a variety of backups are available. Those are terrestrial cables, airborne communication-relay aircraft, and radio signals to include extremely low and very low frequency radio waves that enable communication with submerged submarines carrying ballistic missiles (Carter 1985, 35).

As [Table 1](#) illustrates, the United States and Russia own 100 dedicated military communication satellites between them, whereas the numbers fielded by China and other nuclear-armed states are confined to a few units each. Much larger numbers of commercial satellites – several hundred for the United States and over 30 units each for Russia and China – are readily available to assist military communications. On the positive side, those numbers imply a great deal of spare capacity and redundancy; the

**Table 1.** Selected NC3 assets of nuclear-armed states, as of 2020.

	Missile early-warning satellites and radars					
	GEO satellite	HEO satellite	LEO satellite	Long-range radar	Dedicated military communication satellites	Positioning and timing satellites
US	9 (4 SBIRS, est. 5 DSP)	2 (SBIRS)	2 (STSS)	6 (UEWR, Cobra Dane)	49 (inc. 6 AEHF, 2 EPS, 5 Milstar)	24 (GPS-III, GPS)
Russia		4 (Tundra)		16 (Voronezh, Dnepr, etc.)	51 (inc. 4 Blagovest, 3 Raduga)	24 (Glonass)
China	planned				3 + 33 (military + dual use)	30 (Beidou)
France		2 (Spirale – experimental)		1 (TLP – under development)	4 (1 Athena, 3 Syracuse-3)	24 (Galileo)
UK					4 (Skynet5)	
Israel					2 (Amos dual use)	
India					3 (GSAT, Angrybird)	7 (Navic)
Pakistan					1 (Paksat1R dual use)	
N. Korea						

Sources: (Union of Concerned Scientists 2021; Luzin 2020; Missile Defense Advocacy Alliance 2019; Podvig et al. 2019).

loss of a few communication satellites therefore is unlikely to paralyze or degrade NC3 functions dramatically. Nonetheless, there are reasons to be concerned. Among the large number of dedicated military satellites, only a handful are the prized ones that offer secure, high-capacity strategic communications (Strout 2020b). Consequently, their operators would likely be more sensitive to their loss. Moreover, whether military or civilian, the overwhelming majority of communication satellites are neatly lined up along the GEO belt, making them low-hanging fruit for any hostile proximity operations aimed at diminishing or baffling an adversary's war effort.

Last but not least, even though terrestrial communication channels are available to the United States and Russia as a backup, most of those date back to the Cold War years (Clark 2019). Subsequently, concerns exist over the loss of redundancy of NC3 due to gradual dismantlement of backup communication capabilities (Acton 2018, 63–64). Especially for China – a nuclear power that did not make a comparable investment in terrestrial infrastructure during Cold War years – the situation may be more troubling, because Beijing depends more heavily on a smaller fleet of dedicated military communication satellites (Kulacki 2016).

All told, given the obvious advantages of using space-enabled communications over the cumbersome terrestrial alternatives, there are good reasons to suspect that nuclear powers may react strongly to their loss or tampering. Additionally, their neat lining up along the GEO belt in very close proximity to each other transforms large and cumbersome communication satellites into the easiest targets of space-to-space engagements. Those are not comforting observations against the background of the pivotal roles played by those satellites.

## ***Positioning and Timing Signals***

Over the course of the last three decades, positioning, navigation, and timing (PNT) signals broadcast by satellites positioned in MEO altitudes (at roughly 20,000 kilometers, or halfway between LEO and GEO) have become an intrinsic and indispensable feature of military operations. The United States, Russia, China, and others orbited PNT constellations, which are critical for the proper functioning of NC3. Satellite-assisted position finding and navigation is the more readily visible application, without which navigation and targeting would become enormously complicated, slow, and inefficient. Terrestrial backups are not as practical, reliable, and efficient, and they rely mostly on antiquated equipment and techniques dating back to 1940s (Sivacek 2018). But even more critical are the timing signals emitted from PNT satellites in whose absence a whole range of services such as secure communications, datalinks, sensor fusion, and network operations could come to a complete standstill (Hawkes and Blake 2017). It is doubtful that any military or nation is at all prepared for such an eventuality (Dawson 2018, 5–6).

On the bright side, the MEO altitudes across which PNT satellites are commonly spread are among the least crowded of orbital domains. Therefore, a hostile spacecraft trying to position itself would immediately become conspicuous and alert operators to possible intrusion. Furthermore, PNT constellations have considerable spare capacity, meaning several satellites must be pursued and attacked individually before the performance of the system starts degrading significantly. Even then, the loss of signals would be periodic at any place on Earth and not total. In short, the vulnerability of PNT constellations to space-to-space warfare and proximity operations is in fact rather low (Federation of American Scientists 2004, 34). The recent deployment of a new generation of maneuvering PNT satellites (Hitchens 2020a) and a new backup layer of LEO satellites (Munoz 2020) should further improve the situation. Adversaries intent on interfering with PNT would more plausibly resort to electronic spoofing, which could simultaneously be conducted against several PNT satellites by using Earth-based emitters.

## **Proximity Operations Pitted against NC3: Five scenarios**

NC3 capabilities and the proximity operations targeting them are technologically complex, multifaceted, and constantly evolving subjects. Analyzing the impact of proximity operations on NC3 and the ramifications for strategic stability is by no means easy or straightforward. To facilitate the task, we shall make use of five simplified scenarios. This clearly is not an exhaustive list of contingencies, and several equally plausible scenarios could be added.

### ***Scenario 1: What's Wrong with Our Satellite?***

Amid increased tensions, perhaps even an imminent military confrontation between two nuclear-armed adversaries, a high-value (for example, early-warning or strategic communication) satellite stops functioning or communicating instantly and inexplicably. SSA sensors do not pick up any anomalies. This may be the outcome of a technical malfunction or a natural phenomenon, such as the impact of a collision with a meteoroid or piece of space debris small enough to have evaded detection. Alternatively, the satellite

perhaps becomes the victim of a deliberate, undetected attack. Earth-to-space kinetic, electronic, or directed energy attacks would leave behind some trails. A cyberattack, which is harder to detect and attribute, is a strong possibility. So is a stealthy attack by hostile spacecraft. In fact, the adversary is known to have experimented with ominous small spacecraft that could easily conceal or disguise themselves until conducting a final maneuver to neutralize their targets. The victim would also be aware that, especially at distant GEO and HEO altitudes, SSA is not sufficiently comprehensive to detect and give warning of all suspicious or threatening movements as they happen. As suspicions abound, decision makers are faced with hard choices. Could this perhaps be the harbinger of a wider nuclear or nonnuclear first strike, along with which the attacker is seeking to eliminate the possibility of retaliation by degrading the defender's capacity to command, control, and communicate with its forces? Should the defender react immediately before the remaining space-enabled NC3 elements are also compromised and its control over nuclear and nonnuclear forces degrades even further? In the absence of a clear-cut picture of what actually has happened, there is a risk that impending decisions will be made on the basis of insufficient and potentially erroneous information, and the climate will be ripe for unfounded presumptions and predispositions. The resulting ultimatums, responses, or counteractions could set off a dangerous cycle of escalation and tit-for-tat actions, whereby reactions and overreactions between adversaries lead to potentially catastrophic consequences. At a minimum, heightened tension in orbit would have the outcome of spilling down to Earth so as to further aggravate an already tense situation.

### ***Scenario 2: Unwelcome Guest***

The circumstances of the second scenario are very similar to the first, with the exception that when the satellite goes off, there is an RPO-capable vehicle, inspector satellite, or other unidentified object in its vicinity. But there is no evidence of hostile activity or interference. This is an increasingly plausible scenario because in recent years, suspicious, uncooperative spacecraft getting very close to strategic satellites of others and staying there for a while has become routine and customary. Whereas the dose of uncertainty over the real cause of loss of contact with satellite persists, the victim's presumption that a proximity attack is to blame becomes much more intense. Thus, the considerations and processes are similar to those in the first scenario, but the potential for escalation is elevated exponentially.

### ***Scenario 3: To Preempt or Not to Preempt?***

The circumstances of the third scenario are similar to those of the second in that tensions are already high between nuclear-armed adversaries, but this time there is no loss of contact with a satellite. Instead, a suspicious spacecraft belonging to the adversary has positioned itself nearby or on the same orbital plane as a critical NC3 satellite. Even worse, there are indications that it may be undertaking additional maneuvering. The side whose satellite is being shadowed judges that a hostile action is imminent and that evasive, defensive, or preventive measures – or some combination of those – are warranted. Evasive maneuvering would take the targeted satellite out of its primary mission and achieve the same results the attacker was seeking. Alternatively, if



appropriately equipped, the targeted satellite could resort to defensive measures such as emitting laser beams or HPMS to interfere with the sensors and electronics of the nearby attacker. The side believing its satellite is in imminent danger may decide to move in one of its small “defensive” spacecraft to fend off the “offensive” craft. However, the decision to actually engage the attacker will not be easy. Even when employed in a presumably preemptive and self-defense mode, the use of space-to-space weapons or a guardian spacecraft to inflict damage on the adversary would be tantamount to having the first shot of a military confrontation fired in space. Escalatory risks of launching the first strike in the space domain are evident (Bilsborough 2020).

#### ***Scenario 4: Entanglement***

This scenario involves the opening or evolving phases of a nonnuclear confrontation between two nuclear-armed adversaries, with one or both of them attempting to disorient the other side’s conventional war effort by targeting its satellites. The motivation is simple and straightforward: all forms of modern warfare depend heavily on the services of satellites, and leaving one’s opponent devoid of those services reduces its operational efficacy. For satellites in LEO, a larger array of kinetic and non-kinetic anti-satellite options exist. For satellites in MEO and especially GEO altitudes, space-to-space and proximity operations stand out as the more viable option. However, there is one obvious danger: even when targeted as an extension of conventional skirmishes, most if not all military satellites are serving NC3 and nuclear forces as well. Consequently, their owners would likely become very sensitive to their loss. It is important to underline in this respect that there is no such thing anymore as strategic satellites dedicated exclusively to NC3 and nuclear forces (Acton 2018, 58). For example, early-warning satellites, originally developed to detect nuclear-tipped strategic missiles, are nowadays an indispensable part of active missile defenses aimed at intercepting shorter-range, nonnuclear missiles, which are frequently used in regional conflicts as well. Likewise, strategic communication and PNT satellites serve both tactical and strategic and both nuclear and nonnuclear forces. Therefore if high-value satellites also serving NC3 are targeted during a conventional confrontation, how quickly will their owners feel overly alarmed and cross the nuclear threshold in response? For example, the United States has already threatened to use nuclear weapons if its NC3 came under attack with nonnuclear weapons (Acton 2019). Likewise, when faced with conventional attacks threatening the security of the state, Russia’s nuclear doctrine – described by some in the West as “escalate to de-escalate” – allows a limited nuclear strike to convince the adversaries to back down (Oliker 2018). Even China’s strict “no first use” doctrine may be conducive to setting off preparations for a nuclear response in the face of high-tech conventional weapons used against China’s major strategic targets (Kulacki 2020). All told, the omens are not very comforting.

#### ***Scenario 5: Accident***

In this scenario, a spacecraft capable of proximity operations conducts relatively benign activity, such as close inspection or eavesdropping, near its object of interest and ends up inadvertently harming it. This could be an accidental collision or perhaps unintended

activation of its repertoire of kinetic and non-kinetic tools. That is not implausible, given the continuous presence of such vehicles nowadays in the immediate vicinity of others' sensitive satellites. The trend toward embedding more autonomy and automation in spacecraft increases the probability of such accidents and the consequent rounds of uncontrolled events. In fact, even the debris resulting from in-orbit experiments at more distant orbits (such as the firing of high-speed projectiles) could find its way to a collision with a high-value satellite of an adversary. This may be a particularly discomfiting possibility in the tightly populated GEO belt where the majority of NC3 satellites are located. If such inadvertent events were to take place during times of high tension between two adversaries, would the victim believe that the harm was unintended? Would forbearance and conciliation rule the day? Or would the responses be shaped by suspicion, worst-case assumptions and consequent reprisals, and thus escalation? There is little doubt that this scenario represents a set of dangerous uncertainties.

These five scenarios provide a picture that differs from the previous section's in some important ways. The earlier discussion of the characteristics and likely vulnerabilities of NC3 assets revealed significant backup capacity and thus considerable redundancy in the face of intrusions from space. The subsequent overview of a non-exhaustive list of scenarios points out that by threatening space-based elements of NC3, proximity operations could nonetheless create dangerous, potentially destabilizing, and escalatory pressures. It is true that the danger is not one of catastrophic collapse or complete paralysis of NC3 when its space-based elements come under attack. Rather, in circumstances comparable to those of a cyberattack, the real risks appear to emanate from ambiguities and uncertainties of timely and reliable detection and attribution of proximity attacks (Stoutland 2017). In the absence of complete, reliable, and timely information, decision makers would come under pressure to rapidly determine what they believe are the appropriate courses of action. Yet their decisions run a high risk of being erroneous and potentially catastrophic. This does not bode well for either crisis stability or escalation and crisis management.

An equally important consideration is that when detection and attribution are problematic, effective defenses and retribution become untenable. And in the absence of both defenses and retaliation, deterrence may be doomed too. The consequences could be dire. A potential aggressor may be induced to place accurate or ill-founded confidence in its ability to degrade its opponent's NC3. Or more plausibly, the victim of an actual or presumed space-to-space attack may become extremely worried about the cohesion of its NC3 and therefore resort to hurried, impulsive, and otherwise unthinkable courses of action. The consequence in both cases is the erosion of the long-held assumption that nuclear weapons are so destructive and retaliation so much assured that no sane leaders would risk igniting a general war against a nuclear-armed adversary (Krepinevich 2018). From this perspective, the worries about the destabilizing and escalatory properties of space-to-space warfare and proximity operations fit in with the heated debate since the Cold War period over the dangers of nuclear Sarajevos.

### **Fixes and Remedies: Some suggestions**

Although developing fixes and remedies is not the main goal of this study, it would not be complete without identifying the range of options that could be used to address and

hopefully alleviate the dangers emanating from the use of proximity operations against NC3 satellites. The list below is not exhaustive and the technicalities, background developments, and debates surrounding each option are not elaborated at length. Those are tasks to be undertaken by further studies on the subject, as each one of the available options deserves lengthy, painstaking analysis.

### ***Increasing Redundancy and Resilience***

To evade attackers, satellites could be packed with more fuel for maneuvering, hardened to better withstand non-kinetic attacks, fitted with sensors to warn of intruders, and even equipped with self-defense capabilities such as jammers and decoys. But such features add to the weight, size, complexity, and ultimately cost, and they inescapably eat away at operational life and cost efficiency. In addition, evasive maneuvering prevents the targeted satellite from fulfilling its mission and temporarily creates the result that the attacker was seeking in the first place. Deploying guardian craft in retrograde orbits to fend off intruders appears to be a viable alternative (Bilsborough 2020). But such action risks creating debris, which would have a lasting effect; that is especially true at the GEO altitudes (Reesman and Wilson 2020, 20) at which most NC3 satellites are found. Perhaps more importantly, as the technical features and capabilities would differ little from one to another, one nation's "defensive" small craft would undoubtedly appear "offensive" to others. In a perfect validation of the security dilemma, deploying spacecraft that the owner views as defensive would set off an endless spiral of responses and counter responses resulting in rapid weaponization of space and a situation in which no actors would ever feel secure.

As for resilience, an apparent shortcut is supplementing a handful of critically important and vulnerable GEO satellites with a distributed architecture of several hundred, perhaps thousands, of smaller, cheaper, and expendable LEO satellites. In fact, this is the alternative that United States is currently pursuing (Strout 2019). Yet this approach is not without dangers and complications. LEO altitudes are already overpopulated with large numbers of satellites operating under the constant threat of collisions with other satellites and space debris. Adding thousands more will be rendering life in LEO more perilous and unpredictable. Furthermore, shooting down or neutralizing satellites at closer-to-earth LEO altitudes is comparatively easy. Combined with the trend toward entrusting satellites with ever-expanding functions in support of the conventional warfare, the ease with which they could be targeted risks transforming LEO satellites into low-hanging, first-to-be-shot-at legitimate targets of any future conflict. Once states cross the notional threshold that so far has dissuaded them from destroying one another's satellites, there will be little to keep all satellites, including those at higher MEO and GEO altitudes, from becoming legitimate targets of any conflict. The days of space as a benign domain will be over.

### ***Improving SSA***

If the challenges associated with timely and effective detection and attribution constitute the main complicating property of proximity operations, then improving SSA to provide continuous and complete tracking of all orbital objects would offer an obvious solution.

But as the things stand, SSA is far from providing such complete coverage. It requires the combining of data from a large number of geographically distributed sensors on Earth and in space with operators' data on precise location and upcoming maneuvers of their satellites. Yet no state – not even the United States, the country in possession of the most numerous and varied sensors – can do this entirely by itself (Weeden 2020a, 17). What is required instead is cross-national collaboration between state and commercial and between military and civilian entities. Such exchanges and sharing of SSA data already take place between the closest allies, as well as between space agencies, scientific and academic institutions, amateur satellite observers, and commercial SSA companies (Weeden 2017). But there is nothing resembling a central global authority for SSA (Atherton 2020). For instance, an arrangement to collate and process inputs from multiple states, entities, and locations to allow more complete, real-time monitoring of suspicious or dangerous activity and thus reduce the adverse effects of partial and delayed detection and attribution of space activities could be applicable. Unfortunately, initiatives to explore such possibilities have so far faltered. Similarly, efforts over the years to develop regulatory frameworks to facilitate and ideally obligate the sharing of SSA-relevant data with others have not been successful (Damale 2020). The main challenge in this respect is not technical, legal, or organizational; the more immediate stumbling block is secretive and unilateral behavior by the dominant space powers.

Although a rapid and dramatic shift in those attitudes may not be forthcoming, there is no reason why partial and incremental fixes to enhance SSA could not be pursued. For instance, active RF beacons or other markers (such as optical or RF) could be installed on all objects placed in orbit (Lal et al. 2018, 9–10). In a fashion similar to air traffic control transponders installed on commercial aircraft, such beacons would allow easier, real-time tracking of legitimate spacecraft and enable focusing of SSA sensors on the movements of non-transmitting, unidentified, or suspicious objects in orbit. More strikingly, the explosion in recent years in the number and capabilities of commercial SSA companies has the potential to render states' and defense establishments' defensive reflexes on SSA irrelevant. Indeed, the capabilities of companies that routinely track and report objects in orbit could soon surpass those of governments (Weeden 2017) and pave the way to more efficient and more cooperative SSA – a development that would certainly increase transparency and confidence for the benefit of all.

### ***Norms, Regulations, Treaties***

Sixty years into the space age, there is very little in the way of arms control treaties, transparency, confidence-building measures, or norms of behavior to prohibit or restrain space-to-space engagements. Of the few applicable arrangements in force, the Outer Space Treaty of 1967 does not enforce a hard ban on satellite interference from space or elsewhere. The International Telecommunications Union Constitution and Convention prohibits harmful interference with satellites' operations – a provision that has not been activated even once in the face of several cases of such electronic and directed energy interference in recent years. Nuclear arms control treaties signed by the United States and the Soviet Union/Russia since the 1970s obliged them to refrain from interfering with each other's national technical means of verification (NTM) (Grego 2012, 3; Gleason and Riesbeck 2020, 2), and “Washington and Moscow have tacitly included in that definition

[of NTM] pretty much all satellites” (Hitchens 2019). However, treaties containing NTM are between the United States and Russia. Other spacefaring nations, most notably China, have not adopted this approach: “China has never really acknowledged the prohibition on interference with NTM as something that applies to [their own] activities” (Hitchens 2019).

In 2008, a major Russian-Chinese proposal to ban all space-based weapons did not find much acceptance either. Among its shortcomings were its lack of mechanisms for compliance and verification and its failure to address the problem of dual-use RPO satellites (Patrick and Evanoff 2018). The complications caused by dual-use satellites may indeed be the crux of the matter for arms control in space. Whether civilian or not, all RPO-capable craft are inherently dual use in that they could readily move from benign commercial and scientific uses to hostile and intrusive operations. Thus, any arms control arrangements seeking to ban or restrict spacecraft capable of conducting hostile proximity operations must first tackle the daunting task of differentiating them from legitimate RPO satellites.

It is true that certain telltale characteristics giving away offensive use or intentions could be identified. They include significant onboard power generation and storage, small size, stealth features, propulsion and fuel stocks to allow agile maneuvers, fully autonomous operations, hard-to-detect modes of communication (for example, laser beams or suppressed carrier signals), unjustifiably high numbers in orbit, and perhaps more sightings around others’ satellites than one’s own. But incorporating those into the precise, unequivocal language of a treaty would be a real challenge. So would be the task of unfailing verification in space, where the circumstances would be starkly different from those surrounding inspections on Earth. After all, owing to the additional limitations imposed by secrecy, it may become impossible to judge the real content and purpose of a spacecraft based on its outward appearance and characteristics.

Given the formidable dual-use problem, proximity operations and the spacecraft performing them cannot possibly be banned. If de facto weapons in space are unavoidable, then we better learn how to live with them (Chow 2018). This means that instead of categorical bans and restrictions on the spacecraft themselves, the focus should be on curtailing their irresponsible and potentially threatening activities and on reducing the risks of misunderstandings and miscalculations (Erwin 2021). Under the rubric of “manuals” or “codes of conduct” for responsible behavior in space, several proposals have been developed over the years at the United Nations, as well as by multinational bodies such as the European Union and by individual states (Grego 2012, 14). In broad terms, the expectation is that the signatories will refrain from undertaking activities in space that could pose dangers to satellites. Templates could be binding or nonbinding, voluntary, or mandatory. A pragmatic shortcut in this respect could be to follow the successful example of INCSEA – incidents-at-sea agreements that were successfully used since the Cold War years to deconflict close encounters between military ships and aircraft. Yet despite some exploratory talks recently between US and Russian officials (*Economist* 2020), no one has so far proposed such an accord (Samson and Weeden 2020). A similar approach would be to agree to provide advance notification of planned maneuvers in orbit to minimize suspicions (Johnson 2014). Options could be diversified into a variety of voluntary, nonbinding initiatives, such as declaring a moratorium on destructive anti-satellite testing. A comparable moratorium that was announced in the

1960s to stop all atmospheric nuclear explosions expanded over time to cover all nuclear testing. The shared principle that characterizes all those options is the need to be realistic in addressing the challenges posed by proximity operations in space. The remedy proposed for several disruptive technologies has been to move away from material-based arms control to behavior-based arms control (Bohn 2020). This implies that instead of arms control's traditional preoccupation with objects and capabilities, space arms control should focus more on behavior and how those capabilities are deployed and employed (Moraga 2021). In the specific context of proximity operations this means that rather than trying in vain to restrict or outlaw categories of spacecraft, it makes much more sense to regulate their behavior, especially for cases in which these spacecraft will be operating in close proximity to one another.

## Acknowledgments

The author would like to thank to Bulent Yazici and Nilufer Ayhan, graduate students at Izmir University of Economics, for their preliminary research and literature review in preparation for this essay.

## Disclosure Of Potential Conflicts Of Interest

No potential conflict of interest was reported by the author(s).

## Notes on Contributor

*Sitki Egeli* is an assistant professor in the Political Science and International Relations Department of Izmir University of Economics. He was previously a director for foreign affairs in Turkey's Undersecretariat for Defense Industries (SSM) and vice president in charge of the defense and aerospace sectors of an international consulting firm.

## ORCID

Sitki Egeli  <http://orcid.org/0000-0001-6254-1003>

## References

- Acton, J. M. 2018. "Escalation through Entanglement." *International Security* 43 (1): 56–99. <https://direct.mit.edu/isec/article/43/1/56/12199/Escalation-through-Entanglement-How-the> .
- Acton, J. M. 2019. "Why Is Nuclear Entanglement So Dangerous?." Carnegie Q&A. 23 January 2019. <https://carnegieendowment.org/2019/01/23/why-is-nuclear-entanglement-so-dangerous-pub-78136>
- Atherton, K. D. 2018. "Understanding the Players, Tactics for a Possible War in Space." *C4ISRNET*. 17 April 2018. <https://www.c4isrnet.com/c2-comms/satellites/2018/04/17/understanding-the-players-tactics-for-a-possible-war-in-space/>
- Atherton, K. D. 2020. "We Don't Really Know What We Don't Know in Orbit." *C4ISRNET*. 11 February 2020. <https://www.c4isrnet.com/c2-comms/satellites/2020/02/10/we-dont-really-know-what-we-dont-know-in-orbit/>

- Bateman, A. 2020. "America Can Protect Its Satellites Without Kinetic Space Weapons." *War on the Rocks*. 30 July 2020. <https://warontherocks.com/2020/07/america-can-protect-its-satellites-without-kinetic-space-weapons/>
- Bilsborough, S. 2020. "More Space Wargames, Please." *War on the Rocks*. 17 November 2020. <https://warontherocks.com/2020/11/more-space-wargames-please/>
- Bohn, R. 2020. "EUNPDC Annual Conference – Virtual Room Two." 13 November 2020. <https://www.youtube.com/watch?v=E7fPsEkszNw>
- Bracken, P. 1983. *The Command and Control of Nuclear Forces*. Binghamton: Yale UP.
- Carter, A. B. 1985. "The Command and Control of Nuclear War." *Scientific American* 252 (1): 32–39. doi:10.1038/scientificamerican0185-32.
- Chow, B. G. 2018. "Worker-Bee Satellites Will Weaponize Space – And Help Us Keep the Peace." *Defense One*. 5 June 2018. <https://www.defenseone.com/ideas/2018/06/worker-bee-satellites-will-weaponize-space-we-can-still-keep-peace/148746/>
- Clark, P. S. 2002. "Russia Begins to Expand Early Warning Satellite Network." *Jane's Defence Weekly*. 17 (2002, April): 11.
- Clark, P. S. 2019. "Whither Nuclear Command, Control & Communications?" *Breaking Defense*. 14 February 2019. <https://breakingdefense.com/2019/02/whither-nuclear-command-control-communications/>
- Damale, A. 2020. "Rendezvous Proximity Operations: Not Operating in Isolation." ELN. <https://www.europeanleadershipnetwork.org/commentary/rendezvous-proximity-operations-not-operating-in-isolation/>
- Dawson, L. 2018. *War in Space: The Science and Technology behind Our Next Theater of Conflict*. Chichester: Springer-Praxis Books. <https://doi.org/10.1007/978-3-319-93052-7>
- Economist*. 2019. "Using the Force." 20 July 2019:16–18.
- Economist*. 2020. "A Russian satellite weapon shows the danger of hazy rules in space." 9 August 2020. <https://www.economist.com/science-and-technology/2020/08/09/a-russian-satellite-weapon-shows-the-danger-of-hazy-rules-in-space>
- Erwin, S. 2021. "U.S. To Support International Effort to Set Rules of Behavior in Space." *Space News*. 24 February 2021. <https://spacenews.com/u-s-to-support-international-effort-to-set-rules-of-behavior-in-space/>
- Federation of American Scientists. 2004. *Ensuring America's Space Security: Report of the FAS Panel on Weapons in Space*. [https://fas.org/pubs/\\_docs/10072004164336.pdf](https://fas.org/pubs/_docs/10072004164336.pdf)
- Forden, G., P. Podvig, T. A. Postol. 2000. "False Alarm, Nuclear Danger." *IEEE Spectrum* 37 (3): 31–39. DOI:10.1109/6.825657.
- Gleason, M. P., and L. H. Riesbeck. 2020. *Noninterference with National Technical Means: The Status Quo Will Not Survive*. Center for Space Policy and Strategy, Space Policy Paper. [https://aerospace.org/sites/default/files/2020-01/Gleason\\_NTM\\_20200114.pdf](https://aerospace.org/sites/default/files/2020-01/Gleason_NTM_20200114.pdf)
- Gleason, M. P., and P. L. Hays. 2020. *A Roadmap for Assessing Space Weapons*. Center for Space Policy and Strategy, Space Policy Paper. [https://aerospace.org/sites/default/files/2020-10/Gleason-Hays\\_SpaceWeapons\\_20201005\\_1.pdf](https://aerospace.org/sites/default/files/2020-10/Gleason-Hays_SpaceWeapons_20201005_1.pdf)
- Grego, L. 2012. *A History of Anti-Satellite Programs*. Union of Concerned Scientists. <https://www.ucsusa.org/resources/history-anti-satellite-programs>
- Harrison, T. 2020. "International Perspectives on Space Weapons." CSIS. <https://www.csis.org/analysis/international-perspectives-space-weapons>
- Hawkes, T., and M. Blake. 2017. "Time Warfare: Threats to GPS Aren't Just about Navigation and Positioning." *Defense One*. 10 May 2017. <https://www.defenseone.com/ideas/2017/05/time-warfare-anti-gps-arent-just-about-navigation-and-positioning/137724/>
- Hendrickx, B. 2018. "Silent Hunter." *Jane's Intelligence Review*. November 2018. <https://emagazines.ihs.com/webviewer/#janesintelligencereviewnovember2018/focus>
- Hendrickx, B. 2021. "EKS: Russia's Space-based Missile Early-warning System." *The Space Review*. 8 February 2021. <https://www.thespacereview.com/article/4121/1>
- Hendrix, D. 2020. "Seeing Space Security: The Role of Space Situational Awareness for Verification of Future Space Arms Control." UNIDIR Webinar. 10 November 2020. <https://www.youtube.com/watch?v=-Nv-EqStUHQ>

- Hitchens, T. 2019. "US Missile Warning Sats Fair Game If No New START?" *Breaking Defense*. 19 July 2019. <https://breakingdefense.com/2019/07/us-missile-warning-sats-fair-game-if-no-new-start/>
- Hitchens, T. 2020a. "New GPS Sats Can Maneuver & Resist Jamming." *Breaking Defense*. 26 February 2020. <https://breakingdefense.com/2020/02/new-gps-sats-can-maneuver-and-resist-jamming/>
- Hitchens, T. 2020b. "US, Allies Agree on Threats in Space but Struggle with Messaging." *Breaking Defense*. 11 September 2020. <https://breakingdefense.com/2020/09/us-allies-agree-on-threats-in-space-but-struggle-with-messaging/>
- Hitchens, T. 2020c. "Cyber Attack Most Likely Space Threat: Maj.Gen. Whiting." *Breaking Defense*. 16 September 2020. <https://breakingdefense.com/2020/09/cyber-attack-most-likely-space-threat-maj-gen-whiting/>
- Jah, M. 2020. "Space Situational Awareness and Space Security." UNIDIR Launch Pad Seminars: Episode-1. 20 May 2020. <https://www.youtube.com/watch?v=pgCUB57LzK4>
- Johnson, C. 2014. "The UN Group of Governmental Experts on Space TCBM." SWF Fact Sheet. April 2014 [https://swfound.org/media/109311/swf\\_gge\\_on\\_space\\_tcbms\\_fact\\_sheet\\_april\\_2014.pdf](https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf)
- Kallberg, J. 2018. "Why Older Satellites Present a Cyber Risk." *Fifth Domain*. <https://www.fifthdomain.com/opinion/2018/12/28/why-older-satellites-present-a-cyber-risk/>
- Korda, M., and H. M. Kristensen. 2019. "US Ballistic Missile Defenses, 2019." *Bulletin of the Atomic Scientists* 75 (6): 295–306. doi:10.1080/00963402.2019.1680055.
- Krepinevich, A. F., Jr. 2018. "The Eroding Balance of Terror." *Foreign Policy*. 11 December 2018. <https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror>
- Kulacki, G. 2016. "The United States, China, and Anti-Satellite Weapons." Union of Concerned Scientists. 7 September 2016. <https://allthingsnuclear.org/gkulacki/the-united-states-china-and-anti-satellite-weapons>
- Kulacki, G. 2020. "Would China Use Nuclear Weapons First in a War with the United States?" *The Diplomat*. 27 April 2020. <https://thediplomat.com/2020/04/would-china-use-nuclear-weapons-first-in-a-war-with-the-united-states/>
- Lal, B., A. Balakrishnan, B. M. Cadwell, R.S. Buenconsejo, S. A. Carioscia. 2018. *Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)*. Washington, D.C.: IDA Science & Technology Policy Institute. <https://www.ida.org/-/media/feature/publications/g/gl/global-trends-in-space-situational-awareness-ssa-and-space-traffic-management-stm/d-9074.ashx>
- Lewis, P., and D. Livingstone. 2016. "The Cyber Threat in Outer Space." *Bulletin of the Atomic Scientists*. <https://thebulletin.org/2016/11/the-cyber-threat-in-outer-space/>
- Litvinova, D. 2019. "Russia Is Helping China Build a New Missile Attack Warning System, Putin Says." *CBS News*. 4 October 2019. <https://www.cbsnews.com/news/russia-to-help-china-build-new-missile-attack-warning-system-vladimir-putin-says-today-2019-10-04/>
- Long, A. 2016. "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." *Journal of Cybersecurity* 3 (1): 19–28. doi:10.1093/cybsec/tywo16.
- Luzin, P. 2020. "Russia Is behind in Military Space Capabilities, but that Only Drives Appetite." *Defense News*. 1 April 2020. <https://www.defensenews.com/opinion/commentary/2020/04/02/russia-is-behind-in-military-space-capabilities-but-that-only-drives-its-appetite/>
- Missile Defense Advocacy Alliance. 2019. "U.S. Deployed Sensor Systems." <https://missiledefenseadvocacy.org/missile-defense-systems-2/missile-defense-systems/u-s-deployed-sensor-systems/>
- Moraga, P. 2021. "Security and Stability of Space: What You Need to Know." SWF Webinar. March 16. <https://swfound.org/events/2021/security-and-stability-of-space-what-you-need-to-know>
- Munoz, C. 2020. "Pentagon solicits proposals for new hypersonic advanced warning system." *Jane's 360*, 25 June 2020. <https://www.janes.com/defence-news/news-detail/pentagon-solicits-proposals-for-new-hypersonic-advanced-warning-system>



- Oliker, O. 2018. "Moscow's Nuclear Enigma." *Foreign Affairs*. 15 October 2018. <https://www.foreignaffairs.com/articles/russian-federation/2018-10-15/moscows-nuclear-enigma>
- Patrick, S., and K. L. Evanoff. 2018. "The Right Way to Achieve Security in Space." *Foreign Affairs*. 17 September 2018. <https://www.foreignaffairs.com/articles/space/2018-09-17/right-way-achieve-security-space>
- Pfrang, K., and B. Weeden. 2020a. *U.S. Military and Intelligence Rendezvous and Proximity Operations in Space*. Secure World Foundation. Updated August 2020. [https://swfound.org/media/207054/swf\\_us\\_rpo\\_aug2020.pdf](https://swfound.org/media/207054/swf_us_rpo_aug2020.pdf)
- Pfrang, K., and B. Weeden. 2020b. *U.S. Co-Orbital Anti-Satellite Testing*. Secure World Foundation. Updated August 2020. [https://swfound.org/media/207055/swf\\_us\\_co-orbital-asat\\_aug2020.pdf](https://swfound.org/media/207055/swf_us_co-orbital-asat_aug2020.pdf)
- Pfrang, K., and B. Weeden. 2020c. *Russian Military and Intelligence Rendezvous and Proximity Operations*. Secure World Foundation. Updated August 2020. [https://swfound.org/media/207053/swf\\_russian\\_rpo\\_aug2020.pdf](https://swfound.org/media/207053/swf_russian_rpo_aug2020.pdf)
- Podvig, P. 2012. "Russian Federation". *Assuring Destruction Forever: Nuclear Weapon Modernization around the World*, edited by R. Acheson, 59–66. New York: Reaching Critical Will. <http://reachingcriticalwill.org/images/documents/Publications/modernization/assuring-destruction-forever.pdf>
- Podvig, P., O. Bukharin, T. Kadyshv, E. Miasnikov, I. Sutyagin, M. Tarashenko, B. Zhelezov. 2019. "Early Warning." *Russian Strategic Nuclear Forces*. 9 October 2019. <http://russianforces.org/sprn/>
- Ramana, M. V., R. Rajaraman, Z. Mian . 2004. "Nuclear Early Warning in South Asia." *Economic and Political Weekly* 39 (3): 279–284.
- Reesman, R., and J. R. Wilson. 2020. *The Physics of Space War: How Orbital Dynamics Constrain Space-to-Space Engagements*. Center for Space Policy and Strategy, Space Policy Paper. <https://aerospace.org/paper/physics-space-war-how-orbital-dynamics-constrain-space-space-engagements>
- Samson, V., and B. Weeden. 2020. "US Should Start Space Security Talks With Russia, China." *Breaking Defense*. 12 May 2020. <https://breakingdefense.com/2020/05/us-should-start-space-security-talks-with-russia-china/>
- Sankaran, J. 2019. "Big, Fat, Juicy Targets – The Problem with Existing Early-warning Satellites. And a Solution." *The Bulletin*. 30 September 2019. <https://thebulletin.org/2019/09/big-fat-juicy-targets-the-problem-with-existing-early-warning-satellites/>
- Security, G. 2019. "Chinese Ballistic Missile Early Warning." 10 June 2019. <https://www.globalsecurity.org/space/world/china/warning.htm>
- Sivacek, M. 2018. "The U.S. Military Needs GPS to Fight." *The National Interest*. 28 February 2018. <https://nationalinterest.org/blog/the-buzz/the-us-military-needs-gps-fight-needs-change-24683>
- Stoutland, P. 2017. "Growing Threat: Cyber and Nuclear Weapon Systems." *The Bulletin of the Atomic Scientists*. 18 October 2017. <https://thebulletin.org/2017/10/growing-threat-cyber-and-nuclear-weapons-systems/>
- Strout, N. 2019. "A New Orbit for Some of the Pentagon's Missile Warning Satellites." *C4ISRNET*. 18 September 2019. <https://www.c4isrnet.com/battlefield-tech/space/2019/09/18/a-new-orbit-for-some-of-the-pentagons-missile-warning-satellites/>
- Strout, N. 2020a. "Russia Conducted Anti-satellite Missile Test, Says US Space Command." *C4ISRNET*. 15 April 2020. <https://www.c4isrnet.com/battlefield-tech/space/2020/04/15/russia-conducted-anti-satellite-missile-test-says-us-space-command/>
- Strout, N. 2020b. "Space Operations Command Takes over Final AEHF Satellite." *C4ISRNET*. 8 December 2020. <https://www.c4isrnet.com/battlefield-tech/space/2020/12/08/space-operations-command-takes-over-final-aehf-satellite/>
- Townsend, B. 2020. "Strategic Choice and the Orbital Security Dilemma." *Strategic Studies Quarterly* 14 (1): 64–90.
- Trimble, S. 2020. "Missile Defense Agency Reveals Hypersonic Defense Vision." *Aviation Week & Space Technology*, 17/30 August 2020: 26–27.

- Union of Concerned Scientists. 2021. “UCS Satellite Data Base.” Updated 1 January 2021. <https://www.ucsusa.org/resources/satellite-database>
- Wauthier, P. 2020. “Safety of Space Flight.” SWF Webinar. 29 July 2020. <https://swfound.org/events/2020/safety-of-spaceflight-looking-back-at-the-past-decade-looking-ahead-at-the-next-five-years>
- Weeden, B. 2017. *Space Situational Awareness Fact Sheet*. Secure World Foundation. Updated May 2017. [https://swfound.org/media/205874/swf\\_ssa\\_fact\\_sheet.pdf](https://swfound.org/media/205874/swf_ssa_fact_sheet.pdf)
- Weeden, B. 2020a. *Space Situational Awareness: Examining Key Issues and the Changing Landscape*. Testimony at the Hearing of the Subcommittee on Space and Aeronautics U.S. House of Representatives. Washington, D.C. 11 February 2020. [https://swfound.org/media/206932/weeden\\_house\\_ssa\\_testimony\\_written\\_feb2020.pdf](https://swfound.org/media/206932/weeden_house_ssa_testimony_written_feb2020.pdf)
- Weeden, B. 2020b. *Chinese Direct-Ascent Anti-Satellite Testing*. Secure World Foundation. Updated August 2020. [https://swfound.org/media/207050/swf\\_chinese\\_da-asat\\_aug2020.pdf](https://swfound.org/media/207050/swf_chinese_da-asat_aug2020.pdf)
- Weeden, B., and V. Samson. 2020. *Global Counterspace Capabilities: An Open Source Assessment*. Secure World Foundation. April 2020. [https://swfound.org/media/206970/swf\\_counterspace2020\\_electronic\\_final.pdf](https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf)
- Wright, T. 2020. “Russia Tests Space-based Anti-satellite Weapon.” *IISS Analysis*. 9 September 2020. <https://www.iiss.org/blogs/analysis/2020/09/mdi-russia-tests-space-based-anti-satellite-weapon>