# AFF---SPACE ASSETS---BFHR

### notes

Thanks a ton to Eshan Momin and Hana Bisevac for their extremely hard work on the cyber space assets aff/neg file set. Please email [khirn10@gmail.com](mailto:khirn10@gmail.com) with any questions or concerns.

# 1AC---SPACE ASSETS

## 1AC---SPACE ASSETS

### 1AC---ASATs ADVANTAGE

#### Contention 1 is ASATs.

#### Present NATO commitments in space have fostered strategic ambiguity AND capability gaps for Russia and China to exploit---effectively opening grey zones for China and Russia to test NATO resolve. Only the plan creates united NATO capabilities to deter adversaries.

Aurel Sari & Hitoshi Nasu 21. Associate Professor of International Law and Director of the Exeter Centre for International Law, University of Exeter; Fellow, Supreme Headquarters Allied Powers Europe. The views expressed are those of the author in a personal capacity; Professor of International Law, University of Exeter; Senior Fellow, Stockton Center for International Law, United States (US) Naval War College. The thoughts and opinions expressed are those of the author and not those of the US Government, the US Department of the Navy, or the US Naval War College. “NATO and Collective Defense in Space: Same Mission, New Domain”, ECIL Working Paper 2021/2 (forthcoming in Turkish Policy Quarterly, Summer 2021, Vol 20, No 2, <https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Sari_and_Nasu_-_NATO_and_Collective_Defence_in_Space_-_ECIL_WP_2021-2.pdf> //EM

Strategic Ambiguity: How Much is too Much?

Overall, the Brussels Communiqué sends a strong signal that the Allies are prepared to defend their interests in space, including through the use of force if necessary. However, the clarity of this message is diluted by the uncertainty surrounding the exact conditions which may prompt the Allies to invoke Article 5 in response to an armed attack. This ambiguity may be seen as an asset: leaving hostile powers guessing the exact conditions that could trigger a forceful military response by the Alliance may prompt those powers to proceed with greater caution.25

Strategic ambiguity thus has its benefits. However, hostile actors may also read it as a lack of resolve. In the present case, at least two factors may encourage such a reading. The first relates to the uncertain parameters of the right of self-defense itself and the ambiguities that surround its application in space.26 For example, could non-kinetic interference against space-based assets or services, such as signal jamming, rise to the level of an armed attack? If so, under what circumstances does such interference satisfy the gravity threshold required to constitute an armed attack?27 Is it lawful to declare a space exclusion zone or to deploy “bodyguard” satellites to defend critical space-based assets in anticipation of an attack in the exercise of the right of self-defense? Having recognized the applicability of Article 5 to space attacks, NATO nations need to develop a shared approach to these and related questions in order to demonstrate unity and resolve.

The second factor relates to the geographical limits that Article 6 of the NAT imposes on the operation of Article 5 of the NAT. The first sub-paragraph of Article 6 deals with attacks on Allied territory. It is clear from the language of this sub-paragraph that armed attacks launched into the territory or islands of NATO members from or through space fall squarely within the ambit of Article 5. Armed attacks launched against their assets in space are caught by the second sub-paragraph of Article 6, which deals with attacks against the “forces, vessels or aircraft of any of the Parties.” While neither the notion of a vessel,28 nor that of an aircraft, 29 extends to objects primarily designed for operation in outer space, the concept of ‘forces’ is broad enough to cover spacecraft and their personnel. There is a catch, however. The second sub-paragraph of Article 6 of the NAT refers to attacks taking place “in or over” Allied territories. This means that, at best, attacks against Allied forces in space are covered by Article 5 only whilst in orbit “over” such territories and above their airspace. Accordingly, the destruction of an Allied satellite may engage Article 5 if the satellite was orbiting over the territory of a NATO nation, but not if it was orbiting over the South China Sea, for instance.30

NATO nations thus face a dilemma. The geographical limitations imposed by Article 6 of the NAT on the operation of their mutual assistance commitment increases the vulnerability of their space assets to hostile maneuvers by potential adversaries, especially in the Southern Hemisphere where the Alliance has the fewest Space Surveillance Network (SSN) assets. To address this vulnerability, the Allies may consider Article 5 to be applicable to attacks against their space assets wherever they may operate, that is without any geographical restrictions. However, extending the scope of Article 5 to cover all around Earth may expose NATO to accusations that it seeks to militarize this domain. Also, such a move would lack credibility unless it is underwritten by capabilities necessary to defend Western space assets and the services they provide.

Ignoring the matter is not an option. China and Russia are known for exploiting legal “grey zone” situations by conducting hostile operations below the traditional threshold of physical violence amounting to an armed attack.31 They are likely to test NATO’s legal readiness and political resolve in the space domain, for example, by using blind spots to undertake nefarious activities such as co-orbital jamming or RPOs. Strategic ambiguity on the geographical scope of application of Article 5 is likely to invite, rather than deter, such hostile probing.

#### Specifically, the recent ban on ASAT testing signals US weakness in space deterrence, incentivizing adversaries to proliferate space capabilities.

Kevin Chilton 4-29. Retired, U.S. Air Force Gen, explorer chair for space warfighting studies at the Mitchell Institute for Aerospace Studies. He previously led U.S. Strategic Command and Air Force Space Command, and he served as a NASA astronaut. “The anti-satellite test ban must not undermine deterrence.” Defense News. 4-29-2022. https://www.defensenews.com/opinion/commentary/2022/04/29/the-anti-satellite-test-ban-must-not-undermine-deterrence/ //EM

While the U.S. would like to prevent conflict from escalating to space, many of our adversaries do not share this goal. Instead, they see developing and fielding capabilities to hold our systems on orbit at risk as an opportunity to gain decisive advantages. Our space enterprise is the super glue that empowers a broad range of military functions. It is exceedingly difficult to project modern American combat power without a range of crucial, space-based systems. This includes our communication, weather, intelligence, navigation and missile-warning satellites. It may even be impossible for us to project effective combat power if we lose our space-based capabilities, and our adversaries retain theirs. Our adversaries know this, and it is exactly why they have pressed so hard to hold our satellites at risk by demonstrating and fielding known terrestrial and, likely, space-based anti-satellite weapons.

Given this reality, it is important to present our leaders with a broad range of options that will deter adversaries from attacking U.S. space-based assets. We must convince our adversaries they cannot destroy our critical satellites, while retaining theirs. Several of our opponents are equally dependent on their constellations. A nightmare scenario for the U.S. would see us send our terrestrial forces into combat without the support of our space capabilities, while our enemy retains all of theirs. A far better outcome would see us deter hostile actions in space altogether through holding their assets similarly at risk, thereby empowering deterrence. Should an opponent miscalculate, and deterrence fails, it is crucial our leaders have options, including direct-ascent, anti-satellite missiles, to level the playing field.

This is why the administration’s admirable announcement to unilaterally ban the testing of direct-ascent, anti-satellite missiles must not constrain the development and fielding of U.S. offensive space capabilities. This approach mirrors the policies and posture of our nuclear deterrent forces: Our voluntary compliance with the nuclear test ban treaty does not impede our fielding of a credible triad to deter adversarial strategic attacks on the U.S. or our allies. We understand these realities here on Earth, and we must ensure we apply the same calculus to space. It is why the nuclear triad was so important to check the Soviet Union in the Cold War, and why it remains essential today. We did not invest in nuclear weapons because we wanted to launch them. Quite the contrary: It was so we would never have to employ them or be subject to them.

“Using” our strategic deterrent force means developing the enterprise, fielding the various components and ensuring our adversaries understand the credibility of our commitment. The same will hold true for keeping the peace in space. However, for a set of capabilities to be persuasive, we must ensure our commitment to use is credible. This means we must speak with care and ensure our actions reflect our resolve.

#### Adversarial intent is certain; it’s only a question of NATO resolve.

Courtney Albon 4-14. C4ISRNET's space and emerging technology reporter. She previously covered the U.S. Air Force and U.S. Space Force for Inside Defense. “Defense Intelligence Agency cites 70% growth in Russia and China’s combined space assets since 2019.” C4ISRNet. 4-14-2022. https://www.c4isrnet.com/battlefield-tech/space/2022/04/13/defense-intelligence-agency-cites-70-growth-in-russia-and-chinas-combined-space-assets-since-2019/ //EM

WASHINGTON — A new report from the Defense Intelligence Agency links China and Russia’s increased operational space capabilities in recent years to their growing intent to extend future conflict into space.

The unclassified “Challenges to Security in Space” report follows a 2019 DIA report that surveyed space and counterspace programs being pursued by adversary nations, including Russia, China, North Korea and Iran. The 2022 report highlights growth in Russian and Chinese on-orbit systems as well as efforts to better organize their military space capabilities

“Evidence of both nations’ intent to undercut the United States and allied leadership in the space domain can be seen in the growth of combined on-orbit assets of China and Russia, which grew approximately 70% in just two years,” DIA Intelligence Officer for Space and Counterspace John Huth said during a Tuesday press briefing.

That expansion of capability follows a 200% combined increase between 2015 and 2018 and reflects a recognition by the two countries of the United States’ reliance on space assets and its role as a leader in the domain.

“As the number of spacefaring nations grow and counterspace capabilities become more integrated into military operations, the U.S. space posture will be increasingly challenged and on-orbit assets will face new risks,” Huth said. “A secure, stable and accessible space domain is crucial as challenges to the United States and our allies’ space capabilities continue to increase.”

#### Non-kinetic attacks are most preferable for secrecy and entry---threatening ISR and opening a broader vulnerability for on-orbit systems.

---AT: Alt Causes---AT: Kinetic Attacks

Jon Harper 4-8. Managing Editor of DefenseScoop, a sector of FedScoop. He covers the Pentagon and military technology. “Space Force trying to protect its 'soft underbelly’.” FedScoop. 4-8-2022. https://www.fedscoop.com/space-force-trying-to-protect-its-soft-underbelly/ //EM [ISR = intelligence, surveillance and reconnaissance]

The U.S. military faces a variety of threats to its satellite systems, but the Space Force’s “soft underbelly” is cyber, a top official said Monday.

Cyberattacks could threaten on-orbit capabilities and the ground systems that support them, which are critical for intelligence, surveillance and reconnaissance (ISR), communications, and positioning, navigation and timing. Making U.S. systems secure is a top priority, noted Lt Gen. Stephen Whiting, head of Space Operations Command (SpOC).

“These global networks that we have in Space Force and SpOC are truly not only global — meaning they wrap around the globe — but then they extend out to 22,000 miles above the Earth’s surface into geosynchronous orbit. And that creates a lot of novel cyberattack surface … where bad actors might try to attack us in the cyber domain. So, we have to secure that because that’s our soft underbelly,” Whiting said during a Mitchell Institute event.

“That’s our first priority is to prepare those combat-ready, ISR-led, cybersecure space and combat support forces,” he added.

Advanced adversaries like Russia and China have tested anti-satellite (ASAT) missiles that could destroy U.S. spacecraft in orbit, “but they would prefer to take us on in cyber because it’s just a lower bar” to clear operationally, Whiting said.

Cyberattacks would also be a preferred method for less advanced adversaries such as North Korea because their other counter-space capabilities are lagging, he said.

The Defense Intelligence Agency (DIA) released a report last month on challenges to security in space. The study included cyber among a list of other threats to U.S. space systems such as ASAT missiles, directed energy weapons, electronic warfare and orbital systems.

“With sophisticated knowledge of satellite C2 [command and control] and data distribution networks, actors can use offensive cyberspace capabilities to enable a range of reversible to nonreversible effects against space systems, associated ground infrastructure, users, and the links connecting them,” the report said.

China’s People’s Liberation Army emphasizes offensive cyberspace capabilities as a major component of integrated warfare, the DIA noted.

The PLA could launch cyberattacks against other nations’ space-based assets and other command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks and commercial systems to establish “information dominance” in the early stages of a conflict, the report said.

China also uses cyberespionage to steal other countries’ space and counterspace technologies for its own benefit, according to DIA.

Meanwhile, Russian counterspace doctrine involves using cyber capabilities to target an adversary’s satellites and supporting infrastructure.

“Russia considers the information sphere, especially space-enabled information collection and transmission, to be strategically decisive and has taken steps to modernize its military’s information attack and defense organizations and capabilities,” the DIA report said.

It added: “Since at least 2010, the Russian military has placed a priority on the development of forces and capabilities, including cyberspace operations, for what it terms ‘information confrontation’ — a holistic concept for ensuring information superiority. The weaponization of information is a critical aspect of this strategy and is employed in times of peace, crisis, and war.”

Chinese ASAT attacks create an open window for invasion of Taiwan---extinction.

Brian G. Chow & Brandon Kelley 21. Independent policy analyst with over 160 publications; Director of Debate at Georgetown University <3 and a graduate student in the Security Studies Program. “China’s Anti-Satellite Weapons Could Conquer Taiwan—Or Start a War.” National Interest. 8-21-2021. https://nationalinterest.org/feature/china%E2%80%99s-anti-satellite-weapons-could-conquer-taiwan%E2%80%94or-start-war-192135 //EM thx Marsh <3

On July 1, 2021—the one-hundredth birthday of the Chinese Communist Party—President Xi Jinping declared that China will “advance peaceful national reunification” with Taiwan. It would be easy to dismiss such statements as mere political rhetoric: certainly, Taiwan would never willingly accede to Chinese demands to rejoin the fold. But China’s rapidly advancing anti-satellite (ASAT) capabilities could open up another avenue: deterring United States intervention on Taiwan’s behalf in order to coerce reunification without firing a shot.

If current trends hold, then China’s Strategic Support Force will be capable by the late 2020s of holding key U.S. space assets at risk. Chinese military doctrine, statements by senior officials, and past behavior all suggest that China may well believe threatening such assets to be an effective means of deterring U.S. intervention. If so, then the United States would face a type of “Sophie’s Choice”: decline to intervene, potentially leading allies to follow suit and Taiwan to succumb without a fight, thereby enabling Xi to achieve his goal of “peacefully” snuffing out Taiwanese independence; or start a war that would at best be long and bloody and might well even cross the nuclear threshold.

This emerging crisis has been three decades in the making. In 1991, China watched from afar as the United States used space-enabled capabilities to obliterate the Iraqi military from a distance in the first Gulf War. The People’s Liberation Army quickly set to work developing capabilities targeted at a perceived Achilles’ heel of this new American way of war: reliance on vulnerable space systems.

This project came to fruition with a direct ascent ASAT weapons test in 2007, but the test was limited in two key respects. First, it only reached low Earth orbit. Second, it generated thousands of pieces of long-lasting space junk, provoking immense international ire. This backlash appears to have taken China by surprise, driving it to seek new, more usable ASAT types with minimal debris production. Now, one such ASAT is nearing operational status: spacecraft capable of rendezvous and proximity operations (RPOs).

Such spacecraft are inevitable and cannot realistically be limited. The United States, European Union, China, and others are developing them to provide a range of satellite services essential to the new space economy, such as in situ repairs and refueling of satellites and active removal of space debris. But RPO capabilities are dual-use: if a satellite can grapple space objects for servicing, then it might well be capable of grappling an adversary’s satellite to move it out of its servicing orbit. Perhaps it could degrade or ~~disable~~ it by bending or disconnecting its solar panels and antennas all while producing minimal debris.

This is a serious threat, primarily because no international rules presently exist to limit close approaches in space. Left unaddressed, this lacuna in international law and space policy could enable a prospective attacker to pre-position, during peacetime, as many spacecraft as they wish as close as they wish to as many high-value targets as they wish. The result would be an ever-present possibility of sudden, bolt-from-the-blue attacks on vital space assets—and worse, on many of them at once.

China has conducted at least half a dozen tests of RPO capabilities in space since 2008, two of which went on for years. Influential space experts have noted that these tests have plausible peaceful purposes and are in many cases similar to those conducted by the United States. This, however, does not make it any less important to establish effective legal, policy, and technical counters to their offensive use. Even if it were certain that these capabilities are intended purely for peaceful applications—and it is not at all clear that that is the case—China (or any other country) could at any time decide to repurpose these capabilities for ASAT use.

There is still time to get out ahead of this threat, but likely not for much longer. China’s RPO capabilities have, thus far, lagged about five years behind those of the United States. There are reasons to believe this gap may close, but even assuming that it holds, we should expect to see China demonstrate an operational dual-use rendezvous spacecraft by around 2025. (The first instance of a U.S. commercial satellite docking with another satellite to change its orbit occurred in February 2020.)

At the same time, China is expanding its capacity for rapid spacecraft manufacturing. The Global Times reported in January that China’s first intelligent mass production line is set to produce 240 small satellites per year. In April, Andrew Jones at SpaceNews reported that China is developing plans to quickly produce and loft a thirteen thousand-satellite national internet megaconstellation. It is not unreasonable to assume that China could manufacture two hundred small rendezvous ASAT spacecraft by 2029, possibly more.

If this happens, and Beijing was to decide in 2029 to launch these two hundred small RPO spacecraft and position them in close proximity to strategically vital assets, then China would be able to simultaneously threaten disablement of the entire constellations of U.S. satellites for missile early warning (about a dozen satellites with spares included); communications in a nuclear-disrupted environment (about a dozen); and positioning, navigation, and timing (about three dozen); along with several dozen key communications, imagery, and meteorology satellites. Losing these assets would severely degrade U.S. deterrence and warfighting capabilities, yet once close pre-positioning has occurred such losses become almost impossible to prevent. For this reason, such pre-positioning could conceivably deter the United States from coming to Taiwan’s aid due to the prospect that intervention would spur China to disable these critical space systems. Without their support, the war would be much bloodier and costlier—a daunting proposition for any president.

Should the United States fail to intervene, the consequences would be disastrous for both Washington and its allies in East Asia, and potentially the credibility of U.S. defense commitments around the globe. Worse yet, however, might be what could happen if China believes that such a threat will succeed but proves to be wrong. History is rife with examples of major wars arising from miscalculations such as this, and there are many pathways by which such a situation could easily escalate out of control to a full-scale conventional conflict or even to nuclear use.

This Catch-22 of so-called “peaceful reunification” on the one hand and catastrophic miscalculation on the other is entirely preventable. To do so, however, the United States must act now. To deter such pre-positioning and provide a clear framework for how to handle it if it does occur, the United States should immediately begin coordinating with its allies to establish shared understandings for the rules and operations of warning/self-defense zones in orbit. Additionally, the United States should develop and deploy bodyguard spacecraft to monitor and enforce such rules.

The United States cannot afford to wait; once the potential threat arrives, it will already be too late.

#### Non-kinetic attacks escalate quickly---accidents and ambiguity spur tit-for-tat confrontations that go nuclear.

Sitki Egeli 21. Teaches at Turkey’s Izmir University of Economics. He holds a doctorate in international relations from Bilkent University and a master’s degree in the same field from the University of Chicago. He was the foreign relations director of Turkey’s Undersecretariat for Defense Industries from 1991 to 1999, and afterwards served as vice president of Overseas Development Corporation, a multinational consulting firm specializing in the defense and aerospace industries. “Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability,” Journal for Peace and Nuclear Disarmament, Volume 4, 2021, pp. 116-140, <https://doi.org/10.1080/25751654.2021.1942681> //EM

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 discomforting 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.

#### Conventional entanglement ensures nuclear use.

Robert Farley 1-9. Senior Lecturer at the Patterson School at the University of Kentucky. Dr. “Does a Space War Mean a Nuclear War?.” 19FortyFive. 1-9-2022. https://www.19fortyfive.com/2022/01/does-a-space-war-mean-a-nuclear-war/ //EM

The recent Russian anti-satellite test didn’t tell the world anything new, but it did reaffirm the peril posed by warfare in space. Debris from explosions could make some earth orbits remarkably risky to use for both civilian and military purposes. But the test also highlighted a less visible danger; attacks on nuclear command and control satellites could rapidly produce an extremely dangerous escalatory situation in a war between nuclear powers. James Acton and Thomas Macdonald drew attention to this problem in a recent article at Inside Defense. As Acton and MacDonald point out, nuclear command and control satellites are the connective tissue of nuclear deterrence, assuring countries that they’re not being attacked and that they’ll be able to respond quickly if they are.

For a long time, these strategic early-warning satellites were akin to a center of gravity in ICBM warfare. Nuclear deterrence requires awareness that an attack is underway. Attacks on the monitoring system could easily be read as an attempt to blind an opponent in preparation for general war, and could themselves incur nuclear retaliation. Thus, the nuclear command and control satellites are critical to the maintenance of nuclear deterrence. They make it possible to distribute an order from the chief of government to the nuclear delivery systems themselves. Consequently, their destruction might lead to hesitation or delay in performing a nuclear launch order.

It was only later that the relevance of satellites for conventional warfare became clear. Satellites could reconnoiter enemy positions and, more importantly, provide communications for friendly forces. Indeed, the expansion of the role of satellites in conventional warfare has complicated the prospect of space warfare. States have a clear reason for targeting enemy satellites which support conventional warfare, as those satellites enable the most lethal part of the kill chain, the communications and recon networks that link targets with shooters. Thus, we now have a situation in which space military assets have both nuclear and conventional roles. In a conflict confusion and misperception could rapidly become lethal. If one combatant views an attack against nuclear command and control as a prelude to a general nuclear attack, it might choose to pre-empt.

#### Independently, miscalc from ISR failure escalates to full-scale nuclear war---nothing checks

Dr. Bruce G. Blair 20, Research Scholar in the Program on Science and Global Security at Princeton University, PhD in Operations Research from Yale University, “Loose Cannons: The President and US Nuclear Posture”, Bulletin of the Atomic Scientists, Volume 76, Issue 1 [language modified; abbreviation in brackets]

The fog of nuclear conflict will prove all the thicker because leaders and planners lack adequate knowledge about their adversaries’ mind-set, resolve, wartime aims, and game plans. For instance, de-classified Soviet documents show clearly that the US strategy of “escalation dominance” was completely out of sync with Soviet nuclear strategy and that escalation to full-scale nuclear war was virtually inevitable if the United States struck first.13 After many decades of scholarly research, it is still not known what leaders in Moscow and Beijing were thinking during Cold War crises involving US attempts to threaten nuclear violence to coerce them.14 Today it would be foolhardy in the extreme to presume we would know Putin’s, Xi’s, and Kim’s minds and behavior in wartime. A prudent leader would not only refrain from initiating the actual use of nuclear weapons because of the danger of escalation; that leader would also refrain from brandishing them at all during a confrontation. The fear of an adversary striking first is the leading textbook cause of crisis instability. To stabilize a military crisis situation, what is actually needed is predictability and reassurance that first use is not on the table. For many strategists, however, taking options off the table looks like weakness. Retired Gen. James Mattis (the recent defense secretary) has a favorite military maxim: “Never tell the enemy what you are not going to do.” Strategists weaned on Thomas Schelling’s classic game theory arguments believe threatening, manipulating risk, and blackmailing are the currency of savvy crisis diplomacy. And it is certainly true that past US presidents have regularly played nuclear brinks~~man~~ship with the Soviets and Chinese and displayed incautious risk-taking in their crisis maneuvering. This was in fact the playbook of the Nixon advisors who ordered the world-wide nuclear alert that my crewmate and I helped implement in 1973. This alert sent a provocative message to the Soviets: The United States was prepared to play nuclear roulette to gets its way.15 Nuclear roulette begins at the outset of a crisis as the belligerents intensify their [ISR] intelligence, surveillance, and reconnaissance operations. The aim is to maintain “situation awareness,” but the activities lend themselves to the worst-case interpretation that the adversary is updating its targeting in preparing to strike. Similarly, nuclear forces and command structures are programmed to go to higher readiness to prepare for war if the adversary will not back down. Although the motives may be defensive, these activities may appear to be precursors of a first strike and provoke an action-reaction spiral that spins out of control. Certainly, if even a single nuclear weapon were used, the strategic nuclear forces on both sides would move rapidly to a maximum war footing and project credible mutual threats of large-scale preemptive attack. In sum, a nuclear posture gearing up for a possible enemy first strike risks becoming a self-fulfilling prophecy. From the perspective of presidential decision making, the first-use contingency could easily accelerate escalation to the point of causing mental duress. This contingency is also notable for its absence of guardrails and the ease with which a misguided or rattled president could order it. The launch protocol described earlier for launch on warning applies equally to first use. Although the timeline could be extended greatly, the president could choose at any time to end the discussion and order a strike. During the Cold War, I seldom practiced executing a first strike, and today there are no foreseeable scenarios that would justify transgressing the nuclear taboo of first use. Nevertheless, a first nuclear strike remains the default contingency of the US posture, owing to the huge uncertainties surrounding the alternatives – second-strike retaliation and launch on warning. A crisis that brings the belligerents to the brink of nuclear war would compel consideration of first use. Nuclear warfighters who reject the adage that a nuclear war cannot be won and must never be fought may well brief and tout the purported warfighting advantages of going first. Even though first use runs counter to and undermines the entire framework of the global nuclear order, in which nuclear weapons exist only to deter, leaders may waver if it seems the least fraught choice at the moment of truth. An impulsive president may be drawn to it. Wiser advisors may counsel restraint, but nothing would stand in the way of the president ordering a first strike. The likely if not inevitable consequence of attacking a nuclear adversary with nuclear weapons is nuclear retaliation and uncontrolled escalation that crosses the threshold of acceptable damage to this nation. First use runs an existential risk to the United States and the world. It carries a huge risk of triggering a nuclear exchange of cataclysmic proportions with massive casualties to all the belligerent parties and beyond.

#### A lack of a cooperative framework leaves NATO uncertain on how to respond, undermining deterrence while simultaneously increasing the likelihood of escalation.

Liselotte Odgaard 22. Professor at the Norwegian Institute for Defense Studies in Oslo and a non-resident senior fellow at the Hudson Institute focusing on US-China-Europe relations. “NATO’s China Role: Defending Cyber and Outer Space,” The Washington Quarterly Volume 45, 2022 - Issue 1, 45:1, pp. 167-177, T&F, <https://www.tandfonline.com/doi/full/10.1080/0163660X.2022.2059145>. //EM \*thx Marsh <3

NATO in Cyber and Outer Space

Cyber and space is a promising arena for NATO to address China challenges by building member state resilience. Like the air and sea domains, as areas that belong to no one state and which provide access to much of the globe, they form part of the global commons. Command of the commons has been the key enabler of the US global position of power for many decades.26 However, China wields a sufficient range of sea, air, cyber, and space capabilities such that the global commons is now a contested zone. In contrast to the sea and air domains, cyber and space are sparsely regulated. This lack of international norms enhances the risk of conflict based on misperception, making NATO cooperation pertinent. Adversarial activities toward the US and Europe in the cyber and space domain threaten transatlantic security. These come not just from China, but also from other adversaries such as Russia and Iran. Mechanisms for addressing these challenges in the military sector are essentially generic and not, at least in their basic design, established with a particular country in mind. Thus, cyber and space provide an avenue for NATO to contribute significantly to deterrence of China without having to combat major internal resistance. NATO would also benefit from long-standing US-EU cooperation on cyber and space issues.27

Cyber and space provide an avenue for NATO to contribute without major internal resistance

NATO has vowed to clarify Article Five’s collective defense commitment to encompass threats to satellites in space and coordinated cyberattacks. NATO can design this effort to include adversarial behavior from China. The alliance already has an array of instruments to deal with cyber and space challenges from adversaries. These can be extended to encompass China without pronouncing it a threat.28 This approach allows the US and Europe time to adjust their cooperation to take into account the fact that China poses military threats to them both without explicitly using the language of threat at a time when NATO members do not agree if China should be defined as a challenge that can trigger Article Five responses.

Since the late 1990s, the vulnerability of shared space assets to cyberattacks has been a concern for both the US and Europe. For example, in 1998 a US-German satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun, damaging its High Resolution Imager by exposure. NASA later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. Coordinated cyberattacks have emerged as a major threat to both the US and Europe since the late 1990s. For example, for about eighteen minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic, including government and military traffic, to about 15 percent of the internet’s destinations through servers located in China.29

In the future, the need to enhance situational awareness in space is likely to lead to further integration of space assets between the US and its allies. Civilian entry points are likely to provide a growing opportunity for infiltration. The weak state of cybersecurity in civilian agencies should also be considered. Chinese military doctrine prioritizes weaponry that targets vulnerabilities in the deployment of US and allied power, such as the use of cyberattacks to disrupt surveillance assets, intelligence networks, and command-and-control systems.30 These threats are significant, since next generation systems, including fighter aircraft, destroyers, and special forces, will not function without access to space communication and space-derived data.

Although European and US allies have indigenous space programs outside the NATO framework, cyber security and outer space would be a useful field for joint explorations of how to divert and manage attacks and identify an agency which can coordinate transatlantic responses to attacks. Allies are embedded in a range of information networks which may be disrupted, giving rise to alliance management concerns emerging from attacks. The lack of red lines regarding behavior in cyber and outer space between the US and its allies on one hand, and adversaries such as China on the other, adds to the risk of misperception and escalation, and hence also highlights the need for allied coordination to avoid starting a war by mistake. An improved NATO dialogue on safeguards and alliance consultation could also assist communication with China on arms control and conflict prevention in cyber and outer space, which is not currently taking place.

Looking to the future, NATO’s success in establishing transatlantic mechanisms for cyber and outer space safeguards and consultation will be crucial to allow NATO a key role in taking on the China challenge in ways that help restore faith in NATO’s credibility as a provider of collective defense in all domains. It will also assist NATO in straddling the chasm between member states prioritizing threats from either China, Russia, the Middle East, or North Africa, since cyber and space threats potentially stem from all of them, and the effectiveness of cyber and space defense mechanisms do not necessarily depend on geographical origin.

Cyber and space would allow NATO a key role in the China challenge without prioritizing China.

#### NATO miscalculation goes nuclear.

Brian Radzinsky 21. Postdoctoral research fellow at the Center for Global Search Research (CGSR) at Lawrence Livermore National Laboratory. His work at CGSR focuses on developing new concepts and methods to measure the military balance, applying a net assessment approach. His broader research interests are in nuclear deterrence, advanced and emerging technologies and regional security dynamics, and how these interact to affect strategic deterrence, allied assurance, and escalation. “Miscalculation, Misperception and Risk Reduction.” Under U.S. Department of Energy by Lawrence Livermore National Laboratory. September 2021. https://www.osti.gov/servlets/purl/1820013 //EM

Miscalculation resulting in deterrence failure

Miscalculation in crisis can resulting a failure to deter the outbreak of war via the same pathways as above. First, in a crisis, either side could continue to miscalculate the scope of the other’s interests. Although the immediate interests at stake in a crisis would become clear, Blue might underestimate Red’s willingness to exploit the crisis to secure a related interest; Red might seize on the crisis to engage in horizontal escalation. For instance, Russia annexed Crimea weeks into the Euromaidan crisis. Second, a crisis could escalate to war through Blue or Red’s failure to assess the other’s resolve. Although Blue and Red will have strong incentives to signal their resolve in a crisis over vital interests, in a more complex crisis, miscalculations of resolve may accompany miscalculation of interests. In the Crimean crisis, NATO did not see a need to signal resolve because it miscalculated Russia’s interests. If a crisis arises from a mishap, Blue may be hesitant to engage in overt shows of resolve to avoid provoking rather than deterring Red. A crisis atmosphere may also make signaling harder due to a complex and contested information environment, further limiting each side’s “strategic vocabulary.” Third, a crisis may exacerbate the risk of miscalculating the military balance. All sides will have incentives to be less transparent and predictable. To preserve warfighting advantages, Blue may be hesitant to reveal decisive capabilities, especially those that depend on secrecy. Blue may also hesitate to court escalatory risk through signaling capabilities while Red may conceal forces used for hybrid warfare.

Miscalculation resulting in inadvertent escalation

In a crisis, inadvertent escalation can result from miscalculation of the intent behind mishaps, responses to mishaps, or shifts in the military balance. Although status quo-oriented powers may seek to avoid war and thus may be generous with their interpretations of complex and uncertain events, a sufficiently tense atmosphere could exacerbate paranoia, risk-aversion, and mistrust, fueling escalation. The impact of military behaviors during a crisis on escalation risk are not clear. Blue might respond to a mishap in a way that increases the resilience of their forces, which could allow Blue to avoid further escalation while it assesses the cause of the mishap. Red or Blue might also be aware of the potential for inadvertent escalation and actively seek to manage this risk. Greater senior decision maker attention to military matters during a crisis could contribute to risk management. At the nuclear level, escalation would almost certainly involve deliberate decision making by both sides, reducing the risk. Conversely, crises increase incentives for opacity, limiting the ability to distinguish between true mishaps and guises for aggression. Changes in force readiness could also be escalatory in some contexts, while conventional forces could interactin ways that escalate the conflict even if national leaders do not decide to escalate. Measures to enhance resilience and signal resolve may also cast a nuclear shadow on a crisis and provoke unanticipated escalation. If Blue or Red do not anticipate inadvertence, they might overestimate their ability to control escalation.

Miscalculation in war

Miscalculation resulting in a failure to deter vertical or horizontal escalation. Although each side’s core interests might be well understood when the fighting begins, the war itself may lead Red or Blue’s interests to evolve in ways that increase the risk of miscalculation. Red might view the war as an opportunity to pursue other interests, but Blue might miscalculate Red’s ambitions and fail to deter horizontal escalation. Red might also miscalculate Blue’s interests in the conduct of the war, such as Blue’s reputational interest in punishing violations of the nuclear taboo. Miscalculating Blue’s interests, Red could then see an opportunity to gain advantage through limited nuclear escalation. In a war, both sides will also have strong incentives to signal resolve. Yet the fog of war, as well as a breakdown of diplomatic relations and a shift to a wartime domestic information environment, could make it difficult to send and receive such signals. The conduct of the war itself could also complicate strategic messaging. Forces that might be used to send signals could be committed to other operations or destroyed in the fighting, constraining each side’s strategic “vocabulary.”

Each side’s actions in war may reveal information about the military balance, which could reduce the potential for miscalculation of capabilities. Yet inherent uncertainties about the outcomes of certain military contests may contribute to miscalculation. Some forms of miscalculation may be advantageous. For instance, the US has an interest in encouraging Red to be extremely pessimistic about the outcome of any nuclear exchange. By the same token, however, Red may be prone to overestimate its ability to fight a nuclear war. The uncertainty of how a nuclear war would unfold could make it difficult to dispel Red’s overconfidence without engaging in actions that themselves risk further escalation.

#### US-Russia war causes extinction

Fisher ’15 [Max; June 29; Foreign affairs columnist at Vox; Vox, “How World War III became possible,” http://www.vox.com/2015/6/29/8845913/russia-war[

That is why, analysts will tell you, today's tensions bear far more similarity to the period before World War I: an unstable power balance, belligerence over peripheral conflicts, entangling military commitments, disputes over the future of the European order, and dangerous uncertainty about what actions will and will not force the other party into conflict. Today's Russia, once more the strongest nation in Europe and yet weaker than its collective enemies, calls to mind the turn-of-the-century German Empire, which Henry Kissinger described as "too big for Europe, but too small for the world." Now, as then, a rising power, propelled by nationalism, is seeking to revise the European order. Now, as then, it believes that through superior cunning, and perhaps even by proving its might, it can force a larger role for itself. Now, as then, the drift toward war is gradual and easy to miss — which is exactly what makes it so dangerous. But there is one way in which today's dangers are less like those before World War I, and more similar to those of the Cold War: the apocalyptic logic of nuclear weapons. Mutual suspicion, fear of an existential threat, armies parked across borders from one another, and hair-trigger nuclear weapons all make any small skirmish a potential armageddon. In some ways, that logic has grown even more dangerous. Russia, hoping to compensate for its conventional military forces' relative weakness, has dramatically relaxed its rules for using nuclear weapons. Whereas Soviet leaders saw their nuclear weapons as pure deterrents, something that existed precisely so they would never be used, Putin's view appears to be radically different. Russia's official nuclear doctrine calls on the country to launch a battlefield nuclear strike in case of a conventional war that could pose an existential threat. These are more than just words: Moscow has repeatedly signaled its willingness and preparations to use nuclear weapons even in a more limited war. This is a terrifyingly low bar for nuclear weapons use, particularly given that any war would likely occur along Russia's borders and thus not far from Moscow. And it suggests Putin has adopted an idea that Cold War leaders considered unthinkable: that a "limited" nuclear war, of small warheads dropped on the battlefield, could be not only survivable but winnable. "It’s not just a difference in rhetoric. It’s a whole different world," Bruce G. Blair, a nuclear weapons scholar at Princeton, told the Wall Street Journal. He called Putin's decisions more dangerous than those of any Soviet leader since 1962. "There’s a low nuclear threshold now that didn’t exist during the Cold War." Nuclear theory is complex and disputable; maybe Putin is right. But many theorists would say he is wrong, that the logic of nuclear warfare means a "limited" nuclear strike is in fact likely to trigger a larger nuclear war — a doomsday scenario in which major American, Russian, and European cities would be targets for attacks many times more powerful than the bombs that leveled Hiroshima and Nagasaki. Even if a nuclear war did somehow remain limited and contained, recent studies suggest that environmental and atmospheric damage would cause a "decade of winter" and mass crop die-outs that could kill up to 1 billion people in a global famine.

The AFF solves:

#### 1. HARDENING---military proofing is key---cyber-attacks on NATO assets create cascading effects and destroys deterrence absent military hardening.

Beyza Unal 19. Senior research fellow with the International Security Department at Chatham House. “Cybersecurity of NATO's Space-based Strategic Assets.” Chatham House. The Royal Institute of International Affairs. pp. 7-11. 07-10-2019. <https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets-0/about-author> //EM

In the military domain, some of the major system vulnerabilities include the use of commercial companies for military purposes; ‘back-doors’ in encryption; and the supply-chain security of satellites.27 This list can also be extended to include physical, personnel and procedural vulnerabilities. Risks also arise from the dual-use aspect of most of the space-related technology – where the technology can be used for both civilian and military purposes. For instance – whether fixed or mobile units – communications satellites and broadcasting satellite services have both civilian and military utility. Similarly, the utilization of satellite imagery capability in the civilian sphere for earth observations, environmental monitoring, and the provision of oceanographic and cartographic data, also extends to the military domain.28 There is an increasing need to apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications.

These capabilities aside, terminals located in ground stations constitute a critical vulnerability, as a terminal is an access point to a satellite and is usually not protected by authentication in order not to hinder operational actions. Terminals house software systems that can be compromised and require patching and upgrading. Moreover, software embedded in weapons systems (such as precision-guided munitions) could also be compromised.

At times, NATO allies procure equipment and software to be integrated into their national defence architecture, which becomes part of the overall NATO capability. The commercial supply chain is embedded in nearly every aspect of military equipment. This may not necessarily be a particular vulnerability, as long as commercial equipment is designed to military standards and is secure. However, if military standards are not met, items procured from commercial industry with design flaws may expose NATO’s systems to additional vulnerabilities.

While the absence of data is easy to detect, the manipulation of data or erosion of confidentiality at such an interface is potentially more difficult to discern.

Civil satellites, operated by private companies, may be used to fulfil specific missions in locations where NATO allies do not have their own space equipment. Ground stations constitute further elements that are relevant for the data flow. From a cybersecurity point of view, each interface could present a vulnerability and could become a weakness, as an interface typically requires manual processes to establish its operation, and/or the administration of the components involved. Adversaries infiltrating ground- or space-based systems could exploit weak software implementation, or the incompatibility of network or data transfer protocols in the chain. While the absence of data is easy to detect, the manipulation of data or erosion of confidentiality at such an interface is potentially more difficult to discern. Vulnerabilities can stem from:

* A higher number of data exchange interfaces used between the military and civil sectors;
* The fact that each actor has its own isolated view of its data network, protected by its own security standard;
* The use of old and proprietary IT hardware and software; and
* The failure or inability to conduct regular software updates to remove known vulnerabilities.
* In such an environment, it seems difficult to ensure security of the information delivered.
* Space-specific risks for the NATO alliance and for key NATO countries

Space systems, which include both satellites and ground stations, as well as related space products and services, provide mission-critical information both for NATO’s member states and for the alliance as a whole. NATO relies on space-based assets for almost all of its operations and missions.29 Some of the critical missions that rely on space assets include: defence of NATO’s territory and the neighbouring regions; peacekeeping missions; humanitarian assistance and disaster relief; counterterrorism; and conflict prevention activities.

NATO does not own satellites. It owns and operates a few terrestrial elements, such as satellite communications (SATCOM) anchor stations and terminals. It requests access to products and services but does not have direct access to satellites, leaving it up to its allies to determine whether they provide access to their satellite capabilities. NATO has established memoranda of understanding with allies for possible use of space products and services.

Originally, in the US, space systems used by the military were separated from commercial and civilian assets in terms of their development and operation.30 One of the reasons for this separation was to protect the military structure against physical and cyberthreats. Military space system safety and security requirements were also higher and more stringent than in the commercial sphere (for example, requirements to invest in survivability enhancement mechanisms in order to resist jamming, or special design approaches for military space architecture). In recent years commercial methods, for instance the capture and analysis of satellite imagery, have been shown to be as effective as military means. As a result, NATO uses a mix of military, civilian, commercial, and national/multinational assets to conduct its operations. The joint use of these assets, however, comes with an acceptance of inherent risk, not only to the countries that provide such capability but also to the alliance as a whole. In response, the European Defence Agency, through its Governmental Satellite Communications (GOVSATCOM) development programme, decided to build an intermediary class of satellites between commercial SATCOM and military SATCOM, with security requirements able to address the needs of critical missions, including crisis management.31

There is increased dependence on space-based systems in modern military engagement. During the US engagement in Iraq in 2003, 68 per cent of munitions were guided utilizing space-based means (including laser-, infrared- and satellite-guided munitions); this percentage had risen sharply from 10 per cent in 1990–91, during the first Gulf war.32 In its operations in Afghanistan in 2001, 60 per cent of the weapons used by the US were precision-guided munitions: these included bombs, missiles, and other weapons, many of which had the capability to correct their own positioning to hit the target, using space-derived information.33

Cyber vulnerabilities undermine confidence in strategic systems; they increase uncertainty in information and analysis, which impacts the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for attribution and strategic calculus in crisis decision-making and may increase the risk of misperception.

This dependency on space-based technology has major implications for the way NATO conducts warfare today, and how it will do so in the future. For instance, in order to conduct precision strikes or earth observation through the use of unmanned aerial vehicles (UAVs – such as military drones), systems rely on so-called ‘beyond-line-of-sight’ (BLOS) communication via satellites – especially in times of crisis and conflict, since ground-based line-of-sight communications are vulnerable to physical attacks. Yet, cyberattacks on space technology or on the UAVs may lead them to misinterpret commands, or to lose contact with the command centre and fail in operation. \*\*\*TABLE 1 OMITTED\*\*\* Identification is another important capability that is used in the NATO maritime domain for coastal tracking, and for identifying and locating ships and vessels. Using automatic identification systems (AIS), data is electronically transmitted between ships and the coastal stations. By providing similar functions, AIS supplements and provides resilience to maritime radar and is fundamental for avoiding collisions.36

NATO’s space-dependent capabilities have individual functions, as described above. These capabilities are also coupled to each other, with complex cross-dependencies, so that the loss of one capability may have a collateral impact on other capabilities. For instance, most of the assets that transmit communications to support command and control are also dependent on GPS for timing and synchronization.37 Although there would be a number of contenders for technologies of utmost importance to NATO missions and operations, preliminary research indicates that PNT signals (which utilize GPS) are a much-needed priority capability in almost all NATO operations.

2. COORDINATION---lack of common understanding cracks NATO cohesion---causing reluctance on sharing space capabilities.

Theresa Hitchens 22. Space and Air Force reporter at Breaking Defense. The former Defense News editor was a senior research associate at the University of Maryland’s Center for International and Security Studies at Maryland (CISSM). “New NATO space policy focuses on space support, domain awareness.” Breaking Defense. 1-18-2022. https://breakingdefense.com/2022/01/new-nato-space-policy-focuses-on-space-support-domain-awareness/ //EM

The allies consistently have kept space capabilities firmly on sovereign ground, and traditionally often have been reluctant to share information. The fact that it has taken this long to roll out of the public version of the policy — a first framework document was signed in June 2019 — is a testament to the culture of secrecy that has been even more pervasive in Europe than in the US (and that is saying something).

One reason for allied reluctance to engage on military space issues in public is that, with the exception of France and the United Kingdom, many European countries traditionally have been either deeply uncomfortable with, or downright opposed to, the concept of warfighting in space — especially offensive action. Indeed, in an August 2019 speech, NATO Secretary General Jens Stoltenberg found it necessary to declare that NATO’s declaration of space as an allied operational domain was “not about the militarization of space.”

The public policy released today makes no such caveat, but does signal that there remains some cracks between the allies on military uses of space.

For example, the policy explains that the North Atlantic Council — NATO’s decision-making body that at its highest level involves heads of state — will need to approve any options “across the conflict spectrum to deter and defend against threats to or attacks on Allies’ space systems.” It adds that in the meantime, allies “should develop a common understanding of concepts such as the role of space in crisis or conflict.”

#### NATO cohesion checks extinction.

Gallagher ’19 [Mike and Colin Dueck; January 2019; Representative for Wisconsin’s Eighth District in the U.S. House of Representatives; Professor in the Schar School of Policy and Government at George Mason University; National Review, “The Conservative Case for NATO,” <https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/>]

The conservative case for NATO is not that it strengthens liberal world order. Rather, the conservative case for NATO is that it bolsters American national interests. In an age of great-power competition, as identified by the Trump administration, America’s Western alliance provides the U.S. with some dramatic comparative advantages. The United States, Canada, and their European allies have a number of common interests and common challenges with regard to Beijing, Moscow, terrorism, cyberattacks, migration, nuclear weapons, and military readiness. NATO is the one formal alliance that allows for cooperation on these matters. It is also the only alliance that embodies America’s civilizational ties with Europe — a point forcefully made by President Trump when he visited Poland in 2017. Properly understood, NATO helps keeps America’s strategic competitors at bay, pushing back on Russian and Chinese influence. In all of these ways, the U.S. alliance system in Europe is a bit like oxygen. You may take it for granted, but you’ll miss it when it’s gone.

3. INTEGRATION---interoperability with NATO is key for the signal of deterrence against ASATs AND solves network capabilities to solidify space redundancy.

Sam Wilson & Colleen Stover 21. Senior policy analyst for the Center for Space Policy and Strategy at The Aerospace Corporation; Project manager and researcher at The Aerospace Corporation’s Center for Space Policy and Strategy. “Defense Space Partnerships: A Strategic Priority.” Aerospace Center for Space Policy and Strategy. 09-17-2020. https://csps.aerospace.org/papers/defense-space-partnerships-strategic-priority //EM

Unlike during the Cold War, when space was dominated by a few major powers, space has become increasingly democratized. As of 2019, over 60 countries have a national space budget, over 70 countries own or operate satellites in orbit, and nine countries—plus the European Space Agency—can independently launch into orbit.4 This growing international engagement in space presents enormous opportunities for defense space partnerships. This new era also presents serious risks. Space is becoming increasingly contested. In April 2020, Russia tested a direct ascent anti-satellite missile.5 A few months earlier, U.S. officials called out Russian satellites for trailing a U.S. national security satellite.6 Also in April 2020, Chris Ford, a senior official in the State Department, said that China was exploring capabilities to attack U.S. satellites, including in high orbits such as those of U.S. nuclear command, control, and communications satellites.7 The seriousness of the threat underlines the importance of defense space partnerships—the United States should not try to manage these threats purely on its own.

To enable more international defense space partnerships, U.S. leadership will need to treat such partnerships as a strategic priority, not as an afterthought or add on. This chapter looks at advantages, challenges, and mitigations for broadening and deepening security space partnerships that could prompt key decision points during the next presidential term.

Advantages of Partnerships

Defense space partnerships offer considerable advantages. These include allowing the United States to expand and improve its network and capabilities with fewer resources, deter adversaries from attacking its systems, and coalesce allied and partner thinking on space security concepts.8 A look at some common space maturity metrics suggests that many of the most mature space nations in the world are partners of the United States. Specifically:

The United States and its close partners make up 11 out of the top 15 countries with the biggest national space budgets.9

Of the roughly 2,700 active satellites in orbit, over 500 are operated by international partners and over 1,300 are operated by the United States.10

* Among the world’s 22 active space launch centers, six are operated by partners and five by the United States.11

Many allies are also taking steps to emphasize the seriousness of space security. In the past year, France and Japan have established their own military units dedicated to space.12 The United Kingdom officially recognized space as an operational domain in 2018.13 And NATO, which historically has said little on space, came out with a space policy in 2019.14 Given the space maturity of many of its allies and partners, and the shared recognition of the importance of the domain, the time is advantageous for the United States to place more priority on establishing and deepening space partnerships for defense. Expand and Improve Networks and Capabilities.

Partners have capabilities that can improve U.S. systems and networks in geographically dispersed and strategic locations. This is particularly true in space situational awareness, an area in which a diverse set of geographically-distributed sensors can more accurately and completely capture the operational environment.15 Partners can help us collectively attain more persistent surveillance and continuous global coverage of satellites and debris, which is only possible if we have more and better sensors in a variety of locations. Radars and optical telescopes spread around the world can also more comprehensively identify space threats. For example, Japan is developing a deep-space radar that will observe objects in geosynchronous orbit. Given the counterspace threats from potential adversaries, the radar could also be invaluable to the United States because of its capability and location.

Additionally, space capabilities and operations are expensive. A clear advantage of military space partnerships is that they generate opportunities for sharing the financial burden of operating in space. As an example, the United States putting its security payloads on the Norwegian satellite will reportedly generate up to $900 million in savings.17 Hosting U.S. payloads on foreign systems, like this example, represents an area in which the United States could leverage allied and partner capabilities more so than it does currently. Hosted payloads offer affordable means to expand protected communications satellites; position, navigation, and timing satellites; and space situational awareness capabilities, among other systems. Rather than host payloads, partners can also simply contribute to the cost of a satellite system. For example, through multilateral agreements, Canada, Denmark, Luxembourg, the Netherlands, and New Zealand provided funding for the U.S. Wideband Global SATCOM-9 satellite that launched in March 2017.18 Or the United States can use partners’ satellites. For example, the United States partners with Japan and Europe to obtain weather information from space-based sensors, providing accurate weather information to warfighters around the world and avoiding the need to field additional U.S. systems.19 And it is not just satellites and payloads. Partners have terrestrial infrastructure and user equipment, including for position, navigation, and timing and satellite communications, that can be used collectively to achieve needed capabilities more efficiently. Leveraging allied systems can offer technological insights, system improvements, and capability expansions at lower costs.

Deter Aggression.

Partnerships can create opportunities for integrating allied and partner capabilities, such as incorporating combined systems in satellite networks and ground infrastructure. Such integration can strengthen the cohesiveness of a defense partnership, which could also help deter an attack. A potential adversary may consider an attack on a purely U.S. system differently than an attack on a system that incorporates several allied and partner capabilities. Deployment of NATO’s multinational battlegroups in the eastern part of the Alliance (Estonia, Latvia, Lithuania, and Poland) is an example of this concept in the ground domain. If Russia’s military were to invade Estonia and attack the multinational forces there, the invasion could be seen as not just an attack on Estonia but on all of the countries represented in those forces and perhaps all of NATO.20 A May 2017 NATO fact sheet on its multinational forces reaffirms this: “[The multinational] presence makes clear that an attack on one Ally will be considered an attack on the whole Alliance.”21 Similarly, in the space domain, an attack on a U.S. constellation of satellites with U.S. payloads might prompt a response from the United States; an attack on a satellite constellation with a mix of U.S. and partner capabilities might prompt a response from several countries acting collectively, which may help deter a potential adversary from attacking in the first place.

With integrated allied and partner systems, U.S. satellite networks and ground infrastructure, as well as other equipment and capabilities, can become more resilient. The more systems you have, the larger an attack would need to be to take out a given percentage of capability: all else equal, two satellites would be more resilient than one, three satellites more resilient than two, and so on. The resilience offered by integrating allied and partner capabilities into a network, therefore, may also contribute to deterring a potential adversary from attacking the network.

### 1AC---DOMAIN AWARENESS ADVANTAGE

#### Contention 2 is DOMAIN AWARENESS.

The plan’s space coordination with NATO is essential towards overcoming existing classification standards hindering the development of domain awareness---that bolsters environmental monitoring.

Christopher Fabian 19. Captain Christopher D Fabian, USSF, is currently a Crew Commander in the 3rd Space Operations Squadron. He supports the Delta 9 mission to conduct protect and defend operations from space and provide response options to deter and defeat adversary threats in space. Capt Fabian earned his commission through the U.S. Air Force Academy in 2013. "A Neoclassical Realist’s Analysis Of Sino-U.S. Space Policy.” Jaunary 2019. University of North Dakota: UND Scholarly Commons. <https://commons.und.edu/theses/2455> //EM [SSA = Space Situational Awareness, STT = Space Surveillance and Tracking, STM = Space Traffic Management]

In the absence of a formal treaty, the United States must nonetheless continue to work towards implementing TCBMs that seek to increase transparency, familiarity and clarity of intentions, and provide a basis for strengthening mutual trust building and confidence amongst states.477 Improving space situational awareness (SSA) through an international outreach effort is the ideal platform through which to accomplish these goals. SSA is vital to the long-term sustainability of the space environment because it helps mitigate natural environmental threats and identifies behavior that would be detrimental to responsible use and long-term sustainability.478

Therefore, SSA will be a foundational verification mechanism for potential treaties as well as an opportunity for cooperative trust building. 479 SSA is generally made up of two components: space surveillance and tracking (SST) and space traffic management (STM). First, SST involves using ground-based and space-based optical sensors and radars in order to track, characterize, and analyze space objects. Second, STM utilizes SST data in order to ensure safe passage through the space environment.480 Both SST and STM require cooperative efforts to be successful.

SST necessitates a diverse, geographically dispersed sensor network to provide timely, accurate data on objects in a wide array of orbits.481 A single nation is not able to provide the geographical coverage needed for a comprehensive SST network. STM requires agreed upon standards of behavior to ensure spaceflight safety.482 There is currently no standardized regime for conducting the broad SSA mission in order to analyze and communicate threats to the space domain.483 This creates an opportunity for the U.S. to utilize its position of technical superiority in order to score a soft power coup by taking the lead in a global SSA initiative.

The major obstacle to building an international SSA coalition is the military utility SST data, which can be used to reveal classified military capabilities and conduct ASAT targeting.484 The United States possesses the most comprehensive network of SST sensors and maintains a database of 20,000+ space objects.485 However, the U.S. military did not share this data until an Iridium satellite collided with a Russian military satellite, prompting the amendment of 10 U.S.C. § 2274 to authorize the provision of SSA services if they were consistent with national security interests.486 After this event, the U.S. Strategic Command’s SSA sharing program grew exponentially, providing close approach notices to satellite owner operators and freely sharing SST data on its website.487 This was a good first step, but an increase in the quantity of SST sensors in the past decade has done little to bolster space traffic management efforts due to the disjointed nature of the data.488 As the space community attempts to consolidate SST data as part of a broader SSA régime, multiple nascent SST data sharing organizations show that a U.S. centric model is not guaranteed.489 The U.S. could put itself in a dangerous situation if it attempts to control SST data for the purposes of military use; this could potentially result in having complete control over only a fraction of the SST market, while American commercial SST companies lose their competitive edge.

#### Environmental monitoring solves extinction.

Ben Biggs 18, PhD Researcher in Computer Vision and Deep Learning at the University of Cambridge, “How Satellites Can Protect Planet Earth From Disaster”, HowItWorks Daily, 12/22/2018, <https://www.howitworksdaily.com/how-satellites-can-protect-planet-earth-from-disaster/>, dml

It might not look it, but our planet is a fragile place. A delicate balance of pressure, temperature and gases keeps us alive, as our atmosphere lets in enough heat for us to thrive – but not too much that we get too toasty. For many years our planet has looked after itself with ease. Now, with humans on the scene, things are changing more than ever, from climate change to mass deforestation. If our planet is going to survive long into the future it’s going to need our help.

Fortunately, we’ve got plenty of missions that are working for the benefit of our world already. Using observation satellites in orbit, scientists have been monitoring Earth for decades, watching how the planet pulsates and changes over time. From orbit we can watch how species migrate, identify and predict environmental changes and even fix problems.

A great example of this was the global effort to repair a hole in the ozone above the Antarctic back in 1987. Two years prior, scientists had discovered that chemicals known as chlorofluorocarbons (CFCs) – produced by fridges and aerosols, among other things – were causing the hole to grow. As a result countries around the world agreed to phase out the use of CFC as part of the Montreal Protocol. In early 2018, NASA announced that its Aura satellite had watched the hole successfully close, with it expected to fully repair as early as 2060. It was proof that we could work together to change the planet for the better.

Aura is part of a broader NASA project called the Earth Observing System (EOS). This programme, which began in 1997, has seen NASA launch missions and instruments into orbit. This has included the groundbreaking Landsat series of satellites, which have provided surface images of the whole globe. Then there’s the Terra mission that launched in 2009 and studies clouds, sea ice and more from orbit. Most of these satellites are in polar orbits, which means they orbit the planet from top to bottom so that it rotates underneath and gives them a global view.

Planning for the EOS began back in the 1980s, with NASA keen to regularly fly instruments for at least 15 years. “Human activity has altered the condition of the Earth by reconfiguring the landscape, by changing the composition of the global atmosphere, and by stressing the biosphere in countless ways,” they noted in a handbook in 1993. “There are strong indications that natural change is being accelerated by human intervention.”

More than two dozen missions have been launched as part of the EOS to date. Among the programme’s many accomplishments, scientists watched as an ice shelf collapsed on the Antarctic Peninsula in 2002 using the Terra satellite. The same satellite, along with the Aqua satellite launched in 2002, has provided a global view of how the vegetation cycle changes over the course of a year and the effect the climate has on it. Those same two satellites have also allowed us to see how summer sea ice in the Arctic is decreasing, which means that more of the Sun’s light is being absorbed rather than being reflected, raising global temperatures.

The EOS has helped in other ways too, such as enabling scientists to keep a close eye on the levels of toxic gases like carbon monoxide being emitted from massive fires in the atmosphere. This allows people on the ground to be alerted to these dangers, and they can in turn be advised to limit their outdoor activity to protect their health. The EOS is even helping to track and monitor rare animals, such as chameleons in Madagascar. Here, scientists have been able to use satellite imagery, combined with known habitats of the animals, to map out where they are likely to be living. It would take survey teams on the ground thousands of years to replicate this information without satellites.

It’s not just NASA that has been keeping a close eye on the planet. The European Space Agency (ESA) runs the Copernicus project, billed as the world’s largest single Earth observation campaign. Previously known as the Global Monitoring for Environment and Security (GMES) programme, it began with the launch of the Sentinel-1A satellite in April 2014. This radar imaging satellite provides images both day and night and during all weather conditions, and these are being used to map sea ice, track oil spills and more.

This has been followed by half a dozen more missions, with the latest – Sentinel-3B – launching on 25 April 2018. This mission is focusing on monitoring the behaviour and health of the oceans, but it has a wide range of abilities. It flies in formation with its predecessor, Sentinel-3A, and together the two of them can provide global data for Earth across an entire day. The satellites can measure the temperature over oceans, as well as the colour and height of the sea. They can also monitor wildfires from space, check the health of vegetation and map the way that land is being used around the world. And there are more Sentinel satellites on the way. In the coming years we’ll see the Sentinel-4 and Sentinel-5 missions launch, studying the composition of our planet’s atmosphere, while Sentinel-6 will measure global sea surface height for ocean and climate studies.

“Copernicus will help shape the future of our planet for the benefit of all,” said the ESA, also noting that it isthe “most ambitious Earth observation programme to date,” one that will provide accurate and timely data on the environment, climate change and more. All of this data is vital for directing climate policy and other human activities on Earth. By observing our planet around the clock from space we can see the direct effect that humans are having on it.

These are not the only climate-monitoring missions run by NASA and the ESA. The former has a number of other missions, including the Deep Space Climate Observatory, which observes the sunlit side of Earth. The latter has eight missions on the books in its Earth Explorer programme, including a mission to study how Earth’s gravity field varies over the surface of the planet, called the Gravity field and steady-state Ocean Circulation Explorer (GOCE), which ended in 2013.

In 2016, countries of the world came together to sign the Paris Climate Agreement, a global effort to reduce carbon emissions to prevent the global average temperature rising by two degrees Celsius above pre-industrial levels. While the US later infamously reneged from this agreement, it was proof that with enough level-headed minds, minds that can see the data from missions showing how the planet is changing, t we can take action. Humans continue to have a major effect on the planet, for better or worse, and monitoring that change is vital to our planet’s survival.

#### Cross-sectional space domain awareness unlocks vast tracking of orbital objects---effectively, preventing debris collisions---but revitalizing DoD credibility is key.

AT: Advantage CP---AT: ADR

Bhavya Lal et al. 18. Currently the acting chief technologist of NASA, responsible for providing evidence-driven advice to NASA leadership on internal and external policy issues, strategic planning, and technology investments. She also provides executive leadership and direction to the newly created Office of Technology, Policy and Strategy within the office of the administrator; Asha Balakrishnan is a Research Staff Member at the Science and Technology Policy Institute (STPI), a Federally-Funded Research and Development Center that provides rigorous and objective analysis of science and technology policy issues for the White House Office of Science and Technology Policy. Reina is a PhD student in the Chemistry Department at the California Institute of Technology after completing her undergraduate studies in chemistry at Pomona College. “Global trends in space situational awareness (SSA) and space traffic management (STM).” April 2018. Institute for Defense Analyses Science and Technology Policy, IDA Document D-9074, Washington, DC. <https://www.ida.org/research-and-publications/publications/all/g/gl/global-trends-in-space-situational-awareness-ssa-and-space-traffic-management-stm> //EM thx JY for the OCR.

1. Growing Number of Objects in Space

Space is becoming increasingly more crowded: in the last 60 years nearly 8,500 objects have been launched to space, about 1,500 in geosynchronous Earth orbit (GEO) and about 7,000 in low Earth orbit (LEO) (McDowell 2018). A large fraction remains (Figure 2-1) especially in LEO (Figure 2-2). Going forward, LEO is expected to become more crowded. As an illustration, over 6,200 small satellites (satellites weighing less than 500 kg) are expected to be launched between 2017 and 2026 (Euroconsult 2017a). Although the main space players will continue to dominate (85 percent of the government space market will remain concentrated in the 10 countries with an established space industry—U.S., Russia, China, Japan, India, and the top five European countries), the other 50 countries engaged in space will launch almost 200 satellites by 2026, twice the number they launched over the past 10 years (Euroconsult 2017a, b).

The concern is not just the increasing number of satellites and active payloads, but the amount of debris (rocket bodies, other inert bodies, dead payloads) in earth orbit, which comprises more than 95 percent of the currently tracked objects in space. The U.S. Department of Defense (DoD) is currently tracking 23,000 objects larger than 10 cm in diameter in Earth orbit (of these, almost 16,000 are in LEO, of which nearly 13,000 were classified as space debris ). An estimated 500,000 objects larger than 1 cm in diameter are not currently tracked, and over 100 million objects smaller than 1 mm in diameter are likely not trackable (NASA Orbital Debris Program Office). It is not

trivial to identify space debris and other junk, especially objects under 10 cm, using active beacons or other markers (e.g., radiofrequency tracking); they need to be physically spotted and tracked. Starting in 2019, the U.S. Air Force's Space Fence System will bring the catalog of debris tracked by Space Command from 23,000 to an estimated 200,000 objects. Figure 2-1 and Figure 2-2 visually show the overwhelming fraction of debris in space by orbit.

In addition to implications for the safety and sustainability of the future space environment, these capabilities have other policy implications. For example, the principal reason Swarm Technologies' sandwich-sized "Space Bees" did not get a spectrum license from the Federal Communications Commission (FCC) was due to concerns that they might not be tracked consistently by DoD.7,8

2. Growing Number of Operators in Space

It is not just the number of satellites that is increasing: the number of satellite operators has been increasing steadily over the last 60 years (Figure 2-3). More countries have become active in space. Figure 2-4 plots data on number of satellites launched by country, and shows the crowding in the 2010s. This changing landscape is driven by two primary trends: increasing State interest in independent national space programs and the globalization of the aerospace industry (Schroegl 2018).

Smaller, lighter, and more capable satellites make Earth observation and remote sensing within the reach not just of countries, but also corporations and individuals. For example, Bank Rakyat in Indonesia has launched a satellite, built by Space System Loral and launched by Arianespace, to manage its 50 million accounts. Another example is the satellite launched by NanoRacks by an individual who wanted to fly a cubesat and was able to afford it. This trend is likely to continue, making the space environment increasingly more crowded. \*\*\*FIGURE 2-1,2,3,4 OMITTED\*\*\*There is also growing participation in space by the private sector. It is important to note, however, that private space, especially in the near- and mid-term, is primarily a U.S. phenomenon. For most other countries, space is still a strategically-oriented government-run activity. Of the 44 companies that plan to launch constellations between 2017 and 2025, 20 are in the United States (Lal et al. 2017). Of the almost 10,000 satellites that are expected to launch as part of constellations, over 80 percent are from companies in the United States (Euroconsult 2016). More generally, of the 1,700 space companies listed by NewSpace Ventures, about half are headquartered in the United States; the remaining half were distributed around the rest of the world (see Figure 2-5).

The increased number of owners and operators requires more coordination and governance in space, given that a standardization system to coordinate on-orbit behaviors across operators (other than spectrum, which is coordinated by the ITU) does not currently exist. Each private entity (e.g., universities, research institutes, non-profits, commercial companies) is governed by its licensing nation, potentially resulting in a varied set of behaviors in space. This issue could be exacerbated as the number of nations launching government assets as well as licensing private entities continues to increase.

3. Changing Space Activities and Architectures

The current U.S. military SSA system relies heavily on sensors originally created for missile warning and works relatively well for tracking satellites in simple orbits around Earth. However, emerging architectures will change the way objects will need to be tracked Emerging applications, including missions related to rendezvous and proximity operations, such as satellite servicing and refueling, inspection, space RF mapping, and space-based spacecraft assembly and manufacturing, will require SSA services that would be qualitatively different than the current system.

For example, formation flying—the ability for satellites to act as single units while they maintain similar orbits and operate within close proximity to one another—poses challenges to current DoD SSA systems, as these systems are not optimized to differentiate objects that are closer together; the space of uncertainty around each object is compromised by each object's closeness to other satellites in the constellation. Additionally, tracking and predicting the orbits of constellations containing hundreds of small satellites may challenge existing systems due to the number and size of objects involved. Going forward, the number of satellites in such systems is expected to increase. Figure 2-6 shows 60 companies that have plans to launch constellations. While only a fraction of these plans are likely to pan out, it is an important driver of changes required in the SSA system. Beyond constellations, further changes in the space sector include growing activity in several other areas beyond remote sensing and communication. \*\*\*BEGIN FOOTNOTE 10\*\*\*One example of a new activity is the removal of space debris – the goal being to decrease the number of objects in space and thus reduce collision risk. Beyond the technical and regulatory challenges (e.g., restrictions on the ability to move an object even if it is no longer in use), any debris removal action will require more and more accurate SSA.\*\*\*END FOOTNOTE 10\*\*\* Countries are operating satellites across orbits with varied capabilities, further complicating orbital prediction as the nature of any object in space becomes further unpredictable. Satellite operations automation, the continuous thrust allowed by electric propulsion, and other non- Keplerian activities for which the DoD system is not optimized make tracking difficult as the satellites' orbits can change any time, compromising the effectiveness of orbit prediction.

The popularity of electric propulsion on satellites has grown since the 1990s and implementation has increased sharply in the last decade; many of the proposed large LEO constellations require electric propulsion (Lev et al. 2017) and many GEO satellites now use electric propulsion as well. Unlike chemical thrusters, which impart thrust at one time, electric propulsion systems can impart thrust over the course of many months. This increases the number of observations needed to understand the satellite's new orbit. It also creates challenges for astrodynamics algorithms that model maneuvers as instantaneous, as well as catalog maintenance routines that only update orbits every several hours (such as that of the 18 SPCS). This capability can also be used to change a satellite's orbit mid-life, further complicating tracking. Although many small satellites do not have an on-board propulsion system, some small satellites in low Earth orbit can change their orbit by orienting themselves in such a way to increase atmospheric drag, again affecting projections of the satellites trajectories. Impulsive maneuvers through chemical propulsion bring their own set of challenges, given that a spacecraft moving with electric propulsion can be reflected in the surveillance data (e.g., through a negative drag coefficient) as long as the thrust is constant. Additionally, impulsive maneuvers can be challenging to account for with existing U.S. military satellite surveillance capabilities; thus, the image from a surveillance system is not reliable, given that more impulsive maneuvers may occur. An accurate prediction of such an object requires operator-level data that details whether a maneuver is taking place. This operator data is often not openly shared with providers; the necessity of this information suggests that cooperation for SSA is inevitable. An example of this is the actions of Space Data Association (SDA) in GEO, and a similar effort is likely in LEO, especially in response to the large satellite constellations that have been proposed (Schrogel, 2018).

Materials and specifics of satellites—e.g., size (smaller satellites and components), composition, and antenna technology both hardware and software (e.g., software defined radio)— can make the satellites more difficult to detect, especially given the limitations imposed by the rotation speeds of telescopes, which minimize the opportunities to sight and track objects. More efficient and smaller space electronics mean that power requirements of systems are shrinking, which in turn reduces the need for large solar panels. This not only reduces the satellite cross section, but may also reduce the reflectivity of satellites.

New technologies and smaller satellite components have enabled satellite operators to increase the capabilities of satellites in ever-smaller form factors. New materials used in satellite composition affect tracking attributes such as reflectivity. Cubesats and chipsats have smaller cross-sections and are thus more difficult to observe. These cross-sections are reduced even further by the improved technologies that allow for smaller antennas and solar panels. The cubesat standard is a satellite architecture based on 10 cm-wide units. This standard has led to an increase in commercial availability of small standardized parts, which in turn has led to a decrease in the price of components for such satellites, which can now be mass produced rather than built individually and/or by hand. Additionally, major providers of launch services have designed satellite deployment units for the cubesat standard, further increasing the number of entities that will use this standard when designing satellites. Chipsats are standalone satellites built onto computer chips approximately the size of a credit card. Because of their size, many of these satellites do not have propulsion units, making predictions of their orbits easier once they are detected. However, due to their small form factors, initial and follow-up detection is difficult without higher resolution telescopes. One reason FCC turned down the Swarm Technologies' license application was that there was concern that their satellites were too small to be reliably tracked by DoD.

Future space activities that allow and often require close proximity of space objects (e.g., rendezvous and docking, on-orbit servicing or assembly) will require even more precise orbital estimations and predictions to avoid collisions. Companies engaged in such activities would need to supplement DoD information with on-board or space-based sensors to more precisely assess their location with regard to other objects in close proximity.

B. Growing Concerns about Increasing Collisions

Although relatively few catastrophic collisions have occurred thus far in space, the likelihood of a collision is predicted to increase in the near future, given the expected growing number of objects in both LEO and GEO and limited ability to track objects' orbits, which will make it difficult for operators to adequately avoid threats. This problem may be exacerbated if any of the proposed constellations of small satellites in LEO (shown in Figure 2-6 above) are launched, as they will dramatically increase the number of objects that require tracking, thus increasing the tracking and computational requirements for SSA in general and conjunction warnings in particular. Some industry representatives interviewed for the project noted that the emergence of constellations is driving the need for higher precision knowledge and services to mitigate the risk of collision: if numerous small satellites are deployed at once, tracking can be difficult, as resolution may not be great enough to distinguish multiple satellites.

NASA projects nearly one collision per year in the next 200 years if there is no debris mitigation. Independently, insurance companies have predicted a total exposure of $1.3 billion in LEO and $18 billion in GEO (Lal et al. 2015).

To estimate the number of collisions resulting from the increasing number of small satellites, several simulations of expected collisions per year for a number of large satellite constellations in LEO over 200 years have been conducted (Muelhaupt 2017). One such exercise evaluated the effect of adding two large constellations—those of SpaceX and OneWeb—to the current constellations in LEO (Iridium, Orbcomm, and Globalstar). The simulations found that within its first 20 years in orbit, the first constellation is expected to cause one collision annually; this number would grow to approximately 8 per year at its peak collision rate, which occurs about 190 years after launch (see Figure 2-7). Although the majority of the collisions in the simulation were due to satellites that failed to be deorbited following end-of-life protocol, satellites that did attempt to be deorbited still accounted for approximately 40 percent of the total collisions.

Given that the systems developed to track space objects were developed at a time there were fewer objects in space, the accuracy of prediction is low. Oftentimes, a DoD conjunction warning message has an error ellipse of 100 km or more; the rate of false positives is high as well. Because of these two factors, as traffic in space grows, both the number of conjunction warning messages as well as the rates of both false positives—and false negatives— are likely to increase. For example, one study estimated that upon launch of its proposed constellation, SpaceX would receive 7.2 million conjunction warnings per year, and Iridium would receive about 384,000 per year. Some operators, aware of the increasing risk of collision, will be more likely to pay heed to notifications. This could result in increased maneuvers as operators attempt to avoid collision, even if the warning is not sound. These maneuvers—even if they are reported to the providers of SSA (e.g., the DoD, or commercial vendors), which may often not be the case—will still contribute to uncertainty regarding objects' paths, thus compromising the resulting predictions. Other operators, especially those with low-value assets, are likely to continue to ignore warnings as they currently do, which is equally problematic as they will collide with debris or put the onus to maneuver fully on the operator of the asset it threatens.

To avoid a significant increase in notifications, operators will increasingly look for higher quality SSA information. This could put further pressure on emerging systems to improve their predictions.

C. Changing National Level Motivations

Space is increasingly recognized as a sector of strategic importance with applications for security, capacity building, and social benefit. The increasing number of countries seeking to use space for science, safety, national security, and commercial purposes means increased threats (both accidental and nefarious) of collision and harm to assets (e.g., through radiofrequency interference).

1. Growing Recognition of the Need for Timely and Actionable SSA Services and Products

As space capabilities become integral to more applications (e.g., earth observation, communications, global positioning), a growing number of countries are recognizing the security and economic value of space and increasing their spending in space. The number of countries involved in space continues to increase: a decade ago, fewer than 50 countries were investing in space; today, there are 70. In the coming decade, that number is expected to increase to more than 80 countries, and the annual government space expenditure globally is expected to double, from about $40 billion in 2006 to $80 billion in 2026 (Euroconsult 2017b, c). This increased value (both mission-specific and financial) has led many nations to treat safety of such assets as higher priority, leading to growing efforts to develop norms and guidelines for behavior in space. Additionally, many countries (e.g., Brazil, China, France, Japan, and South Africa) want to be (and be viewed as) responsible stewards of space, and thus support these efforts.

In our dataset of 18 countries, most of those actively pursuing SSA focus on protecting their assets from satellite collisions—due to both the increasing number of assets and the increasing amount of space debris on orbit. Some countries (e.g., Japan, Canada) generally pursue protection of their space assets and interests—either for the sake of those assets specifically, or for the role they play in national security broadly. Some countries are more interested in the application of SSA (e.g., the data products) while others (e.g., Japan) value the collection and analysis side as well. SSA can also help with safe operation and control of assets. Though most are concerned with on-orbit collision warnings, some, such as India, use SSA only to avoid collision on launch.

Interviewees from some nations, such as Germany, noted that SSA can be useful in protecting what has been achieved in space thus far and avoiding major incidents. ESA's SSA program is interested in developing a hazard warning system by federating existing European assets and developing new sensor technology, with the goal of securing Europe's access to space, protecting the involved economies, and strengthening European industry.

Some countries prioritize detection of risks to their territory, and thus seek to detect either threats on reentry such as rogue space assets (e.g., France) or natural threats such as space weather and asteroids (e.g., South Africa). Some are specifically interested in protecting their satellites used for Earth observation; for example, representatives of Brazil note the importance of using space to protect its borders given significant issues with drug trafficking. This increasing reliance on space assets for security necessitates greater interest in and efforts toward SSA. For some (e.g., UK), SSA is seen as underpinning all other space roles in that it details the hazards, risks, and threats to the domain.

Our discussions with stakeholders demonstrated some countries' concerns that if they do not participate in global discussions (e.g., long term sustainability [LTS] guidelines), their national interests will not be appropriately reflected in the rules, and they will miss out on critical opportunities. This involvement suggests that more countries are becoming concerned with safe and sustainable operations in space—keeping space open to activities in the future and preventing problems (e.g., proliferating debris) from adversely impacting or precluding space activities. It is important to note that smaller and less powerful countries benefit greatly from these international discussions, as they are given a voice in the proceedings. More powerful and established nations may not always agree, as these deliberations have to include more players and typically take longer to conclude negotiations. This is specifically true for European countries; stakeholders noted that Europe can only have a voice in future regulations regarding the creation of global space traffic regulation if the EU and ESA work together. They noted that for European industry to become involved in challenging projects and thus be competitive on a global scale, the involved nations need to organize at the European level.

2. Lack of Confidence in DoD-Provided Data

Many stakeholders indicated that they need to have trust and confidence in the data being shared for collision warnings and other SSA products; many acknowledged the usefulness of verifying the information that is part of any database. There are many concerns with the current systems for provision of SSA. Some operators question the accuracy and especially the completeness of the information provided to them by the DoD. For example, some South Korean government officials estimate that their country receives data on only about 40 percent of the objects tracked by the DoD, due to sensitivity of U.S. assets.

This distrust is further complicated by the lack of transparency related to computing outcomes such as probabilities of collision. Owners and operators believe they require more [high quality] information to make well-informed decisions about maneuvering. But because they do not know the process by which U.S.-provided information on an object's location is processed into a collision assessment or warning, they often do not feel confident maneuvering based on that warning. Skepticism regarding the reliability of the shared information is exacerbated by the nonstandard and nontransparent methods of calculation (often referred to by stakeholders in our discussions as "black box processing"). Beyond the distrust, some users perceive the U.S. DoD systems as limited, given that they are not well-suited to the emerging space environment; additionally, given the separation of the provision of SSA from the DoD's core mission, it is also perceived as overworked and understaffed, leading to further dissatisfaction. There is also some concern that going forward, the United States will either not share data or will charge for it. This last concern has heightened the sense of urgency in some countries to set up parallel SSA systems.

3. National Security Considerations

Many of the 18 countries are interested in developing or strengthening their strategic early warning capacities, specifically regarding space-based intelligence, surveillance, and reconnaissance (e.g., South Korean awareness of potential North Korean targeting, France's goal of detecting objects presenting a risk to its territory). Often the national security goal is two- pronged: entities are interested in protecting their own assets while building knowledge of the location and intention of adversary assets.

Beyond threats, some of these countries' concerns have been driven by recent space events— natural and accidental, such as the February 2013 meteor explosion over Chelyabinsk, Russia, and the de-orbiting of Tiangong-1 in April 2018. China, for example, desires increasing information from improved national SSA and strategic early warning capacity.

#### Collisions trigger cascades, blanketing the LEO---extinction.

Mark Sturza & Gemma Carretero 21. President of 3C Systems Company, which he founded 30 years ago to provide consulting expertise in the design, development, analysis, and regulation of satellite communications systems; MsC Astronautics and Space Engineering, Astronautics and Space Engineering, Senior Mission Systems Design Lead, Senior Systems Design Engineer at Viasat. “Design Trades for Environmentally Friendly Broadband LEO Satellite Systems.” Advanced Maui Optical and Space Surveillance Technologies Conference (AMOS). 10-22-2021. ResearchGate. //EM thx JY for the OCR.

ABSTRACT

Humanity faces an existential crisis; space debris are at risk of becoming the equivalent of a "drifting island of plastic." Large constellation (LC) systems plan to operate tens of thousands, or even hundreds of thousands, of satellites in low Earth orbit (LEO), posing the threat of an inglorious end to the Space Age. Satellites that cannot maneuver, cannot avoid collisions. Even satellites that can maneuver, can be involved in collisions. Collisions between LEO satellites tend to be catastrophic resulting in large numbers of new debris objects spread across LEO altitudes.

A model is developed to explore the dependence of the time to Kessler Syndrome on the number of satellites, the satellite sizes, and the orbits of LCs. Simulations show: 1) that LCs of small satellites (<25 kg) are significantly safer than constellations of medium (25 to 300 kg) or large (>300 kg) satellites, and 2) that if LCs of medium or large satellite are deployed, they are safer at lower orbits, such as 450-km rather than at 600-km or 1,200-km orbits. The orbital capacity (number and type of satellites that can be sustainably deployed) and tipping point (at which it is no longer possible to avoid a Kessler Syndrome by ceasing launches) concepts are demonstrated.

1. INTRODUCTION

Humanity faces an existential crisis; space debris are at risk of becoming the equivalent of a "drifting island of plastic" [1]. Large constellation (LC) systems plan to operate tens of thousands, or even hundreds of thousands, of satellites in low Earth orbit (LEO) [2], posing the threat of an inglorious end to the Space Age. A "take risks and fail often" approach to new technology is being extended to space without considering that mistakes in space cannot be cleaned up as easily as they can on Earth.

Satellites that cannot maneuver, cannot avoid collisions. Loss of maneuverability can result from failures of satellite sub-systems in the maneuver chain or from collisions with small (untracked) objects that disable these subsystems. Passive deorbit times can be minimized with lower LEO altitudes and larger area-to-mass ratios but can still require years depending on the solar cycle and larger area-to-mass ratios realized by increasing area can lead to increased collision risk.

Even satellites that can maneuver, can be involved in collisions. Conjunction warnings may not be generated, not all lethal debris are trackable. Every time a satellite is not maneuvered in response to a low probability conjunction warning, there is a non-zero collision risk that depends on the space situational awareness (SSA) accuracy. Additionally, every time a satellite is maneuvered, there is another non-zero probability that the maneuver will result in a collision. In both cases, with a sufficient number of conjunctions occurring, even six sigma events can become likely.

Collisions between LEO satellites are typically catastrophic resulting in large numbers of new debris objects spread across LEO altitudes. For example, there are currently 1439 tracked debris objects in orbit from the 2009 collision between Iridium-33 and COSMOS-2251 [3]. Even though the collision occurred at 800-km, the debris' apogees now range from 400 km to over 1,600 km.

Constellations are appropriately analyzed over their orbital lifecycles. LCs are incrementally deployed, and satellites are replenished as they fail, reach end-of-life, or are replaced with more capable models. This replenishment can be reasonably modeled to continue until the constellation is no longer economically viable. The result is a continuing process of orbit raising and phasing, and a combination of active and passive deorbiting.

Sub-system failures and small object collisions can be mitigated with sub-system redundancy, and small objects collision can be further mitigated with shielding. Operational techniques, such as initiating deorbit immediately after the (N - 1)-th failure with N-th redundancy, can be used to improve the effective satellite reliability.

The debris environment naturally evolves over time as objects decay and new objects are created by collisions between existing debris objects. Satellite collisions can cause step increases in the debris population. In addition, there are over 900 derelict rocket bodies remaining in orbit which pose further debris generating risk.

Previous work [4] using a simplistic model showed that reducing the number of non-maneuverable satellites significantly increases the time to Kessler Syndrome, a self-sustaining collision cascade [5]. Another approach [2] used simplified rate equations to model population evolution. One of the simplifications was ignoring collisions of debris with other debris, precluding the possibility of a Kessler Syndrome.

This paper expands on the previous work with more sophisticated Markov models and Monte Carlo simulations to explore the dependence of time to Kessler Syndrome on key parameters of LCs (the number of satellites, the satellite sizes, and the orbits). The approach is not only useful in the design of environmentally friendly broadband LEO systems, but also in assessing the environmental impact of existing and planned LC systems. Further, it can help in understanding the implications of multiple LCs occupying interleaving or overlapping orbits.

While it is generally agreed that LEO is a finite resource and that collisions may lead to loss of access to space [6][7][8][9], this work can be used to help address the key questions:

1) How many satellites are too many? What is the "orbital capacity", the number and type of satellites that can be sustainably deployed in each orbit without risking a Kessler Syndrome?

2) How close are we to a "tipping point", i.e., how urgent is this issue? A tipping point in that point in time at which it is no longer possible to avoid a Kessler Syndrome by ceasing launches.

This is an active area of research with numerous contributions, including [10][11][12].

The models are described in Section 2, Section 3 discusses the simulation results, and the conclusions are summarized in Section 4.

2. MODELS

A model is developed to explore the dependence of time to Kessler Syndrome on the constellation sizes and orbits, and on the size of the satellites deployed. The key simplifying assumptions employed to create this model are:

1. Only the LCs being studied are replenished over time, other constellations and individual satellites are not replaced as they deorbit, fail, or fragment.

2. No new rocket bodies are left in orbit.

3. Collisions with debris between 1 cm and 10 cm never result in fragmentation, only the possibility of damage resulting in loss of maneuverability, and the estimated 128 million debris from 1 mm to 1 cm [13] are ignored.

4. All orbits are circular, including those of satellites, debris, and rocket bodies, and orbits are fully characterized by their altitude and inclination.

5. Objects are grouped into classes with one set of characteristics modeled for each class.

6. The probability of non-maneuverable satellites experiencing catastrophic collisions is approximated as described in Section 2.4.1.

The first three assumptions are believed to be optimistic. Further work is required to access the impact of the last three.

Objects are divided into 10 classes. At the top level, objects are categorized as satellite (S), debris (D), or rocket body (RB). Satellites are sub-categorized as maneuverable (SM) or non-maneuverable (SN). They are further sub-categorized by mass: large (SML and SNL) for mass greater than 300 kg, medium (SMM and SNM) for mass

between 25 kg and 300 kg, and small (SMS and SNS) for mass less than 25 kg. Debris are sub-categorized by diameter, large (DL) for 1 to 3 m diameter, medium (DM) for 0.3 to 1 m diameter, and small (DS) for 0.1 to 0.3 m diameter. Rocket bodies (RB) are not further sub-categorized.

For each class, the number of objects in each orbit is stored in a matrix with the structure shown in Fig. 1. The possible orbits include all altitudes between 200 km and 2,000 km in 25 km bins (Sh = 25 km), and all inclinations between 0° and 180° in 10° bins (Si = 10°). The number of objects in each bin at time tm is X^ . These matrices are initialized using Space-Track SATCAT data [3]. A total of 16,621 LEO orbits were used - 3,773 maneuverable satellites, 920 non-maneuverable satellites, 10,992 debris, and 957 rocket bodies.

The LC orbit models are discussed in Section 2.1 and the object models in Section 2.2. Section 2.3 introduces the state evolution model, and the state transition probabilities are derived in Section 2.4. The object life process models are discussed in Section 2.5.

2.1 Large Constellation (LC) Orbit Models

Three LC orbits are considered: 1) 450 km altitude at 40° inclination, 2) 600 km altitude at 50° inclination, and 3) 1,200 km altitude at 60° inclination. These were selected to be representative of the LC orbits proposed for various NGSO systems [2].

2.2 Object Models

The key parameters for each object class are shown in Tab. 1. They are representative of objects in each class and are not based on any specific objects. The area-to-mass ratios (A/M) of the non-maneuverable satellites are modeled as one-half of those for the maneuverable satellites to account for tumbling.

2.3 State Evolution Model

State evolution is modeled as shown in Fig. 2. Newly launched satellites start in the Maneuverable State. At each time step, there are four possibilities for evolution of maneuverable satellites (SML, SMM, SMS): 1) transition to

the Non-Maneuverable State due to a failure or due to small object collision damage that disables maneuverability, 2) transition to the Fragmentation Process as the result of a large object collision, 3) transition to the Decay Process due to atmospheric drag, or 4) remain in the Maneuverable State.

Non-maneuverable Satellites (SNL, SNM, SNS), Debris (DL, DM, DS), and Rocket Bodies (RB) are always in the Non-Maneuverable State. There are three possibilities for these objects: 1) transition to the Fragmentation Process as the result of a large object collision, 2) transition to the Decay Process due to atmospheric drag, or 3) remain in the Non-Maneuverable State.

2.4 Transition Probability Models

These models are used to calculate the transition probabilities for the objects in each state at each time step. 2.4.1 Probability of Non-Maneuverable Object Catastrophic Collision

PN2F is the probability of an object transitioning from the Non-Maneuverable state to the Fragmentation process. The probability that an object with radius r, in an orbit with altitude hj, inclination ik, and shell thickness Sh experiences a collision over one orbit period at time tm is given by

where is the total number of objects at altitude hj and inclination iq at time tm, and noting that orbits are modeled as circular and the object radius, r, is much less than Sh so that

The probability that an object in an orbit with altitude hj and inclination ik experiences a collision with an object in an orbit with altitude hj and inclination iq is approximated by

The first factor in the "otherwise" value approximates the probability that both objects are inside a square with sides 2r on the surface of a sphere. When the difference in inclinations is such that the crossing angles for planes in a LC are near 0 or n, the geometry degenerates to a single dimension, and the appropriate probability to consider is that of both objects being in a segment of the orbit circle with length 2r. The second factor is the probability that two objects in a square on the surface of the sphere are in the same cube within an orbit shell of height Sh, or equivalently for the degenerative case.

2.4.2 Probability of Maneuverable Object Catastrophic Collision

The probability of a maneuverable satellite transitioning to the fragment process (PM2F) is the probability of a collision avoidance failure, either due to an untracked object, a low probability conjunction prediction being ignored, or an avoidance maneuver causing a collision. It is modeled as

PM2F = AvoidanceFailureRate x PN2F

The avoidance failure rate is set to 0.1%, which assumes that 999 out of every 1,000 collisions that would be experienced if the satellite did not maneuver are avoided using maneuverability.

2.4.3 Probability of Maneuverable Object Orbit Decay

PM2D is the probability of a satellite object transitioning from the Maneuverable state to the Decay process. It is modeled based on the estimated satellite lifetime as

where St is the simulation step size in seconds and SatelliteLifetime is in years.

Satellite design life is modeled as 5 years.

2.4.4 Probability of Non-Maneuverable Object Orbit Decay

PN2D is the probability of a non-maneuverable object transitioning from the Non-Maneuverable state to the Decay process. Assuming that atmospheric drag is the only nonconservative force and modeling the orbits as circular the change in altitude over one period is given by [14]

where St is the simulation time step in seconds and Sh is the object matrix altitude bin size in kilometers. 2.4.5 Probability of Satellite Becoming Non-Maneuverable

The probability of a maneuverable satellite transitioning to the non-maneuverable state (PM2N) is the probability of loss of maneuverability. This can occur either due to a failure mechanism or a small object collision. It is modeled based on the estimated satellite lifetime, satellite failure rate over lifetime, and probability of maneuverability being lost due to a small object collision

where St is the simulation step size in seconds and SatelliteLifetime is in years.

The small collision factor is set to 5.3 assuming that only 20% of the collisions with debris between 1 cm and 10 cm result in loss of maneuverability and noting that ESA estimates [13] that there are 900,000 debris objects in that range compared to 34,000 above 10 cm (0.2 x 900,000 / 34,000 = 5.3).

2.5 Object Life Process Models

The launch, decay, and fragmentation processes manage the life cycle of the objects.

2.5.1 Launch Process

The launch process maintains the LC(s) being evaluated at a fixed size for the duration of the analysis. The appropriate object flux matrix (SML, SMM, or SMS) is updated by maintaining a constant number of satellites in the object matrix cell corresponding to the orbit (altitude and inclination) of each LC at each timestep.

2.5.2 Decay Process

The decay process moves non-maneuverable objects to the next lower row of the object matrix. If an object in the h1 row decays, it is assumed to have completed deorbit, and is removed from the object matrix. For maneuverable satellites, the decay process moves them to a 300-km circular disposal orbit as non-maneuverable satellites.

2.5.3 Fragmentation Process

When a collision occurs, the fragmentation process removes the objects involved from the associated object matrices, determines the numbers and characteristics of the fragments, and adds the new objects to the appropriate debris matrices. Fragments with perigee <200 km or mean altitude outside the 200 km to 2,000 km LEO range are dropped from the model.

The Fragmentation Process is modeled based on the MASTER-8 version of the EVOLVE 4.0 NASA Standard Breakup Model for spacecraft [15]. The number of fragments is determined from a power law distribution characterized by the object masses and the minimum and maximum object sizes. It is well known that the NASA model does not conserve mass, and many workarounds have been proposed. However, for this analysis, the important quantiles are the number of fragments, their diameter distribution, and their velocity distribution.

The number of fragments with size in the range from dMIN (m) to dMAX (m) is given by

Assuming that all collisions are fragmenting (specific kinetic energy of projectile, greater than 40 J/g) and truncating at a minimum fragment size to dMIN and maximum fragment size to dMAX, the cdf for fragment diameter is given by

Area-to-mass ratio is characterized by a bi-normal distribution parametrized based on 5 = log10 (dF) for x = logw(A/MF)

where the parameters a, p1, oi, and a2 are functions of S.

The fragment delta velocity (m/s) is related to the fragment A/M (m2/kg) for fragmenting collisions by

The delta velocity is uniformly distributed over a sphere, added to the state vector for a randomly located object in the original orbit, and the resulting state vector converted to orbital elements to determine the delta altitude and inclination of each fragment relative to the original orbit.

The number of fragments and distributions for the fragment diameters, area-to-mass ratio, and delta altitude are shown in Fig. 3 for dMIN = 0.1 m and dMAX = 3 m. \*\*\*FIGURE 3 OMITTED\*\*\*

3. SIMULATIONS

Monte Carlo simulations are used to characterize the debris population sensitivity to LC orbits and satellite sizes over one hundred years, or until a Kessler Syndrome occurs. The simulation flow is shown in Fig. 4. \*\*\*FIGURE 4 OMITTED\*\*\*Initially, 146 cases were run, a baseline case with the initial object matrices and no new satellite launches, and an additional 145 cases based on 29 configurations (combinations) of small (15 kg), medium (250 kg), and/or large (500 kg) satellites in the three orbits considered. Each configuration results in 5 cases with 10,000, 20,000, 30,000, 40,000, or 50,000 satellites maintained in each orbit. Depending on the case, from 10,000 to 150,000 satellites are maintained in orbit.

The simulation parameters are summarized in Tab. 2. The start year is used to determine the solar flux at each time step, which is used to compute the atmospheric density in Section 2.4.4. The 100-year duration was selected to focus on near-term (in a cosmic sense) events. The time step, altitude bin size, and inclination bin size are selected to provide reasonable simulation times. Reducing the first two by an order of magnitude did not significantly change the results. Reducing the inclination step size by an order of magnitude resulted in an observable increase in the time to Kessler Syndrome but did not change the relative times between cases. LC satellites typically range from 3 to 10 year predicted lifetimes; 5 years is selected as a representative value. The ODMSP [16] requires that LC satellites have a 90% probability of successful post mission disposal with a goal of 99%. The 5% failure rate (95% success rate) is chosen to be in the middle of this range. The small constellation factor is discussed in Section 2.4.5 and avoidance failure rate in Section 2.4.2. Sensitivity analysis was not preformed with respect to the last 4 parameters.

The baseline case does not result in a Kessler Syndrome after 100 years. Tab. 3 shows the time to Kessler syndrome (years) for the remaining 145 cases. There are twenty-nine rows for the configurations and 5 columns for the number of satellites per orbit. The Satellite Size/Orbit columns indicate which orbits are populated for each configuration and with which size satellites: S - small (15 kg), M - medium (250 kg), or L - large (500 kg). For example, the Configuration 1 / 10K case is 10,000 small satellites in 450-km orbits, for that case a Kessler Syndrome did not occur within 100 years. Another example, the Configuration 22 / 30K case is 30,000 small satellites in 450-km orbits and 30,000 medium satellites in 600-km orbits, that case results in Kessler Syndrome in 23.4 years.

It is seen that the number of satellites, the satellite size, and the orbit altitude all matter. None of the cases consisting of only small (15-kg) satellites experiences a Kessler Syndrome within 100 years. This includes the 150,000-satellite case with 50,000 satellites in each orbit. The cases with at least 30,000 medium (250-kg) satellites in the 600-km or 1,200-km orbits experience a Kessler Syndrome within 25 years. The cases with at least 10,000 large (500-kg) satellites in the 600-km or 1,200-km orbits experience a Kessler Syndrome within 12.5 years.

Configurations 28 and 29 are interesting. In Configuration 28, small satellites (15-kg) are maintained in the 450-km orbit and large satellites (500-kg) in the 1,2000-km orbit. In Configuration 29, the sizes are reversed, large in 450km and small in 1,200-km. In both configurations, medium satellites are maintained in the 600-km orbit. The time to Kessler Syndrome for of the numbers of satellites per orbit is from 3 to over 10 times longer for the Configuration 29 cases. All these cases have the same number of satellites and the same total mass in orbit. The only difference is the switch of which orbits the small and large satellites occupy. Clearly, the larger satellites in lower orbit are safer than the larger satellites in higher orbit.

Four cases are explored in more detail. The baseline case in Section 3.1, the 150,000 small satellite case in Section 3.2, the 30,000 medium satellite 600-km orbit case in Section 3.3, and the 10,000 large satellite 1,200-km orbit case in Section 3.4.\*\*\*TABLE 3 OMITTED\*\*\*

3.1 Baseline Case

The time evolution of the baseline case is shown in Fig. 5. The maneuverable (active) satellites (solid lines) completely decay due to the 5-year lifetime model and post mission disposal of maneuverable satellites. The number of rocket bodies (dash-dot-dash line) decreases due to drag and collisions. The number of non-maneuverable (passive) satellites (dashed lines) deceases initially due to decay at the lower altitudes and then stabilizes. The debris (dotted lines) are observed to grow exponentially with an approximately 6-year time constant until the active satellites decay, and then at a much slower rate (approximately 100-year time constant). \*\*\*FIGURE 5 OMITTED\*\*\*

Fig. 6 compares the object fluxes at the start of simulation and at the end, 100 years later. After 100 years, debris growth has increased the number of objects in the orbits that had the higher object concentrations.

Graphical user interface

Description automatically generated

The evolution of objects by altitude in the baseline case is shown in Fig. 7. An interesting feature is the clear indication of the solar cycle in the decay below 400 km. It is also interesting to note the spread of objects into higher orbits over time. As there are no new launches, the only mechanism for this in the model are fragmentation events.

A picture containing graphical user interface

Description automatically generated

3.2 150,000 Small Satellites Case (Configuration 19 / 50K)

In this case the LCs consist of 50,000 small satellites in the 450-km orbits, 50,000 small satellites in the 600-km orbits, and 50,000 small satellites in the 1,200-km orbits, for a total of 150,000 satellites. After 100 years, there is little difference in object distribution by orbit compared to the baseline (no new launches) case, as shown in Fig. 8. The additional objects around 1,200 km are from the operational satellites at that orbit, the debris spread around that orbit, and the non-maneuverable satellites decaying from that orbit.

Graphical user interface

Description automatically generated

3.3 30,000 Medium Satellite at 600-km Orbit Case (Configuration 5 / 30K)

In this case the LC consists of 30,000 medium satellites in the 600-km orbits. The result is a Kessler Syndrome in slightly more than 22 years, consuming the satellites in that orbit and creating millions of debris objects. The evolution of the object classes in shown in Fig. 9. The SMM curve jumps to 30,000 at time zero and continues at that level until just before the Kessler Syndrome when the satellites are consumed by the debris. Fragmentation of LC satellites that lose maneuverability due to failures or small object collisions cause the increase in the SNM curve. Fragments from these non-maneuverable satellites as they experience collisions result in the increases of the DL, DM, and DS curves. The approximately 11,000 lethal debris objects at time zero grows to over 33 million at the start of Kessler Syndrome.

Chart, line chart

Description automatically generated

The debris evolution by altitude is shown in Fig. 10. The spike in debris around 600-km leading to the Kessler Syndrome is apparent.

Graphical user interface

Description automatically generated with low confidence

An interesting question raised by these results - when is the tipping point? Additional simulations were run to address this question for the 30,000 medium satellites in the 600-km orbit case. The previous results showed a Kessler Syndrome occurring in 22 years. Stopping launches after year 15 was found to reliably avoid a Kessler Syndrome within the 100-year simulation time.

Fig. 11 compares the object evolution for the continuous launch and the launch stop after 15 years cases. Note that the time scales are different. The continuous launch case plot ends at the time of Kessler Syndrome while the stop after 15 years case plot continues for 100 years.

Graphical user interface, chart

Description automatically generated

As shown in Fig. 12 and Fig. 13, stopping launches after 20 years delays the Kessler Syndrome by 4 years but does not prevent it - the tipping point has been reached.

Graphical user interface, application

Description automatically generated

10,000 Large Satellites in 1,200-km Orbit Case (Configuration 9 / 10K)

In this case the LC consists of 10,000 satellites in the 1,200-km orbit. The result is a Kessler Syndrome in 10 years. The object evolution is shown in Fig. 14. The SML curve jumps to 10,000 at time zero and continues at that level until just before the Kessler Syndrome when the satellites are consumed by the debris. The tail of the curve are the remaining large satellites from the baseline case at orbit altitudes away from the debris spike. Fragmentation of LC satellites that lose maneuverability due to failures or small object collisions cause the increase in the SNL curve.

#### It turns every impact.

Johnson 13 [Les Johnson, Deputy Manager for NASA's Advanced Concepts Office at the Marshall Space Flight Center, Co-Investigator for the JAXA T-Rex Space Tether Experiment and PI of NASA's ProSEDS Experiment, Master's Degree in Physics from Vanderbilt University, Popular Science Writer, and NASA Technologist, Frequent Contributor to the Journal of the British Interplanetary Sodety and Member of the American Institute of Aeronautics and Astronautics, National Space Society, the World Future Society, and MENSA, Sky Alert!: When Satellites Fail, p. 9-12]

Whatever the initial cause, the result may be the same. A satellite destroyed in orbit will break apart into thousands of pieces, each traveling at over 8 km/sec. This virtual shotgun blast, with pellets traveling 20 times faster than a bullet, will quickly spread out, with each pellet now following its own orbit around the Earth. With over 300,000 other pieces of junk already there, the tipping point is crossed and a runaway series of collisions begins. A few orbits later, two of the new debris pieces strike other satellites, causing them to explode into thousands more pieces of debris. The rate of collisions increases, now with more spacecraft being destroyed. Called the "Kessler Effect", after the NASA scientist who first warned of its dangers, these debris objects, now numbering in the millions, cascade around the Earth, destroying every satellite in low Earth orbit. Without an atmosphere to slow them down, thus allowing debris pieces to bum up, most debris (perhaps numbering in the millions) will remain in space for hundreds or thousands of years. Any new satellite will be threatened by destruction as soon as it enters space, effectively rendering many Earth orbits unusable. But what about us on the ground? How will this affect us? Imagine a world that suddenly loses all of its space technology. If you are like most people, then you would probably have a few fleeting thoughts about the Apollo-era missions to the Moon, perhaps a vision of the Space Shuttle launching astronauts into space for a visit to the International Space Station (ISS), or you might fondly recall the "wow" images taken by the orbiting Hubble Space Telescope. In short, you would know that things important to science would be lost, but you would likely not assume that their loss would have any impact on your daily life. Now imagine a world that suddenly loses network and cable television, accurate weather forecasts, Global Positioning System (GPS) navigation, some cellular phone networks, on-time delivery of food and medical supplies via truck and train to stores and hospitals in virtually every community in America, as well as science useful in monitoring such things as climate change and agricultural sustainability. Add to this the [destruction] ~~crippling~~ of the US military who now depend upon spy satellites, space-based communications systems, and GPS to know where their troops and supplies are located at all times and anywhere in the world. The result is a nightmarish world, one step away from nuclear war, economic disaster, and potential mass starvation.

#### The impact is certain---natural underestimation dismisses interdependencies and non-linear effects.

Olga Sokolova et al. 21. Risk Analyst with Engineering and Business Administration background. She received her Ph.D. degree in 2017 from St. Petersburg Polytechnic University; Dan Oltrogge is the Director of the Center for Space Standards and Innovation at Analytical Graphics Inc. (AGI). Mr. Oltrogge led the formation of and serves as administrator for the Space Safety Coalition; Matteo Madi is an entrepreneur, business developer and space-tech specialist with over ten years of work experiences in the Swiss and International public and private sectors. Dmitriy A. Grishko is an Associate Professor of Bauman Moscow State Technical University, Department of Theoretical Mechanics, PhD (PhysMath). Space Debris Peril: Pathways to Opportunities: Capacity Building in the New Space Era (1st ed.). CRC Press. [T&F.](https://doi.org/10.1201/9781003033899) //EM [italics in original] [fat-tailed = represents a greater likelihood of extreme events occurring, since the magnitude of fat tails are so difficult to predict]

Often, space debris risk is defined as an emerging risk, since it is difficult to quantify and its potential impact on businesses not sufficiently taken into account. This is based on the following promises: the rapid change of space debris environment, the growing interconnectivity between space and ground-based infrastructures, the development of new technologies for problem assessing and mitigation, though “systemic risk” approach is a more appropriate concept for space debris risk assessment. Systemic risk is also sometimes called network risk, since it emerges from complex non-linear cause-effect interactions among individual elements or agents with different and often conflicting interests. In addition, each element or agent is characterized by its own risk portfolio. The examples of systemic risks are the financial crisis of 2008, pandemics, cybersecurity, global climate change. Systemic risks can trigger unexpected largescale changes to a system or imply uncontrollable large-scale threats to it [82]. In other words, they tend to be *fat-tailed.*

The lack of knowledge about interdependencies requires advanced approaches to problem solving through risk thinking. The traditional linear methods have limited application. The concept of “femtorisks” stresses the importance of challenging standard approaches for risk assessment [83]. Because in a systems-approach there may be many competing solutions with no clear best, the challenge for their governance is to assure transparency, accountability, and inclusiveness of the risk management process, and effectiveness, stationarity, equity, and sustainability of the outcome [84]. One of the solutions is the principle of collective responsibility proposed by Helbing, D. [85].

Compared to critical risks, systemic risks do not attract the same attention and tend to be underestimated. The OECD defines critical risks as a rapid-onset event that pose the strategically significant risks as a result of their probability and likelihood. Another spaceborne hazard, space weather, was defined as a future global shock by the OECD [86]. Therefore, the concept of critical infrastructure resilience with respect to space threats is mainly focused on ground-based critical infrastructures, especially on power grids, which is the current backbone of modern critical infrastructures [87, 88]. Governments established the programs for assessing space weather risk, and this risk is included in the national risk portfolio of several countries (USA, Canada, Finland, Sweden, Norway, United Kingdom, Germany, the Netherlands, Hungary). They specified the tasks that will lead to improvements in policies, practices and procedures for decreasing vulnerability.

Integrated domain awareness sufficiently creates advanced warning of solar storms.

Gene H. McCall & Jack Darrah 14. Served as chief scientist, Air Force Space Command; laboratory fellow, Los Alamos National Laboratory; and chairman, USAF Scientific Advisory Board. Adjunct staff member at the Institute for Defense Analysis in D.C. where he supports the commander, US Northern Command; commander, Air Force Space Command; assistant secretary of defense (OSD/C3I); and other DOD and government offices and agencies. “Space Situational Awareness: Difficult, Expensive-And Necessary.” Air & Space Power Journal: Senior Leader Perspective. November–December 2014. <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28_Issue-6/SLP-McCall_Darrah.pdf> //EM

Passive Threats

Passive threats primarily consist of objects such as debris or uncontrolled satellites or rockets. Almost always, the important factor for SSA is location. Since orbital parameters can be derived from location measurements, it is possible to determine which objects could prove dangerous to US space assets and generate warnings at proper times to stimulate defensive actions.

Another set of passive threats, sometimes not included in SSA estimates, are those from high-energy particles and photons. These particles may be generated by natural events such as solar storms or caused by events like nuclear explosions in the atmosphere or in space. In either case, detection by space assets would most effectively determine the characteristics and possible dangers of such threats.

#### Advanced warning solves the catastrophic risks of a probable solar storm---only new integrated SSA can solve.

Ramin Skibba 21. Freelance writer and journalist based in San Diego. “Solar storms can wreak havoc. We need better space weather forecasts.” Science News. 02-26-2021. https://www.sciencenews.org/article/sun-solar-storms-earth-havoc-space-weather-forecasts //EM

Since December 2019, the sun has been moving into a busier part of its cycle, when increasingly intense pulses of energy can shoot out in all directions. Some of these large bursts of charged particles head right toward Earth. Without a good way to anticipate these solar storms, we’re vulnerable. A big one could take out a swath of our communication systems and power grids before we even knew what hit us.

A recent near miss occurred in the summer of 2012. A giant solar storm hurled a radiation-packed blob in Earth’s direction at more than 9 million kilometers per hour. The potentially debilitating burst quickly traversed the nearly 150 million kilometers toward our planet, and would have hit Earth had it come just a week earlier. Scientists learned about it after the fact, only because it struck a NASA satellite designed to watch for this kind of space weather.

That 2012 storm was the most intense researchers have measured since 1859. When a powerful storm hit the Northern Hemisphere in September of that year, people were not so lucky. Many telegraph systems throughout Europe and North America failed, and the electrified lines shocked some telegraph operators. It came to be known as the Carrington Event, named after British astronomer Richard Carrington, who witnessed intensely bright patches of light in the sky and recorded what he saw.

The world has moved way beyond telegraph systems. A Carrington-level impact today would knock out satellites, disrupting GPS, mobile phone networks and internet connections. Banking systems, aviation, trains and traffic signals would take a hit as well. Damaged power grids would take months or more to repair.

To avoid such destruction, in October then-President Donald Trump signed a bill that will support research to produce better space weather forecasts and assess possible impacts, and enable better coordination among agencies like NASA and the National Oceanic and Atmospheric Administration.

“We understand a little bit about how these solar storms form, but we can’t predict [them] well,” says atmospheric and space scientist Aaron Ridley of the University of Michigan in Ann Arbor. Just as scientists know how to map the likely path of tornadoes and hurricanes, Ridley hopes to see the same capabilities for predicting space weather.

The ideal scenario is to get warnings well before a storm disables satellites or makes landfall, and possibly even before the sun sends charged particles in our direction. With advance warning, utilities and governments could power down the grids and move satellites out of harm’s way.

Ridley is part of a U.S. collaboration creating simulations of solar storms to help scientists quickly and accurately forecast where the storms will go, how intense they will be and when they might affect important satellites and power grids on Earth. Considering the havoc an extreme solar storm could wreak, many scientists and governments want to develop better forecasts as soon as possible.

Ebbs and flows

When scientists talk about space weather, they’re usually referring to two things: the solar wind, a constant stream of charged particles flowing away from the sun, and coronal mass ejections, huge outbursts of charged particles, or plasma, blown out from the sun’s outer layers (SN Online: 3/7/19). Some other phenomena, like high-energy particles called cosmic rays, also count as space weather, but they don’t cause much concern.

Coronal mass ejections, or CMEs, the most threatening kind of solar storms, aren’t always harmful — they generate dazzling auroras near the poles, after all. But considering the risks of a storm shutting down key military and commercial satellites or harming the health of astronauts in orbit, it’s understandable that scientists and governments are concerned.

Astronomers have been peering at our solar companion for centuries. In the 17th century, Galileo was among the first to spy sunspots, slightly cooler areas on the sun’s surface with strong magnetic fields that are often a precursor to more intense solar activity. His successors later noticed that sunspots often produce bursts of radiation called solar flares. The complex, shifting magnetic field of the sun also sometimes makes filaments or loops of plasma thousands of kilometers across erupt from the sun’s outer layers. These kinds of solar eruptions can generate CMEs.

“The sun’s magnetic field lines can get complicated and twisted up like taffy in certain regions,” says Mary Hudson, a physicist at Dartmouth College. Those lines can break like a rubber band and launch a big chunk of corona into interplanetary space.

It was 19th century German astronomer Samuel Heinrich Schwabe who realized that such solar activity ebbs and flows during 11-year cycles. This happens because the sun’s magnetic field completely flips every 11 years. The most recent sun cycle ended in December 2019, and we’re emerging from the nadir of sun activity while heading toward the maximum of cycle 25 (astronomers started numbering solar cycles in the 19th century). Solar storms, particularly the dangerous CMEs, are now becoming more frequent and intense, and should peak between 2024 and 2026.

Up and down

The number of sunspots, and other solar activity that generates solar storms, rises and falls in an 11-year cycle. Solar cycle 25 began in December 2019 and is expected to peak in 2025.

Solar storms develop from the sun’s complex magnetic field. The sun rotates faster at its equator than at its poles, and since it’s not a solid sphere, its magnetic field constantly roils and swirls around. At the same time, heat from the sun’s interior rises to the surface, with charged particles bringing new magnetic fields with them. The most intense CMEs usually come from the most vigorous period in a particularly active solar cycle, but there’s a lot of variation. The 1859 CME originated from a fairly modest solar cycle, Hudson points out.

A CME has multiple components. If the CME is on a trajectory toward Earth, the first thing to arrive — just eight minutes after it leaves the sun — is the electromagnetic radiation, which moves at the speed of light. CMEs often produce a shock wave that accelerates protons to extremely fast speeds, and those arrive within 20 minutes of the light. Such energetic particles can damage the electronics or solar cells of satellites in high orbits. Those particles could also harm any astronauts outside of Earth’s protective magnetic field, including any on the moon. A crew on board the International Space Station, inside Earth’s magnetic field, however, would most likely be safe.

But a CME’s biggest threat — its giant cloud of plasma, which can be millions of kilometers wide — typically takes between one and three days to reach our planet, depending on how fast the sun propelled the shotgun blast of particles toward us. Earth’s magnetic field, our first defense against space weather and space radiation, can protect us from only so much. Satellites and ground-based observations have shown that a CME’s charged particles interact with and distort the magnetic field. Those interactions can have two important effects: producing more intense electric currents in the upper atmosphere and shifting these stronger currents away from the poles to places with more people and more infrastructure, Ridley says. With an extremely powerful storm, it’s these potentially massive currents that put satellites and power grids at risk.

Anyone who depends on long-distance radio signals or telecommunications might have to do without them until the storm blows over and damaged satellites are repaired or replaced. A powerful storm can disturb airplanes in flight, too, as pilots lose contact with air traffic controllers. While these are temporary effects, typically lasting up to a day, impacts on the electrical grids could be worse.

A massive CME could suddenly and unexpectedly drive currents of kiloamps rather than the usual amps through power grid wires on Earth, overwhelming transformers and making them melt or explode. The entire province of Quebec, with nearly 7 million people, suffered a power blackout that lasted more than nine hours on March 13, 1989, thanks to such a CME during a particularly active solar cycle. The CME affected New England and New York, too. Had electricity grid operators known what was coming, they could have reduced power flow on lines and interconnections in the power grid and set up backup generators where needed.

Early warning

But planners need more of a heads-up than they get today. Perhaps within the next decade, improved computer modeling and new space weather monitoring capabilities will enable scientists to predict solar storms and their likely impacts more accurately and earlier, says physicist Thomas Berger, executive director of the Space Weather Technology, Research and Education Center at the University of Colorado Boulder.

Space meteorologists classify solar storms, based on disturbances to the Earth’s magnetic field, on a five-level scale, like hurricanes. But unlike those tropical storms, the likely arrival of a solar storm isn’t known with any precision using available satellites. For storms brewing on Earth, the National Weather Service has access to constantly updated data. But space weather data are too sparse to be very useful, with few storms to monitor and provide data.

Two U.S. satellites that monitor space weather are NASA’s ACE spacecraft, which dates from the 1990s and should continue to collect data for a few more years, and NOAA’s DSCOVR, which was designed at a similar time but not launched until 2015. Both orbit about 1.5 million kilometers above Earth — which seems far but is barely upstream of our planet from a solar storm’s perspective. The two satellites can detect and measure a solar storm only when its impact is imminent: 15 to 45 minutes away. That’s more akin to “nowcasting” than forecasting, offering little more than a warning to brace for impact.

#### Extinction.

Ilan Noy & Tomáš Uher 22, Chair, Economics of Disasters, Victoria University of Wellington. Professor, Economics, Victoria University of Wellington; Research Fellow, Economics & Finance, Victoria University of Wellington, "Four New Horsemen of An Apocalypse? Solar Flares, Super-Volcanoes, Pandemics, And Artificial Intelligence," Economics of Disasters & Climate Change, 01/15/2022, Springer.

Active regions on the surface of the sun can produce solar flares, which are jets of solar energy and coronal mass ejections (sudden release of plasma accompanied by a magnetic field) (Kahler 1992). These phenomena are produced when local regions of the sun's magnetic field suddenly change configuration (Knipp and Biesecker 2015) and are typically interconnected, occurring within a relatively short period of time. The resulting electromagnetic radiation can create disruptions of the Earth's magnetic field (termed geomagnetic storms), commonly known as “space weather events” (Schwenn 2006).

The most important implication of these events is in terms of disruptions to electricity-powered technology. Due to the global economy’s increasing reliance on such technologies, it has grown increasingly more vulnerable to the impacts of space weather.Footnote1 An extended power outage that lasts for weeks or months, affecting a large population (potentially tens of millions), can easily become a major catastrophe, and even a systemic threat to society.

Societal Impacts of Severe Space Weather and Solar Flares

Space weather events have been associated with a multitude of negative, mainly technological, direct economic consequences such as blocked radio communications, satellite damage and malfunctions, disruption to rail networks and wireless networks, and global navigation systems such as GPS (Cannon et al. 2013; Eroshenko et al. 2010). However, the most consequential possible effect is extensive damage to electricity transformers and therefore potentially long-term disruption to the electricity transmission infrastructure (Khurshid et al. 2020; Kappenman 2012). Such a disruption would cause severe problems with the supply of many basic services, including the access to pumped potable water, and the loss of all perishable foods and medications that depend on refrigeration (National Research Council 2009; Kappenman 2012).

The observed history of space weather in modern economies is very limited. The biggest geomagnetic storm of the last few decades happened in 1989 and caused transformer damage in multiple countries and an approximately 9 h-long power outages for over 6 million inhabitants of Quebec (Lakhina et al. 2004; Barnes and Van Dyke 1990).

The most severe directly observed events were the storms of 1859 (the Carrington Event) and 1921, which were roughly three times as powerful as the 1989 event and are typically considered to be a 1 in a 100-year events (Kappenman 2010). However, since economies at the time were not so dependent on electricity (especially, of course, in 1859), the impact of both these events was much less severe than the impacts of the 1989 event and consisted mostly of disruption to the telegraph service (Boteler 2006).

While these historical events are associated only with relatively mild societal impacts, a similar event today would have severe global consequences. Many of the studies attempting to analyse the future potential impacts of such an event focus on the economic effects associated with major power outages. A study by Kappenman (2010) estimates that a Carrington storm hitting the United States could put more than 200 large power transformers at risk of permanent damage and cause severe damages to the power grid, leading to long-lasting (months or potentially years) blackouts for approximately 130 million people in the US and a full recovery time of 4–10 years. The total cost of a long-term power outage affecting a significant area is estimated at USD 1–2 trillion during the first year (National Research Council 2009).

In a report for Lloyd’s, Maynard et al. (2013) points out that the duration of the power outage depends largely on the availability of spare transformers. These authors estimate that, in the worst-case scenario of no spare transformers, a Carrington-like event would lead to a power outage in the US affecting 20–40 million people and lasting 5 months. They estimate an associated economic loss of USD 0.5–2.6 trillion.Footnote2

Moran et al. (2014) analyse the economic impacts of space weather from a global perspective and conclude that “a severe space-weather event could be the worst natural disaster in modern history” (p. 8). Assuming a power outage lasting 1 year for an event of a magnitude between the 1989 storm and the Carrington event (with annual probability of occurrence likely to be higher than 1%), the authors conclude a major disruption of global supply chains affecting all industries and estimate a global economic loss of up to USD 3.4 trillion (5.6% of global GDP) in the first year.

Oughton et al. (2016) find that an extended power outage in the US caused by a similar space weather event would lead to global economic losses with respect to global supply chain disruptions valued at USD 0.5–2.7 trillion. Using a globally integrated economic model to account for the post-event dynamic responses of global trade, they estimate a decrease of global GDP by up to USD 1.1 trillion over a five-year period. The economic loss to the US manufacturing industry is estimated to be USD 350 billion with approximately half of the losses being indirect (roughly equally split between the losses associated with upstream and downstream disruptions to the supply chain). The losses to the US insurance industry are estimated to be up to USD 334 billion, with 90% of the losses caused by service interruption within property insurance policies.

In another paper, Oughton et al. (2017) suggest that a severe geomagnetic storm, causing a power outage for 66% of the population in the US, would create a daily economic loss of USD 41.5 billion. Approximately half of the total economic loss is estimated to be inflicted indirectly outside of the blackout zone due to supply chain disruptions; Moran et al. (2014) reach similar conclusion for the global economy.

Oughton et al. (2019) estimate an economic impact of a significant geomagnetically-induced power grid failure in the UK and distinguish between scenarios in terms of the ability to forecast the event. They find that a 1 in a 100-year event with the current level of forecasting would cause a GDP loss of GBP 2.9 billion in the UK, but an enhanced forecasting ability based on further investment in this technology would bring the loss down significantly, to GBP 0.9 billion.

In all these modelling exercises, power outages for a significant portion of the population are assumed to lead to cascading effects over many sectors. National Research Council (2009) emphasised banking and finance, government services and emergency response. Eventually, however, all economic sectors would be adversely affected (Moran et al. 2014; Riley et al. 2018). Apart from the sectoral vulnerability to power outages due to the reliance on electricity, Moran et al. (2014) note that the global economic production system today is made even more vulnerable due to the common use of practices such as just-in-time production, reduced inventories, and increased reliance on long-distance supply chains with many links.

More difficult to model, but maybe not less important to evaluate, is the public response to such an event. Hapgood et al. (2021) suggest that a power grid disruption caused by a severe space weather event would lead to panic buying and stockpiling of essential goods such as petrol, bottled water, non-perishable foods, and toilet paper. There could be various flow-on effects from this panic. Ultimately, the longer-term economic consequences of that are unclear.

It is uncontroversial that an extended power outage for a significant portion of the population would lead to disastrous economic impacts. However, the potential of space weather events of the magnitudes discussed above to cause such extended power outages are questioned by studies such as NERC (2010, 2012) and Cannon et al. (2013). They argue that extensive power grid hardware damage is unlikely, and the more probable consequence is a temporary system collapse due to voltage instability. In their view, this will result in only short-term stoppages in electricity supply and thus modest economic consequences.

Superflares

Research focusing on the risk of even more severe space weather events is scarce, partially because there have so far been no direct observations of “superflares” in our solar system. Some evidence suggests that a superflare 100 times stronger than the Carrington event may have happened in AD 775 (Melott and Thomas 2012; Usoskin et al. 2013; Mekhaldi et al. 2015) and may have led to regional changes in the Earth’s surface temperature (Sukhodolov et al. 2017). The nature of this AD 775 event, however, is inconclusive (Cliver et al. 2014; Stephenson 2015; Neuhäuser and Neuhäuser 2015). Another extremely powerful event possibly happened in AD 993 (Miyake et al. 2013; Mekhaldi et al. 2015). Furthermore, astronomical observations of other sun-like stars in our galaxy suggest that such events are indeed possible (Maehara et al. 2012; Nogami et al. 2014).

Lingam and Loeb (2017a) propose that the most powerful superflares might have been the cause of some of the previous mass extinction events and that a very rare superflare with energy 100,000 times larger than the Carrington event might be able to destroy the ozone layer and lead to widespread destruction of ecosystems with potentially existential consequences. In a follow-up paper, Lingam and Loeb (2017b) suggest that the societal vulnerability to superflares in terms of economic damage is increasing rapidly, due to the growth of technological infrastructure. They propose a mitigation strategy of setting up a protective shield between the Earth and the Sun to avoid these dire consequences.

#### Space weather threats are underestimated---risks extinction.

Rosen ’16 [Julia; July 14; Ph.D. and science reporter for the Los Angeles Times; Science Mag, “Here’s how the world could end—and what we can do about it,” <https://www.sciencemag.org/news/2016/07/here-s-how-world-could-end-and-what-we-can-do-about-it>]

As end-of-humanity scenarios go, that bleak vision from Fritz Leiber’s 1951 short story “A Pail of Air” is a fairly remote possibility. Scholars who ponder such things think a self-induced catastrophe such as nuclear war or a bioengineered pandemic is most likely to do us in. However, a number of other extreme natural hazards—including threats from space and geologic upheavals here on Earth—could still derail life as we know it, unraveling advanced civilization, wiping out billions of people, or potentially even exterminating our species.

Yet there’s been surprisingly little research on the subject, says Anders Sandberg, a catastrophe researcher at the University of Oxford’s Future of Humanity Institute in the United Kingdom. Last he checked, “there are more papers about dung beetle reproduction than human extinction,” he says. “We might have our priorities slightly wrong.”

Frequent, moderately severe disasters such as earthquakes attract far more funding than low-probability apocalyptic ones. Prejudice may also be at work; for instance, scientists who pioneered studies of asteroid and comet impacts complained about confronting a pervasive “giggle factor.” Consciously or unconsciously, Sandberg says, many researchers consider catastrophic risks the province of fiction or fantasy—not serious science.

A handful of researchers, however, persist in thinking the unthinkable. With enough knowledge and proper planning, they say, it’s possible to prepare for—or in some cases prevent—rare but devastating natural disasters. Giggle all you want, but the survival of human civilization could be at stake.

Threat one: Solar storms

One threat to civilization could come not from too little sun, as in Leiber’s story, but from too much. Bill Murtagh has seen how it might start. On the morning of 23 July 2012, he sat before a colorful array of screens at the National Oceanic and Atmospheric Administration’s Space Weather Prediction Center in Boulder, Colorado, watching twin clouds of energetic particles—known as a coronal mass ejection (CME)—erupt from the sun and barrel into space. A mere 19 hours later, the solar buckshot blazed past the spot where Earth had been just days before. If it had hit us, scientists say, we might still be reeling.

Now the assistant director of space weather at the White House Office of Science and Technology Policy in Washington, D.C., Murtagh spends much of his time pondering solar eruptions. CMEs don’t harm human beings directly, and their effects can be spectacular. By funneling charged particles into Earth’s magnetic field, they can trigger geomagnetic storms that ignite dazzling auroral displays. But those storms can also induce dangerous electrical currents in long-distance power lines. The currents last only a few minutes, but they can take out electrical grids by destroying high-voltage transformers—particularly at high latitudes, where Earth’s magnetic field lines converge as they arc toward the surface.

The worst CME event in recent history struck in 1989, frying a transformer in New Jersey and leaving 6 million people in Quebec province in Canada without power. The largest one on record—the Carrington Event of 1859, named after the U.K. astronomer who witnessed the accompanying solar flare—was up to 10 times more intense. It sent searing currents racing through telegraph cables, sparking fires and shocking operators, while the northern lights danced as far south as Cuba.

“It was awesome,” says Patricia Reiff, a space physicist at Rice University in Houston, Texas. But if another storm that size struck today’s infrastructure, she says, “there would be tremendous consequences.”

Some researchers fear that another Carrington-like event could destroy tens to hundreds of transformers, plunging vast portions of entire continents into the dark for weeks or months—perhaps even years, Murtagh says. That’s because the custom-built, house-sized replacement transformers can’t be bought off the shelf. Transformer manufacturers maintain that such fears are overblown and that most equipment would survive. But Thomas Overbye, an electrical engineer at the University of Illinois, Urbana-Champaign, says nobody knows for sure. “We don’t have a lot of data associated with large storms because they are very rare,” he says.

What’s clear is that widespread blackouts could be catastrophic, especially in countries that depend on highly developed electrical grids. “We’ve done a marvelous job creating a great vulnerability to this threat,” Murtagh says. Information technologies, fuel pipelines, water pumps, ATMs, everything with a plug would be rendered useless. “That’s going to affect our ability to govern the country,” Murtagh says.

#### Independently, a perfected TCBM controls responses to every risk.

José Monserrat Filho 15. Head of the international Affairs Office of the Ministry of Science and Technology Brazil, Vice President of the Brazilian Association of Air and Space Law, an honorary board member of the International institute of Space Law, member of the Space Law Committee of the International Law Association as well as the International Academy of Astronautics, Professor at the Hague Academy of International Law. 2015. “Earth in Danger and Space Law.” Proceedings of the International Institute of Space Law, edited by Rafael Moro-Aguilar et al., vol. 2015, Eleven International Publishing, pp. 657–674.

We live in “a time of profound transformations to our global context,” stressed Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, during the presentation of the Global Risks Report 2015,4 in Davos, Switzerland. For him, mankind faces the accelerated effects of climate change and the increasing uncertainty about the global geopolitical context. Going further, the Bulletin of the Atomic Scientists Science and Security Board, in a recent analysis, pointed out that “ in 2015, unchecked climate change, global nuclear weapons modernization, and out-sized nuclear weapons arsenals pose extraordinary and undeniable threats to the continued existence of humanity.”5 That led its Doomsday Clock to be advanced by two minutes. Today it marks three minutes to midnight, the moment of the Earth's collapse.

There are many other reports and studies alerting to this catastrophe. Such an immeasurable disaster on Earth may affect all space activities, and their legal achievements. While focusing on outer space and space activities, international space law can be considered not only a probable victim of this disaster, but also an important instrument capable of preventing it. The fundamental 1967 Outer Space Treaty,6 as its Preamble points out, is inspired “ by the great prospects opening up for humanity as a result of man’s entry into outer space” and recognizes “ the common interest of all mankind in the progress of exploration and use of outer space for peaceful purposes.”

This obviously means that the fate of humanity is in the core of its attention. This paper attempts to demonstrate the ability and the need for international space law to face the critical situation of the Earth in extreme danger, including the legal examination and the use of juridical provisions presented in the recommendations of the main scientific documents already drawn up on this transcendental subject. In conclusion, some viable initiatives in the space law field are proposed as contributions to efforts to provide Earth with new guarantees of survival.

I. The Preventive Function of Law

The paper’s proposals raise the opportunity and the need to expand the scope and the objectives of international space law, including in it specific space issues of the Earth and of its life expressions. Furthermore, it is timely to underline that “ in today’s world, the preventive function of law is more vital than ever,” as observed Manfred Lachs (1914-1993) about 28 years ago. For him, it would be necessary for men around the world to feel this reality, “ in order to incite them to abandon something of the parish spirit and give them the feeling of the existence of a common interest, and of responsibility in application of law in the everyday life of nations, as well as to make them understand that, as usually is said, it is worth more act wisely together than commit follies separately,” At the same time, as a notable jurist and thinker, Lachs foresaw the dangers that the Earth is currently experiencing: “Today, it is required to work at a time when science and technology have placed in man’s hands weapons capable of creating a danger to life and even cause total destruction; when modern techniques create other dangers threatening the earth, water and air; when economic and political relations between the states require that a new order abolishes abyss between rich and hungry [...]” .7 If the world already was in great danger in the 1980s, what could be the magnitude of danger today?

II, Poly-Catastrophe

“Dark times [...] are not only not new, they are not a rarity in history,” as Hannah Arendt (1906-1975) observed.8 But today we are certainly living in often darker times. According to the Global Solidarity, Global Responsibility: An Appeal for World Governance - launched in Geneva, Switzerland, on 6 March 2012, and endorsed by the Collegium International members

"we are facing a conjunction of global crises that are unprecedented in history: depletion of natural resources, irreversible destruction of biodiversity, disruption of the global financial system, dehumanization of the international economic system, hunger and food shortages, viral pandemics and breakdown of political orders [...] none of these phenomena can be considered independently of the others. All are highly interconnected, constituting a single ‘poly-crisis’ that threatens the world with a ‘poly-catastrophe’ [...]”

The Appeal stresses that “ the great crises of the 21st century are planetary,” and that “ this is no butterfly effect, but the realization, grave and strong, that our common home is in danger of collapsing and that our salvation can only be collective.”9

III. Our World Today

The new Global Sustainable Development Goals - Transforming our World: the 2030 Agenda for Sustainable Development10 - have been adopted by Heads of State and Government and High Representatives, during the meeting at the United Nations (UN) Headquarters in New York from 25-27 September 2015 - with the UN celebrating its 70th anniversary. Paragraph 14 of this historic document presents the vision of the UN General Assembly (UNGA) on the world global situation today, as follows: “We are meeting at a time of immense challenges to sustainable development. Billions of our citizens continue to live in poverty and are denied a life of dignity. There are rising inequalities within and among countries. There are enormous disparities of opportunity, wealth and power. Gender inequality remains a key challenge. Unemployment, particularly youth unemployment, is a major concern. Global health threats, more frequent and intense natural disasters, spiraling conflict, violent extremism, terrorism and related humanitarian crises and forced displacement of people threaten to reverse much of the development progress made in recent decades. Natural resource depletion and adverse impacts of environmental degradation, including desertification, drought, land degradation, freshwater scarcity and loss of biodiversity, add to and exacerbate the list of challenges which humanity faces. Climate change is one of the greatest challenges of our time and its adverse impacts undermine the ability of all countries to achieve sustainable development. Increases in global temperature, sea level rise, ocean acidification and other climate change impacts are seriously affecting coastal areas and low-lying coastal countries, including many least developed countries and small island developing States. The survival of many societies, and of the biological support systems of the planet, are at risk.”

“ Climate change will amplify existing risks and create new risks for natural and human systems. Risks are unevenly distributed and are generally greater for disadvantaged people and communities in countries at all levels of development,” as Intergovernmental Panel on Climate Change (IPCC) says in Climate Change 2014 - Synthesis Report - Summary for Policymakers.11

IV. Care for Our Common Home

Pope Francis in his 2015 Encyclical Letter Laudato Si ~ On Care for Our Common Home - issued in 25 May - makes an “ urgent appeal for a new dialogue about how we are shaping the future of our planet.” According to Pope, “we require a new and universal solidarity,” as “ our present situation is in many ways unprecedented in the history of humanity.”

“ The Earth, our home,” - he stresses - “ is beginning to look more and more like an immense pile of filth,” because “ each year hundreds of millions of tons of waste are generated, much of it non-biodegradable, highly toxic and radioactive, from homes and businesses, from construction and demolition sites, from clinical, electronic and industrial sources.”

Pope Francis also warns:

“A very solid scientific consensus indicates that we are presently witnessing a disturbing warming of the climatic system [...} most of global warming in recent decades is due to the great concentration of greenhouse gases (carbon dioxide, methane, nitrogen oxides and others) released mainly as a result of human activity [...] The problem is aggravated by a model of development based on the intensive use of fossil fuels, which is at the heart of the worldwide energy system. Another determining factor has been an increase in changed uses of the soil, principally deforestation for agricultural purposes.”

“Warming has effects on the carbon cycle. It creates a vicious circle which aggravates the situation even more, affecting the availability of essential resources like drinking water, energy and agricultural production in warmer regions, and leading to the extinction of part of the planet’s biodiversity. If present trends continue, this century may well witness extraordinary climate change and an unprecedented destruction of ecosystems, with serious consequences for all of us,” as “ climate change is a global problem with grave implications: environmental, social, economic, political and for the distribution of goods.”

Moreover, Pope Francis remarks:

“We all know that it is not possible to sustain the present level of consumption in developed countries and wealthier sectors of society, where the habit of wasting and discarding has reached unprecedented levels. The exploitation of the planet has already exceeded acceptable limits and we still have not solved the problem of poverty. ”

“Caring for ecosystems demands far-sightedness, since no one looking for quick and easy profit is truly interested in their preservation. But the cost of the damage caused by such selfish lack of concern is much greater than the economic benefits to be obtained,” points out Pope Francis, And he adds that “ the alliance between the economy and technology ends up sidelining anything unrelated to its immediate interests.”

“The failure of global summits on the environment makes it plain that our politics are subject to technology and finance. There are too many special interests, and economic interests easily end up trumping the common good and manipulating information so that their own plans will not be affected.”

“ It is foreseeable that, once certain resources have been depleted, the scene will be set for new wars, albeit under the guise of noble claims. War always does grave harm to the environment and to the cultural riches of peoples, risks which are magnified when one considers nuclear arms and biological weapons [...] Politics must pay greater attention to foreseeing new conflicts and addressing the causes which can lead to them. But powerful financial interests prove most resistant to this effort, and political planning tends to lack breadth of vision.” 52

Wouldn’t these observations also applicable to outer space?

V. The Tragedy f Common Goods

To explain how we arrived to it at current bad situation of the common resources of Earth, Eduardo Felipe P. Matias recalls the article Tragedy of Common Goods, written in 1968 by American ecologist Garrett Hardin (1915-2003). Hardin recounts the case of a village of shepherds, whose sheep used a pasture in common. Each shepherd was engaged in putting more and more sheep in the pasture in order to increase his income. Over time, the pasture was saturated, and there was no pasture left to feed all the sheep. Most of them died. In sum, a tragedy. The shepherds abused the common good to increase their individual gains, ignoring the limits of nature. Although they gained more in short term, they lost out in long run. Already in 1999, it was recognized that “ a globalized world requires a theory of global public goods to achieve crucial goals such as financial stability, human security or the reduction of environmental pollution.” And that “many of today’s international crises have their roots in a serious under supply of global public goods.” 13

As to global human security as a public good, the 1994 Human Development Report has showed threats to world peace in transborder challenges: unchecked population growth, disparities in economic opportunities, environmental degradation, excessive international migration, narcotics production and trafficking and international terrorism,” It was equally said that the society would be “willing to pay for public goods that serve our common interest, be they shared systems of environmental controls, the destruction of nuclear weapons, the control of transmittable diseases such as malaria and HIV/AIDS, the preservation of ethnic conflicts or the reduction of refugee flows,” 14

Addressing the present question of common goods in his 2015 Encyclical Letter, Pope Francis points out:

“Whether believers or not, we are agreed today that the Earth is essentially a shared inheritance, whose fruits are meant to benefit everyone. Hence every ecological approach needs to incorporate a social perspective which takes into account the fundamental rights of the poor and the underprivileged. The principle of the subordination of private property to the universal destination of goods, and thus the right of everyone to their use, is a golden rule of social conduct He also notes that “ the natural environment is a collective good, the patrimony of all humanity and the responsibility of everyone. If we make something our own, it is only to administer it for the good of all. If we do not, we burden our consciences with the weight of having denied the existence of others.”

Antonio Cassese (1937-2011) commented that “ the concept of ‘common good’ is not yet felt by the members of the international society. Only state interests and their occasional convergence regulate international relations.” 15 The refugees tragedy in Europe today proves it.

VI. Uncertainty

According to Klaus Schwab, Executive Chairman of World Economic Forum, “ in the coming decade [...] our lives will be even more intensely shaped by transformative forces that are under way already. The effects of climate change are accelerating and the uncertainty about the global geopolitical context and the effects it will have on international collaboration will remain. At the same time, societies are increasingly under pressure from economic, political and social developments including rising income inequality, but also increasing national sentiment [...] [N]ew technologies, such as the Internet or emerging innovations will not bear fruit if regulatory mechanisms at the international and national levels cannot be agreed upon.”

The Global Risks Report 2015, in turn, stresses: “ 2015 differs markedly from the past, with rising technological risks, notably cyber-attacks, and new economic realities, which remind us that geopolitical tensions present themselves in a very different world from before. Information flows instantly around the globe and emerging technologies have boosted the influence of new players and new types of warfare [...] Past warnings of potential environmental catastrophes have begun to be borne out, yet insufficient progress has been made - as reflected in the high concerns about failure of climate-change adaptation and looming water crises in this year’s report.”

The Report sees three risk constellations that bear out its findings:

“ 1) The interconnections between geopolitics and economics are intensifying because States are making greater use of economic tools, from regional integration and trade treaties to protectionist policies and cross-border investments, to establish relative geopolitical power. This threatens to undermine the logic of global economic cooperation and potentially the entire international rulebased system;

2) The world is in the middle of a major transition from predominantly rural to urban living, with cities growing most rapidly in Asia and Africa. If managed well, this will help to incubate innovation and drive economic growth. However, our ability to address a range of global risks - including climate change, pandemics, social unrest, cyber threats and infrastructure development - will largely be determined by how well cities are governed; and

3) The pace of technological change is faster than ever. Disciplines such as synthetic biology and artificial intelligence are creating new fundamental capabilities, which offer tremendous potential for solving the world’s most pressing problems. At the same time, they present hard-to-foresee risks. Oversight mechanisms need to more effectively balance likely benefits and commercial demands with a deeper consideration of ethical questions and medium to long-term risks - ranging from economic to environmental and societal. Mitigating, preparing for and building resilience against global risks is long and complex, something often recognized in theory but difficult in practice.”

How to govern the emerging technologies and uncertainties?

VII. The Doomsday Clock

It is a symbolic clock face, marking countdown to doomsday. On 19 January 2015, it went on to score 23:57h, three minutes to midnight - the time of global catastrophe able to extinguish the human species inhabiting the Earth for many thousands of years. The decision to advance the clock by two minutes was taken after consultations with more than 20 scientists, including 17 Nobel laureates, among them famous physicists, such as the British Stephen Hawking, the Japanese Masatoshi Koshiba, pioneer in the study of neutrinos, and the American Leon Lederman. The clock has been maintained since 1947 - when the Cold War between the USA and the former USSR began - by the members of the Bulletin of the Atomic Scientists Science and Security Board. In 68 years, this sui generis indicator has been adjusted 22 times. Its worst moment came in 1953, triggered by American and Soviet tests with hydrogen weapons when the Clock scored 23:58h.

The Clock was conceived by the celebrated Chicago Atomic Scientists, that had actively participated in the Manhattan Project in the creation of the atomic bombs launched over Hiroshima and Nagasaki, Japan, in August 1945. Haunted with these bombings - that killed more than 100,000 people just on the first day, and many more in the following months - they started to publish a mimeographed warning newsletter and then the Bulletin. The closer they set the Clock to midnight, the closer the scientists believe the world is to a global disaster.

The Clock hangs on a wall in a Bulletin's office in the University of Chicago. Originally, it represented an analogy to the threat of global nuclear war. But since 2007 it has also reflected climate change, and new developments in the life sciences and technology that could inflict irrevocable harm to humanity.

The analysis of the Bulletin - addressed “to the leaders and citizens of the world” - says in sum: “ In 2015, unchecked climate change, global nuclear weapons modernizations, and out-sized nuclear weapons arsenals pose extraordinary and undeniable threats to the continued existence of humanity.” The group said in a statement: “ [Wjorld leaders have failed to act with the speed or on the scale required to protect citizens from potential catastrophe. These failures of political leadership endanger every person on Earth.” In 2014, with the Doomsday Clock at five minutes to midnight, the members of the Science and Security Board concluded their assessment of the world security situation by writing: “We can manage our technology, or become victims of it. The choice is ours, and the Clock is ticking.”

In 2015, with the Clock hand moved forward to three minutes to midnight, the Bulletin feels compelled to add, with a sense of great urgency: “The probability of global catastrophe is very high, and the actions needed to reduce the risks of disaster must be taken very soon.”

In face of the dangers affecting today civilization on a global scale, the Bulletin urges the citizens of the world to demand that their leaders, among other measures, "dramatically reduce proposed spending on nuclear weapons modernization programs” , as “ the USA and Russia have hatched plans to essentially rebuild their entire nuclear triads in coming decades, and other countries with nuclear weapons are following suit.”

At the start of 2015, nine States - the USA, Russia, the United Kingdom, France, China, India, Pakistan, Israel and Democratic People’s Republic of Korea (North Korea) - possessed about 15,850 nuclear weapons, of which 4,300 were deployed with operational forces. Roughly 1800 of these weapons are kept in a state of high operational alert, according to the Stockholm International Peace Research Institute (SIPRI). Launched on 15 June 2015, the SIPRI Yearbook 2015, which assesses the current state of armament, disarmament and international security, notes as one of its key findings that “ all the nuclear weapon-possessing states are working to develop new nuclear weapon systems and/or upgrade their existing ones.” 16

“There are too many nuclear weapons,” said Sharon Squassoni, an expert in nuclear weapons nonproliferation at the Center for Strategic and International Studies in Washington, USA. And she added: “The existence of these weapons takes a lot of time, effort, and money to keep them safe, and the bureaucracies are poised to keep these systems going indefinitely.” 17

For Hans M Kristensen, director of the Nuclear Information Project at the Federation of American Scientists, “ the projected costs of the nuclear weapons modernization program are indefensible, and they undermine the global disarmament regime.” 18

That is why another demand from Bulletin, addressed to world leaders, is to “ re-energize the disarmament process.” In practice it means that “ the USA and Russia, in particular, need to start negotiations on shrinking their strategic and tactical nuclear arsenals.”

The creation of “ institutions specifically assigned to explore and address potentially catastrophic misuses of new technologies,” is also a requirement proposed by the Bulletin.

The Bulletin’s appeals are also, to some extent, applicable to outer space, and some of its requirements can be objects of proper regulation by international space law.

VIII. Transparency and Confidence

The Earth being in danger, the transparency and confidence-building measures (TCBMs) are as vital as those of collective security. These actions are means by which Governments can share information aiming at creating mutual understanding and trust, reducing misconceptions and miscalculations and thereby helping both to prevent military confrontation and to foster regional and global stability. They played an important role during the Cold War, contributing to reducing the risk of armed conflict through mitigating misunderstandings on military actions, particularly in situations where States lacked clear and timely information.19 The need for such measures in outer space activities has increased significantly over the past 20 years, The world’s growing dependence on space-based systems and technologies and the information they provide requires collaborative efforts to address threats to the sustainability and security of outer space activities. TCBMs “ can reduce, or even eliminate, misunderstandings, mistrust and miscalculations with regard to the activities and intentions of States in outer space” , This is the conclusion of the Report of the Group of Governmental Experts on TCBMs in Outer Space Activities - a study adopted by consensus and issued on 29 July 2013.20

The Report adds that “ these measures can augment the safety, sustainability and security of day-to-day space operations and can contribute both to the development of mutual understanding and to the strengthening of friendly relations between States and peoples.”

It is acknowledged that “ the existing treaties on outer space contain several TCBMs of a mandatory nature. Non-legally binding measures for outer space activities should complement the existing international legal framework on space activities and should not undermine existing legal obligations or ham per the lawful use of outer space, particularly by emerging space actors.” The Group also discussed other measures, including those of a legally binding nature. The Group further agreed that “ such measures for outer space activities could contribute to, but not act as a substitute for, measures to monitor the implementation of arms limitation and disarmament agreements,” help States to enhance clarity of their peaceful intentions and create conditions for establishing a predictable strategic situation in both the economic and security arenas.

Similarly, included in the Report were "coordination and consultative mechanisms aimed at improving interaction between participants in outer space activities and clarifying information and ambiguous situations.” Likewise the Report recommended a coordination between the Office for Disarmament Affairs, the Office for Outer Space Affairs (OOSA) and other appropriate UN entities. Moreover, the Report drafted “ a series of measures for outer space activities, including exchange of information relating to national space policy such as major military expenditure in outer space, notifications of outer space activities aimed at risk reduction, and visits to space launch sites and facilities.”

The Group took note of the “Guidelines for appropriate types of confidencebuilding measures and for the implementation of such measures on a global or regional level” , as contained in the “ Study on the application of confidence- building measures in outer space”21

TCBMs for outer space activities are integrated in a broader context. The UN General Assembly endorsed, in its resolution 43/78 H, the guidelines on confidence- building measures adopted by the Disarmament Commission at its 1988 session. This resolution noted that “ confidence-building measures, while neither a substitute nor a precondition for arms limitation and disarmament measures, can be conducive to achieving progress in disarmament” .

The Report indicates the following categories of TCBMs for space activities as relevant: “ a) General transparency and confidence-building measures aimed at enhancing the availability of information on the space policy of States involved in outer space activities; b) Information exchange about development programs for new space systems, as well as information about operational space-based systems providing widely used services such as meteorological observations or global positioning, navigation and timing; c) The articulation of a State’s principles and goals relating to their exploration and use of outer space for peaceful purposes; d) Specific information-exchange measures aimed at expanding the availability of information on objects in outer space and their general function, particularly those objects in Earth orbits; e) Measures related to establishing norms of behavior for promoting spaceflight safety such as launch notifications and consultations that aim at avoiding potentially harmful interference, limiting orbital debris and mini mizing the risk of collisions with other space objects; f) International cooperation measures in outer space activities, including measures aimed at promoting capacity-building and disseminating data for sustainable economic and social development, that are consistent with existing international commitments and obligations.

In fact, some TCBMs for outer space activities have already been enacted at the multilateral and/or the national level. They include pre-launch notifications, space situational awareness data-sharing, notifications of hazards to spaceflight safety and other significant events, and the publication of national space policies. But they need to be further developed.

IX. Common Law of Mankind and Earth

More than ever, it is time to think big. International space law is usually defined as dealing with outer space, celestial bodies - Moon and asteroids, Mars and other planets as well as with the space activities which so far are carried out only by the human species from the planet Earth, However, the very specific situation of Earth as celestial body responsible for the creation and development of the international space law is not taken into the due consideration. Earth is not recognized as one of the main objectives of this branch of law.

Ironically, in this context, we could say that the international space law takes care of the solar system and the universe as a whole, minus of Earth, although it is the cradle of the exploration and use of outer space in general, and, therefore, of international space law.

Let’s take just two examples. “At its broadest, space law comprises all the law that may govern or apply to outer space and activities in and relating to outer space,” write Francis Lyall and Paul B. Larsen.22 In the same sense, the Education Curriculum of Space Law, adopted by United Nations Office For Outer Space Affairs (UNOOSA), on March, 2014, states that “ space law can be described as the body of law applicable to and governing space related activities.”23

Nevertheless, the Outer Space Treaty, of 1967, has, at least, two extremely important norms for the security of Earth and its inhabitants in Articles IV and IX, respectively: 1) “not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction,” and 2) to avoid “harmful contamination and adverse changes in the environment of the Earth resulting from introduction of extraterrestrial matter.” The sky always has played a crucial role in the evolution of mankind and all life manifestations on Earth. However, today the importance of outer space to our planet and its common life has increased as never before. The data coming from satellites are absolutely fundamental for any efforts to assure the sustainability of Earth and all its life expressions. In this global reality it is sheer recklessness to ignore the imperative of protecting our planet and its population, based on inclusive international space legislation. Hence the necessity of a Common Law of Mankind24 and Earth, specially related with international space law.

More and more, outer space protection25 must be seen as an indispensable factor to Earth protection, and vice-verse. As the globalization of Earth - with the interdependence of physical, social and political events - is more than ever recognized as an undeniable fact, the universalization of outer space {its cosmic reach), with the interconnection of everything with everything, cannot be bypassed, as it has been in the past. As Ervin Laszlo remarks, “ the reality we call universe is a seamless whole, evolving over eons of cosmic time and producing conditions where life, and then mind and consciousness can emerge.”26 Or, as Edgar Morin says, “we carry inside of us all the cosmos” and “we are all children of the sun.”27

X. It Is up to International Space Law

If we are really determined to avoid a likely apocalypse visible on the horizon, one of the main tasks of the international space law that we must trigger is to help save the Earth from space, using the powerful scientific and technological resources we have installed there.

Centuries ago Earth ceased to be the center of the universe, as our ancestors thought. But in face of unprecedented global dangers that threaten our planet today, its place cannot be other than the center of our universal concerns. Probably, a collapse of Earth would deprive the universe of a specie of intelligent life.

In reality, as Jonathan Schell (1943-2014) pointed out, “ the vision that counts is the view from Earth, from life,” as “ from our strategic position on Earth different view opens, bigger even than the one taken from space. It is the vision of our children and grandchildren, of all future generations of mankind, stretching ahead of us into the future.”28

The question, as posed by Antonio Cassese, is that “ international society is still grounded in the mere juxtaposition of its subjects - not in their solidarity, let alone in their integration.” 29

In any event, “ from the microbes inhabiting the earth beneath our feet to environments of the universe unknown to us now, the next 100 years of ecological discoveries will influence our lives. We enter a time when society is armed with the scientific knowledge and ability to make responsible decisions,” as a recent editorial of Science affirms.30 And with “ a new human consciousness ” , as says Edgar Morin.31

So, “ the choice is our: form a global partnership to care for Earth and one another or risk the destruction of ourselves and the diversity of life,” according to The Earth Charter.32

The current global situation seems to be so serious that the titanic work of saving mankind and our planet can be seen as a kind of utopia, maybe the major utopia of all times. A dream still far from having a general support. Coincidentally we’ll commemorate in 2016 the 500 years since the English humanist and statesman Thomas More (1478-1535) published his Utopia„ considered “ a playfully serious social critique to a social reality deadly and tragically grave.”33

In this context, it is urgent to build a positive agenda for the international space law.

### 1AC---PLAN

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of cybersecurity of space-based strategic assets.

### 1AC---SOLVENCY

#### Contention 3 is **SOLVENCY**.

The plan streamlines NATO cooperation over non-kinetic ASATs---US leadership ensures threat assessments and military exercises, vital for allied planning and collective deterrence.

Frank A. Rose 20. Senior fellow and the co-director of the Center for Security, Strategy, and Technology in the Foreign Policy program at the Brookings Institution. While at Brookings, he focused of nuclear strategy and deterrence, arms control, strategic stability, missile defense, space security, and emerging security challenges. “NATO and outer space: Now what?.” Brookings. 4-22-2020. https://www.brookings.edu/blog/order-from-chaos/2020/04/22/nato-and-outer-space-now-what/ //EM [IC = intelligence community]

THE EMERGING ANTI-SATELLITE THREAT

The threat to U.S. and allied space systems from anti-satellite weapons continues to grow. As former Director of National Intelligence Dan Coats noted in testimony before Congress in January 2019: “China and Russia are training and equipping their military space forces and fielding new anti-satellite weapons to hold U.S. and allied space systems at risk.” Coats’ testimony is complemented by numerous reports and studies by government and non-governmental organizations like the Defense Intelligence Agency, the National Air and Space Intelligence Center, the Center for Strategic and International Studies, and the Secure World Foundation.

NATO has also been the victim of real-world anti-satellite activities. In March 2019, the Norwegian government accused Russia of “harassing” communications systems during NATO exercises. Recent press reporting notes that the Norwegian Intelligence Service has documented a number of incidents in which “GPS signals and other secured communications between the Norwegian Armed forces, or NAF, units engaged in exercises were subjected to ‘blocking’ measures from sites located in Russia.” And just last week, U.S. Space Command released a statement claiming that on April 15th, Russia had conducted a direct-ascent anti-satellite missile test. Faced with these real threats, how should NATO respond?

IMPROVE INTELLIGENCE-SHARING

Collective action by NATO on outer space security issues will only happen when allies reach a consensus on the anti-satellite threat. As a first step, an appropriate organization at NATO (e.g., the Assistant Secretary General for Intelligence) should be directed to develop a comprehensive assessment of the anti-satellite threat to the alliance.

To be successful, this effort will require the full support of the U.S. intelligence community. Additionally, NATO officials should ensure relevant alliance political and military bodies (e.g., the North Atlantic Council, Military Committee, Senior Political Committee, and Defense Policy and Planning Committee) receive regular updates on the anti-satellite threat.

MAINSTREAM OUTER SPACE AT NATO

NATO should ensure that outer space is “mainstreamed” and fully integrated within alliance political and military institutions, and is not treated as merely a “novelty item.” For instance, overall responsibility for outer space should be placed in an organization like the Office of the Assistant Secretary General for Defense Policy and Planning, or the Office of the Assistant Secretary General for Defense Investment, which are responsible for defense policy, planning, and capability investment at NATO. Furthermore, noting the interrelationship between outer space and other domains like nuclear and cyber, NATO will need to establish mechanisms that encourage effective coordination and cooperation across the entire organization, including the military commands.

At the operational level, the alliance should ensure that outer space is incorporated in its major military exercises and wargames. This is critical because if NATO ever comes into a major conflict with Russia, one of Russia’s first targets would be the alliance’s space assets and space-derived information. Therefore, it is important for NATO to conduct its exercises with this in mind. Allied Command Transformation, NATO’s warfare development command, should be tasked to make this a reality.

If NATO ever comes into a major conflict with Russia, one of Russia’s first targets would be the alliance’s space assets.

ENSURE COOPERATION AND COORDINATION WITH THE UNITED STATES

At the end of the day, NATO’s ultimate effectiveness in outer space will depend on its cooperation with the alliance’s most important space power: the United States. To date, U.S. leadership has been the key driver of NATO decision-making on outer space, and senior U.S. officials have actively engaged the alliance leadership. For example, in October 2019, General John Raymond, commander of U.S. Space Command and chief of space operations, briefed the NATO Military Committee on outer space security issues. These types of senior-level engagements between U.S. political and military leaders should continue and be expanded.

In addition to senior-level engagements, there are a number of other actions NATO and the United States could take to improve cooperation and coordination. Specifically, they should establish clear consultative mechanisms between NATO, U.S. Space Command, and the U.S. Space Force. One relatively easy step that could be taken quickly would be to establish a NATO liaison officer at U.S. Space Command and/or U.S. Space Force headquarters. Indeed, a number of allied officers are currently attached as liaisons at several U.S. combatant commands like U.S. Strategic Command (STRATCOM).

The United States should also seek to incorporate NATO representatives into its outer space-related wargames where possible, especially the Schriever Wargame, the premier U.S. space wargame. According to a U.S. Air Force press release, several allies including Australia, Canada, New Zealand, the United Kingdom, France, Germany, and Japan, have participated in previous Schriever Wargames. The United States should invite NATO political and military officials to participate in the next Schriever Wargame.

COOPERATE WITH THE EU

NATO should also explore ways to cooperate with the EU on outer space, primarily because the EU has developed and deployed the Galileo global navigation satellite system, which like the U.S. Global Position System (GPS), provides accurate positioning and timing information. In particular, Galileo includes a capability known as the Public Regulated Service (PRS), an encrypted navigation service for governmental authorized users and sensitive applications that require high continuity. In a crisis situation, PRS could provide NATO important redundancy against an adversary’s attempt to jam or destroy GPS. While many members of NATO are also members of the EU and have access to PRS, non-EU NATO members, and NATO as an organization, currently does not. Therefore, NATO should begin consultations with the EU about the possibility of gaining access to PRS for the alliance.

DON’T FORGET DIPLOMACY

Military solutions alone will not allow the United States and its allies to address the increasing anti-satellite threat. While I have generally supported many of the Trump administration’s space security initiatives like the re-establishment of U.S. Space Command, a key element missing from the Trump administration’s outer space security strategy has been the complete lack of a diplomatic component. Without a more comprehensive strategy that includes a strong diplomatic element, it will make it difficult for NATO to maintain enough political cohesion to pursue effective military policies. These tensions were highlighted in a recent article that noted: “With the exception of France and the United Kingdom, many Europeans countries are deeply uncomfortable with, or down right opposed to, the development and use of weapons in space.”

This is not a problem unique to outer space. Throughout its history, there has been constant tension within NATO over the appropriate balance between defense and diplomacy in its strategy. Since the late 1960s, with the approval of the Harmel Report, named after former Belgian foreign minister Pierre Harmel, NATO has sought to more effectively balance some of the inherent tensions between defense and diplomacy. One of the key findings from the Harmel Report was that “military security and a policy of détente are not contradictory but complementary.” Arms control was considered an essential element of this strategy. The general Harmel Report approach has shaped the key strategic decisions that the alliance has taken over the past 50 years, most notably the “Double-Track” decision in 1979 to deploy intermediate-range nuclear forces in Western Europe, while simultaneously engaging the Soviet Union in arms control negotiations.

As part of its overall strategy for outer space, NATO should develop options and recommendations on how it can advance diplomatic solutions to address the emerging threat to outer space systems. In particular, NATO should task the Arms Control and Disarmament Committee to examine what role the alliance could play in developing norms of behavior to encourage responsible use of outer space. And even though the Trump administration has generally been opposed to arms control, it has expressed openness to the development of norms for outer space. In an recent speech, Assistant Secretary of State Christopher Ford stated: “We clearly need to do more to develop non-legally–binding international norms of responsible behavior that are complementary to the existing legal regime.”

U.S. LEADERSHIP WILL BE KEY

With the increasing role that outer space is playing in military operations, and the rise of the anti-satellite threat, NATO was correct in its decision to declare space as an operational domain in December 2019. The question now is whether the alliance will be able to translate this broad political guidance into an effective strategy.

An effective NATO strategy for outer space will depend on the ability of the alliance to build consensus on the threat; mainstream outer space into NATO’s political and military institutions; find ways to cooperate with the EU; and incorporate diplomacy into that strategy. But at the end of the day, all of this will require clear, sustained, and consistent U.S. leadership.

#### Expanding wargames revitalizes transatlantic cooperation.

Stephen Ganote et al. 19 (Stephen Ganote is a Managing Director at Avascent where he serves clients in space communications and select defense tech markets and leads its commercial space practices, Janie Yurechko is a Strategic Development Specialist at Ball Aerospace and a MBA Candidate at Georgetown University, Diana Jack is a manager in Avascent's Space practice where she provides strategic guidance to major primes, New Space companies, and governments, Connor O’Shea is President and Co-Founder at Westgen Technologies Inc, a remote power generation and methane reduction technology company, 9-30-19, accessed on 6-19-2022, Atlantic Council Scowcroft Center for Strategy and Security, “Reenergizing Transatlantic Space Cooperation”, <https://issuu.com/atlanticcouncil/docs/reenergizing_transatlantic_space_cooperation>, HBisevac)

In an increasingly tense geopolitical context, formalized security cooperation becomes even more vital: NATO and other groups of allies have played key roles in many new contexts since the Cold War, and today should be no different. Yet, the US political commitment to NATO and other multilateral institutions has slipped, and transatlantic cooperation in training and doctrine in the space domain remains uncoordinated and insufficient. Key NATO mission areas (such as ballistic missile defense and signals intelligence) are supported by a patchwork of sovereign US, French, German, Italian, and British space assets and data resources. NATO and its member states have recognized the need for better joint doctrine development in a number of recent reports, but a clear, holistic, and specific NATO space policy remains elusive.34 Training also remains a point of weakness: nearly two decades after the US Air Force held its first Schriever Wargame (the first large space wargame), there continues to be little in the way of large, joint training or exercises for space.

# ASATs Advatange

## Mechanics

### U---A5

#### Article V results in overreactions and produces slow responses.

Ethan Williamson, 19 (Ethan Williamson, Federal Contractor with GridIron IT as a Cyber Task Order Analyst at the Joint Service Provider, 5-13-2019, accessed on 5-29-2022, Charged Affairs, “NATO’s Expanding Role in Cybersecurity”, <https://chargedaffairs.org/natos-expanding-role-in-cybersecurity/>, HBisevac)

Through these organizations and agreements, NATO has improved and strengthened its unified cyber defense capability, seemingly positioning itself to be a standard bearer for cybersecurity. However, these commitments lack specifics and could hamper NATO’s ability to respond to an attack because of bureaucratic and security protocols. Following the inclusion of cyber attacks under Article 5, NATO and its allies could not agree on what kind of attack would trigger the collective defense response. Allies still use their own incident standards to define cyber incidents and in some cases do not make these standards public. This results in an uneven response and makes it difficult for NATO and its allies to provide a unified, Article 5 response to cyber incidents. Stoltenberg has defended this vague definition by stating that, “a clearly defined threshold only invites attacks immediately beneath it.” This clarification does not address the larger issue of which attacks would trigger an Article 5 response, as NATO already defends against low-level cyber attacks daily. Ambiguous guidelines could also cause NATO to misappropriate responses to cyber attacks, leading to potentially embarrassing overreactions to minor incursions or devastating slow responses to crippling attacks. Without a clear definition, NATO will struggle to respond to attacks. As stated earlier, NATO’s focus is on deterring attacks—to such an extent that the cost of an attack would outweigh any benefits. However, this focus has resulted in NATO lacking the offensive capabilities to respond in the same capacity as its allies, like the United States.

### U---Russia

#### Specifically, Russia will lash-out---attacking US space-assets to prevent intelligence support to Ukraine.

Courtney Albon 2-24. ISRNET's space and emerging technology reporter. She previously covered the U.S. Air Force and U.S. Space Force for Inside Defense. “US space officials expect Russia, Ukraine conflict to extend into space.” C4ISRNet. 2-24-2022. https://www.c4isrnet.com/battlefield-tech/space/2022/02/24/us-space-officials-expect-russia-ukraine-conflict-to-extend-into-space/ //EM

CHANTILLY, Va. — Top U.S. space officials this week said it’s likely Russia’s invasion of Ukraine will extend to space, predicting continued GPS jamming and spoofing and urging military and commercial space operators to be prepared for possible cyber attacks.

“Ensure that your systems are secure and that you’re watching them very closely because we know that the Russians are effective cyber actors,” National Reconnaissance Office Director Chris Scolese said Feb. 23 during a National Security Space Association conference in Chantilly, Va. “It’s hard to say how far their reach is going to go in order to achieve their objectives, but it’s better to be prepared than surprised.”

Reports from the Secure World Foundation and the Center for Strategic and International Studies document Russia’s use of non-kinetic disruptive space capabilities in Ukraine in recent years, including spoofing and jamming as well as cyber-attacks.

“Russia places a high priority on integrating electronic warfare into military operations and has been investing heavily in modernizing this capability,” the Secure World Foundation said in its 2021 Global Counterspace Capabilities report. “Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of unmanned aerial vehicles, guided missiles and precision guided munitions, but has no known capability to interfere with GPS satellites themselves using radio frequency interference.”

One such electronic warfare platform is the Tirada-2, which entered service in 2019. According to SWF, the system can reportedly performing uplink jamming on communication satellites. Another system, Bylina-MM, is being designed to “suppress the on-board transponders” of some communication satellites.

In its 2021 Space Threat Assessment, the Center for Strategic and International Studies noted that Russia’s arsenal of electronic counterspace capabilities include two radar jammers — Karushka-2 and Karushka-4 — which could interfere with radar reconnaissance satellites.

Scolese said this week it’s likely Russia will employ jamming and spoofing capabilities to some extent – though he noted it’s not clear how far it will go.

“I think it’s fair to assume that to the extent that they can and to the extent that they feel it won’t extend the conflict out of their control, that they will extend it into space,” he said. “You can imagine they’re already doing GPS jamming, for example, and doing things against Ukraine.”

Kinetic weapons

As for kinetic counterspace capabilities, Russia’s most recent demonstration of a direct-ascent anti-satellite (ASAT) weapon in November created an estimated 1,500 pieces of debris. Speaking at the NSSA conference Feb. 23, Lt. Gen. Michael Guetlein, head of the Space Force’s acquisition command, said actions like the recent ASAT test reinforce Russia’s interest in denying space access to adversaries.

Chief of Space Operations Gen. John Raymond has on multiple occasions referred to Russia’s July 2020 test of what he calls a “nesting doll” capability. The test — which CSIS said in its report was more sophisticated than some previous ASAT demonstrations — involved a Cosmos 2542 satellite that contained a smaller Cosmos 2543 space vehicle inside of it. During the 2020 test, the smaller satellite fired a projectile near another Russian satellite.

“This is further evidence of Russia’s continuing efforts to develop and test space-based systems, and consistent with the Kremlin’s published military doctrine to employ weapons that hold U.S. and allied space assets at risk,” Raymond said at the time.

CSIS notes in its report that Cosmos 2543 was very active after being released from its “mother satellite.”

“Before firing the projectile in July 2020, the inspector satellite was constantly changing its orbit to synchronize with other Russian satellites,” the report states. “This is out of the ordinary for most satellites, which rarely maneuver in this way.”

While not an on-orbit capability, Russia has also developed an aircraft called the Beriev A-60, which detects and tracks satellites with the intent of aiming laser beams at them, according to the SWF report. The aircraft has flown multiple times since 2010, and the country is reportedly installing a laser on it.

SPACECOM Support

U.S. Space Command head Gen. James Dickinson said this week that space units are currently playing a supporting role to U.S. European Command to ensure it has “the space effects necessary to respond and characterize the situation in Ukraine.

SPACECOM’s Joint Integrated Space Teams, which are made up of intelligence planners and space professionals, have been working closely with EUCOM to coordinate space capabilities and integrate them into the command’s planning activities.

Dickinson said one of his command’s supporting functions has been to provide battlespace awareness of the space domain and provide the missile warning and GPS-enabled tracking capabilities over EUCOM.

Scolese noted that the response of the space enterprise to the ongoing Russian aggression in Ukraine is showing how integrated U.S. agencies are in providing key capabilities in a time of conflict.

“What we do in space and our technology and our partnerships are really coming to bear, and it’s going to show how we work together as a community to achieve some very significant objectives and to understand what’s going on in the world,” he said.

#### Russia has the intent now to attack the West.

* Russia wants to attack now and has the intent
* destroying sats makes U.S vulnerable to attacks

Brandon Weichert, 21 (Brandon Weichert is a geopolitical analyst who runs The Weichert Report and is a former Congressional staff member who holds a Master of Arts in Statecraft & National Security Affairs from the Institute of World Politics, 11-16-2021, accessed on 6-23-2022, Asia Times, “Russia threatening space war with US”, <https://asiatimes.com/2021/11/russia-threatening-space-war-with-us/>, HBisevac) \*\*edited for ableist language\*\*

Last week, US President Joe Biden’s administration briefed NATO members about the imminence of a Russian invasion of Ukraine. This came after months of increasing tensions between the North Atlantic Treaty Organization and Russia over Crimea, the small peninsula that juts out into the Black Sea from Ukraine, which Russia annexed in 2014.

Shortly after these caustic US intelligence warnings to Europe, Russia test-fired an anti-satellite (ASAT) weapon that created such a large debris field in orbit that the astronauts on the International Space Station (ISS) were forced to take refuge in the SpaceX capsule, in anticipation of having to abandon the station.

(As an aside, there were Russian cosmonauts on the ISS who were also forced to take refuge in the Soyuz capsule docked on the Russian side of the ISS.)

Western media reported the US intelligence community’s warning to NATO about an imminent Russian invasion of Ukraine and Russia’s testing of an ASAT that threatened the ISS as separate events. They are not separate.

The US government has been distracted by the absurdity of its domestic politics. Russian leaders have sensed weakness they seek to exploit. The US appears ~~paralyzed~~ [disoriented] by bad leadership and internal dissent. Now may be the time for Russia to strike hard against the West and rewrite the European regional order in its favor.

While Ukraine is not part of NATO, the United States and its European allies have consistently articulated their opposition to any further Russian military actions in Ukraine. Throughout former president Donald Trump’s administration, for example, the United States gave Ukraine’s besieged military much-needed lethal aid to assist in the defense of its territory from greater Russian aggression.

Various NATO countries have also helped Ukraine enhance its national defenses while Russia has intensified its commitment to expanding its threat to Ukraine.

Whether the West would risk direct military confrontation with Russia over a non-NATO member like Ukraine is another matter entirely. Given the constant declarations of support for Ukrainian sovereignty, though, Moscow cannot be certain that the Western alliance would not intervene if it decided to cleave away more of Ukraine.

Therefore, Moscow has likely initiated plans to neuter any potential threat of a NATO defense of Ukraine against any Russian invasion by going after sensitive American and NATO satellites.

The surprise Russian demonstration in orbit was probably an example of radical deterrence: Moscow is letting Washington, Brussels and London know just how far it is willing to go to achieve its strategic objectives in what it views as its “near abroad” (in this case, Ukraine).

The Kremlin is asking the West if it values the security and economic prosperity of Ukraine over its own security and prosperity. Moscow is likely banking on the West saying that, in fact, it does not put its own interests behind those of Ukraine (it doesn’t).

Washington is now in a strategic quandary: Failure to respond with at least an in-kind demonstration in orbit would lead Moscow’s leaders to conclude that they can have their way with Ukraine. This conclusion would lead to the inevitable annexation of more of Ukraine by Russia while reinforcing the claims of both Russia and China that the United States is a great power in terminal decline.

On the heels of the disastrous Afghanistan withdrawal, given how much moral and diplomatic capital the West has (~~stupidly~~) invested in Ukraine, the failure of Western powers to respond to this Russian provocation would lead to greater aggression directed against the West, not just in Europe but around the world – and in space.

The United States relies on satellites more than any other nation on Earth. Not only are satellites key for modern communications and economic transactions, but they are critical in modern military operations.

Satellites form the backbone for the most basic functions of America’s global military. Removing those key satellite interlinks would render the US military impotent, leaving America and its allies vulnerable to attack from a predatory power, such as Russia.

In space, the United States has more to lose than any other country – and the Kremlin knows this. That fact explains why Russia began a rapid military modernization in 2010 to reorganize its forces to better fight – and win – a space war against the United States.

To deter Russia, the US must immediately test its own ASAT capability while deploying swarms of smaller, “bodyguard” satellites designed to protect America’s sensitive satellites in Earth orbit from ASAT attack.

At the same time, Washington must clarify its position on Ukraine: Either it stands with the embattled country, or it does not. Strategic ambiguity, in this case, invites greater challenge from Moscow – which is most unwelcome currently.

Failure to draw red lines clearly will lead to a Russian strike on US satellites that might precipitate a war. Or worse, a US defeat.

### U---Russia---Intent---AT: Alt Causes

#### Russia is empirically subtle---erring towards non-kinetic attacks for discreet attacks.

Kate E. Lee 21. Assistant Staff Judge Advocate/Prosecutor at United States Air Force, former Judicial Fellow at the United States Courts. “The Future of Warfare and Russian Engagement in Space.” March 2021. Squadron Officer School Air University Advanced Research. <https://www.airuniversity.af.edu/Portals/10/ISR/student-papers/AY21-22/FutureofWarfareandRussianEngagementinSpace_Lee.pdf> //EM thx HBisevac

In light of the above, Russia is likely to favor subtler methods of NGW. While kinetic attacks are easily attributable to a belligerent actor, cyber and electronic warfare (EW), by contrast, are not. Both are essential tools of the Russian military, and their combined application will form the foundation for Russian space warfare. Russia has demonstrated proficiency in EW capabilities such as downlink jamming—interfering with a ground stations’ ability to receive transmissions from a satellite—and spoofing, both of which can be used to interfere with an adversary’s command and control (C2), communications, and intelligence, surveillance, and reconnaissance (ISR) capabilities. Cyber operations, which have become increasingly central to Russian hybrid warfare, provide another avenue for domineering, degrading, or even destroying adversaries’ space assets and associated capabilities.

Cyberattacks are likely to become Russia’s preferred method of warfare in the space domain, as successful attacks could allow Russia to gain full control of adversaries’ satellites and C2 systems from a terminal far, far away, whereas EW may be dependent on proximity to the target asset. The 1998 ROSAT incident, in which Russian hackers hijacked control of a U.S.-German satellite and issued commands that caused the satellite to rotate toward the sun, thereby “frying its optics and rendering it useless,” is proof that Russia is willing and able to use cyberattacks against space systems. Russian focus on cyberattacks and large-scale cyber offensives against space assets is especially likely considering the current vulnerabilities of U.S. and NATO space architecture.

### U---China

#### China is increasing space power now---priming space as the new territory for conflict.

Chris Impey, 21 (Chris Impey is a professor of astronomy at the University of Arizona, 10-8-2021, accessed on 6-18-2022, The Hill, "Is conflict in space inevitable?", https://thehill.com/opinion/international/575903-is-conflict-in-space-inevitable, HBisevac)

For now, we are witnessing nations testing their space technology. There has never been an armed conflict in space — but it is the **next arena for combat**. Charles Richard, the deputy commander of U.S. Strategic Command, warned in 2017 that the country needs to be prepared to fight and win wars in all domains, including space. “While we’re not at war in space, we’re not exactly at peace either,” Richard said. Last month, Defense One issued a report highlighting the lack of international rules governing behavior in space, the growth of China’s military space program, the problem of space debris, a proposed space arm of the U.S. National Guard, the potential for conflict in ownership of sites on the Moon and ways satellites might be used to spot hypersonic missiles. Existing space law offers little reassurance. The foundation of international space law is the U.N. Outer Space Treaty of 1967. Ratified by 99 countries and signed by another 27, it says that space is the “province of mankind,” and all nations have the freedom to “use” and “explore” outer space, provided it is done in a way to “benefit all mankind.” Some of its sweeping and vague terms have never been clearly defined. The treaty prohibits weapons of mass destruction, but it says nothing about conventional weapons. Ownership is addressed by the U.N. Moon Treaty of 1979. It declares the Moon to be part of the common heritage of mankind and says lunar and other off-Earth resources are “not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.” Unfortunately, the treaty is moot since none of the major space-faring powers signed it. Lawlessness and **lack of regulation** are showing an effect in the dramatic increase in **space junk** — the detritus of our activity in space. Chunks of metal that no longer serve a useful purpose include non-functional spacecraft, abandoned launch vehicles, cast-off materials from space missions and fragmentation debris. There are 23,000 pieces of debris larger than a softball orbiting the Earth, tracked by the Defense Department’s space surveillance network. Estimates of smaller sizes are half a million the size of a marble or larger and 100 million a millimeter or larger. The problem is that they are all moving at extremely high speeds, up to 17,500 mph — and even a tiny fleck of paint can damage a spacecraft at that speed. The situation is getting worse. As more satellites and spacecraft are launched and more obsolete hardware accumulates in orbit, the odds of collisions increase. Commercial space companies like SpaceX are planning to launch tens of thousands of satellites in the next decade to facilitate wireless Internet in parts of the world that currently have no coverage. Even before these plans, it was predicted that large collisions could cause cascading collisions, exponentially increasing the number and density of small pieces, and potentially rendering low Earth orbit completely unusable. This dire scenario is called the Kessler syndrome. The problem has an ominous overtone because world powers are arming themselves to take out each other’s satellites, offensively or defensively. It is going to get increasingly difficult for a country to tell why their satellite went down or fell silent. Was it a collision with debris, space “weather,” or a hostile action? No international treaty governs space debris. Mitigation strategies exist, but governments have been dragging their feet. Earth orbit is a new “**tragedy of the commons**,” where we ruin something because we profit by exploiting it and cannot exclude others from doing the same. Space junk is a headache, but space weapons are a **nightmare**. China is a **rapidly rising** space power, with ambitious plans for a space station, a Moon base and a Mars base. Unlike the United States, where NASA is a civilian agency with plans available for scrutiny, China’s space program is blended with its **military** and operates under a **veil of secrecy**. A recent report from the Office of the Director of National Intelligence said China is working on an array of capabilities to **weaponize space**, and it plans to “**match** or **exceed** U.S. capabilities in space to gain the military, economic, and prestige benefits that Washington has accrued from space leadership.” **Conflict is not inevitable**. The world depends on the smooth functioning of thousands of satellites that whirl over our heads. Without them, there would be no high-speed data flow or GPS positional data, and billions of dollars of economic activity would grind to a halt. **Every major power** has a **vested interest** in avoiding a ruinous war of attrition in space.

### Internal---Cyber

#### Satellites serve as force multipliers for NATO, compromising ISR AND SEW---absent countermeasures, cyber-attacks become inevitable.

Antonio Carlo & Nikolaos Veazoglou 20. Previous analyst at the European Space Agency, Sapienza University of Rome; Researcher at the National and Kapodistrian University of Athens “ASAT Weapons: Enhancing NATO’s Operational Capabilities in the Emerging Space Dependent Era.” In: Mazal, J., Fagiolini, A., Vasik, P. (eds) Modelling and Simulation for Autonomous Systems. J. Mazal et al. (Eds.): MESAS 2019, LNCS 11995, pp. 417-425, 03-20-2020. Springer, Cham. //EM edited for grammar.

2 The Applications of Space Platforms

Since the dawn of the space age, outer space has been regarded as the ultimate high ground, which could provide a decisive military advantage to the State that retains superiority over it [2]. In the context of NATO operations space-based assets play an essential role, providing a multitude of services for more than 35 years. Some of the most advanced space-faring States are part of the alliance [3]. It is highly anticipated that in the next leaders’ summit taking place in London NATO will recognize space as a domain of warfare [4].

Since NATO does not own any satellites in orbit, it relys on services provided by governments, military, civilian and commercial entities. NATO has terrestrial SATCOM capabilities and units (terrestrial SATCOM anchor stations, transportable satellite ground terminals and equipment). The C2 for SATCOM is managed by NATO Communication and Information Agency (NCIA) and operated by NATO CIS Group (NCISG) [5].

Space-based assets function as force multipliers, providing support and crucial information during the strategic, operational and tactical levels of war. According to the Allied Joint Doctrine for Air and Space Operations, space capabilities provide a wide range of applications such as: global, strategic and intra-theatre satellite communications (SATCOM); positioning, navigation, and timing (PNT) services; terrestrial and space environmental monitoring; space situational awareness (SSA); intelligence, surveillance, and reconnaissance (ISR); NATO Shared Early Warning [6].

1. Satellite Communications (SATCOM): One of the most widespread functions of satellites, either civilian or military, is telecommunications. SATCOM provides support to C2 through its multiple applications, such as the establishment of communications in regions with minimal or even non existent infrastructure; transmission of intelligence; relay of messages and control of UVs.

2. Position, Navigation and Timing (PNT): The PNT data provided by space-based assets are essential for the prosecution of NATO operations, since they are used for precision targeting; tracking of friendly and enemy forces; provision of precise timing which is also vital for the function of networks and accurate navigation of troops.

3. Environmental Monitoring: Meteorological and oceanographic data collected by satellites are crucial to NATO forces since they play an important role in the planning of missions and the selection of the optimal weapons system to be deployed based on weather conditions. Also the knowledge of the conditions on the theater of operations allows forces to take advantage of them, for example the prediction of flooding based on maps developed in Afghanistan was used enhancing military operations and provide humanitarian support [7].

4. Space Situational Awareness (SSA): Space situational awareness is the knowledge regarding the outer space environment, natural and operational, and its effects on NATO operations. SSA applications includes knowledge regarding the operational capabilities and limitations of both allied and adversary space platforms; tracking of space debris; observation of space weather; tracking of adversary activities in outer space and detecting attacks against space based assets. SSA is essential for the function of satellites and the conducting of their missions.

5. Intelligence, Surveillance and Reconnaissance (ISR): Space based assets equipped with sophisticated sensors provide a host of services, such as intelligence gathering, including Signal Intelligence (SIGNIT); target information and damage assessment; warning of attacks and situational awareness.

6. NATO Shared Early Warning (SEW): Dedicated sensors onboard satellites can detect the launch of ballistic missiles and track their trajectory. Satellites also provide NATO with the capacity to detect nuclear explosions (Nuclear Detonation Detection System) which is essential for identifying any violations of international treaties banning nuclear detonations (e.g. the Partial Test Ban Treaty).

Satellites are divided into two main categories of use, military and civilian. At the dawn of the space age, satellites were predominantly used for military purposes but with the passing of time and the advancement of technology satellites have also become of civil use. The main difference between the two systems is the end user. Dual Use technology addresses both military and commercial markets. In the US sector dual use satellites serve both the federal government and the civilian market.

A historical case example of Dual Use technologies can be traced in the context of the Space race that saw the US and the USSR in competition to rule outer space. This race was carried out with military and civilian personnel to develop technologies that could carry satellites in outer space for scientific, as well as military purposes. The re-entry of the launcher with scientific data was used by the military for the potential deployment of multiple independently targetable re-entry vehicles. This is exactly what has also been experienced at national level in the EU and in the US where there is a strong tendency to look for synergies.

In the early 1990s the US Agency DARPA started a Dual Use collaboration in the Global Mobile Information Systems (GloMo) programme. This programme aimed to accelerate the development of mobile computing and looked at Dual Use technologies for digitising military and civilian communications.

In late 1993, DARPA was managing the Dual Use programme “Technology Reinvestment Program” [8] (TRP), with the goal of forging stronger collaborations between the military and commercial R&D sectors. This collaboration granted security investment for this field. The synergies between the military and the Civilian intertwined with the R&D is still carried out with the development of technologies that are used by both the field for security and defence.

The driver for both American and Soviet space programmes was the acquisition of military capabilities: in terms of capacity of delivering nuclear weapons as well as placing satellites in orbit for strategic communications and acquisition of information on the adversary’s territory [9]. Another contribution that highlights the role of outer space as a geopolitical variable meant to enhance state power is Everett Dolman’s Astropolitik which “encompass[es] the social and cultural effects of new technologies, in this case space technologies, on the subsequent evolution of political institutions” [10].

3 ASAT

Bearing in mind the host of services that satellites provide, it is a natural consequence that, parallelly with the development of satellite technology, the space powers sought ways to deny their adversaries such services by neutralising their space platforms. This led to the development of Anti-Satellite weapons (ASAT). These weapons function by Denying, Disrupting, Disabling, Destroying or Deceiving their targets (5Ds) [11]. Denying and disrupting have temporary effects, while disabling may be of permanent nature. The kinetic destruction of satellites has permanent and irreversible effects. Except for the targeting [12] of space based assets, their supporting ground facilities can be the targets of an attack as well.

3.1 Hard-Kill and Soft-Kill ASAT Weapons

ASAT weapon systems are divided in two categories, hard-kill and soft-kill.

• Hard-kill ASAT weapons are based on the use of a projectile or other methods in order to achieve the kinetic destruction of the target. Due to the predictability of satellite orbits and their restricted maneuverability, satellites are particularly susceptible to such attacks [13].

• Soft-kill ASAT attacks, on the other hand, rely on interfering with the satellite’s sensors (via jamming, spoofing or blinding through the use of powerful lasers), or with the satellite’s software (via cyber attack). These attacks can render a satellite defunct without destroying it.

3.2 ASAT Testings

USA

The United States, along with Russia, were the precursors of ASAT weapons and have carried out a number of successful testings. The most recent ASAT testing was Operation Burnt Frost, entailing the interception of the reconnaissance satellite USA-193, which failed one month after its launch and was decaying from orbit. The interception was carried out on 20 February 2008 from the USS Lake Erie using a RIM-161 Standard Missile 3 [14].

Russia

Russia tested five ASAT experiments between November 2015 and December 2018. The testings were carried out with the russian anti-ballistic/anti-satellite missiles A-235 PL-19 Nudol, without intercepting any targets.

Russian R&D continue to improve on-orbit capabilities that could serve dual-use purposes and that can be deployed anywhere. Since 2010, Russia stated that the “weaponization of information is a key aspect of this strategy and is employed in times of peace, crisis, and war. Russia considers the information sphere to be strategically decisive and has taken steps to modernize its military’s information attack and defense organizations and capabilities”. Moreover Russia’s President Vladimir Putin stated that the laser weapon system is a “new type of strategic weapons” [15].

China

On 11 January 2007, China targeted and destroyed the aging weather satellite Feng Yun 1C in LEO with a single ballistic missile launched from the Xichang Space Center. This ASAT testing led to the creation of more than 2000 pieces of trackable space debris [16, 17].

China put a great focus on the development of launchers such as the Long March 11 (LM-11) defined as quick response, which can support military operations in a conflict or civilian in the event of a disaster. Unlike other launchers, these can be transported by wheeled vehicles or railroad in unmarked containers. On 5 June 2019, a LM-11 was launched from a floating platform from the chinese Yellow Sea. This operation demonstrated the deployment capabilities of stealthy ballistic missiles and Anti-Satellite Weapons (ASATs). This operation had previously only been completed by Russia.

By 2020 China’s military is expected to deploy a laser weapon (ASAT) capable of damaging satellites in low earth orbit. This is a development of the 2006 chinese test from a ground based laser that dazzle an orbiting satellite [18]. Moreover China “probably intends to pursue additional ASAT weapons capable of destroying satellites up to GEO” [19].

India

On 27 March 2019, India intercepted and destroyed Microsat-R Earth observation satellite on Low Earth Orbit with an Prithvi Defence Vehicle (PDV) Mark-II interceptor [20]. This test proved that India has the necessary capabilities to perform an anti-satellite operation. Moreover India is performing a large number of launches of nano and small satellites. India is providing the necessary equipment to other nations that have no launch capabilities, mitigating the monopoly that the US and Russia have established in the last years.

3.3 Future Threats

Nations with a space objective, such as North Korea, are increasingly getting to the point of developing technologies that would allow them to reach space. The numerous missile test that the nation is carrying out is the proof of a strong interest and a potential threat to the space ecosystem. A militaristic nation such as North Korea may develop and implement their technologies in ASAT weapons due to the high rewards with little investments.

4 The Legal Approach of ASAT Weapons

The legal implications of using ASAT weapons should be examined under international space law as well as international humanitarian law.

4.1 Space Law

Article IV OST

As far as it concerns international space law, the military uses of outer space are regulated by Article IV of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies [21] of 1967. Article IV dictates that “States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner”. Only the “placement” of WMDs in outer space is forbidden, while on the other hand, the use of direct ascent systems loaded with WMDs and their detonation in outer space is not restricted by the OST (but the detonation of a nuclear warhead would violate the 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Partial Test Ban Treaty, PTBT) [22]. Hence the deployment and use of ASAT weapons in Earth’s orbit as well as in the void of Outer Space is permitted as long as they do not constitute WMDs.

The same is not true regarding the placement of ASAT weapons on celestial bodies, like the Moon. Article IV dictates that “the Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes”. Hence the deployment and use of ASAT weapons on celestial bodies is prohibited by the OST, since it constitutes an aggressive use of said bodies.

Article IX OST

Article IX OST imposes on States Parties the responsibility to undertake international consultations before proceeding with an activity or experiment that the State has reason to believe could potentially cause harmful interference with the activities of other States

Parties in the peaceful exploration and use of Outer Space. The kinetic destruction of a satellite generates a large number of space debris that could hinder the activities of other States, hence the State that has planned the attack is obligated to undertake consultations with any State that could be affected, prior to the attack [23]. This is why the Chinese FY-1C ASAT test was criticized by the international community, since there was no prior notice.

4.2 International Humanitarian Law

Customary international humanitarian law dictates that attacks must be fulfil the criteria of discrimination, proportionality and necessity [24].

• Discrimination: Articles 48 and 52(2) of the Additional Protocol I to the 1949 Geneva Conventions [25] dictate that only military objectives can be the targets of an attack, with military objectives being assets which “by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage”. Hence civilian satellites can only be targeted if they provide a military advantage to the adversary.

• Proportionality: The damage caused by the planned attack must not be excessive in proportion to the military advantage gained from it.

• Necessity: The attack must be necessary in order to overcome the enemy.

This is why an ASAT attack based on the electromagnetic pulse created by a nuclear detonation in outer space would violate the regulations of international humanitarian law, since it is by nature indiscriminate and the damage caused would not be proportional to the advantage gained [26]. The same issues appear regarding the kinetic destruction of a space object which results in the creation of a large amount of space debris. On the other hand by using soft kill methods like jamming or cyber attack no issues of proportionality or discrimination arise if the target is a legitimate military objective.

5 Actions that Can Be Taken to Contrast ASAT Weapons

In order to protect its space-based assets from adversary ASAT attacks, NATO needs to take certain countermeasures. These countermeasures can be either passive or active. Passive countermeasures are practices such as stationing decoy satellites, increasing the maneuverability of satellites, so as to be able to avoid kinetic attacks, and hardening their components, such as their remote sensors, in order to withstand an attack. Active countermeasures would entail equipping satellites with defense mechanisms or non destructive countermeasures such as jamming [27].

The increase and the wide range of ASAT has ensured that resilience was used to safeguard activities in Space. There has been an increase in the number of cybernetic systems with defence and security strategies.

Cyber security should reduce the risk of a cyber-attack and protect the satellite. This would reduce the risk but would not eliminate it because there is always the possibility of the satellite being hacked. The only activity that can be done is to work on the capacity of cyber resilience because this allows the continuity of the satellite’s operation in such a way as not to influence the activities of the system.

The US Department of Defence considered the occurrence of an attack on a single or multiple satellites. On this end, there has been an increase in the number of satellites in order to have a continuous coverage even with the failure of some units of the system.

With the increase of nano-satellites and mega-constellations an attack would be able to stop an entire system because a single satellite is interconnected with others for sharing information. For this reason not only the number of satellites should be higher but there should be several constellations isolated from each other so that the operation of the constellation or satellite continues even after an attack. This would be considered as a redundancy that prevents data and activity loss.

Good practices that support the creation and sustainability of effective national capacities in order to provide system resilience are those that can prevent and what can be “emergency plans” that should provide “an overview of national incident response mechanisms; in addition to highlight how cybersecurity incidents are classified, based on their impact on critical goods and services”.

Information sharing is another key point because during an attack accurate and appropriate communication can eventually lead to the identification of the attackers. Many organisations in the World, such as NATO, are conducting exercises in this field. Periodically NATO implements exercises and simulations of war and cyber attack (CMX) [28].

These international computer security simulations help to strengthen the responsiveness and resilience of states and strengthen trust between countries and improve overall international resilience and preparedness levels. Resilience should focus on two topics: “Critical Infrastructure” and “Critical Information Infrastructures”. The first is essential for the functioning and security of a company and an economy while the second is the system that manages the key functions of the critical infrastructure. These two must be protected in accordance with the principle of risk management and resilience.

6 Conclusion

With the military and economic importance of space-based assets increasing so does the need to develop systems that could target and neutralize these assets. This led to the development of Anti-Satellite weapons that can temporarily or permanently damage the adversary’s satellites.

The development and use of ASAT created a new field were NATO and its member States can enhance their offensive operational capabilities in order to safeguard their security. NATO already embraced this domain with the implementation of personnel and infrastructure. The fast development of technologies and threats should be faced with the formation and information of NATO and non-NATO personnel.

NATO should also take into consideration the threat adversary ASAT weapons pose to its own space-based assets and take the necessary defensive measures. Such measures would be the enhancement of its cyber-security and the deployment of resilient systems.

#### Russia poses mass threats to NATO cyber capabilities in space.

Liina Lumiste, 18 (Liina Lumiste, Legal researcher on international law and advisor on domestic public law at Government Office of Estonia, 2018, accessed on 6-10-2022, NATO Cooperative Cyber Defence Centre of Excellence, “Chatham House report: Space – NATO cyber security’s weak spot”, https://ccdcoe.org/library/publications/chatham-house-report-space-nato-cyber-securitys-weak-spot/, HBisevac)

In 2018, Norwegian military and allied officials confirmed that Russia had disrupted NATO’s Trident Juncture exercise in Europe’s High North region by persistently jamming GPS signals during the exercise. China has claimed ‘the ability to use space-based systems and to deny them to adversaries as central to modern warfare’. As the dependence of military operations on space-based assets has increased exponentially over the last few decades and space-based assets are potential targets for cyber attack, the newly released Chatham House research paper ‘Cybersecurity of NATO’s Space-based Strategic Assets‘ suggests that NATO should bring space more to the spotlight. The research paper lists cyber threats to space-based strategic assets and capabilities, analyses capability requirements and gives concrete recommendations for ways improve the resilience of the space-based systems. Strategic military systems depend on space-based assets for the provision of data and for many capabilities, such as positioning, navigation and timing (PNT), intelligence, surveillance and reconnaissance (ISR), missile defence, communications, space situational awareness (SSA) as well as environmental monitoring. For accurate timing and navigation in PNT systems, NATO uses the global positioning system (GPS) which is also well known and widespread in civil use. ISR information and imagery is collected through surveillance and reconnaissance sensors. Both systems are satellite-based. Unmanned aerial vehicle (UAV) systems also rely on satellite-based ‘beyond-line-of-sight’ communication. These are only a few of the possible examples. In addition to the abundance of capabilities, it is noteworthy that the capabilities are also linked and therefore affecting one capability may cause collateral effects on others. As explained in the Space Threat Assessment 2018 published by the Centre for Strategic and International Studies (CSIS), there are several intrusion points for space-based assets: antennas on satellites and ground stations, landlines that connect ground stations to terrestrial networks, and user terminals that connect to satellites. This can result in data or data traffic monitoring, inserting false or corrupted data in the system, or even the permanent loss of a satellite. As with every other technology, people have the potential to be the weakest link in the cyber defence of space-based assets – social engineering is an important tool for the adversary. The research paper highlights some of the most important vulnerabilities: use of commercial companies; ‘back-doors’; dual use of satellites; and supply chain security of space technology. Chatham House reports have touched on these topics before. The question of supply chain was raised in the Livingstone and Lewis 2016 report, which observed that there was no coherent global organisation with regard to cyber security in space and that existing approaches had only limited reach into the supply chain. In this year’s research paper, it is again stressed that when the supply chain does not ensure that military security standards are met, items procured may expose NATO systems to vulnerabilities. NATO by itself does not own satellites, but is dependent on member states. In case of need, NATO requests access to products and services from the allies. NATO allies procure equipment and software, which will be integrated into their national defence infrastructure. In most cases, military and commercial assets are not separate. Therefore, NATO does not rely only on military assets, but also uses commercial, civilian and national or multinational assets for operations. Even though commercial methods have proven to be effective, they are accompanied by the inherent risk of lower security requirements. Data exchange between civil and military sectors may cause extra vulnerabilities. As most of the space-based capabilities are dual-use, meaning that assets are used both for military and civilian purposes, the Chatham House research paper recommends that operators ‘apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications’. The research paper also highlights the aspect of NATO’s dependency on member states for communication capacity as a possible source of vulnerabilities. NATO owns satellite communications (SATCOM) ground stations, but no satellites; it is therefore highly reliant on allies to provide space-sourced data, information and services. In addition, ensuring the security of space capabilities is mostly in the hands of the allies. This puts NATO into a position where its main option to protect capabilities of vital importance is to encourage allies to put effort into securing the space-based assets and foster cooperation in space-based systems cyber security. During the Brussels Summit in 2018, the Alliance recognised space as a ‘highly dynamic and rapidly evolving area, which is essential to a coherent Alliance deterrence and defence posture’ and on 27 June 2019, it approved new space policy. As claimed by NATO’s Secretary General, Jens Stoltenberg, the space policy gives guidance on opportunities and challenges and is not about militarising space, but about information sharing and increasing interoperability. The research paper suggests that, in addition to policy, NATO needs to agree upon space doctrine. While policy directs, assigns tasks and prescribes desired capabilities, doctrine provides principles of how operations should be planned, prepared, commanded, conducted, sustained, terminated and assessed.1 This suggestion becomes even more relevant when taking into consideration recent announcements by some NATO diplomats about NATO’s aims to recognise space as a domain of warfare during the London summit at the end of 2019. This indeed would be a big step towards focusing more on space-based assets and their vulnerabilities. Considering the current context, in which China and Russia are increasing their presence in space, this action by NATO is inevitable. Whether or not NATO claims space as a domain, adversaries will nevertheless develop their aggressive capabilities, from cyber operations to anti-satellite missiles. Therefore, it is prudent to update the approach towards space and space-based assets to face new challenges. Yet, claiming space to be a domain of warfare highlights legal considerations. The Chatham House research paper raises a question from the cyber perspective: whether a cyber attack on a space system has to have kinetic consequences in order to give grounds for collective self-defence according to the Washington Treaty. This can be supplemented with a question on whether causing kinetic consequences that result in debris breaches the responsibility not to cause widespread, long-term and severe damage to the natural environment, as stipulated in article 35 of Additional Protocol I to the Geneva Conventions of 12 August 1949.2 Another question raised is targeting dual-use space technology in international humanitarian law (IHL). The principle of distinction foresees the duty to distinguish between the civilian population and combatants and between civil and military objects. As in the case of cyber objectives,3 dual-use satellites should be counted as military objectives, but would be subject to the rule of proportionality and requirement to take precautions in attack.4 The Chatham House research paper makes recommendations that more or less all stress the same things: NATO is highly dependent on space capabilities; space-based systems are vulnerable to cyber attacks and will become more and more appetising targets for adversaries; and NATO must foster cooperation and information sharing between member states. Overlooking these aspects could undermine the credibility of the information provided through the space-based systems, which would in turn affect deterrence and strategic liability. In the broader view, destabilising space-based assets would not only affect military conduct, but also have severe effects on civil infrastructures.

#### Russia, China, & NoKo are undermining transatlantic space dominance.

Stephen Ganote et al. 19 (Stephen Ganote is a Managing Director at Avascent where he serves clients in space communications and select defense tech markets and leads its commercial space practices, Janie Yurechko is a Strategic Development Specialist at Ball Aerospace and a MBA Candidate at Georgetown University, Diana Jack is a manager in Avascent's Space practice where she provides strategic guidance to major primes, New Space companies, and governments, Connor O’Shea is President and Co-Founder at Westgen Technologies Inc, a remote power generation and methane reduction technology company, 9-30-19, accessed on 6-19-2022, Atlantic Council Scowcroft Center for Strategy and Security, “Reenergizing Transatlantic Space Cooperation”, <https://issuu.com/atlanticcouncil/docs/reenergizing_transatlantic_space_cooperation>, HBisevac)

But, proliferation is not the only challenge in twenty-first-century space operations. New and renewed geopolitical threats in space and on Earth are contributing to space becoming contested, as well as congested. Seeking to erode US and European space dominance, strategic competitors such as Russia and China have increased their own space capabilities, particularly their counter-space weaponry (see Figure 7). As the US Defense Intelligence Agency (DIA) warns, both nations “view space as important to modern warfare” and desire the “means to reduce U.S. and allied military effectiveness.”25 For example, in traditional, kinetic weaponry, Russia has transformed Cold War technology into a direct-ascent ASAT system code-named Nudol (see Figure 7).26 China, a comparatively new major space player, achieved its first successful anti-satellite weapons test in 2007 and has been investing aggressively in a wide range of space capabilities ever since.27 Other nations, too, have been suspected of developing ASAT technologies.28 Russia and China, and likely others, have also nurtured non-kinetic and co-orbital ASAT technologies and techniques; these are harder to detect, characterize, or attribute. Among unclassified examples, China was able to effectively hack US National Oceanic and Atmospheric Administration (NOAA) weather satellites in 2014, while Russia spoofed GPS signals in the Black Sea in 2017 and was accused of parking a “ghost satellite” next to an operating commercial satellite the previous year.29 The significance of these issues is compounded by the reliance of US and European militaries, and the societies they protect, on space-enabled systems for applications as diverse and important as missile defense, communications, and hurricane tracking. Space also has an enormous second-order impact. For instance, in the United States, GPS increases the efficiency of precision agriculture by an estimated 10–15 percent, and enables billions of dollars of commerce.30 This dependence shows every sign of continuing; the European Global Navigation Satellite Systems (GNSS) Agency estimates that, by 2022, there will be nearly one GNSS device for every human being.31 All of these challenges and sensitivities present unprecedented threats to US and European space assets— whether commercial, civil, or military—and to broader security, space dominance, and economic welfare. Add to this the current fraught geopolitical context, in which Russia is resurgent, China has reached near-peer status, and other nuclear countries such as North Korea are flexing military muscles, and it becomes clear that the transatlantic security partnership faces new, urgent questions about its capabilities in space. In light of these developments, the United States and France have announced changes to domestic governmental agencies, such as “space forces” and the US Department of Commerce’s new Office of Space Commerce, but these organizational adaptions fail to fully address the international implications of changes in space, and to leverage partner capabilities.32 These questions must be addressed quickly and cooperatively.

### Internal---Cohesion

#### Divergent views surrounding how to use force in space inevitably fracture NATO

**Berthiaume 19** [Lee Berthiaume, “Canada in a tough spot as U.S., NATO differ on weaponizing space,” Nov 24, 2019, <https://globalnews.ca/news/6211076/nato-us-canada-weaponizing-space/>]

The NATO military alliance looked to space, the final frontier, earlier this week as members formally recognized the cosmos as integral to their mutual security, agreeing to bolster ways to defend their satellites and other space-based infrastructure from enemy attacks.

NATO Secretary General Jens Stoltenberg insisted the measure was purely defensive and did not include plans to put weapons into orbit. But it represented a marked departure from the United States, which is preparing to fight a future war in space if necessary.

The divergent views of the alliance, on the one hand, and its largest and most influential member, on the other is in many ways emblematic of the challenge Canada itself is facing when it comes to working with the U.S. on space.

“Because of Canada’s alliance with the United States, there might be some pressure to adopt or toe a very similar line to the United States,” said David Kuan-Wei Chen, executive director of the Centre for Research in Air and Space Law at McGill University.

“But so far, I think the political leadership and people at the Department of National Defence have resisted that.”

The federal government’s 2017 defence policy laid out a broad vision for the Canadian Armed Forces’ operations in space, which recognized its importance to the country’s peace, security and prosperity — and the need to ensure satellites and other assets are protected.

The policy also spoke to the need to work with Canada’s intelligence partners known as the Five Eyes — the U.S., United Kingdom, Australia and New Zealand — “with the aim of strengthening deterrence (and) improving the resilience of space systems on which Five-Eyes militaries rely.”

Yet it also called for Canada to work with other countries to promote “the peaceful use of space and provide leadership in shaping international norms for responsible behaviour in space” while supporting efforts “to ensure that space does not become an arena of conflict.”

“There are members in (NATO) who are vehemently opposed to the entire idea of waging conflict in space, among which Canada is one,” said Kuan-Wei Chen, who is overseeing development of a manual dealing with international law and the use of military force in space.

#### Space integration’s a prereq to effective allied consultation

Silverstein 20 (Benjamin Silverstein, researcher with experience in the National Laboratory network conducting research on the use of counterspace technologies to support deterrence goals, past research at the United Nations offers a field guide for identifying arms races in the wild, with special attention to arms racing in outer space, “NATO’s Return to Space”, War on the Rocks, AUGUST 3, 2020, <https://warontherocks.com/2020/08/natos-return-to-space/>)

NATO also lacks the tools, tactics, and procedures to effectively operate in space. NATO has neither announced an intent to implement a space situational awareness program to identify and attribute on-orbit interference, nor convened debate on a collective threat-assessment process. These are two core tasks that should be accomplished to support the alliance’s relevance in space security. Shared threat-assessment tools are key for states interested in building meaningful coalitions to address space security. Without agreed-upon threat-assessment processes, allies may arrive at different conclusions about threats to space systems, based in part on their differing abilities to collect and analyze data. This directly impacts the alliance’s ability to come to a consensus decision under the processes outlined by Article 4 of the NATO Charter. While some actors like the United States have robust space situational awareness capabilities, others don’t. NATO members may not have comparable capacities to observe or monitor space activities, leaving allies unable to assess independently collected data. Compounding this, even perfect data cannot protect NATO from disagreements based on differing opinions about a space actor’s intent. Without common methods or an established procedure for space observation and shared threat-assessment tools, NATO may be unable to arrive at a conclusion and may cede initiative back to an adversary.

### Internal---Entanglement

#### A5 applies.

Laura Winter 19. Space journalist for Al-Jazeera. “NATO declares space an ‘operational domain’.” Al-Jazeera. 12-4-2019. https://www.aljazeera.com/economy/2019/12/4/nato-declares-space-an-operational-domain //EM

The 29 NATO heads of state on Wednesday jointly declared space a “domain of operations” during a summit in London that marked the security alliance’s 70th anniversary.

“Today, we took a wide range of important decisions,” said NATO Secretary General Jens Stoltenberg immediately following the summit’s conclusion.”We have declared space as the fifth operational domain for NATO, alongside land, air, sea, and cyber.”

The declaration expands the scope of collective-defence commitment for NATO, the North Atlantic Treaty Organization. That commitment is enshrined in Article 5 of the alliance’s founding document, known as the Washington Treaty.

Analysts say Wednesday’s announcement was overdue and serves two purposes: to meet the challenges posed by Russia and China’s military space activities and to assuage United States President Donald Trump’s view that the alliance is both a military and economic burden without qualifying benefits.

“President Trump’s repeated NATO bashings have definitely left the allies worried,” Michael John Williams, director of the International Relations Program at New York University, told Al Jazeera. “His declaration of a US Space Force was taken as a sign of interest and thus advancing space as a fifth military domain is a way of adding to NATO’s value.”

NATO’s “collective defence” principle obligates all member nations to consider an attack against one ally as an attack against all allies. If such an attack were to occur, all NATO members are bound to take the necessary measures, including the use of force, to secure the member under attack and the alliance.

The only time NATO has activated Article 5 was on September 12, 2001, in the wake of the 9/11 attacks against the US on the World Trade Center and the Pentagon.

In the wake of the declaration, Russian President Vladimir Putin said on Wednesday that while his government categorically opposes the militarisation of space, the recent establishment of the US Space Command is forcing his country to develop its own space systems.

Satellites as tools for waging war

The rise of satellites as tools for waging war and keeping the peace has made space crucial to many national and defence plans – now including the plan of the NATO alliance.

Security experts have pointed to the threat posed by some nations that are reportedly developing anti-satellite systems, including signal jammers to disrupt communications, lasers, and kinetic kill systems that issue missile-like projectiles.

Militaries use satellites to command and control their personnel and weaponry, and to gather intelligence on their adversaries’ activities. If one nation’s satellites were to be paralysed or destroyed, that country’s ability to defend itself against an attack could be fatally crippled.

Commercially-operated satellites also facilitate business transactions, help people navigate unfamiliar destinations, and control critical infrastructure, such as power stations and air traffic control systems.

“Declaring space a fifth military domain opens it up to NATO Article 5 protection, and given the number of assets controlled by the US and the danger that those satellites might face from Russia and China, this move is a way to show more European support for the US and to internationalise,” said Williams.

#### Official NATO policy is ad-hoc and unclear, but space attacks can trigger Article 5.

Nagashima '20 [Jun; 5/8/20; Senior Analyst at the Sumitomo Corporation; "NATO’s Response to the Coronavirus Pandemic: Security Implication for Japan," https://www.spf.org/iina/en/articles/nagashima\_01.html]

The “vulnerability” anticipated by NATO will gradually change with the environment surrounding the alliance, as revealed in its new strategic concepts and summit communiques. Recently, after the NAC Foreign Ministers’ Meeting on April 2, NATO Secretary-General Jens Stoltenberg suggested that the spread of infectious diseases such as Covid-19 should be included in the category of vulnerabilities for NATO,[3] along with cross-border threats such as international terrorism and attacks on cyber- and outer space systems. It can be assumed, then, that NATO will conduct full-scale discussions on developing resilience against large-scale epidemics.

Collective Defense and Resilience

So far, NATO’s military response to Covid-19 has consisted of (1) mediating and coordinating assistance requests centered on the European Atlantic Disaster Coordination Center (EADCC); (2) airlift assistance using the NATO airlift scheme; (3) the Rapid Air Mobility (RAM) initiative; and (4) utilization of innovative technologies like 3D printing. These have remained within the framework of direct and indirect support.[4] NATO operations are continuing at present in Afghanistan, Kosovo, and the Mediterranean Sea, so the highest priority is being given to minimize the pandemic’s impact on those operations.[5]

Among NATO’s core missions of “collective defense,” “crisis management,” and “cooperative security,” these actions can be included in the category of “crisis management,” but, in the future, it is conceivable for responses to pandemics such as Covid-19 to be carried out as part of a “collective defense” mission. This is suggested by the confirmation at the NATO Warsaw Summit in 2016 that the resilience of the military alliance would be enhanced against a diversifying range of threats.[6]

NATO positioned cyberspace as a fourth operational domain along with land, sea, and air at this summit, and its defense was confirmed as falling within the scope of collective security. And at the London summit in 2019, “space” was newly confirmed as a fifth operational domain. There was also clarification of the diversifying threats covered by Article 5 missions.

## Impact---ASATs

### Impact---ASATs---AT: Defense

#### Dual-use satellites are prone to create misperceptions---triggering inadvertent escalation.

Andrew Futter 22, Professor of International Politics at the University of Leicester; Samuel I. Watson, Associate Professor at the University of Warwick; Peter J. Chilton, Research Fellow at the University of Birmingham; Richard J. Lilford, Professor of Public Health at the University of Birmingham, “Disruptive Technologies and Nuclear Risks: What’s New and What Matters,” Survival, 64:1, Survival: Global Politics and Strategy, Vol. 64, No. 1, pg. 108-110, 2022, T&F. //EM

Escalation pathways across different domains

Modern militaries, especially the United States’, are increasingly reliant on outer space. While most military space-based assets are designed to support conventional military missions, some also play a role in nuclear operations with respect to missile-launch detection and early warning, tracking incoming missiles or aircraft, guiding precision munitions (including nuclear-armed cruise or hypersonic missiles), and providing broader situational awareness and military communications. An increasing dependence on such assets has created two interlinked concerns. Firstly, satellites might be targeted early in a crisis by an adversary; this makes targeting and destroying anti-satellite capabilities a priority, which could trigger escalation. Secondly, attacks on space assets may be misinterpreted because some satellites have dual functions.39

Anti-satellite weapons are not new.40 Nuclear-armed blasts were contemplated in the 1950s and 1960s, and kinetic kill can be traced back to the 1980s. But the ability to conduct non-nuclear counter-space operations, through direct ascent and co-orbital weapons or by other means such as directed-energy weapons, has returned to the forefront of strategic thinking and planning.41 All major nuclear-armed states are engaged in the development of anti-satellite weapons – which are technically similar to anti-ballistic missiles – and some already have demonstrated capabilities.42 In 2007, a Chinese weapon destroyed a weather satellite at an altitude of 850 kilometres. The US destroyed a reconnaissance satellite at an altitude of 250 km in 2008.43 In 2019, India destroyed a satellite at an altitude of 282 km.44 And most recently, in November 2021, Russia destroyed a satellite at an altitude Disruptive Technologies and Nuclear Risks: What’s New and What Matters | 109 of 480 km.45 It is unlikely that a state could orchestrate a ‘perfect storm’ and destroy all space assets in one go, but their vulnerability is clear.

Space capabilities are part of a broader quest for information superiority and dominance in an increasingly complex world. On account of real-time information flows facilitated by information technology, social-media platforms and global networks, it is becoming more difficult to discern what is and isn’t true in a nuclear environment abundant with raw data.46 This new environment complicates nuclear signalling and presents new challenges for crisis communications and crisis management. Different sources may use unorthodox means, such as Twitter.47 Ambiguous communications could be interpreted incorrectly.48 US Strategic Command’s ill-conceived New Year’s Eve tweet about ‘dropping a bomb’ appeared to be an example of this.49 In addition, international events and actions that might preclude or exacerbate a nuclear crisis will be reported in real time and publicly available. This may make it difficult for leaders to take the time required to think through actions and increase the potential for an adversary to shape public opinion in dangerous ways. Imagine how the Cuban Missile Crisis would have played out if it had arisen today,50 or what impact the 2018 false missile alert in Hawaii might have had during a real nuclear crisis.51 There is also greater potential for ‘weaponised social media’, disinformation and misinformation, particularly from third-party actions that might lead to what Rebecca Hersman has described as ‘wormhole escalation’.52 Deep fakes or other types of fake news could be used deliberately to deepen a crisis. A bogus news story about how Israel might respond to Pakistani military assistance to Syria prompted Pakistan to issue a public warning to Israel in 2016.53 It should be assumed that sophisticated information operations will be part of any future nuclear crisis or conflict.54

The possible pathways to inadvertent and deliberate escalation that could result in nuclear use are changing. This is due to both growing competition over the control of outer space and, less directly, changes in the global information ecosystem within which nuclear decisions and operations take place. Given the centrality of space and cyberspace to almost all aspects of nuclear operations, these developments will inevitably affect other military domains, missions and weapons systems.

#### ASATs ensure nuclear miscalculation.

Beauchamp 14 [Zack Beauchamp, editor for Vox, citing a study done by Micah Zenko, senior fellow with the Center for Preventive Action at the Council on Foreign Relations, April 21, 2014. “How space trash could start a nuclear war.” https://www.vox.com/2014/4/21/5625246/space-war-china-north-korea-iran]

Panic in the skies! "The threats to U.S. space assets are significant and growing," according to a new report from the Council on Foreign Relations, which warns that there's a real chance of breaching conflict's final frontier. This isn't idle fearmongering. The report makes a not-crazy case that efforts by China and other powers to limit America's total military dominance of space could accidentally destroy an American satellite, inadvertently convincing the US that war was coming and prompting retaliation on Earth. Its author, Micah Zenko, has [made a name](http://www.theamericanconservative.com/articles/the-anti-warrior/) for himself in report-after-report downplaying the threat to the United States from China, terrorists, and, really, [most things](http://blogs.cfr.org/zenko/2012/02/23/clear-and-present-safety-the-united-states-is-more-secure-than-washington-thinks/). So that fact that Zenko is this [concerned about space](http://www.cfr.org/space/dangerous-space-incidents/p32790?sp_mid=45655631&sp_rid=emFjay5iZWF1Y2hhbXBAZ21haWwuY29tS0) should tell you something. The basic dynamic is simple: the US controls space and its opponents don't. Of all the money spent on space by all countries combined, America [spends](http://www.cfr.org/space/dangerous-space-incidents/p32790?sp_mid=45655631&sp_rid=emFjay5iZWF1Y2hhbXBAZ21haWwuY29tS0) 75 percent. It also owns 43 percent of all satellites. It uses that huge satellite network for, among other things, all sorts of military spying and coordination purposes. At one point, the Bush Administration [mused openly](http://www.armscontrol.org/act/2004_11/Krepon) about putting actual weapons pointed at Earth in space. Countries who might hypothetically fight a war with the United States hate that space dominance, which gives the US a real strategic edge. Some have [developed](http://www.stimson.org/images/uploads/Anti-satellite_Weapons.pdf) anti-satellite (ASAT) weapons, usually missiles that shoot into space. Zenko thinks ASAT weapons are really dangerous, particularly those owned by China, North Korea, and Iran. The threat comes from both deliberate use and the risk of a misunderstanding that could spiral out of control. The "greatest threat to international space security," in Zenko's view, is a Chinese accident. China is [seriously investing](http://america.aljazeera.com/articles/2014/4/16/china-s-presidentxiurgesgreatermilitaryuseofspace.html) in ASAT weaponry, which it has tested by blowing up old satellites in low earth orbit, one of the places place where satellites live. These explosions create debris, which can travel tens of thousands of miles per hour and shred up other satellites and spacecraft. If debris from a Chinese test destroys a US military satellite, the US could mistake it as a preemptive strike against its space capabilities — some of which are [designed](http://www.pbs.org/wgbh/nova/military/nuclear-false-alarms.html) to detect nuclear missile launches. If the US thinks China is trying to take out its ability to detect a nuclear launch, things could get very bad, very quickly. Accidents aren't the only concern. Zenko also worries about intentional space attacks, either during peacetime or a crisis. Here, Iran and North Korea are probably bigger threats, though their ASAT capabilities are far from proven. North Korea has a pattern of crazy military moves designed to extort concessions from South Korea and the West; it could extend that behavior to space. Iran, according to Zenko, "already views space as a legitimate arena in which to contest US military power." He worries that Iran might fire missiles into space "during a major crisis, especially if it believes war is imminent — an assessment that could have self-fulfilling consequences." But even if none of these scenarios for war are likely, preparing and testing for space war is intrinsically dangerous. Space debris don't discriminate between military and non-military satellites; the more ASAT testing there is, the more hazardous space travel becomes for everyone. As satellites become increasingly important to the economy and scientific research, even preparation for space war becomes deadly.

### Impact---ASATs---Russia

#### Nuclear escalation is certain. Past NATO exercises prove this is the most likely scenario for space war.

Wilson ‘20 [David; October 19; Writer for Broadview; Broadview, "Could outer space be the world’s next battleground?" https://broadview.org/weaponization-of-space/]

West directed the research team for the 2019 edition of the Space Security Index, an exhaustive annual report on developments related to safety, security and sustainability in outer space. According to the report, in 2018 the United States, Russia and China had a combined total of 263 dedicated military satellites in orbit, in addition to operating several dozen GPS (or equivalent) satellite systems. Eighteen other countries, including Canada, operate military satellites of their own or piggyback military functions on top of civilian uses.

“There’s always been this fear of war in space, as distinct from war on Earth,” says Brian Weeden, who contributed a chapter to the report. “It’s not [distinct]. It’s the integration of space into terrestrial warfare, not something that happens separately.”

Within that integration lurks the trigger for a kind of conflict never seen before — where events on Earth spark a clash in space, or where events in space incite hostilities on Earth, with unpredictable consequences up to and including a nuclear exchange. “The most likely way to initiate a conflict would be one country disabling a satellite or spacecraft of another country,” says Dawson. “Depending on the result, the conflict could escalate into further destruction in orbit or the beginning of more traditional warfare back on Earth.”

Using projectiles to smash enemy satellites would create vast fields of space debris that could imperil other satellites, including those belonging to the attacker, and set in motion an escalating chain of collisions that could ultimately render orbit unusable. For that reason, cyberwarfare — the electronic jamming, hijacking or “spoofing” of enemy satellites so they send misleading signals back to Earth — is the most likely form that a conflict in space would take. (In fact, the Space Security Index reports that cyberattacks have already taken place in the Middle East and Ukraine, and during 2018 NATO exercises in Finland and Norway.) The arsenals of the major space powers are also believed to include lasers and other directed-energy weapons, as well as stalker satellites that can manoeuvre alongside an enemy spacecraft to spy on it or disable it.

### Impact---ASATs---Recon

#### Failure of satellite recon causes a wave of global nuclear testing

Thalif Deen 16, Master’s Degree in Journalism from Columbia University, UN Bureau Chief at the Inter-Press Service, “CTBTO’s Verification System Thwarts Nuclear Tests”, 2/9/2016, http://www.ipsnews.net/2016/02/ctbtos-verification-system-thwarts-nuclear-tests/

The Vienna-based Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) – a 24-hour international watchdog body – is known never to miss a beat.

The Organization’s international monitoring and verification system has been tracking all nuclear explosions -– in the atmosphere, underwater and underground –- including all four nuclear tests by the Democratic Republic of Korea (DPRK) – the only country in the world to test nuclear weapons in the 21st century.

“The CTBTO’s International Monitoring System has found a wider mission than its creators ever foresaw: monitoring an active and evolving Earth,” says Dr. Lassina Zerbo, Executive Secretary of CTBTO, an Organization which also monitors earthquakes, volcanic eruptions, large storms and drifting icebergs.

He said some compare the system to a combined giant Earth stethoscope and sniffer that looks, listens, feels and sniffs for planetary irregularities.

It’s the only global network which detects atmospheric radioactivity and sound waves which humans cannot hear, said Dr. Zerbo.

Asked how effective the CTBTO’s verification system is, Daryl Kimball, Executive Director of the Washington-based Arms Control Association told IPS since the Comprehensive Nuclear-Test-Ban Treaty (CTBT) was opened for signature 20 years ago, national and international test ban monitoring and verification capabilities have improved immensely and they now far exceeds original expectations.

He said there have been significant advances in the U.S. national monitoring and the International Monitoring System capabilities across all of the key verification technologies deployed worldwide to detect and deter nuclear test explosions, including seismic, hydroacoustic, infrasound, radionuclide, and satellite monitoring, as well as on-site inspections — “as demonstrated in the November 2014 integrated field exercise in Jordan, which I observed directly.”

With the combined capabilities of the International Monitoring System (IMS), national technical means (NTM), and civilian seismic networks, no potential CTBT violator could be confident that a nuclear explosion of any military utility would escape detection.

By detecting and deterring clandestine nuclear-explosion testing, the CTBT and its monitoring systems effectively inhibit the development of new types of nuclear weapons, Kimball said.

“With the option of short-notice, on-site inspections, as allowed under the treaty once it enters into force, we would have even greater confidence in detecting evidence of a nuclear explosion,” he added.

According to CTBTO, the verification regime is designed to detect any nuclear explosion conducted on Earth – underground, underwater or in the atmosphere, and the purpose of the verification regime is to monitor countries’ compliance with the CTBT which bans all nuclear explosions on the planet.

Michael Schoeppner, Programme on Science and Global Security, Woodrow Wilson School of Public and International Affairs at Princeton University, told IPS the verification system of the CTBT relies on diplomatic and technical means.

The technical verification aims at the physical proof whether a nuclear explosion has occurred or not, he said.

“The CTBTO has built an efficient and effective system to monitor the Earth around the clock for underground, underwater and atmospheric nuclear explosions. It delivers data to all member states and thus enables a sound decision-making of the international community,” he added.

The CTBT and its verification regime establish an international norm for countries to refrain from developing and testing new nuclear weapon types, Schoeppner said.

Alyn Ware, Global Coordinator for Parliamentarians for Nuclear Nonproliferation and Disarmament, told IPS the effectiveness of the verification system provided by the CTBTO demonstrates that similar real-time global verification required for nuclear disarmament is indeed possible.

He said the CTBTO and the International Atomic Energy Agency (IAEA), which monitors nuclear reactors to ensure there is no diversion of fissile materials into nuclear weapons programmes, could meet some of the verification tasks for nuclear disarmament.

However, there would also need to be verification of the destruction of existing stockpiles and the destruction or conversion of delivery vehicles, he noted.

The United States has launched an International Partnership for Nuclear Disarmament Verification which is exploring the technologies and systems required, Ware said.

“The experience of the CTBTO shows that such verification systems can begin operating even before disarmament agreements are fully ratified and operational.”

In addition, Ware pointed out, the CTBTO provides additional benefits beyond the verification of nuclear tests.

Real-time information from the CTBTO network of seismic and hydro-acoustic monitoring stations is now available for the tsunami warning centres – providing warning time for tsunamis when there are earthquakes in ocean regions.

“The CTBTO network of radionuclide monitoring stations provides information which can be useful in time of a nuclear accident, such as the Fukushima disaster. It is likely that additional verification systems developed to monitor nuclear disarmament agreements could also provide spin-off benefits,” he pointed out.

According to CTBTO, the verification regime consists of the following elements: International Monitoring System International Data Centre; Global Communications Infrastructure Consultation and clarification; On-Site Inspection and Confidence-building measures.

The International Monitoring System (IMS) consists of 321 monitoring stations and 16 laboratories world wide. These 337 facilities monitor the planet for any sign of a nuclear explosion.

Asked whether there was even a remote possibility of a nuclear test circumventing the verification system, Kimball told IPS: “No monitoring system is one-hundred percent foolproof, but only a foolish leader would try to conduct a clandestine nuclear weapon test explosion because the likelihood of detection today is extremely high and the cost would be particularly severe.”

Unfortunately, he said, Pyongyang’s Jan. 6 blast is an uncomfortable reminder that 20 years after the conclusion of the CTBT, the door to further nuclear testing remains ajar.

#### That irradiates the globe and ignites conflict with Russia, China, India, and Pakistan

Philip E. Coyle 18, Senior Science Fellow at the Center for Arms Control and Non-Proliferation, Served in Top Security Roles in the Clinton and Obama Administrations and Previously was a Top Official at the Lawrence Livermore National Laboratory, and James McKeon, Policy Analyst at the Center for Arms Control and Non-Proliferation, “Mushroom Clouds Beneath The Surface: The Dangers Of A Return To Nuclear Testing”, War on the Rocks, 4/20/2018, https://warontherocks.com/2018/04/mushroom-clouds-beneath-the-surface-the-dangers-of-a-return-to-nuclear-testing/

On Oct. 2, 1992, President George H.W. Bush reluctantly made history with the stroke of a pen. One year after Soviet leader Mikhail Gorbachev declared a unilateral moratorium on nuclear weapons testing, Bush signed into law an appropriations bill that placed a similar unprecedented restriction on the United States. Ironically, the president personally opposed this specific measure, but his signature has become one of his lasting legacies. The U.S. nuclear testing moratorium has been upheld by all of Bush’s successors, and remains in effect today.

Year after year, the heads of U.S. nuclear weapons laboratories have assessed that the U.S. stockpile is reliable, and that resuming explosive nuclear testing is unnecessary. In fact, the Stockpile Stewardship program, which “tests” nuclear weapons by other means, including advanced simulations via supercomputers, has provided laboratory scientists with more information about the U.S. stockpile than when explosive tests were regularly occurring.

But today, the Trump administration is indicating that those assessments may not be enough. While the Obama administration’s Nuclear Posture Review included a blanket commitment not to conduct explosive nuclear tests, the Trump administration’s 2018 version of the document argues that the United States “must remain ready to resume nuclear testing if necessary to meet severe technological or geopolitical challenges [emphasis added].” Severe technological challenges that could merit a return to testing do not currently exist. Specific geopolitical challenges, a new criterion, are not defined. Does this mean the administration could resume testing if China continues making aggressive moves in the South China Sea? If North Korea tests another missile? If Russian hackers disrupt U.S. government websites?

In November 2017, the National Nuclear Security Administration (NNSA) released its annual Stockpile Stewardship and Management Plan, the first under the Trump administration. Buried in this 328-page document lies new language that the agency stands ready to conduct a “simple” nuclear test as little as six months after receiving an order. A “simple” test is an explosion underground without full scientific instrumentation to analyze and assess the reliability of a nuclear weapon. As former NNSA administrator Linton Brooks told Kyodo News, such a test would be done not for scientific or security advancement, but to demonstrate “political resolve.” The benefit of such a test, likely at what once was the Nevada Test Site (the home of more than 900 U.S. nuclear tests), largely amounts to nuclear braggadocio at the expense of U.S. national security.

Combined, the two documents suggest that the Trump administration is laying the groundwork to resume explosive nuclear testing at its discretion. History reminds us that this would have catastrophic consequences. Resumed nuclear testing would bring with it not just environmental and health risks, but also the erosion of an important international norm and the likely setting off an international testing race – with no benefits for the United States.

Over the course of nearly 50 years prior to Bush’s signature, the United States conducted over 1,000 explosive nuclear tests (five underwater, approximately 200 in the atmosphere, and about 800 underground), the most of any country on Earth. These tests, particularly the atmospheric explosions, created environmental, social, and health consequences through radiation dispersal and other effects, some of which continue to be evident.

New explosive tests, even if only underground, would also present many dangers. Visitors in high-rise hotels in sprawling Las Vegas, 70 miles south of the test site, would physically feel the ground shake. And since underground tests sometimes leak, the surrounding area may be exposed to radioactive fallout.

The geopolitical consequences would be worse, amounting to a nuclear testing race. In 1961, the Soviet Union caught the world by surprise and broke its pledge with the United States and Great Britain to refrain from testing, conducting well over 100 tests over the next two years. The United States rushed to keep up, also carrying out more than 100 tests, mostly underground, by the end of 1962. France and Great Britain also tested during this time period, and China conducted its first test in 1964.

If the United States were to resume nuclear testing today, a similar international reaction would likely occur. Russia and China, attempting to keep up, would almost certainly resume testing themselves. India and Pakistan, bitter archrivals that both reserve the right to resume nuclear testing, would likely see a green light to explode nuclear weapons once more. India may see an opportunity to test new, unproven thermonuclear weapons – which it is allegedly pursuing – and Pakistan would be compelled to respond, similar to the infamous nuclear tests conducted by both countries in 1998.

In the early 1960s, with nuclear explosions taking place at a rate of roughly every other day, international and domestic pressure brought the United States, Great Britain, and the Soviet Union to the negotiating table once again. (The Cuban Missile Crisis was also a major factor). What resulted was the Limited Test Ban Treaty, a 1963 agreement still in effect that bans all nuclear explosions, except underground.

It took three more decades, and the end of the Cold War, for a complete international nuclear test ban to appear. The United States was the first of 183 countries to sign the Comprehensive Nuclear Test-Ban Treaty, which bans all explosive nuclear tests anywhere on earth. Only North Korea, a non-signatory, has explosively tested nuclear weapons in the 21st century.

But the United States has not yet ratified the treaty, meaning that it has signaled its intent to follow the treaty but is not legally bound by it. Because the U.S. Senate has yet to provide its advice and consent to ratify, some hawkish voices argue the United States can – and should – resume explosive nuclear testing. Former Sen. Jon Kyl (R-Ariz.), for example, has argued that “the reliability of U.S. nuclear weapons still cannot be guaranteed without testing them.” This is patently untrue, and it ignores the serious geopolitical and health consequences that resumed nuclear testing could cause.

#### Each scenario causes extinction

Eric Schlosser 18, Pulitzer Prize Finalist, Former Contributing Editor at The Atlantic, Writer for Rolling Stone, The Atlantic, and The New Yorker, “The Growing Dangers Of The New Nuclear-Arms Race”, The New Yorker, 5/24/2018, https://www.newyorker.com/news/news-desk/the-growing-dangers-of-the-new-nuclear-arms-race

The advent of hydrogen bombs seemed to endanger no less than the future of humanity. The new weapons could be made hundreds, if not thousands, of times more powerful than the bomb that destroyed Hiroshima. J. Robert Oppenheimer, known as the “father of the atomic bomb,” opposed the development of the H-bomb, and, in 1951, he strongly advocated the development of low-yield, “tactical” nuclear weapons that would be aimed at military targets. He hoped to minimize civilian casualties and limit the scale of a nuclear war. If the Soviet Union invaded Western Europe, Oppenheimer supported using tactical weapons against tanks, troops, and airfields. The idea of bringing “the battle back to the battlefield” was later endorsed by a young Harvard academic, Henry Kissinger, who imagined nuclear wars in which adversaries fired only tactical nuclear weapons at each other, obeyed rules of engagement, paused the fighting to negotiate, and agreed to spare cities from harm.

Confronted with a choice between tactical weapons and more powerful strategic weapons, the United States decided to build both. The Navy got nuclear depth charges, torpedoes, cruise missiles, gravity bombs, and submarine-launched ballistic missiles. The Army got nuclear artillery shells, land mines, anti-aircraft missiles, ground-to-ground missiles, and even the Davy Crockett, a recoilless rifle carried by infantrymen that shot a small nuclear projectile. The U.S. Special Forces got “backpack nukes” for sabotage missions behind enemy lines. And the Air Force got the most lethal nuclear weapons of all, mounted on cruise missiles, ballistic missiles, and bombers.

American war plans relying on tactical weapons and those relying on strategic weapons were in many ways incompatible. The Atomic Energy Act of 1946 specified that the President had the sole authority to order the use of a nuclear weapon. That authority was later embodied in America’s main nuclear-war plan, the Single Integrated Operational Plan (siop)—a highly-centralized scheme that launched nuclear weapons in an all-out attack on the Soviet Union and its allies. But a Soviet invasion of Western Europe might sideline the siop: tactical weapons would only be effective on the battlefield if they could be used immediately. The commander of an American infantry division, about to be overrun by the Red Army, might not have time to call the White House and wait for Presidential approval before authorizing the firing of his nuclear artillery shells and Davy Crocketts.

As a result, during the Eisenhower Administration, the authority to use nuclear weapons was secretly delegated to relatively low-level American officers assigned to nato. They could decide when to go nuclear. Once the first tactical weapon detonated on a battlefield, the escalation of the conflict would be hard to control. Communications could prove impossible amid the nuclear blasts, and a Third World War might begin without the President’s knowledge or approval. By deploying large numbers of both tactical and strategic weapons, the United States embraced a nuclear decision-making process that was simultaneously centralized and decentralized—and bound to be chaotic in a crisis.

Throughout the Cold War, the proper size and composition of America’s nuclear arsenal was a continual source of debate, as each military service championed its own role in any conflict. During the Kennedy and Johnson Administrations, Secretary of Defense Robert McNamara concluded that the United States should have enough nuclear weapons to fulfill two objectives: deter a Soviet attack and limit the damage of such an attack by destroying Soviet nuclear forces. If deterrence failed, at a bare minimum, regardless of the circumstances, McNamara believed that the United States should always be able to kill at least a quarter of the Soviet population and eliminate at least two-thirds of its industrial capacity. That level of “assured destruction,” he later told President Lyndon B. Johnson, “would certainly represent intolerable punishment to any industrialized nation and thus should serve as an effective deterrent.” But the nuclear-weapon requirements for “damage limitation” could become endless, as the Soviet Union expanded its nuclear arsenal and the number of military targets there multiplied.

The U.S. Air Force initially wanted ten thousand long-range ballistic missiles to attack Soviet nuclear forces, leadership bunkers, and other strategic targets, but later settled for a tenth of that number. The Army wanted a hundred and fifty-one thousand tactical nuclear weapons to hit battlefield targets, but eventually obtained about a twentieth of that number. The Navy argued that a few hundred nuclear warheads, mounted atop missiles in its submarines and aimed at Soviet cities, would keep the peace, guarantee deterrence, and render all those Army and Air Force weapons unnecessary. Although the Navy’s strategy of “minimum deterrence” would limit the size of America’s nuclear arsenal, it would focus almost entirely on slaughtering civilians.

The interservice rivalries and competing nuclear strategies led to a remarkable degree of overkill. America’s first nuclear-war plan approved by the joint chiefs, known as Halfmoon, had assumed that dropping fifty atomic bombs on the Soviet Union would devastate the country. By the late nineteen-eighties, the United States had more than twenty thousand nuclear weapons, and planned to use almost four hundred of them just to strike targets in Moscow. The Soviet Union built a similar mix of tactical and strategic forces to deter the United States—and had more than forty thousand nuclear weapons at the end of the Cold War.

The world’s other nuclear powers harbored much smaller arsenals and simpler ambitions. In China, Chairman Mao was dismissive of America’s “small stack of atom bombs,” suggesting that his country’s huge population could survive any attack and wouldn’t be “cowed by U.S. atomic blackmail.” China pursued a policy of minimum deterrence, planned only to destroy American cities, and never had more than a few hundred nuclear weapons. The United Kingdom showed little interest in hitting Soviet military targets, and its nuclear-war plans increasingly focussed on “the Moscow criterion,” a threat to destroy the capital of the Soviet Union. France had a nuclear policy known as “deterrence of the strong by the weak,” operating a command structure independent of nato and targeting Soviet cities. President Charles de Gaulle compared the thinking behind the strategy to that of a man walking in an ammunition dump with a cigarette lighter. “Of course, if he lights up, he’ll be the first to blow,” de Gaulle explained. “But he will also blow all those around.”

The Fourth Geneva Convention extends legal protection to civilians during wartime. The rules against deliberately harming noncombatants were expanded by two additional protocols, in 1977. “The civilian population . . . shall not be the object of attack,” Protocol II states. “Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.” Despite that admonition, today’s nuclear-targeting policies in many ways resemble medieval hostage-taking. The innocent are threatened with murder in order to preserve the peace.

Pakistan is now moving away from that sort of minimum deterrence to a more complex strategy known as “full-spectrum deterrence,” building tactical nuclear weapons to offset India’s superiority in troop strength and conventional weapons. Much like nato during the Cold War, Pakistan assumes that tactical weapons will deter an invasion or defeat the invading army without endangering cities. But Pakistan now faces many of the same risks and challenges that nato once encountered.

To be effective on the battlefield, tactical weapons need to be widely dispersed and available for immediate use, making them more vulnerable to theft, sabotage, and unauthorized use. They may also make nuclear war more likely. Because the destructive effects of tactical weapons are smaller, the temptation to use them may be greater. Once the “nuclear taboo” has been broken, nobody can be certain what will happen next. At Hiroshima and Nagasaki, nuclear weapons were used against a nation that didn’t have them.

Russia and the United States possess about ninety per cent of the world’s approximately fifteen thousand nuclear weapons, maintaining arsenals large and diverse enough to hit a variety of targets. The most recent Nuclear Employment Strategy of the United States, issued by the Obama Administration, in 2016, is a veritable jobs program for weapons of mass destruction. It emphasizes the importance of destroying counterforce (military) targets rather than countervalue (civilian) targets, and it vows to “minimize collateral damage to civilian populations,” in keeping with international law. The Trump Administration’s Nuclear Posture Review advocates a strategy that sounds oddly elegant: “tailored deterrence.” Its objectives include preventing a nuclear attack on the United States, protecting American allies from attack, and, if deterrence fails, ending “any conflict at the lowest level of damage possible and on the best achievable terms.”

Russia has also changed its nuclear strategy. During the Cold War, the Soviet Union claimed that it would never be the first to use nuclear weapons. But Russia is no longer confident that its conventional forces are superior to those of NATO, and so it has embraced an “escalate to de-escalate” strategy, raising the possibility of the use of tactical weapons against NATO troops. The strategy is based on a faith that low-yield nuclear blasts will impose “tailored” damage on NATO, de-escalate the conflict, and force a ceasefire. The strategy presumes that NATO won’t retaliate by using nuclear weapons, too. The change in Russian doctrine has prompted the Trump Administration to seek new low-yield, tactical weapons. The Administration believes that its new tactical weapons will deter the Russians from ever using their own—reversing a bipartisan consensus that for the past quarter century has regarded these weapons as gravely and needlessly dangerous.

At the height of the Cold War, the United States kept about seven thousand tactical nuclear weapons in Europe. The utility of those weapons was always in doubt. During Carte Blanche, a war game conducted in 1955, three hundred and thirty-five nato tactical weapons were used against invading Soviet tanks and troops, for the most part on battlefields in Germany. Robert McNamara later outlined the results: “It was estimated that between 1.5 and 1.7 million people would die and another 3.5 million would be wounded—more than five times the German civilian casualties in World War II—in the first two days.” Those estimates did not include deaths from illness, radiation poisoning, or Soviet nuclear weapons. Subsequent war games confirmed the findings of Carte Blanche: if NATO ever used tactical weapons to defend Germany, it would destroy Germany. The mere existence of tactical weapons could destabilize a crisis and make it end badly. During the Cuban Missile Crisis, President John F. Kennedy and his advisers didn’t know that the Soviet forces on the island and in the sea surrounding it not only had tactical weapons but also had the ability to use them without consulting Moscow. An American attack—contemplated for days at the White House and nearly set in motion—would have unwittingly led to a nuclear war.

After the collapse of the Soviet Union, in 1991, the United States unilaterally removed all of its tactical weapons from South Korea and almost all of them from Europe. The Chairman of the Joint Chiefs of Staff at the time, General Colin Powell, had trained in the employment of tactical nuclear weapons as a young officer and thought that they “had no place on a battlefield.” With the support of every member of the Joint Chiefs of Staff, Powell persuaded Secretary of Defense Dick Cheney and President George H. W. Bush to get rid of them, and over the years the size of nato’s tactical nuclear stockpile fell by ninety-seven per cent.

Today, the United States keeps about two hundred tactical weapons at six nato bases in Germany, Belgium, Turkey, Italy, and the Netherlands. The weapons are B-61 bombs designed to be carried by fighter planes. They have no assigned role in nato’s war plans, and their military usefulness is “practically nil,” according to General James Cartwright, a former commander of the United States Strategic Command. The B-61 bombs have been retained as symbols of America’s commitment to the defense of nato, despite concern that the weapons are vulnerable to theft by terrorists, sabotage, and attack, especially in Turkey. A few B-61s could fit in the bed of a pickup truck.

The Trump Administration is moving forward with plans to modernize the B-61 and would like to mount low-yield tactical warheads on submarine-based missiles. The advantage of basing tactical weapons on a submarine is that they will be hidden underwater—and therefore will be less likely to be stolen, attacked, or become the subjects of political protests. The disadvantage is that Russia will have no way of knowing whether a missile launched from a submarine is carrying a tactical warhead meant to destroy a tank battalion on the battlefield or a strategic warhead fired to destroy an underground leadership bunker in Moscow.

The glaring problem of how the President of the United States and the President of Russia might reliably communicate and negotiate during a limited nuclear war has never been resolved. The Moscow-Washington Direct Communications Link, known as the “hotline,” isn’t a voice link with matching red telephones, as portrayed in Hollywood thrillers. It’s a dedicated computer link that transmits encrypted e-mails between the Kremlin and the Pentagon. A recent photograph of the hotline is not reassuring: it looks like a computer terminal you might find in the business center at a Marriott hotel.

The return of tactical weapons is the most controversial aspect of Trump’s Nuclear Posture Review. The new policy assumes that American tactical weapons will deter the use of Russian tactical weapons, raising “the nuclear threshold” and making “nuclear employment less likely.” Sam Nunn, a former chairman of the U.S. Senate Committee on Armed Services and a co-founder of the Nuclear Threat Initiative, has argued against that sort of thinking for more than forty years. He fears that the chance of accidents, miscalculations, and blunders with tactical weapons—as well as the pressure to “use them or lose them” in battle—greatly increase the risk of an all-out nuclear war. Like so many of the disagreements about nuclear strategy, this one cannot be settled with empirical evidence, and selecting the wrong policy could be catastrophic. As Nunn observed in 1974, after a tour of nato’s tactical nuclear units, “Nobody has any experience in fighting nuclear wars, and nobody knows what would happen if one were to start.”

On the morning of August 6, 1945, Setsuko Thurlow, then thirteen years old, was preparing to decode messages on the second floor of the Army headquarters in Hiroshima. About twenty girls from her school worked beside her, and thousands of other middle schoolers were employed at patriotic tasks throughout the city as part of the Student Mobilization Program. Thurlow noticed a bright bluish-white flash outside the window at 8:15 a.m. She never saw the mushroom cloud; she was in it. She felt herself fly through the air, blacked out, and awoke pinned in the rubble of the collapsed building, unable to move. Lying there in silence and total darkness, she had a feeling of serenity. And then she heard the cries of classmates trapped nearby: “God, help me!,” “Mother, help me!” Someone touched her, removed the debris on top of her, and told her to crawl toward the light. She somehow made it out safely and realized that what was left of the headquarters was on fire. A half dozen or so other girls survived, but the rest were burned alive.

The smoke and dust in the air made the morning look like twilight. As Thurlow and a few classmates left the city center and walked toward the hills, they witnessed one grotesque scene after another: dead bodies; ghostly figures, naked and burned, wandering the streets; parents desperately searching for lost children. She reached an Army training ground in the foothills, about the size of two football fields. Every inch of ground was covered with wounded people begging for water. There seemed to be no doctors, no nurses, no medical help of any kind. Thurlow tore off strips of her clothing, dipped them in a nearby stream, and spent the day squeezing drops of water from them into the mouths of the sick and dying. At night, she sat on the hillside and watched Hiroshima burn.

Thurlow was reunited with her parents. But her sister and her sister’s four-year-old son died several days later. Her sister’s face had grown so blackened and swollen that she could only be recognized by her voice and her hairpin. Soldiers threw her body and that of her son into a ditch, poured gasoline on them, and set them on fire. Thurlow stood and watched, in a state of shock, without shedding a tear. Her favorite aunt and uncle, who lived in the suburbs outside Hiroshima and appeared completely unharmed, died from radiation poisoning a few weeks after the blast.

More than seven decades later, on the afternoon of December 10, 2017, I watched Thurlow accept the Nobel Peace Prize on behalf of the International Campaign to Abolish Nuclear Weapons (ican). It was a remarkable moment, as she slowly walked to the podium with a cane, and the crowd in Oslo’s City Hall gave a standing ovation. After the bombing, Thurlow attended universities in Hiroshima and Lynchburg, Virginia. Later, she earned a master’s degree in social work at the University of Toronto. She married a historian and settled in Canada. She began her anti-nuclear activism in 1954, and became a leading advocate for survivors of the atomic bombings, known as the hibakusha. A few years ago, I spent time with her in Stockholm, meeting with academics and legislators to discuss the nuclear threat. In her early eighties, she was sharp, passionate, tireless, and free of bitterness. “Today, I want you to feel in this hall the presence of all those who perished in Hiroshima and Nagasaki . . . a great cloud of a quarter of a million souls,” Thurlow said in her Nobel speech. “Each person had a name. Each person was loved by someone. Let us insure that their deaths were not in vain.”

The movement to abolish nuclear weapons began soon after the destruction of Hiroshima and Nagasaki. In January, 1946, the first resolution of the United Nations General Assembly called for “the elimination from national armaments of atomic weapons,” and during the Cold War every American President supported that goal, with varying degrees of sincerity. On September 25, 1961, addressing the U.N. General Assembly, President Kennedy gave perhaps the most eloquent speech on behalf of abolition. “Every man, woman, and child lives under a nuclear sword of Damocles, hanging by the slenderest of threads, capable of being cut at any moment by accident or miscalculation or madness,” he said. “The risks inherent in disarmament pale in comparison to the risks inherent in an unlimited arms race.”

That week, Kennedy also secretly met with military advisers at the White House to discuss the pros and cons of launching a nuclear surprise attack on the Soviet Union. American and Soviet troops were confronting each other in Berlin, and a war between the superpowers seemed possible. Kennedy wanted to hear the benefits of striking first. The casualties that would result from the Single Integrated Operational Plan seemed excessive to him: an estimated two hundred and twenty million deaths in the Soviet Union and China (not including fatalities caused by fire). A Kennedy aide, Carl Kaysen, had come up with a surprise-attack plan, focussing solely on air bases and missile sites. He predicted that it would kill “less than 1,000,000, and probably not much more than 500,000.” The problem with the plan, he acknowledged, was that it might not eliminate all of the Soviet Union’s nuclear weapons—which could prove unfortunate for cities like New York and Chicago. If the United States launched a surprise attack on the Soviets, the likely American death toll was somewhere between five million and thirteen million. But, if the Soviets attacked the United States first, perhaps a hundred million Americans would die. “In thermonuclear warfare,” Kaysen observed, “people are easy to kill.” Kennedy wrestled with the dilemma, decided not to launch a surprise attack, and made his feelings clear at the U.N.: “Together we shall save our planet, or together we shall perish in its flames.”

The height of anti-nuclear sentiment in the United States occurred during the Reagan Administration, amid renewed tensions with the Soviet Union. An opinion poll in 1983 found that about half of the American people thought that they’d die in a nuclear war. The Nuclear Freeze Movement and worldwide anti-nuclear protests helped to transform Ronald Reagan from an ardent Cold Warrior into a nuclear abolitionist. At a 1986 summit in Reykjavik, Reagan and the Soviet leader at the time, Mikhail Gorbachev, nearly reached an agreement to get rid of all of their countries’ nuclear weapons. After the collapse of the Soviet Union, the fear of nuclear war receded, and arms-control agreements between the United States and Russia cut the number of nuclear weapons by about eighty per cent.

Republican Presidents had proved especially effective at reducing the nuclear threat. President Richard Nixon signed the Treaty on the Non-Proliferation of Nuclear Weapons, committing the United States to seek “cessation of the nuclear arms rate at an early date and nuclear disarmament.” President George H. W. Bush cut the size of America’s nuclear arsenal by half. And President George W. Bush cut it in half again.

In 2007, the abolition movement was revived by an unlikely group of people: the leadership of the American national-security establishment. Two former Republican Secretaries of State, Henry Kissinger and George Shultz, joined two influential Democrats, former Secretary of Defense William J. Perry and Sam Nunn, the former chairman of the Senate Armed Services Committee, in writing an editorial for the Wall Street Journal, whose title aptly conveyed their goal clear: “A World Free of Nuclear Weapons.”

A new anti-nuclear group, Global Zero, was formed in 2008 by an international assortment of military, diplomatic, and political leaders. Both the Democratic and the Republican candidates for President that year, Barack Obama and John McCain, supported nuclear abolition. The revitalized movement reached its apogee on April 6, 2009, when Obama gave a speech about nuclear weapons in Prague’s Hradčany Square. He said that the United States had a moral responsibility, as the only country that has used nuclear weapons, to lead the international effort to abolish them. “Some argue that the spread of these weapons cannot be stopped, cannot be checked,” Obama said. “Such fatalism is a deadly adversary, for, if we believe that the spread of nuclear weapons is inevitable, then in some way we are admitting to ourselves that the use of nuclear weapons is inevitable.”

Nine years later, nuclear weapons have regained their sinister allure. North Korea has repeatedly threatened to launch a nuclear attack on the United States, producing elaborate videos that show the destruction of the White House and the U.S. Capitol. During a speech by the Russian President, Vladimir Putin, in March, computer animations projected on a large screen behind him showed Russian nuclear warheads descending over the state of Florida, perhaps aimed at Mar-a-Lago. And President Trump has delivered the sorts of nuclear threats that only Soviet leaders used to make, promising to unleash “fire and fury” and boasting about the size of his “button.” Nuclear weapons are once again being depicted as good, valuable things, the measure of national status and strength. The current arms race between the United States and Russia betrays the same assumptions as the last one: that new weapons will be better, and that technological innovations can overcome the nuclear threat. It’s a familiar delusion.

William Perry, who’s been involved in nuclear matters for more than half a century, believes that the risk of a nuclear catastrophe is greater today than it was at any time during the Cold War. The Bulletin of the Atomic Scientists, unfortunately, agrees with him, and in January moved the hand of its Doomsday Clock to two minutes before midnight. The Cold War arms race between the United States and the Soviet Union has been replaced by a multipolar nuclear competition, with far more volatile dynamics. Russia faces possible nuclear attacks by the United States, China, France, and the United Kingdom. India must worry about China and Pakistan. China must deter the United States, India, and Russia. North Korea feels threatened by the United States, while some politicians in Japan and South Korea advocate developing their own nuclear weapons to counter those of North Korea. Nuclear terrorism poses a global threat. And everyone, it seems, hates the United States.

Moreover, the aftermath of a nuclear war may be even more dire than anything anticipated during the Cold War. In the nineteen-eighties, the astronomer Carl Sagan brought public attention to the danger of “nuclear winter,” a sudden and extreme form of climate change that would be precipitated by the dust and debris rising into the atmosphere as mushroom clouds from obliterated cities. The latest studies suggest that a relatively small nuclear exchange would have long-term effects across the globe. A war between India and Pakistan, involving a hundred atomic bombs like the kind dropped on Hiroshima, could send five million tons of dust into the atmosphere, shrink the ozone layer by as much as fifty per cent, drop worldwide temperatures to their lowest point in a thousand years, create worldwide famines, and cause more than a billion casualties. An all-out war between the United States and Russia would have atmospheric effects that are vastly worse.

#### Irradiation causes extinction

Dr. Marjia H. Nadesan 14, Associate Dean and Professor of Communication in the School of Social and Behavioral Sciences, New College of Interdisciplinary Arts and Sciences at Arizona State University, Former Assistant Professor, Syracuse University, Ph.D. in Communication Studies from Purdue University, B.S. and M.S. from San Diego State University, “3 Years Since Fukushima: Nuclear Power ‘Road To Our Extinction’”, Geoengineering Watch, 5/27/2014, https://www.geoengineeringwatch.org/3-years-since-fukushima-nuclear-power-road-to-our-extinction/

The thing that so tragic is that radiation damage accumulates across time for a variety of reasons. First, because animals and plants and people all bioaccumulate radionuclides. And so across time people and animals and vegetation will become more contaminated rather than less contaminated. And the effects of radiation don’t just affect one generation, they affect multiple generations.

There is quite a bit of research, done in the Chernobyl region, for example, by Anders Møller and Timothy Mousseau, who found that the increased background radiation from Chernobyl has significant effects on immunology, mutation and disease frequency across animal species and in fact they found decline in population and long-term mutation accumulations.

Over time, each generation inherits the mutations of their parents and acquires their own. And then children have even more germline cell mutation and micro delusions in DNA than their parents. Micro-deletions in DNA are increasingly linked to diseases such as autism and congenital heart disease. So we can assume that over the long-term the health of the people in the zones and the animals in the zones – their health also is going to decrease as bioaccumulation, bio-magnification and trans-generational mutations increase. And it is a human tragedy what is occurring there.

It can happen anywhere in the world because of a solar flare that knocks out a transformer, an earthquake, for example, that might affect Diablo Canyon in California which is sitting on a fault, terrorism – all of these forces could create another Fukushima any place in the world.

Nuclear power is going to be the road to our extinction. We don’t know what the trans-generational effects are going to be, but we know they are going to be detrimental. And as humans acquire more of them, their ability to successfully reproduce is going to decline. So we might already have forged our extinction and we are just waiting for it to unfold.

### Impact---ASATs---Recon---Satellites Key

#### Satellites are key for breakout states

Ryan Gallagher 12, Journalist at Slate, “U.S. Launches New Spy Satellite for Secret National-Security Mission”, Slate Magazine, 4/9/2012, http://www.slate.com/blogs/future\_tense/2012/04/09/nrol\_25\_spy\_satellite\_launched\_by\_national\_reconnaissance\_office\_.html

Spy satellites are particularly useful for monitoring the development of potential nuclear capabilities in countries such as North Korea and Iran, where the United States has a limited presence on the ground. But that intelligence can be misleading—sometimes disastrously so. This was illustrated in the lead up the 2003 invasion of Iraq, when the United Nations cited satellite images of “unexplained construction” as evidence Baghdad was possibly developing nuclear weapons. It was later discovered, infamously, that no such weapons had ever existed.

#### Norms matter---despite outliers like North Korea---failure causes global testing and extinction

Michael Krepon 14, Co-Founder of the Stimson Center, “Caging the Bomb”, Arms Control Wonk, 11/25/2014, http://www.armscontrolwonk.com/archive/404345/caging-the-bomb/

Success has been far more elusive with nuclear newcomers, who now pose the greatest threats to nuclear order. Each new member of the nuclear club believes in the utility of nuclear weapons, challenging the norms accepted with deep reluctance by earlier entrants. Newcomers increase stockpile size to shore up systemic weaknesses or to deter stronger states. They aren’t yet ready to sign the Comprehensive Test Ban Treaty. It will take many years of strenuous effort to cage the Bomb in these hard cases. The pathways for doing so are familiar, including constraints on nuclear testing, the slow accretion of nuclear risk-reduction measures, and diplomacy to ameliorate security concerns.

Caging the bomb in the hardest cases seems as unlikely now as during the first decades of the U.S.-Soviet competition. Nevertheless, progress is possible when unlikely combinations of national leaders permit. Norms still matter, even for outliers: Who wants to join North Korea in testing nuclear weapons and threatening to use them? Caging the Bomb in hard cases is still possible because disgrace as well as incalculable danger will result from the first battlefield use of nuclear weapons after a hiatus of almost 70 years. If, by a combination of luck, common sense, and wise leadership, the superpowers could avoid Armageddon, India and Pakistan may be able to, as well. But they aren’t working nearly hard enough to succeed.

Trend lines reflecting the Bomb’s diminishing utility for major powers have withstood the advent of new states (also less than predicted) possessing nuclear weapons. Sudden shocks to well-established norms remain entirely possible, and one of these days, we may finally be shaken from our sense of complacency against all things nuclear except for Iran. Even then, major powers will have great difficulty finding utility in weapons too powerful to test, let alone use.

### Impact---ASATs---Recon---Laundry List

#### Testing breakout causes extinction

* Arms racing
* Space militarization
* Bioweapons

Rebecca Johnson 1, Executive Director of the Acronym Institute for Disarmament Diplomacy, The Guardian, 7/17/2001, Lexis

Then the international arms control and non- proliferation regimes collapsed. Americans weren't bothered at first, for hadn't the government promised a super-sophisticated force field round the whole nation that no terrorist or missile would ever penetrate? So nuclear testing resumed in Nevada for new warheads to improve the kill prospects of missile interceptors and to penetrate deep into enemies' bunkers. India had been waiting for just such a go-ahead, and Pakistan soon followed; both raced to test warheads to fit on to missiles, upping the tension in Kashmir and along the borders with China. Free now to resume its own testing, China boosted its programme to modernise and increase the size of its small nuclear arsenal. Somewhat reluctantly, Russia followed. Moscow suspended all further reductions and cooperative security and safety programmes for its still-large nuclear arsenal and facilities. Within a few short years, the nuclear non-proliferation treaty was just another discarded agreement. Many governments with nuclear power programmes developed nuclear weapons as well, while others fitted anthrax or sarin on to weapons, just in case. Most hadn't wanted to, but fearful that their neighbours would, all felt compelled. Regional rivalries grew quickly into major international problems. Alliances collapsed amid suspicion and recriminations. The burgeoning arms races even spread into outer space, threatening military surveillance, as well as public communication, entertainment and navigation. No one knew who had what. Deterrence was empty, as defence analysts calculated the advantages of the pre-emptive strike. In that terrified atmosphere of insecurity and mistrust, someone launched first. And then it was too late to speak out. The Republicans hadn't yet managed to get missile defence to work. Such a doomsday scenario is not so fanciful. On July 7, the New York Times announced that President Bush wants to ditch the comprehensive test ban treaty. A week before, the administration asked nuclear laboratories to work out how quickly the US could resume testing after its nine-year moratorium. If Bush were to back out of the test ban treaty or break the moratorium on nuclear testing - undertaken with China, Russia, Britain and France - he would also explicitly breach agreements made last May, when 187 countries negotiated measures to strengthen and implement the non- proliferation treaty. The test ban is no outdated cold war instrument, but a fundamental tool to prevent new, destabilising developments in nuclear weapons. Over several decades, from the Arctic to the Pacific, from the capitals of Europe to the deserts of Nevada, people have marched, petitioned, demonstrated and even sailed or hiked into test sites. Many have been imprisoned, and some even lost their lives trying to stop the nuclear weapons governments from polluting our oceans and earth with radioactivity from nuclear explosions, conducted for one purpose only - to make "better" nuclear bombs. It took three arduous years to complete negotiations on the comprehensive test ban treaty. It isn't perfect. No product of compromise ever is. The verification system is very thorough, but it also had to be affordable, financially and politically. The treaty stopped short of closing and dismantling the known test sites or banning laboratory testing, which the weapon states said they needed to assure the safety and reliability of weapons in the stockpiles (pending achievement of their other treaty obligations to eliminate the nuclear arsenals com pletely). But it does ban all nuclear test explosions in all environments. India panicked, because the treaty would close off its nuclear options. It refused to sign, and then let off a string of nuclear explosions in May 1998. Pakistan followed, to prove it could. Even so, the treaty held. Neither government has felt able to keep testing, which means their options for further developments were curbed. Bush has embarked on a very slippery slope that could potentially put at risk the future of the citizens of even the most advanced military nation. Mumbling and grumbling won't keep us safe. It is time to speak out.

### Impact---ASATs---Recon---Atmospheric Fusion

#### It ignites the atmosphere---extinction

Alex **Wellerstein 18**. Historian of Science and Nuclear Weapons and Professor at the Stevens Institute of Technology, creator of the NUKEMAP. 6/29/2018. "Restricted Data: The Nuclear Secrecy Blog." Restricted Data: The Nuclear Secrecy Blog. http://blog.nuclearsecrecy.com/

What would it take to turn the world into one big fusion reaction, wiping it clean of life and turning it into a barren rock? Asking for a friend. Graphic from the 1946 film, “One World Or None,” created by the National Committee on Atomic Information, advocating for the importance of the international control of atomic energy. One might wonder whether that kind of question presented itself while I was reading the news these days, and one would be entirely correct. But the reason people typically ask this question is in reference to the story that scientists at Los Alamos thought there was a non-zero chance that the Trinity test might ignite the atmosphere during the first wartime test. The basic idea is a simple one: if you heat up very light atoms (like hydrogen) to very high temperatures, they’ll race around like mad, and the chances that they’ll collide into each other and undergo nuclear fusion become much greater. If that happens, they’ll release more energy. What if the first burst of an atomic bomb started fusion reactions in the air around it, say between the atoms of oxygen or nitrogen, and those fusion reactions generated enough energy to start more reactions, and so on, across the entire atmosphere? It’s hard to say how seriously this was taken. It is clear that at one point, Arthur Compton worried about it, and that just the same, several scientists came up with persuasive reasoning to the effect that this could not happen. James Conant, upon feeling the searing heat of the Trinity test, briefly reflected that maybe this rumored thing had, indeed, come to pass: Then came a burst of white light that seemed to fill the sky and seemed to last for seconds. I had expected a relatively quick and bright flash. The enormity of the light and its length quite stunned me. My instantaneous reaction was that something had gone wrong and that the thermal nuclear [sic] transformational of the atmosphere, once discussed as a possibility and jokingly referred to a few minutes earlier, had actually occurred. Which does at least tell us that some of those at the test were still joking about it, even up to the last few minutes. Fermi reportedly took bets on whether the bomb would destroy just New Mexico or in fact the entire world, but it was understood as a joke. The introduction of the Konopinski, Marvin, and Teller paper of 1946. Filed under: “SCIENCE!“ In the fall of 1946, Emil Konopinski, Cloyd Marvin, and Edward Teller (who else?) wrote up a paper explaining why no detonation on Earth was likely to start an uncontrolled fusion reaction in the atmosphere. It is not clear to me whether this is exactly the logic they used prior to the Trinity detonation, but it is probably of a similar character to it. In short, there is only one fusion reaction based on the constituents of the oxygen that had any probability at all (the nitrogen-nitrogen reaction), and the scientists were able to show that it was not very likely to happen or spread. Even if one makes assumptions that the reaction was much easier to initiate than anyone thought it was likely to be, it wasn’t going to be sustained. The reaction would cool (through a variety of physical mechanisms) faster than it would spread. This is all a common part of Manhattan Project lore. But I suspect most who have read of this before have not actually read the Konopinski-Marvin-Teller paper to its end, where they end on a less sure-of-themselves note: There remains the distant possibility that some other less simple mode of burning may maintain itself in the atmosphere. Even if the reaction is stopped within a sphere of a few hundred meters radius, the resultant earth-shock and the radioactive contamination of the atmosphere might become catastrophic on a world-wide scale. One may conclude that the arguments of this paper make it unreasonable to expect that the N+N reaction could propagate. An unlimited propagation is even less likely. However, the complexity of the argument and the absence of satisfactory experimental foundations makes further work on the subject highly desirable.

### Impact---ASATs---Recon---Chalko

#### Mass testing causes planetary core overheating---extinction

Dr. Tom J. Chalko 3, MSc, PhD, Professor of Geophysics at Mt Best, Australia, “Can a Neutron Bomb Accelerate Global Volcanic Activity?”, Scientific Engineering Research, 3-3, http://sci-e-research.com/neutron\_bomb.html

Consequences of using modern nuclear weapons can be far more serious than previously imagined. These consequences relate to the fact that most of the heat generated in the planetary interior is a result of nuclear decay. Over the last few decades, all superpowers have been developing so-called "neutron bombs". These bombs are designed to emit intensive neutron radiation while creating relatively little local mechanical damage. Military are very keen to use neutron bombs in combat, because lethal neutron radiation can peneterate even the largest and deepest bunkers. However, the military seem to ignore the fact that a neutron radiation is capable to reach significant depths in the planetary interior. In the process of passing through the planet and losing its intensity, a neutron beam stimulates nuclei of radioactive isotopes naturally present inside the planet to disintegrate. This disintegration in turn, generates more neutrons and other radiation. The entire process causes increased nuclear heat generation in the planetary interior, far greater than the initial energy of the bomb. It typically takes many days or even weeks for this extra heat to conduct/convect to the surface of the planet and cause increased seismic/volcanic activity. Due to this variable delay, nuclear tests are not currently associated with seismic/volcanic activity, simply because it is believed that there is no theoretical basis for such an association. Perhaps you heard that after every major series of nuclear test there is always a period of increased seismic activity in some part of the world. This observable fact CANNOT be explained by direct energy of the explosion. The mechanism of neutron radiation accelerating decay of radioactive isotopes in the planetary interior, however, is a VERY PLAUSIBLE and realistic explanation. The process of accelerating volcanic activity is nuclear in essence. Accelerated decay of unstable radioactive isotopes already present in the planetary interior provides the necessary energy. The TRUE danger of modern nuclear weaponry is that their neutron radiation is capable to induce global overheating of the planetary interior, global volcanic activity and, in extreme circumstances, may even cause the entire planet to explode.

## Impact---Entanglement

### Impact---Entanglement---Miscalc

#### NATO miscalculation goes nuclear.

Brian Radzinsky 21. Postdoctoral research fellow at the Center for Global Search Research (CGSR) at Lawrence Livermore National Laboratory. His work at CGSR focuses on developing new concepts and methods to measure the military balance, applying a net assessment approach. His broader research interests are in nuclear deterrence, advanced and emerging technologies and regional security dynamics, and how these interact to affect strategic deterrence, allied assurance, and escalation. “Miscalculation, Misperception and Risk Reduction.” Under U.S. Department of Energy by Lawrence Livermore National Laboratory. September 2021. https://www.osti.gov/servlets/purl/1820013 //EM

Miscalculation resulting in deterrence failure

Miscalculation in crisis can resulting a failure to deter the outbreak of war via the same pathways as above. First, in a crisis, either side could continue to miscalculate the scope of the other’s interests. Although the immediate interests at stake in a crisis would become clear, Blue might underestimate Red’s willingness to exploit the crisis to secure a related interest; Red might seize on the crisis to engage in horizontal escalation. For instance, Russia annexed Crimea weeks into the Euromaidan crisis. Second, a crisis could escalate to war through Blue or Red’s failure to assess the other’s resolve. Although Blue and Red will have strong incentives to signal their resolve in a crisis over vital interests, in a more complex crisis, miscalculations of resolve may accompany miscalculation of interests. In the Crimean crisis, NATO did not see a need to signal resolve because it miscalculated Russia’s interests. If a crisis arises from a mishap, Blue may be hesitant to engage in overt shows of resolve to avoid provoking rather than deterring Red. A crisis atmosphere may also make signaling harder due to a complex and contested information environment, further limiting each side’s “strategic vocabulary.” Third, a crisis may exacerbate the risk of miscalculating the military balance. All sides will have incentives to be less transparent and predictable. To preserve warfighting advantages, Blue may be hesitant to reveal decisive capabilities, especially those that depend on secrecy. Blue may also hesitate to court escalatory risk through signaling capabilities while Red may conceal forces used for hybrid warfare.

Miscalculation resulting in inadvertent escalation

In a crisis, inadvertent escalation can result from miscalculation of the intent behind mishaps, responses to mishaps, or shifts in the military balance. Although status quo-oriented powers may seek to avoid war and thus may be generous with their interpretations of complex and uncertain events, a sufficiently tense atmosphere could exacerbate paranoia, risk-aversion, and mistrust, fueling escalation. The impact of military behaviors during a crisis on escalation risk are not clear. Blue might respond to a mishap in a way that increases the resilience of their forces, which could allow Blue to avoid further escalation while it assesses the cause of the mishap. Red or Blue might also be aware of the potential for inadvertent escalation and actively seek to manage this risk. Greater senior decision maker attention to military matters during a crisis could contribute to risk management. At the nuclear level, escalation would almost certainly involve deliberate decision making by both sides, reducing the risk. Conversely, crises increase incentives for opacity, limiting the ability to distinguish between true mishaps and guises for aggression. Changes in force readiness could also be escalatory in some contexts, while conventional forces could interactin ways that escalate the conflict even if national leaders do not decide to escalate. Measures to enhance resilience and signal resolve may also cast a nuclear shadow on a crisis and provoke unanticipated escalation. If Blue or Red do not anticipate inadvertence, they might overestimate their ability to control escalation.

Miscalculation in war

Miscalculation resulting in a failure to deter vertical or horizontal escalation. Although each side’s core interests might be well understood when the fighting begins, the war itself may lead Red or Blue’s interests to evolve in ways that increase the risk of miscalculation. Red might view the war as an opportunity to pursue other interests, but Blue might miscalculate Red’s ambitions and fail to deter horizontal escalation. Red might also miscalculate Blue’s interests in the conduct of the war, such as Blue’s reputational interest in punishing violations of the nuclear taboo. Miscalculating Blue’s interests, Red could then see an opportunity to gain advantage through limited nuclear escalation. In a war, both sides will also have strong incentives to signal resolve. Yet the fog of war, as well as a breakdown of diplomatic relations and a shift to a wartime domestic information environment, could make it difficult to send and receive such signals. The conduct of the war itself could also complicate strategic messaging. Forces that might be used to send signals could be committed to other operations or destroyed in the fighting, constraining each side’s strategic “vocabulary.”

Each side’s actions in war may reveal information about the military balance, which could reduce the potential for miscalculation of capabilities. Yet inherent uncertainties about the outcomes of certain military contests may contribute to miscalculation. Some forms of miscalculation may be advantageous. For instance, the US has an interest in encouraging Red to be extremely pessimistic about the outcome of any nuclear exchange. By the same token, however, Red may be prone to overestimate its ability to fight a nuclear war. The uncertainty of how a nuclear war would unfold could make it difficult to dispel Red’s overconfidence without engaging in actions that themselves risk further escalation.

# Domain Awareness Advantage

## Mechanics

### Internal

#### Cross-atlantic satellite capabilities key to SSA.

Antonio Carlo & Nikolaos Veazoglou 20. Previous analyst at the European Space Agency, Sapienza University of Rome; Researcher at the National and Kapodistrian University of Athens “ASAT Weapons: Enhancing NATO’s Operational Capabilities in the Emerging Space Dependent Era.” In: Mazal, J., Fagiolini, A., Vasik, P. (eds) Modelling and Simulation for Autonomous Systems. J. Mazal et al. (Eds.): MESAS 2019, LNCS 11995, pp. 417-425, 03-20-2020. Springer, Cham. //EM edited for grammar.

2 The Applications of Space Platforms

Since the dawn of the space age, outer space has been regarded as the ultimate high ground, which could provide a decisive military advantage to the State that retains superiority over it [2]. In the context of NATO operations space-based assets play an essential role, providing a multitude of services for more than 35 years. Some of the most advanced space-faring States are part of the alliance [3]. It is highly anticipated that in the next leaders’ summit taking place in London NATO will recognize space as a domain of warfare [4].

Since NATO does not own any satellites in orbit, it relys on services provided by governments, military, civilian and commercial entities. NATO has terrestrial SATCOM capabilities and units (terrestrial SATCOM anchor stations, transportable satellite ground terminals and equipment). The C2 for SATCOM is managed by NATO Communication and Information Agency (NCIA) and operated by NATO CIS Group (NCISG) [5].

Space-based assets function as force multipliers, providing support and crucial information during the strategic, operational and tactical levels of war. According to the Allied Joint Doctrine for Air and Space Operations, space capabilities provide a wide range of applications such as: global, strategic and intra-theatre satellite communications (SATCOM); positioning, navigation, and timing (PNT) services; terrestrial and space environmental monitoring; space situational awareness (SSA); intelligence, surveillance, and reconnaissance (ISR); NATO Shared Early Warning [6].

1. Satellite Communications (SATCOM): One of the most widespread functions of satellites, either civilian or military, is telecommunications. SATCOM provides support to C2 through its multiple applications, such as the establishment of communications in regions with minimal or even non existent infrastructure; transmission of intelligence; relay of messages and control of UVs.

2. Position, Navigation and Timing (PNT): The PNT data provided by space-based assets are essential for the prosecution of NATO operations, since they are used for precision targeting; tracking of friendly and enemy forces; provision of precise timing which is also vital for the function of networks and accurate navigation of troops.

3. Environmental Monitoring: Meteorological and oceanographic data collected by satellites are crucial to NATO forces since they play an important role in the planning of missions and the selection of the optimal weapons system to be deployed based on weather conditions. Also the knowledge of the conditions on the theater of operations allows forces to take advantage of them, for example the prediction of flooding based on maps developed in Afghanistan was used enhancing military operations and provide humanitarian support [7].

4. Space Situational Awareness (SSA): Space situational awareness is the knowledge regarding the outer space environment, natural and operational, and its effects on NATO operations. SSA applications includes knowledge regarding the operational capabilities and limitations of both allied and adversary space platforms; tracking of space debris; observation of space weather; tracking of adversary activities in outer space and detecting attacks against space based assets. SSA is essential for the function of satellites and the conducting of their missions.

5. Intelligence, Surveillance and Reconnaissance (ISR): Space based assets equipped with sophisticated sensors provide a host of services, such as intelligence gathering, including Signal Intelligence (SIGNIT); target information and damage assessment; warning of attacks and situational awareness.

6. NATO Shared Early Warning (SEW): Dedicated sensors onboard satellites can detect the launch of ballistic missiles and track their trajectory. Satellites also provide NATO with the capacity to detect nuclear explosions (Nuclear Detonation Detection System) which is essential for identifying any violations of international treaties banning nuclear detonations (e.g. the Partial Test Ban Treaty).

## Impact---Kessler

### Impact---Kessler---AT: Defense

#### NASA models validate Kessler

Dennis M. **Bushnell and** Robert W. **Moses 19**, Bushnell, NASA scientist and lecturer, chief scientist at NASA Langley Research Center, Moses, NASA Rocket Scientist, “Reliability, Safety, and Performance for Two Aerospace Revolutions - UAS/ODM and Commercial Deep Space,” https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190025268.pdf

Since the late 1950s, we have launched around 6600 satellites, approximately 1130 of which are still operational. However, many of the non-operational satellites are still in space. There have been approximately 240 explosions in space and many collisions, two of which were major events. All of this has contributed to the current space debris issue. The amount of this space debris is daunting. Estimates indicate about 6000 tons, with some 5000 pieces greater than 1 meter in size, 22,000 greater than 10 cm, 700,000 greater than 1 cm, and 150,000,000 bits greater than 1 mm. Even the smaller pieces, given the closure speeds, can create worrisome effects upon impact. As an example, an impact speed of 12 km/sec has approximately 10 times the energy density of dynamite. A quote from a 2011 National Research Council report entitled Limiting Future Collision Risk to Spacecraft, summarizes that year’s outlook, which is becoming ever more serious: “When a handful of reasonable assumptions are used in NASA’s models, scenarios are uncovered that conclude that the current orbital debris environment has already reached a ‘tipping point,’ meaning the amount of debris currently in orbit–in terms of the population of large debris objects, as well as overall mass of debris in orbit–has reached a threshold where it will continually collide with itself, further increasing the population of orbital debris.” The increase in orbital debris will lead to corresponding increases in spacecraft failures, which will only result in more debris in orbit. The increase thus far has been most rapid in LEO, with GEO potentially suffering the same fate, although over a much longer time period. The exact timing and pace of this exponential growth are uncertain, but the serious implications of such a scenario require careful attention because of the strategic and commercial importance of U.S. space operations. In the literature, this cascading of collisions producing ever more debris until the space region is essentially unusable is termed the Kessler Effect. Given the increasing worldwide reliance upon space assets, our positional Earth utilities have made space debris an increasingly serious problem.

#### As well as ESA models and NASA and NORAD catalogues

Elisabetta **Bergamini et al**, Department of Enterprise EngineeringUniversity of Rome Tor VergataRomeItaly, Francesca Jacobone, Department of EngineeringUniversity of Rome ThreeRomeItaly Donato Morea, Department of Industrial EngineeringUniversity of Rome Tor VergataRomeItaly, Giacomi Primo Sciortino, Italian Space Agency (ASI)RomeItaly, **’18**, “The Increasing Risk of Space Debris Impact on Earth: Case Studies, Potential Damages, International Liability Framework and Management Systems” Enhancing CBRNE Safety & Security: Proceedings of the SICC 2017 Conference pp 271-280

The words “space debris” refer to the uncontrolled and unwanted fall onto Earth of no longer functional space vehicles or parts of any size (no asteroids involved whose trajectories and their potential dangers are considered uninsurable acts of God). This definition1 excludes whatever is generated at launch areas, which are conceived to encompass this risk. Since the beginning of human activities in space, the number of variously defined objects in orbit around the Earth has increased exponentially, and the trend is up now more than ever with the new wave of the so-called small satellites. NASA (US National Aeronautics and Space Administration) and ESA (European Space Agency) estimate in their webpages that there are over 150 million “objects” orbiting between the LEO (low Earth orbit)—up to 10,000 km from Earth’s surface—and GEO (geostationary Earth orbit), above this mark, for a total weight of more than 5000 tons. This definition applies to objects ranging from submillimetric (propellant dust, paint flakes, etc.) to “baseball” sizes (ca. 20,000 objects) and more. Figure 1 offers, based on the same aforementioned sources, a dynamic ownership’s graph of these objects, divided by the launching State’s property. The sharp rise of newcomers like China appears very clearly.

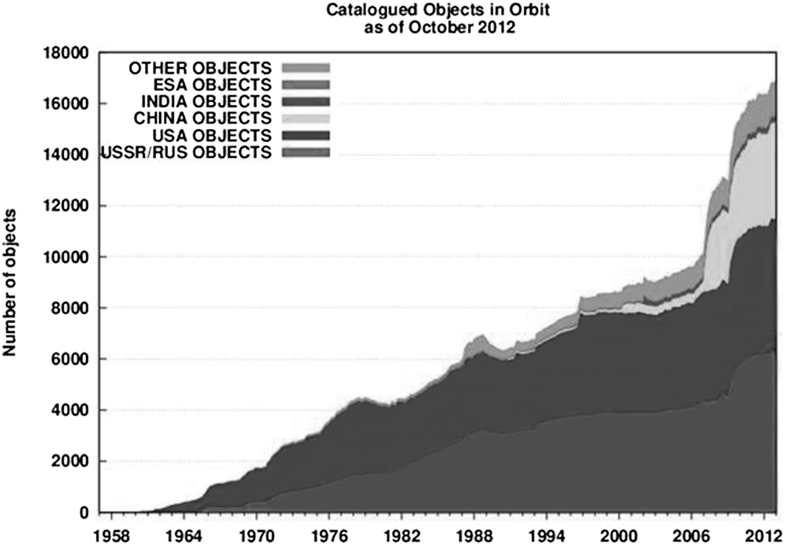


Fig 1. Space debris: how dangerous is it to people on Earth (Source: Globalnews.ca—Nicole Mortillaro [1])

We reasonably estimate that by the end of the decade, the overall quantity will at least triple for the combined effect of the big increase of small satellite cheap launches (Google—Planet Labs, OneWeb, SpaceX, etc.), space and suborbital tourism finally becoming popular in the more dangerous LEOs. What could amplify these fears is mostly the so-called Kessler syndrome [2], which is the massive propagation of debris ensuing collisions in space. As an evidence of this, ESA reports that 65% of the ca. 20,000 notable orbiting objects result from 250 breakups and from just 10 collisions [1]. As an example, consider that the Chinese Feng Yun SO1C antisatellite test, in 2007, created 3300 pieces of sizeable debris, and in February 2009, 2200 more fragments were created by the crash between the US Iridium 33 and the Russian Kosmos 2251 satellites. Consider in fact that at an average speed of 30,000 km/h in LEO, where gravity is stronger [3], even 1-cm-large (there are approximately 300,000 of them) items can destroy a satellite, while risk mitigating techniques, such as vehicle route monitoring and adjustments, debris cleaning, onboard protections, etc., are still shy of being effective. Although 75% of objects launched into space are recorded as they re-entered into the atmosphere in a controlled way (by saving fuel for the end-of-life assisted deorbiting and demise) and the atmosphere itself, should these manoeuvers fail, is a natural “firewall” that destroys anything re-entering at that speed, the risk of impacts on Earth is surging, and its magnitude might be soon perceivable, on persons, land and properties. An elaboration on NASA-NORAD’s archive of catalogued space debris shows that the actual rate of one reported uncontrolled impact a day (>10 wide objects) [4] could increase from three to ten times by the end of the decade, including large items. Our work examines case studies and various levels of debate on the impact of space debris on Earth (legal, liability, surveillance and tracking, debris cleaning techniques, insurance) to identify possible risk management solutions to be developed in the future.

### Impact---Kessler---AT: Debris Good

#### No intrinsic internal link AND concedes that we have an impact.

Gregory 1NC Miller, 21 (Gregory Miller holds a Ph.D. in Political Science from The Ohio State University and is a Professor and Chair of the Department of Spacepower and Director of the Schriever Space Scholars program at the Air Command and Staff College, November 2021, accessed on 6-24-2022, Space Policy, Vol 58, “Deterrence by Debris: The Downside to Cleaning up Space”, https://www.sciencedirect.com/science/article/abs/pii/S0265964621000394#:~:text=An%20unintended%20consequence%20of%20debris,hostile%20actions%20against%20orbital%20objects., HBisevac)

This article does not suggest that orbital debris is the only way to deter attacks in space. Nor does it suggest that we should ignore the deepening problem of space debris, which by itself poses a significant threat to international space interests. It does highlight some of the dangers of rushing into a solution without considering the unintended consequences. While others discuss the potential danger posed by the militarization of technological solutions to debris removal, this article suggests that the danger posed by debris also prevents states from targeting orbital objects more than they otherwise would, simply as a result of international norms or existing law. One cannot prove that debris is a deterrent to states using kinetic interceptors in space. However, if we assume rational actors and that states understand the potential threat that debris pose to their own interests, then they should be reluctant to take actions that will increase the probability they suffer that cost. As a result, there is a downside to cleaning up debris, which is to weaken its deterrent effects.

#### In fact, it increases conflict!

Ian Sample 16. Science editor at The Guardian. “Rise in space junk could provoke armed conflict say scientists.” The Guardian. 1-22-2016. https://www.theguardian.com/science/2016/jan/22/rise-in-space-junk-could-provoke-armed-conflict-say-scientists //EM

The steady rise in space junk that is floating around the planet could provoke a political row and even armed conflict, according to scientists, who warn that even tiny pieces of debris have enough energy to damage or destroy military satellites.

Researchers said fragments of spent rockets and other hurtling hardware posed a “special political danger” because of the difficulty in confirming that an operational satellite had been struck by flying debris and had not fallen victim to an intentional attack by another nation.

Space agencies in the US and Russia track more than 23,000 pieces of space junk larger than 10cm, but estimates suggest there could be half a billion fragments ranging from one to 10cm, and trillions of even smaller particles.

The junk poses the greatest danger to satellites in low Earth orbit, where debris can slam into spacecraft at a combined speed of more than 30,000mph. This realm of space, which stretches from 100 to 1200 miles above the surface, is where most military satellites are deployed.

In a report to be published in the journal Acta Astronautica, Vitaly Adushkin at the Russian Academy of Sciences in Moscow writes that impacts from space junk, especially on military satellites, posed a “special political danger” and “may provoke political or even armed conflict between space-faring nations. The owner of the impacted and destroyed satellite can hardly quickly determine the real cause of the accident.”

Adushkin adds that in recent decades there have been repeated sudden failures of defence satellites which have never been explained. But there are only two possibilities, he claims: either unregistered collisions with space debris, or an aggressive action by an adversary. “This is a politically dangerous dilemma,” he writes.

The warning comes after an incident in 2013 when a Russian satellite, Blits, was disabled after apparently colliding with debris created when China shot down one of its own old weather satellites in 2007. The Chinese used a missile to destroy its satellite, an act that demonstrated its anti-satellite capabilities, and left 3,000 more pieces of debris in orbit.

According to the report, the amount of debris cluttering low Earth orbit has risen dramatically in half a century of spacefaring. Without efforts to clean up the space environment, Adushkin warns of a “cascade process” in which chunks of debris crash into one another and produce ever more smaller fragments.

Data in the study from the Russian space agency show that the International Space Station took evasive action five times in 2014 to avoid space debris. Even small flecks of paint that have flaked off spacecraft can be hazardous. Nasa’s space shuttle was struck by flying paint several times in orbit, forcing ground staff to replace some of the spaceship’s windows.

The report follows a report commissioned by Nasa in 2011 which warned that the level of space junk was rising exponentially, and had reached a “tipping point” in the threat it posed to satellites and the International Space Station.

## Impact---Space Weather

### Impact---Space Weather---AT: Defense

#### Space weather catastrophes ensure extinction.

Julia Rosen, 16 (Julia Rosen is a science reporter for the Los Angeles Times with a PhD in geology, accessed on 10-20-2021, Science.org, 7-14-2016, “Here's how the world could end—and what we can do about it", https://www.science.org/content/article/here-s-how-world-could-end-and-what-we-can-do-about-it-rev2, HBisevac)

As end-of-humanity scenarios go, that bleak vision from Fritz Leiber’s 1951 short story “A Pail of Air” is a fairly remote possibility. Scholars who ponder such things think a self-induced catastrophe such as nuclear war or a bioengineered pandemic is most likely to do us in. However, a number of other extreme natural hazards—including threats from space and geologic upheavals here on Earth—could still derail life as we know it, unraveling advanced civilization, wiping out billions of people, or potentially even exterminating our species. Yet there’s been surprisingly little research on the subject, says Anders Sandberg, a catastrophe researcher at the University of Oxford’s Future of Humanity Institute in the United Kingdom. Last he checked, “there are more papers about dung beetle reproduction than human extinction,” he says. “We might have our priorities slightly wrong.” Frequent, moderately severe disasters such as earthquakes attract far more funding than low-probability apocalyptic ones. Prejudice may also be at work; for instance, scientists who pioneered studies of asteroid and comet impacts complained about confronting a pervasive “giggle factor.” Consciously or unconsciously, Sandberg says, many researchers consider catastrophic risks the province of fiction or fantasy—not serious science. A handful of researchers, however, persist in thinking the unthinkable. With enough knowledge and proper planning, they say, it’s possible to prepare for—or in some cases prevent—rare but devastating natural disasters. Giggle all you want, but the survival of human civilization could be at stake. Threat one: Solar storms One threat to civilization could come not from too little sun, as in Leiber’s story, but from too much. Bill Murtagh has seen how it might start. On the morning of 23 July 2012, he sat before a colorful array of screens at the National Oceanic and Atmospheric Administration’s Space Weather Prediction Center in Boulder, Colorado, watching twin clouds of energetic particles—known as a coronal mass ejection (CME)—erupt from the sun and barrel into space. A mere 19 hours later, the solar buckshot blazed past the spot where Earth had been just days before. If it had hit us, scientists say, we might still be reeling. Now the assistant director of space weather at the White House Office of Science and Technology Policy in Washington, D.C., Murtagh spends much of his time pondering solar eruptions. CMEs don’t harm human beings directly, and their effects can be spectacular. By funneling charged particles into Earth’s magnetic field, they can trigger geomagnetic storms that ignite dazzling auroral displays. But those storms can also induce dangerous electrical currents in long-distance power lines. The currents last only a few minutes, but they can take out electrical grids by destroying high-voltage transformers—particularly at high latitudes, where Earth’s magnetic field lines converge as they arc toward the surface. The worst CME event in recent history struck in 1989, frying a transformer in New Jersey and leaving 6 million people in Quebec province in Canada without power. The largest one on record—the Carrington Event of 1859, named after the U.K. astronomer who witnessed the accompanying solar flare—was up to 10 times more intense. It sent searing currents racing through telegraph cables, sparking fires and shocking operators, while the northern lights danced as far south as Cuba. “It was awesome,” says Patricia Reiff, a space physicist at Rice University in Houston, Texas. But if another storm that size struck today’s infrastructure, she says, “there would be tremendous consequences.” Some researchers fear that another Carrington-like event could destroy tens to hundreds of transformers, plunging vast portions of entire continents into the dark for weeks or months—perhaps even years, Murtagh says. That’s because the custom-built, house-sized replacement transformers can’t be bought off the shelf. Transformer manufacturers maintain that such fears are overblown and that most equipment would survive. But Thomas Overbye, an electrical engineer at the University of Illinois, Urbana-Champaign, says nobody knows for sure. “We don’t have a lot of data associated with large storms because they are very rare,” he says. What’s clear is that widespread blackouts could be catastrophic, especially in countries that depend on highly developed electrical grids. “We’ve done a marvelous job creating a great vulnerability to this threat,” Murtagh says. Information technologies, fuel pipelines, water pumps, ATMs, everything with a plug would be rendered useless. “That’s going to affect our ability to govern the country,” Murtagh says.

#### It's try or die – we’re not ready for space storms, and disruptions collapse society

Hurska, 16

(Joel, citing Joseph N. Pelton, the former dean of the International Space University, “Space invasion: Solar storms pose critical threat to internet, US infrastructure”, <https://www.extremetech.com/extreme/161301-space-invasion-solar-storms-pose-critical-threat-to-us-infrastructure>, 9/13/16)//NRG

Ordinarily, the Earth’s magnetosphere shapes the Van Allen Belts and deflects the charged particles emitted by the sun (called the solar wind), while the VABs act to block high-energy electrons. Periodically, however, the sun releases solar flares. These flares are high-energy events that release a concentrated burst of energy in a particular direction. If that direction happens to be towards us, it can temporarily compress the magnetic field and allow high-energy particles through the Van Allen Belts. The largest flares are sometimes accompanied by a coronal mass ejection — and as Pelton notes, these have the potential to wreak serious damage on both satellites and Earth infrastructure. There’s certainly reason for concern. On September 1, 1859, the most powerful geomagnetic storm of modern times hit the Earth. Aurorae, normally visible only at high latitudes, reached the Caribbean. The glow over the Rocky Mountains was so bright, gold miners reportedly exited their tents and began preparing breakfast. Telegraphs failed across the world — though in some areas, they continued to send and receive messages, even after being disconnected from their electrical supplies. The event became known as the Carrington Event, after British astronomer Richard Carrington — but what caused small problems and unusual events in the 1800s would be absolutely devastating today. The handful of moderate geomagnetic storms in the last 40 years have caused significant damage to the grid; a full hammerblow would destroy the US electrical grid for several years. The economic impact of a similar disaster today is estimated at $2.6 trillion. Often, when online publications write disaster-themed science stories, there are a number of comforting facts buried below the lede to take the edge off. Sure, a dinosaur-level extinction event could make for a really rocky millennium or two on Earth, but the chances of a rock that big hitting the planet are minuscule. Reading up on the potential impact [PDF] a coronal mass ejection (CME) could have on Earth offers no such comfort. The truth is, solar flares as large as the one that caused the 1859 Carrington Event happen fairly regularly. Since we started monitoring the Sun’s solar cycle, we’ve gotten lucky on a number of occasions — CMEs that would have hit us even harder than 1859 have merely glanced us due to a non-ideal trajectory. Meanwhile, the United States’ grid is more vulnerable to such events than ever before — our transformer grid is, on average, nearly 40 years old, high-voltage power lines are carrying far more energy than they used to on a day-to-day basis, and there’s virtually no way to quickly repair the damage such a storm would cause. Cloudy with a chance of civilization-~~crippling~~[destroying] electromagnetic forces Just how much of a threat is this? We consulted the Department of Energy’s own research to get a better idea. According to that report, transformers are custom-designed, highly intricate, take up to two years to manufacture, cost between $5-7 million apiece, and weigh between 100 and 400 tons. Ordinary transformers are far too bulky and heavy to ship by road, and must be moved around the country in specially-designed railcars. Smaller models are available, but are typically more expensive. The United States power grid is utterly incapable of weathering a devastating geomagnetic storm. In worst-case scenarios, the sheer amount of energy flowing down the high-voltage wire would blow transformers in quick succession. The automatic load balancing and considerable safety margins that are built into plants are designed to deal with terrestrial disasters, not space invasions. Offline power capacity normally used for supplementing baseline power during peak hours might survive, but these plants are not staffed or fueled for long duration. Up to 92% of the Northeast’s power generation capability could be taken offline for periods of several years. A cascade failure that took out such a huge swath of our power generation would have untold downstream effects, as people lost the ability to contact emergency services, lost water pressure in areas that rely on electrical pumps, and were forced to rely on limited generator power. The damage estimates aren’t just theoretical — we know the electrical grid is sensitive to such geomagnetic storms after a surge in 1989 caused a major failure of a hydroelectric generator in Quebec. In the wake of that event, some of the US-based power companies instituted safeguards, but they’re woefully lacking compared to what could hit us. Infrastructure protection Even moderate geomagnetic storms cause significant damage or accelerate failures in equipment. Two years after the 1989 storm, 12 mid-sized transformers had failed — all of them significantly earlier than had otherwise been expected. During solar storms on April 3-5 1994, major transformers failed in Illinois at the Zion Nuclear plant as well as facilities in Braidwood and at the Powerton coal plant. The good news is, there are ways to protect the grid and mitigate the damage that another Carrington event would cause. The bad news is, we’re mostly not doing them, despite the catastrophic damage such an event will cause. The Washington DC/New York City corridor is considered to be most at-risk, with 20-40 million people in danger. It would cost several billion dollars to protect existing lines, far less than the $2.6 trillion quoted above from an actual impact.

#### Lack of SSA causes extinction

**Dancer 16** [Benjamin Dancer, Director of Public Relations for the Colorado EMP Task Force on National and Homeland Security, which is the Colorado branch of a Congressional Advisory Board., 5-22-2016 https://www.benjamindancer.com/blog/2016/5/7/space-weather-an-existential-threat]

Could space weather threaten our civilization? It’s not a question most people think about. I started thinking about it for the first time in 2010 when I did the research for my novel Patriarch Run. That research introduced me to a lot of interesting people, and it brought me inside a pretty eclectic community: the small group of experts who understand just how close it is our civilization has chosen to dance to the apocalypse. The sun emitted a mid-level solar flare, peaking at 3:01 p.m. EDT on Oct. 2, 2014. NASA's Solar Dynamics Observatory, which watches the sun 24-hours a day, captured images of the flare. Solar flares are powerful bursts of radiation. Harmful radiation from a flare cannot pass through Earth's atmosphere to physically affect humans on the ground, however -- when intense enough -- they can disturb the atmosphere in the layer where GPS and communications signals travel. This flare is classified as an M7.3 flare. M-class flares are one-tenth as powerful as the most powerful flares, which are designated X-class flares. The Old Man RSS It was that community of experts who invited me in April to the Space Weather Workshop in Broomfield, Colorado. The workshop had three co-sponsors: National Oceanic and Atmospheric Administration (NOAA) Space Weather Prediction Center National Science Foundation (NSF) Division of Atmospheric and Geospace Sciences National Aeronautics and Space Administration (NASA) Heliophysics Division So I got to hang out with the world's foremost experts on the subject of space weather. And let me tell you it was quite surreal to be in a room full of scientists who understood that the factual conversation they were having in the conference hall would be dismissed as the stuff of conspiracy theories if it were to be heard on the street. The gist of what they were talking about is this: over the course of the last century, our civilization has unintentionally evolved to become utterly dependent on an electronic infrastructure that was built without a full understanding of the havoc space weather could wreak on its critical components. In other words, our critical infrastructure is ridiculously vulnerable to the sun's normal weather patterns. Diffuse gas—called plasma—flows outward from the sun as the “solar wind” and carries with it solar magnetic field lines that become entangled with the Earth's own magnetic field lines. Location of "holes" were detected in indicated pink layers, near Earth. One of the most unsettling moments occurred at a talk tucked away in the basement of the hotel given by Bill Murtagh, the Assistant Director of Space Weather for the White House Office of Science and Technology Policy (OSTP). Murtagh summarized what the scientific community currently understands about the impact severe space weather could have on modern civilization. It was a pretty grim analysis. “These space weather events are massive.” Murtagh spread his hands as wide as his arms would allow and said, “If this represents the size of a large coronal mass ejection, the earth would be about the size of a grain of sand between my hands being buffeted by that storm.” Although such events seem rare on a human timescale, the probability is near certainty that the Earth will be hit by very large storms. Such storms could result in economic catastrophe. But it gets worse. A storm large enough could pose an existential threat to the human species. At this point, there are two important questions to answer. 1. How is it that weather from space could threaten electronic systems like the power grid? 2. And how is it that humanity has become so dependent on electricity that the sudden collapse of that infrastructure could threaten systems as rooted in the soil as our food supply? When a coronal mass ejection disturbs the Earth's magnetic field, geomagnetically induced currents (GICs) are created that can fry circuits and melt the windings of heavy-duty transformers. If large transformers at enough substations were to fail, the entire electric grid could go down. A prolonged power outage could last anywhere between a few weeks to forever, depending on the severity of the damage. One of the many issues we'd be facing in such a crisis would be the replacement of the transformers. The windings for these large transformers are handcrafted, and it takes months, if not years, to fulfill an order when the electrical infrastructure is intact. In the event of a crisis, it would be very difficult, if not impossible, to fulfill a large order of replacement transformers. The repair couldn't happen quickly. Meanwhile, if the power is out across the country, a lot of bad things will take place. There is an historical example of this phenomenon. In 1859 the earth was buffeted by a coronal mass ejection known as the Carrington Event. That storm took down the electrical infrastructure of the planet. Fortunately for the people alive in 1859 (and their descendants), civilization wasn't yet dependent on that infrastructure. At this point, I'll transition and answer the second question. If you'd like to learn more about space weather and the mechanisms of destruction to our critical infrastructure, you could read other posts on this blog (there are some great resources at the links in this post) or you could read the intelligence report given to Jack in Patriarch Run. The second question... 100 years ago you didn't need electricity to feed the population. The "pre-electrical" carrying capacity of the planet was less than 2 billion people. Our electrical infrastructure has increased the planet's carrying capacity to 7.5 billion. Before refrigeration, food was grown just outside the urban centers. In other words, everybody ate locally. You can't feed our population of 325 million Americans (and growing) without our electrical infrastructure. The loss of the grid wasn't an existential threat 100 years ago because our grandparents were more self-reliant. They had more agricultural area per capita around their urban centers to meet their needs, as there were only 76 million Americans in 1900. It's just not possible for today's population, which is 4 times as large, to live as close to the land (as locally) as our grandparents did 100 years ago. It is a statement of fact to say that our major metropolitan centers have outstripped their local carrying capacities. To meet the human need we now outsource the production of food and basic goods from around the world. That outsourcing makes us quite vulnerable to an interruption in supply. Moreover, there is a whole list of things we can't do without electricity: irrigate crops, refine fuel, produce fertilizer, produce pesticides, process food, refrigerate food, transport food, etc. So let's examine a worst-case scenario. Without electricity, we could not distribute clean water to our cities or provide sanitation or healthcare. There would be no commerce as we have come to know it. Such a collapse would probably result in widespread starvation, the reintroduction of diseases vanquished by modern sanitation, unprecedented social unrest, and a skyrocketing mortality rate. But what if it's just a little storm? When the big players in Washington, like FEMA, wrapped their heads around the potential catastrophe, they asked Bill Murtagh to answer a couple very important questions. "If we were to prepare for a 100 year storm, what does that look like? What about a 1,000 year storm?" Murtagh's answer. "We don't know. This is a fairly new science, and we don't have enough data yet." The Washington players wanted to know just how big the Carrington Event was? "What do we need to do to prepare for a storm like that?" The answer. "We don't have enough data to know how big that storm was." "Well, then what's the maximum? What's the most the sun can throw at us?" Murtagh's answer. "We don't know." What we do know is that there are critical components to our infrastructure that cannot be easily replaced, which means that there is a damage threshold that if crossed would render the situation unrecoverable.

#### It is a systemically underestimated risk.

Rosen ’16 [Julia; July 14; Ph.D. and science reporter for the Los Angeles Times; Science Mag, “Here’s how the world could end—and what we can do about it,” <https://www.sciencemag.org/news/2016/07/here-s-how-world-could-end-and-what-we-can-do-about-it>]

As end-of-humanity scenarios go, that bleak vision from Fritz Leiber’s 1951 short story “A Pail of Air” is a fairly remote possibility. Scholars who ponder such things think a self-induced catastrophe such as nuclear war or a bioengineered pandemic is most likely to do us in. However, a number of other extreme natural hazards—including threats from space and geologic upheavals here on Earth—could still derail life as we know it, unraveling advanced civilization, wiping out billions of people, or potentially even exterminating our species.

Yet there’s been surprisingly little research on the subject, says Anders Sandberg, a catastrophe researcher at the University of Oxford’s Future of Humanity Institute in the United Kingdom. Last he checked, “there are more papers about dung beetle reproduction than human extinction,” he says. “We might have our priorities slightly wrong.”

Frequent, moderately severe disasters such as earthquakes attract far more funding than low-probability apocalyptic ones. Prejudice may also be at work; for instance, scientists who pioneered studies of asteroid and comet impacts complained about confronting a pervasive “giggle factor.” Consciously or unconsciously, Sandberg says, many researchers consider catastrophic risks the province of fiction or fantasy—not serious science.

A handful of researchers, however, persist in thinking the unthinkable. With enough knowledge and proper planning, they say, it’s possible to prepare for—or in some cases prevent—rare but devastating natural disasters. Giggle all you want, but the survival of human civilization could be at stake.

Threat one: Solar storms

One threat to civilization could come not from too little sun, as in Leiber’s story, but from too much. Bill Murtagh has seen how it might start. On the morning of 23 July 2012, he sat before a colorful array of screens at the National Oceanic and Atmospheric Administration’s Space Weather Prediction Center in Boulder, Colorado, watching twin clouds of energetic particles—known as a coronal mass ejection (CME)—erupt from the sun and barrel into space. A mere 19 hours later, the solar buckshot blazed past the spot where Earth had been just days before. If it had hit us, scientists say, we might still be reeling.

Now the assistant director of space weather at the White House Office of Science and Technology Policy in Washington, D.C., Murtagh spends much of his time pondering solar eruptions. CMEs don’t harm human beings directly, and their effects can be spectacular. By funneling charged particles into Earth’s magnetic field, they can trigger geomagnetic storms that ignite dazzling auroral displays. But those storms can also induce dangerous electrical currents in long-distance power lines. The currents last only a few minutes, but they can take out electrical grids by destroying high-voltage transformers—particularly at high latitudes, where Earth’s magnetic field lines converge as they arc toward the surface.

The worst CME event in recent history struck in 1989, frying a transformer in New Jersey and leaving 6 million people in Quebec province in Canada without power. The largest one on record—the Carrington Event of 1859, named after the U.K. astronomer who witnessed the accompanying solar flare—was up to 10 times more intense. It sent searing currents racing through telegraph cables, sparking fires and shocking operators, while the northern lights danced as far south as Cuba.

“It was awesome,” says Patricia Reiff, a space physicist at Rice University in Houston, Texas. But if another storm that size struck today’s infrastructure, she says, “there would be tremendous consequences.”

Some researchers fear that another Carrington-like event could destroy tens to hundreds of transformers, plunging vast portions of entire continents into the dark for weeks or months—perhaps even years, Murtagh says. That’s because the custom-built, house-sized replacement transformers can’t be bought off the shelf. Transformer manufacturers maintain that such fears are overblown and that most equipment would survive. But Thomas Overbye, an electrical engineer at the University of Illinois, Urbana-Champaign, says nobody knows for sure. “We don’t have a lot of data associated with large storms because they are very rare,” he says.

What’s clear is that widespread blackouts could be catastrophic, especially in countries that depend on highly developed electrical grids. “We’ve done a marvelous job creating a great vulnerability to this threat,” Murtagh says. Information technologies, fuel pipelines, water pumps, ATMs, everything with a plug would be rendered useless. “That’s going to affect our ability to govern the country,” Murtagh says.

### Impact---Space Weather---AT: Resiliency

#### Space super storms wipe out the Earth---solar maximum ensures extinction.

Sebastian Kettley 19. Science reporter citing Dr Kaku, a theoretical physicist at the City College of New York. “Space weather WARNING: 'All hell will break loose' when solar flare CRIPPLES Earth.” January 25, 2019. https://www.express.co.uk/news/science/1077603/Space-weather-warning-solar-flare-hit-earth-michio-kaku-sunspot.

Major solar flares triggered by a solar maximum in [space](https://www.express.co.uk/latest/space) will wreak havoc on Earth and it is only a “matter of time”. Dr Kaku, a theoretical physicist and book author at the City College of New York, has warned modern technology is defenceless against such reckless power. Solar flares are highly-charged streams of gaseous energy particles violently ejected from the Sun out into the solar system. When solar flares strike the atmosphere, they create beautiful displays of light near the North and South Poles, known as aurora. But solar flares also have the power to wipe out communications satellites, disable electronic devices and cause aeroplanes to malfunction. At their worst, solar flares can blow out power stations, disable GPS navigation and ground emergency services. Speaking live on Coast to Coast AM Radio, Dr Kaku said solar flares on this scale are rare – they only strike once every 100 to 200 years. But the last known solar flare this powerful struck 150 years ago, suggesting the planet could be due another solar attack soon. Dr Kaku said: “These are rare events, maybe once in 100 years or once in 200 years, but is it is inevitable.” And once the solar flare does strike, the effects will be much more devastating than the aftermath of Hurricane Katrina. In 1859, a major solar flare struck the planet, lighting up the night skies from the North Pole all the way down to Cuba. The flare was caused by a so-called Coronal Mass Ejection (CME) from the surface of the Sun and has caused one of the largest geomagnetic storms on record. Dr Kaku said: “It’s a matter of time, you know, we’ve had a big one 150 years ago in 1859. We’ve had a huge solar flare that hit the Earth. One of these days one of these solar flares is going to hit the Earth Dr Michio Kaku, Theoretical physicist “Back then they only had telegraph poles but even they got shorted out and you could read the newspaper in Cuba at night by the light of the Northern Lights, the Aurora Borealis, as far south as Cuba. “From that, we physicists can recalculate how big that solar flare of 1859 must have been. “If we were hit by another one like that, it would fry our satellites, communications would go down instantly, power plants would be shorted out, and in the worst case – remember this a worst case scenario – we physicists believe that it could be 20-times worse than Hurricane Katrina. “So image 20 Hurricane Katrinas ravaging the Earth simultaneously and you can begin to estimate the kind of damage if there is a direct hit from one of these solar flares. “And we’re headed toward the maximum, so more flares are going off the Sun – we had a big one last month.” The solar maximum is a period of the tumultuous solar activity during an 11-year-long cycle. During a solar maximum, the highest number of sunspots appears and the amount of energy radiating from the star has been known to change the weather on Earth. According to Dr Kaku, the solar maximum is the most likely window of opportunity for a major solar flare to hit the Earth. He said: “So far we’ve dodged the bullet, so far we’ve been able to miss these sale flares, but these solar flares are like bullets and sunspots are like rifles. “Think of rifles shooting bullets into outer space and missing Earth. “Of course outer space is quite big but one of these days one of these solar flares is going to hit the Earth like what happened in 1858 and all hell can break loose.”

#### Mass ejections will destroy all technology globally and collapse the world by 2022.

Michelle Marchante 16. Michelle Marchante, degree in Communication from Florida International University, citing John Kappenman, a space weather consultant; Daniel Baker, a geophysicist of the University of Colorado’s Laboratory for Atmospheric and Space Physics, April 12, 2016. “Humanity to be unplugged in 2022.” http://panthernow.com/2016/04/12/humanity-to-be-unplugged-in-2022/

How long do you think you could survive without technology? A week? A month? How about years? Unfortunately, the sad truth is that almost none of us would be able to survive more than a few days without aid from some type of technological advancement. With our civilization becoming more technologically dependent, even if we think we’re moving into the future, we’re actually moving backwards. We’re capable of doing far more than our ancestors were ever able to thanks to these advancements but if we were to be entirely stripped of them, we would be far worse off. Being stripped away of every possible tech-equipment in the world may seem impossible but it’s [it is] actually a reality that is quickly approaching; all that is required is contact from an electromagnetic pulse (EMP) to Earth from space, and unfortunately, it’s coming. Experts have estimated that there is a significant chance of the Earth sustaining a direct hit by a massive geomagnetic solar storm, consisting of solar flares, which are sudden bursts of solar radiation that occur when the Sun suddenly releases a buildup of magnetic energy and coronal mass ejections- massive bursts of magnetic field and plasma that arise from the solar corona- by 2022. Although these types of space weather events are rare, scientists have recognized for decades that they’re potential threats to our modern-day, technology-driven society and economy. If the Earth were to be hit by a storm such as this, the EMP would be so strong that it’ll easily be able to wipe out every piece of technology found across the world. Electric grid lines, telephone poles and satellites, would be shut down, leaving us powerless and sending civilization as we know it to a complete stop. This may sound far-fetched, almost to the point of coming across as an apocalyptic science fiction, but we have reason to worry, as the Earth already went through an event like this in 1859. The Carrington event caused telegraph equipment everywhere to spark, shut down and in some cases even catch fire, with widespread power failure occurring all over North America and Europe. The results of that space storm in 1859 were devastating. We can infer that the results of this upcoming storm will be worse especially since our global economy is even more dependent on power grids, communications and navigation systems than ever before. “Frankly, this could be one of the most severe natural disasters that the country, and major portions of the world, could face,” John Kappenman, a space weather consultant, told Gizmodo. “Imagine large cities without power for a week, a month or a year,” Daniel Baker, a geophysicist of the University of Colorado’s Laboratory for Atmospheric and Space Physics, said in an interview with National Geographic. “The losses could be $1 to $2 trillion, and the effects could be felt for years.” He said.

### Impact---Space Weather---Turns X Impact

<https://iopscience.iop.org/article/10.1088/1538-3873/ab028e/pdf>

#### TAG.

Robert D. Loper 19. Ph.D. from the Air Force Institute of Technology, Assistant Professor of Space Physics, Spring 2019. “Carrington-class Events as a Great Filter for Electronic Civilizations in the Drake Equation.” Publications of the Astronomical Society of the Pacific. 3-1-2019. https://iopscience.iop.org/article/10.1088/1538-3873/ab028e/meta //EM

3. Potential CME Impacts to an Electronically

Dependent Civilization

Eastwood et al. (2017), the National Academy of Sciences

(2008), and the Royal Academy of Engineering (2013) outline

the potential economic impacts of severe space weather. In

particular, major direct impacts from a Carrington-class CME

could be outlined as including the following.

1. Power grid failure due to destruction of large transformers

by geomagnetically induced currents. The large transformers in question here generally cost about $1 million per

unit and require about 18 months to manufacture, ship, and

install. The National Academy of Sciences (2008) report

estimates such a power grid failure would cost $1–2 trillion

per year6 and last four to ten years.

2. Outages or failures of LEO (low Earth orbit) space assets

due to enhancement of the inner Van Allen belt. A severe

solar storm can also cause ionospheric uplift which can

dramatically increase satellite drag (Tsurutani et al.

2012). Additionally, LEO spacecraft operation could be

disrupted by solar energetic protons (SEPs) generated in

2 At an average speed of 2300 km s–1

, this was faster than a typical CME and

about five times faster than the average solar wind speed.

3 The initial discovery of co-rotating interaction regions was reported by

Smith & Wolfe (2016). 4 Named for the Sumerian god of wind and storms. 5 Located at https://ccmc.gsfc.nasa.gov/models/modelinfo.php?model=ENLIL. 6 The NAS report does not specify if this is a cost for replacing U.S. power

grid components or a global cost, but one could infer from the source that the

$1–2 trillion cost might be only to the U.S. and that the global cost could be

greater.

2

Publications of the Astronomical Society of the Pacific, 131:044202 (5pp), 2019 April Loper

Figure 1. ENLIL model output of proton density (top) and radial velocity from the Sun (bottom) for the 2012 July 23 solar storm. The storm is the result of a corotating interaction region that has just impacted Earth in this picture. Shown also is a CME that launched from the Sun approximately two days earlier and did not hit

Earth. (Courtesy: NASA/GFSC, Community Coordinated Modeling Center).

3

Publications of the Astronomical Society of the Pacific, 131:044202 (5pp), 2019 April Loper

the shock of the CME passage through the solar wind

(Royal Academy of Engineering 2013).

3. Outages or failures of GEO (geosynchronous equatorial

orbit) space assets due to enhancement of the outer Van

Allen belt or due to SEPs generated in the shock of the

CME passage (Royal Academy of Engineering 2013).

4. GPS outages due to GEO spacecraft outages or failures,

or GPS degradation due to ionospheric uplift and

enhancement, potentially lasting several days or longer.

5. Communications outages due to high-frequency and ultrahigh-frequency radio blackouts, as well as cellular communication network and internet collapse due to extended

power outages beyond the limits of generators and stored

fuel. In particular, although optical fiber cables are the

foundation of much of the global communication network,

electrical power is still needed to power optical repeaters

and transmitters (Royal Academy of Engineering 2013).

6. Increased radiation doses to astronauts and airline

passengers (Royal Academy of Engineering 2013). This

is more of a risk for long-haul airline flights or manned

spaceflight.

Major indirect effects could include, but are by no means

limited to, the following:

1. water and waste water shortages due to reduced or

eliminated pumping from power grid failure;

2. fuel shortages due to reduced or eliminated pumping

from power grid failure, which could result in transportation stoppages;

3. food shortages due to transportation stoppages, which

could contribute to increased death rates and incite rioting

and/or looting;

4. reduced hospital care due to water shortages and power

outages, which could contribute to increased death rates

and rates of infection; and

5. a years-long power grid and internet degradation or

outage might irrevocably damage the global economy, in

turn greatly prolonging the time to restore the power grid

beyond the estimate of four to ten years.

If one recalls major disasters caused by terrestrial weather

events like hurricanes Katrina (New Orleans, 2005) and Maria

(Puerto Rico, 2017), one can imagine the sorts of major effects

on people and life in those areas. The most striking difference is

that, whereas humanitarian aid came to bear on these disasters, a

Carrington-class event would be a global catastrophe with little

or no aid forthcoming. Much greater loss of life could result, and

our civilization could be driven back to a much more fractured

and pre-electronic one. For the purposes of another planet’s

Drake equation, our civilization would be eliminated from

the calculation. Conversely, another planet whose electronic

civilization were struck by a Carrington-class CME would be

eliminated from our calculation.

Riley (2012) estimates the probability of another Carringtonclass event occuring within the following decade at about 12%.

This estimate preceded the solar storm of 2012, but a good rule of

thumb would be to estimate this to be the probability of having a

Carrington event during any given solar cycle. Love (2012) and

Kataoka (2013) have calculated probabilities in rough agreement,

but there are a wide range of probabilities in the literature, ranging

from once per 60 years (Tsubouchi & Omura 2007) to once per

500 years (Yermolaev et al. 2018). This work will retain the result

of Riley (2012), which is also used in National Academy of

Sciences (2008) and Royal Academy of Engineering (2013). This

roughly agrees with the “once in a century” designation usually

given to the Carrington event. Royal Academy of Engineering

(2013) indicates that this designator is not well understood given

the relative lack of data, but also that there are several tens of

Carrington-class CMEs every century that either miss Earth or

have lesser impact due to a northward orientation of the

interplanetary magnetic field. As shown in Figure 1, such a

CME has a very wide angular extent (in the 2012 July event, the

CME extended in about a 135° arc from the Sun), which could

strike Earth in three out of eight occurrences.

There is also some indication that a solar storm could trigger

other Great Filter events. Knipp et al. (2016) outlines a solar

storm in 1967 May that nearly triggered a nuclear war, as

American radar operators initially mistook a solar storm for

Soviet jamming. It might also be possible that a Carrington-class

event could unleash or exascerbate an infectious disease due to

reduced hospital care at a critical time, resulting in a pandemic.

### Impact---Space Weather---Bias

#### Solar superstorms supersede every impact---there’s a cognitive bias to dismiss high magnitude, low frequency events.

Rosen 16 [Julia Rosen, science reporter citing Anders Sandberg, a catastrophe researcher at the University of Oxford’s Future of Humanity Institute, Bill Murtagh, serves in the White House Office of Science and Technology Policy as the assistant director for Space Weather, Energy, and Environment Division, Patricia Reiff, a space physicist at Rice University in Houston, Texas, “Here’s how the world could end—and what we can do about it.” July 14, 2016. <https://www.sciencemag.org/news/2016/07/here-s-how-world-could-end-and-what-we-can-do-about-it>]

As end-of-humanity scenarios go, that bleak vision from [Fritz Leiber’s 1951 short story “A Pail of Air”](http://www.gutenberg.org/ebooks/51461) is a fairly remote possibility. Scholars who ponder such things think a self-induced catastrophe such as nuclear war or a bioengineered pandemic is most likely to do us in. However, a number of other extreme natural hazards—including threats from space and geologic upheavals here on Earth—could still derail life as we know it, unraveling advanced civilization, wiping out billions of people, or potentially even exterminating our species. Yet there’s been surprisingly little research on the subject, says Anders Sandberg, a catastrophe researcher at the [University of Oxford’s Future of Humanity Institute](http://www.fhi.ox.ac.uk/) in the United Kingdom. Last he checked, “there are more papers about dung beetle reproduction than human extinction,” he says. “We might have our priorities slightly wrong.” Frequent, moderately severe disasters such as earthquakes attract far more funding than low-probability apocalyptic ones. Prejudice may also be at work; for instance, scientists who pioneered studies of asteroid and comet impacts complained about confronting a pervasive “giggle factor.” Consciously or unconsciously, Sandberg says, many researchers consider catastrophic risks the province of fiction or fantasy—not serious science. A handful of researchers, however, persist in thinking the unthinkable. With enough knowledge and proper planning, they say, it’s possible to prepare for—or in some cases prevent—rare but devastating natural disasters. Giggle all you want, but the survival of human civilization could be at stake. Threat one: Solar storms One threat to civilization could come not from too little sun, as in Leiber’s story, but from too much. Bill Murtagh has seen how it might start. On the morning of 23 July 2012, he sat before a colorful array of screens at the [National Oceanic and Atmospheric Administration’s Space Weather Prediction Center](http://www.swpc.noaa.gov/) in Boulder, Colorado, watching twin clouds of energetic particles—known as a coronal mass ejection (CME)—erupt from the sun and barrel into space. A mere 19 hours later, the solar buckshot blazed past the spot where Earth had been just days before. If it had hit us, scientists say, we might still be reeling. Now the assistant director of space weather at the [White House Office of Science and Technology Policy](http://www.whitehouse.gov/administration/eop/ostp) in Washington, D.C., Murtagh spends much of his time pondering solar eruptions. CMEs don’t harm human beings directly, and their effects can be spectacular. By funneling charged particles into Earth’s magnetic field, they can trigger geomagnetic storms that ignite dazzling auroral displays. But those storms can also induce dangerous electrical currents in long-distance power lines. The currents last only a few minutes, but they can take out electrical grids by destroying high-voltage transformers—particularly at high latitudes, where Earth’s magnetic field lines converge as they arc toward the surface. The worst CME event in recent history struck in 1989, frying a transformer in New Jersey and leaving 6 million people in Quebec province in Canada without power. The largest one on record—the Carrington Event of 1859, named after the U.K. astronomer who witnessed the accompanying solar flare—was up to 10 times more intense. It sent searing currents racing through telegraph cables, sparking fires and shocking operators, while the northern lights danced as far south as Cuba. “It was awesome,” says Patricia Reiff, a space physicist at Rice University in Houston, Texas. But if another storm that size struck today’s infrastructure, she says, “there would be tremendous consequences.” Some researchers fear that another Carrington-like event could destroy tens to hundreds of transformers, plunging vast portions of entire continents into the dark for weeks or months—perhaps even years, Murtagh says. That’s because the custom-built, house-sized replacement transformers can’t be bought off the shelf. Transformer manufacturers maintain that such fears are overblown and that most equipment would survive. But Thomas Overbye, an electrical engineer at the University of Illinois, Urbana-Champaign, says nobody knows for sure. “We don’t have a lot of data associated with large storms because they are very rare,” he says. What’s clear is that widespread blackouts could be catastrophic, especially in countries that depend on highly developed electrical grids. “We’ve done a marvelous job creating a great vulnerability to this threat,” Murtagh says. Information technologies, fuel pipelines, water pumps, ATMs, everything with a plug would be rendered useless. “That’s going to affect our ability to govern the country,” Murtagh says. A major event could occur within our lifetimes. Research suggests that Carrington-like storms strike Earth once every few centuries; a recent study found a 12% chance that such a storm will occur in the next decade.

#### Space weather monitoring systems are overdue for failure.

Debra Werner 1. Master’s degree in Journalism from Northwestern University, a recipient of the 1989 Gerald Ford Prize for Distinguished Reporting on National Defense, citing Daniel Baker, director of the University of Colorado’s Laboratory for Atmospheric and Space Physics, Douglas Biesecker, NOAA National Space Weather Prediction Center’s research and customer requirements section lead, Dave Klumpar, director of Montana State University’s Space Science and Engineering Laboratory, March 6, 2019. “Are small satellites the solution for space weather monitoring?” <https://spacenews.com/are-small-satellites-the-solution-for-space-weather-monitoring/>]

With key space weather satellites expected to fail before U.S. and European agencies launch replacements, “small satellites may be the only way of averting a bleak future,” said Daniel Baker, director of the University of Colorado’s Laboratory for Atmospheric and Space Physics. Many of the instruments the U.S. relies on to monitor solar flares, coronal mass ejections and other phenomena that pose a threat to satellites in orbit and technology on the ground are well beyond their anticipated life spans. The National Oceanic and Atmospheric Administration (NOAA) is sending new instruments into orbit on its latest generation of geostationary weather satellites but other updates to the space weather constellation are likely to fly years after current instruments fail. That’s prompting government, industry and academic experts to consider how cubesats and small satellites could help. “Most of the measurements we’re making for operational space weather certainly can be done with smaller satellites,” said Douglas Biesecker, NOAA National Space Weather Prediction Center’s research and customer requirements section lead. “For certain problems, you want a bunch of distributed satellites.” To date, large government satellites have been packed with multiple state-of-the-art sensors to provide exquisite detail of the space weather environment at a single point in space. While cubesats are not likely to replace the large observatories at the Earth-Sun L1 Lagrange point anytime soon, a constellation of the miniature spacecraft orbiting Earth at all longitudes and various altitudes would be helpful in monitoring energetic particles and magnetic fields, said Biesecker, a solar physicist and program scientist for NOAA’s Deep Space Climate Observatory, a 570-kilogram satellite launched in 2015 to track solar wind from L1, a gravitationally stable perch 1.5 million kilometers from Earth. An aging observing network Key space weather instruments only have a few years left. NASA’s Advanced Composition Explorer, sent to L1 in 1997 to monitor solar wind and energetic particles, is expected to run out of the propellant it needs to maintain its position around 2024. The Deep Space Climate Observatory [DSCOVR] has performed many of the same jobs at L1 since 2015 but it doesn’t have ACE’s ability to measure energetic particles. One of NASA’s two Solar Terrestrial Relations Observatory or STEREO satellites, sent in 2006 to orbit the sun and provide imagery of coronal mass ejections and other phenomena, still works but by 2022 it will be too close to Earth to act as an L5 proxy, meaning it will no longer offer the unique vantage point to detect solar activity days before it reaches Earth. Space weather forecasters face multiyear gaps in several key monitoring capabilities even as existing satellites such as ACE and SOHO continue to operate many years beyond their intended lifetimes. Credit: NOAA graphic. The European Space Agency plans to continue operating the Solar and Heliophysics Observatory (SOHO) until sometime in the first half of the 2020s, when the spacecraft’s solar panels are expected to reach the point where they no longer provide necessary power. SOHO has monitored the sun’s coronal mass ejections from L1 since 1995. To make up for those shortfalls, NOAA launched Geostationary Operational Environment Satellite-16 in 2016 and GOES-17 in 2018 with four space weather instruments. The next satellite in the series, GOES-T, is equipped with the same sensors and was slated to launch in 2020 before NASA discovered problems with the Advanced Baseline Imager’s cooling system. NOAA is seeking funding to install a fifth instrument, a Naval Research Laboratory compact coronagraph, on GOES-U set to launch in 2024. In addition, NASA began soliciting information in October on future space weather satellites, instruments and services in anticipation NOAA’s proposed Space Weather Follow-On, an observatory at L1 to gather imagery of coronal mass ejection and monitor solar wind. Meanwhile, Ball Aerospace is installing an energetic charged particle sensor on Weather System Follow-on-Microwave, an Air Force satellite to track ocean surface winds and tropical cyclone intensity. Starting in the early 2020s, the Air Force plans to install energetic charged particle sensors on all spacecraft. Filling in holes The new programs promise valuable data but space weather monitoring is an enormous job. It requires ongoing observation of the sun, its magnetic field and solar wind as well as Earth’s magnetosphere, ionosphere and thermosphere. “The space weather environment is vast, reaching from the surface of the sun almost to the surface of the Earth,” said Dave Klumpar, director of Montana State University’s Space Science and Engineering Laboratory. “It is a large, highly complex, dynamic and nonlinear system.” The new programs are not likely “to fill the holes in our observing platform; to look at sun in three-dimensions and understand its interactions with nearEarth space,” Baker said. In 2012, Baker and NASA associate administrator Thomas Zurbuchen cochaired the National Research Council’s decadal survey on solar and space physics. That committee recommended annual expenditures of $100 million to $200 million, or $1 billion to $2 billion over a decade, for an operational space weather system. “The agencies and Congress have not had the stomach for doing that,” Baker said. “We have a better chance of getting some pieces of this with small satellites rather than with large satellites.”

## Impact---AT: MC Bad

### Mega Constellations Bad---2AC

#### Redundancy prevents collapse

Paul Brodsky 18, Senior Analyst at TeleGeography, "Submarine Cable Redundancy, Explained," No Publication, https://blog.telegeography.com/what-is-submarine-cable-redundancy

Most cable-using companies follow a “safety in numbers” approach, spreading their networks’ capacity over multiple cables so that if one goes down, their network will run smoothly over other cables while service is restored on the damaged one. This is redundancy.

When multiple submarine cables are available between two nodes, data transmission may take multiple paths. Two cables traveling between nodes provide one level of redundancy. Three provide two levels of redundancy, and so on.

So take David Belson’s story for Dyn, which explains that “with multiple submarine cables landing in Western African countries that provide service between countries…network providers in these countries have an opportunity to take advantage of this redundancy to mitigate the potential impact of problems.”

#### Internet collapse is all hype.

Finnie 14 {Matthew, Chief Technology Officer for Interoute, degrees in electrical and electronic engineering, regular advisor to the European Commission on ICT research and innovation and a member of the CONNECT Advisory Forum, “Is the Internet Really Going to Collapse -- Again?,” Wired, 6/2, http://insights.wired.com/profiles/blogs/is-the-internet-really-going-to-collapse-again#axzz3EeAfWS5k# }

Every couple of months a major report is released that foretells the demise of the things we hold dear in the digital world. These are usually produced in an effort to shock people into reading the report and then promote the author’s solution to the problem. A recent example of this comes from storage behemoth EMC which cited that by 2019 the internet would collapse under the weight of content being relentlessly generated. The general theme of EMC’s report is that our desire to consume and share is ever present. In fact, the accepted assumption now is that if you’re an organisation, you want the content you create to spread globally. By doing that, combined with all you can eat storage offers from the likes of Dropbox and Microsoft, we are all heading for a technological apocalypse as our data centre infrastructure crumbles under the pressure of our storage needs. But actually, that’s just not the case. Technology has a knack of relentlessly improving its capacity to support our insatiable demand. Gordon Moore could be the father of the modern global economy when in 1965 he analysed the density with which you can put transistors onto a silicon wafer. The paper he wrote, called, ‘Cramming more components onto integrated circuits’, Electronics Magazine 19 April 1965, noted that the number of components in integrated circuits had doubled every year from the invention of the integrated circuit in 1958 until 1965. The paper concluded saying that that there was no reason this consistent ‘upgrade’ would ever stop. . What is striking is that the paper was right. The hard disk you bought 10 years ago cost the same, but the volume is 1000 times more. The networks we use are 100 times cheaper and bigger in both direction. The shift to cloud computing is as much about efficiently using silicon as convenience for the customer. Whether it’s to make financial trading faster, take photos with millions of pixels or watch TV on the train, we simply want to do everything everywhere all the time, faster. Technology simply looks at what’s hindering us and removes it. Making technology the ultimate convenience enabler. So will technology just keeping on improving, enabling us to keep up with demand? It might, but there’s a second powerful factor to consider, and that’s our fickle nature as human beings. Our love of convenience feeds our impatience. So if, a great social media site gets overly exploited by people trying to sell to you, or your inbox gets rammed full of promotions we simply switch off and move on to the new thing. Despite all the choice available to us in the big wide digital world, we end up selecting what works for us and leaving what doesn’t to fade away on the digital scrap heap. In essence, we are self correcting our consumption. So will the party carry on forever? Most likely, through a combination of technology-enabling convenience to keep up with demand and humans simply discarding what’s not needed.

# Solvency

## Mechanism

### Solvency---Exercises Key

#### Military exercises are essential towards space capabilities.

Paul A. Tombarge 14. Bachelor of Arts degree in Political Science from the University of Minnesota, a Master of Arts degree in Public Administration from the University of Maryland-Europe, a Master of Arts degree in International Security Studies from the Naval Postgraduate School, and a Graduate Certificate in Space Systems from the Naval Postgraduate School. He was also a U.S. Senior Fellow at the George C. Marshall European Center for Security Studies from 2013-2014. “NATO Space Operations.” George C. Marshall: Euopean for Security Studies from 2013-2014. 12-2014. https://www.marshallcenter.org/en/publications/occasional-papers/nato-space-operations-0 //EM

Exercises

With the upcoming end of the International Security Assistance Force’s (ISAF) mission in Afghanistan, NATO is expected to shift its emphasis from operational engagement to operational preparedness through its CFI. CFI is intended to build on the Alliance’s recent experience in Afghanistan and ensure the Allies can work even more effectively together in the future.102 A key pillar of this initiative is increased exercises as “an essential means for forces to practice tactics, techniques and procedures, promote and gauge interoperability, validate training and, when required, certify headquarters, units and formations.”103

In order to ensure the Alliance is able to fully exploit space capabilities, space operations should be incorporated into a variety of tactical, operational, and strategic level exercises and war games. At the tactical level, this could include such things as a multi-national RED FLAG exercise. RED FLAG is a realistic combat training exercise involving the air forces of the United States and its allies. Conducted on the vast bombing and gunnery ranges of the Nevada Test and Training Range, RED FLAG was established in 1975 to maximize the combat readiness, capability and survivability of participating units by providing realistic training in a combined air, ground, space and electronic threat environment as well as a free exchange of ideas between forces.104 Participating units execute missions against an opposing “Aggressor” force specially trained to replicate the tactics and techniques of potential adversaries. While Red Flag originally developed a flyer's combat proficiency, the last eight years have slowly incorporated space and cyberspace capabilities.105 Previously segregated from the CAF participants, space and cyber operators are now fully integrated at the tactical level as a primary training audience.

At the operational level, NATO could participate in a BLUE FLAG exercise. BLUE FLAG is an U.S. Air Force “Air Combat Command-sponsored exercise program that provides doctrinally-correct air, space, and cyberspace crisis action planning (CAP) and command and control (C2) training for joint/coalition air components and operational-level headquarters at the operational level of war.”106 Just as RED FLAG is intended to increase the combat survivability of tactical forces, the goal of BLUE FLAG is to train commanders and staff officers at the operational level of war so “they can immediately participate in directing an air war and make smart decisions during the critical first days of an engagement.”107

### Solvency---Military Key Warrant---Interoperability

#### Intel sharing key.

Beyza Unal 19. Senior research fellow with the International Security Department at Chatham House. “Cybersecurity of NATO's Space-based Strategic Assets.” Chatham House. The Royal Institute of International Affairs. pp. 7-11. 07-10-2019. <https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets-0/about-author> //EM

Interoperability has been an issue in the land, air, and maritime domains. Space-assets planning would benefit from the lessons learned in those domains – for instance, by studying and understanding the complexities involved in intelligence- and information-sharing across all domains. Allies could allocate funds towards a body of work that could focus on interoperability in space. Doctrines and standardization could help to improve interoperability among allied systems. Yet, allies should also realize that standardization would mean using the same vectors as a baseline, thus leading to an increase in risk (in the remaining vulnerabilities) across the alliance as a whole.

Allies should realize that standardization would mean using the same vectors as a baseline, thus leading to an increase in risk across the alliance as a whole.

In order to share secure information through SATCOM units, France, Germany, Norway and the US have formed the multilateral Coalition Network for Secure Information Sharing (CoNSIS). Through secure communications systems, CoNSIS’s objective is to enable better and more accurate decision-making, within a shorter period of time.71 In order to ease interoperability, CoNSIS uses commercial standards as its baseline.72 For future applications, it is advisable to check whether commercial standards meet cybersecurity demands for military requirements.

Interoperability in technology is desirable but remains a challenging construct. It could become the role of NATO to make national space services interoperable. Creating a catalogue of national services might be a good starting point. Interoperability could also be established at the product level (for example, in the field of space weather information) where the products are standardized across the alliance. In order to incentivize nations to invest in this endeavour, it might be helpful to calculate the cost of inadequate interoperability across the alliance to demonstrate current or potential monetary losses.

**The AFF is key to conflict mitigation---otherwise miscalc is inevitable.**

Himanshu Joshi, 21 (Himanshu Joshi, Research Associate at Allied Market Research., 6-25-2021, accessed on 6-19-2021, Geospatial World, "Increasing role and relevance of geospatial technologies in defense and security", https://www.geospatialworld.net/article/increasing-role-and-relevance-of-geospatial-technologies-in-defense-and-security/, HBisevac)

The demand for the services offered by the geospatial technologies for different applications, such as utilities, transportation, defense & intelligence, infrastructural development, and others, has grown significantly over the years. Geospatial technology is an evolving area of interest that comprises Remote Sensing, Global Positioning System, and Geographic Information System. Companies operating in the geospatial technology field offer satellite imagery, aerial survey mapping services, and satellite data services, among others. This technology allows us to obtain information about the Earth’s surface which is used for further analysis and visualization. The rising advancements and miniaturization of sensors have opened new prospects for geospatial data collection. The smaller versions of the existing systems, for instance, mini-satellites to drones, which are equipped with various sensors, are allowing the experts to gather data that seemed impossible in the past decade. Geospatial technology is playing a crucial role in revolutionizing space missions. A few years back, designing, launching and operating satellites used to be an expensive deal. But, with the advent of small satellites and CubeSats, which are integrated with geospatial technology, space missions are becoming more economical. With the modernization of military technologies, the manner in which the wars are being fought today has completely transformed over the years. Today, the defense forces have to be prepared against the insurgency strategies, advanced weaponry, and the emerging virtual warfare, which makes the use of intelligence regarding the prediction and prevention of such movements just as crucial as on-the-ground warfare operations. Geospatial tools provide the ability to predict, monitor, and counter threats, and help to plan and support the field operations. The use of cutting-edge geospatial analytics software, Big Data, and advanced imaging technologies along with the high-resolution Remote Sensing satellites, drones, and other sensors. This allows a smooth flow of crucial data among law enforcement and intelligence agencies to address pre, actual, and post-war scenarios. The real-time images and insights of the affected areas are critically important to enhance the emergency response time particularly in highly risky zones such as national borders. Considering the fact that the situations can completely transform at any time, the importance of situational awareness has been acknowledged by the defense authorities across the world. Geospatial data is quite helpful for the border security operations to provide precise situational awareness information permitting fast decision-making, while on the other hand, reducing the risks, and increasing national security. To support the army operations across the world and help army units stay ready for any unfavorable circumstances, the U.S. Army Environmental Command’s (USAEC) Geospatial Information & Services team makes use of the geospatial technologies. It uses the technologies to effectively collect, store, interpret, examine and display the information to enhance the decision making of the defense forces. The Israel defense forces are modernizing their equipment to be at par with the capabilities of the global forces. In line with the modernization programs, the Israeli Navy Hydrographic Branch (INHB) is shifting towards the adoption of Geographic Information System (GIS) technology. This forms a part of completely advanced Marine Spatial Data Infrastructure (MSDI) in the country. Some of the prominent players that offer geospatial technologies for defense and security applications are ESRI, Trimble Inc., Maxar Technologies, and Harris Geospatial Solutions, Inc., among others. The companies have been investing in R&D and technological advancements to offer more efficient geospatial technologies for defense and security purposes. For instance, in January 2020 Maxar Technologies signed a long-term subscription deal for SecureWatch (cloud-based earth intelligence platform) with the Defence Geographic Agency (DGeo) of The Netherlands Ministry of Defence. Maxar Technologies also renewed international defense and intelligence contracts for customers in the Middle East and Asia region worth more than $120 million in July 2020. Besides this, in 2017 DigitalGlobe, Esri, and Harris Corporation partnered to provide the expertise of Geospatial Deep Learning and Big Data analytics technologies to Esri’s ArcGIS (Geographic Information System) users. The challenges associated with geospatial data are regarding its processing and analysis. These issues can be easily rectified and the valuable geospatial data can be effectively used by the application of technologies such as Artificial Intelligence (AI) and Machine Learning (ML). A good understanding of geospatial intelligence is crucial for battlespace situational awareness for the defense forces. With the growing digitization of intelligence, surveillance, and reconnaissance (ISR) platforms and sensors, there is an increased demand for Artificial Intelligence, Big Data, and Machine Learning tools to collect, store, and analyze an ever-increasing size of satellite images and intelligence data. AI and ML processes can evaluate images and videos and identify threats more rapidly and more effectively than human operators can. Project Maven- a United States Department of Defense program to create an AI-powered investigation system for unmanned aerial vehicles (UAVs) is based on the AI and ML algorithms which is presently using a TensorFlow-based platform to prepare predictive analytics of drone footage. Geospatial technologies hold great prospects in strengthening the defense and security forces by offering real-time images and insights of the affected areas that help in strategizing the military operations. The incorporation of Big Data and AI with geospatial technologies further enhances the usability of the geospatial data. Geospatial data plays an important role in detecting the developments and movements of the armies. It helps in preparing the strategies to counter the attacks and minimize the losses to weaponry and save the lives of soldiers in a battleground. Investments in the Space program help nations to drive the technology development, advancement in digital service & products for defense and security purposes. COVID-19 pandemic created havoc across the world and severely impacted the cash flow into the defense sector as more and more budget had to be allocated for supporting the healthcare systems. The small and medium-sized players are severely impacted by the economic crisis and are struggling to continue their operations. With the start of COVID-19 vaccination programs across the world, the threats regarding the infection are diminishing and the normalcy in businesses across the world is anticipated to resume soon. This is expected to give a boost to government investment in the defense and security sector, which will benefit the geospatial technology market in the future. The emergence of geospatial technologies in the field of defense and security are expected to enhance the efficiency of the defense intelligence bodies and boost the capabilities of the armed forces over the years. Allied Market Research believes that the adoption of geospatial technologies will lead to an enhancement in the decision-making of the defense and security forces and will help the military establishments to plan robust and technologically driven strategies that will enhance the Defense Intelligence of the nations.

### Solvency---NATO Key---Domain Awareness

#### NATO creates the clear regulatory framework

Alessio Di Mare, 21 (Captain Alessio Di Mare, Italian Airforce, May 2021, accessed on 6-11-2022, Joint Air Power Competence Centre, “The Role of Space Domain Awareness”, https://www.japcc.org/essays/the-role-of-space-domain-awareness/, HBisevac)

NATO neither has its own Space assets nor operates any. It relies on Space capabilities that Alliance nations provide on a voluntary basis. NATO operations strongly depend on Space services, so SDA also becomes a key resource for NATO and it needs more than just a ‘donation’ from Member States. First of all, NATO could be the leading entity to promote the importance of SDA, encouraging the development and improvement of the current architectures and advocating for ideas ranging from the SSA concept of ‘simple routine catalogue maintenance’ to a tactical, predictive, and intelligence-driven capability integrated with Ballistic Missile Defence and Command and Control infrastructure. Moreover, without jeopardizing the independence of a single nation to use its assets as it prefers, NATO could play the role of coordinator for the various national capabilities, integrating them to have a clearer picture of Space and to be able to detect any change or potential threat on the Alliance, similarly to what happens in civil contexts (e.g., EUSST). Our nations’ use of and dependence on Space requires the development of policies and doctrine, tools and resources to maintain the Alliance’s superiority in Space. As mentioned before, no country can face this situation alone. The birth of the new NATO Space Centre at Allied Air Command in Ramstein, Germany,8 could represent the first NATO step in that direction.

#### deterrence

Kai-Uwe Schrogl, 20 (Professor Dr. Kai-Uwe Schrogl is the President of the International Institute of Space Law, 2020, accessed on 6-20-2022, Springer, “Handbook of space security: policies, applications and programs”, <https://link-springer-com.proxy.lib.umich.edu/content/pdf/10.1007/978-3-030-23210-8.pdf>, HBisevac)

Alliances, international cooperation, and the global proliferation of space power also play a significant role in deterrence by denial. This international dimension influences deterrence in several ways. First, the proliferation of states operating or deriving benefits from satellites creates stakeholders who would likely prefer that their satellites were not put in jeopardy. States outside of the deterrence relationship may have their satellites affected negatively if deterrence fails and conflict ensues, such as by orbital debris from kinetic attacks or the indiscriminate effects of broad radio-frequency jamming. Second, the deterring state may provide a global or multinational space-derived service, such as the US Global Positioning System satellites, which if attacked could potentially draw countries reliant on this service into the conflict on the side of the non-aggressor (Harrison et al. 2009). In these situations, an aggressor may be hesitant to attack space systems if it will have to potentially contend with an international response (Sheldon 2008). Third, allied or partner states may assist the deterring state when a conflict breaks out. The space systems of friendly countries can complement and supplement the deterrer’s own capabilities, such as through data sharing agreements, interoperability, or even by assisting in the reconstitution of lost space capabilities. Adversary leadership may be deterred from targeting US satellites if they perceive that the United States could leverage the capabilities of its allies to nullify any anticipated benefit (Sheldon 2008).

Some security experts consider the North Atlantic Treaty Organization (NATO) as being uniquely positioned to bolster deterrence in space through its cooperative alliance. The alliance is increasingly reliant on space for its collective defense and economic prosperity, and an attack on the space assets of any one ally impacts the security of all allies (Schulte 2012). Security experts assert that while NATO is dependent on space-enabled capabilities, its space doctrine and planning have not kept up. Presently, NATO officials are considering how the alliance should address the growing military capabilities of Russia and China, to include issuing NATO’s first strategy for space. The strategy is expected to make space an official domain of operation, giving structure to discourse on military developments in space and NATO’s response. The alliance may also decide that attacks in space would trigger the organization’s Article 5 provisions on collective defense, although internal differences on the subject remain. Analysts have long held that NATO should continue to build the expertise and capacity to conduct operations enabled by space; ensure that doctrine, requirements, and planning account for the operational advantages provided by space; and adapt exercises and training to ensure forces can effectively exploit space-based capabilities (Schulte 2012). It is still uncertain whether NATO’s space strategy will implement these recommendations.

### Solvency---AT: Say No

Framing issue---they might have generic ‘say no’ cards in reference to space generally, BUT the plan is distinct, protecting space assets that all allies agree on.

#### Allies say yes---it’s a threat to their systems and military survival.

Isabel van Brugen 1-18. Award-winning journalist and currently a news reporter at The Epoch Times and she holds a master's in newspaper journalism from City University of London, 1-18-2022, accessed on 6-23-2022, The Epoch Times, “NATO’s ‘Space Policy’ Outlines Readiness to Jointly Respond to Attacks in Space”, <https://www.theepochtimes.com/natos-space-policy-outlines-readiness-to-jointly-respond-to-attacks-in-space_4219754.html>, HBisevac

“At the 2021 Brussels Summit, Allies agreed that attacks to, from, or within space present a clear challenge to the security of the Alliance, the impact of which could threaten national and Euro-Atlantic prosperity, security, and stability, and could be as harmful to modern societies as a conventional attack. Such attacks could lead to the invocation of Article 5. A decision as to when such attacks would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis,” [the document states](https://www.nato.int/cps/en/natohq/official_texts_190862.htm).

Article 5 of NATO’s founding treaty states that an attack on any one of the 30 allies will be considered an attack on them all. Until now, it has only applied to more traditional military attacks on land, sea, or in the air, and more recently in cyberspace.

Considering that members have recognized that space is essential to NATO’s deterrence and defense, NATO will consider a range of potential options, for council approval, across the conflict spectrum to deter and defend against threats to or attacks on allies’ space systems, it said.

Around 2,000 satellites orbit the earth, over half operated by NATO countries, ensuring everything from cellphone and banking services to weather forecasts. Military commanders rely on some of them to navigate, communicate, share intelligence, and detect missile launches.

In December 2019, NATO leaders declared space to be the alliance’s “fifth domain” of operations. Many member countries are concerned about what they say is increasingly aggressive behavior in space by China and Russia.

Space has become “increasingly important” for the security and prosperity of NATO members, the alliance added.

“Space is an inherently global environment and any conflict that extends into space has the potential to affect all users of space. Even in cases where NATO is not involved in conflict, Allies’ space systems could be affected,” the document reads.

NATO noted that a number of nations are developing counter-space and anti-satellite systems.

“Potential adversaries” in particular are pursuing the development of a wide range of capabilities from non-kinetic (such as dazzling, blinding, and jamming of space assets) to kinetic destructive systems (such as direct-ascent anti-satellite missiles, on orbit anti-satellite systems, and laser and electromagnetic capabilities), it said.

“Such space destruction, disruption, degradation, and denial capabilities are further exacerbated by the susceptibility of space to hybrid approaches and the associated difficulty of attributing harmful effects to space systems. Some threats, such as signal jamming and cyber attacks, can potentially be caused also by non-state actors, including terrorist organizations.”

The document says, “Many threats to Allies’ space systems originate in the cyber domain and are likely to increase.”

#### Says yes---it’s wise spread consensus among members.

Jacob Knutson, 1-18 (Jacob Knutson is a newsdesk reporter for Axios covering breaking news, 1-18-2022, accessed on 6-22-2022, Axios, “NATO reveals how it will operate in outer space”, <https://www.axios.com/2022/01/18/nato-extends-defense-principles-outer-space>, HBisevac)

NATO will consider an attack against a member country's assets in space as an assault on the alliance, and such actions could lead to a coordinated armed response from all members if necessary, according to NATO's first formal, public space policy released Monday. Why it matters: The policy reflects the increasing importance of space to more countries. It also normalizes NATO's intentions in space as China, Russia, India and other countries push forward on their science and military ambitions in **orbit and beyond**. It is being published roughly two months after Russia endangered the International Space Station and its crew by testing an anti-satellite weapon against one of its defunct satellites and amid heightened tensions between Moscow and NATO from the crisis over Ukraine. Details: The policy expands on NATO's 2019 classified space policy and a communique released by the heads of member states last year, which said an attack against one member in space will be considered an attack against all. The new policy from NATO goes further and defines its key roles in space, including coordinating allies' space capabilities to help NATO's deterrence and defense efforts in other operational domains: land, maritime, air and cyberspace. It includes a list of principles and tenets the alliance seeks to uphold in accordance with international law, including that the use of outer space for peaceful purposes is in the common interest of all nations and that no country can claim space as its own. Of note: NATO said it is not aiming to become "an autonomous space actor" with its own capabilities but will rather rely on member countries that voluntarily provide "space data, products, services or effects that could be required for the Alliance’s operations, missions, and other activities." What they're saying: NATO has yet to define what constitutes an attack, says Kaitlyn Johnson, a space policy expert at the Center for Strategic and International Studies. It's unclear how it would respond to forms of satellite warfare that temporarily disable or blind targets without permanently damaging them. "They're restating that there's a connection to Article 5 and Article 6, but reading that and interpreting it, we as the public don't know how serious this is, or where are these redlines," she said. "I think the alliance is intentionally being vague about this to leave its options open." Johnson added that NATO's commitment to rely on allies' space capabilities is notable, considering it was one of the first entities to deploy strategic satellites starting in the 1970s. The big picture: Militaries around the world have already become reliant on space-based technologies, and increased competition in space may pressure more countries to pursue or improve their anti-satellite weapons in order to dominate their enemies or deter attacks on their satellites or private industries.

### Solvency---AT: Logistics

#### All organizational and operational challenges are solved by existing systems.

Paul A. Tombarge 14. Bachelor of Arts degree in Political Science from the University of Minnesota, a Master of Arts degree in Public Administration from the University of Maryland-Europe, a Master of Arts degree in International Security Studies from the Naval Postgraduate School, and a Graduate Certificate in Space Systems from the Naval Postgraduate School. He was also a U.S. Senior Fellow at the George C. Marshall European Center for Security Studies from 2013-2014. “NATO Space Operations.” George C. Marshall: Euopean for Security Studies from 2013-2014. 12-2014. https://www.marshallcenter.org/en/publications/occasional-papers/nato-space-operations-0 //EM

Organizational and Operational Challenges

As noted above, one of the key challenges to instituting a new NATO COE – and executing multi-national space operations in general – is security classification and data sharing. The release of classified information to multi-national partners is governed by the national disclosure policies of each NATO member. In order to effectively execute Allied space operations, the Alliance would need to share missile warning, space situational awareness, and other space related data. This is already being done to some level with ballistic missile warning data via the Shared Early Warning System (SEWS) program through which the U.S. Air Force “provides NATO with a continuous enhanced Space-based early warning data feed…in support of the [ballistic missile defense] mission. [Through SEWS,] NATO receives data from space- based sensors with the same accuracy and timeliness as US forces.”98

Moreover, NATO is working on a Coalition Shared Data (CSD) server project that will “allow commanders to instantly tap into real-time data from a number of NATO and national systems…regardless of where those products are stored.”99 The concept was successfully tested during NATO’s BOLD AVENGER/TRIAL QUEST 2007 as well as German Bundeswehr experiment Common Shield 2008 and could be extrapolated for use in a broader NATO space data sharing enterprise.

A second challenge is ensuring member nation systems have some minimum level of interoperability. NATO does already have a multitude of Standardization Agreements (STANAGs), some of which address space related systems and components such as STANAG 4636: Space and Nuclear Hardening Guidelines for Military Satellites, STANAG 4633: NATO Common ELINT Reporting Format, and STANAG 7023: NATO Primary Image Format. However, in light of the Smart Defence initiative which “encourages nations to get the most capability from their defense spending by focusing on greater prioritization, specialization and multinational cooperation in equipment acquisition,”100 NATO should take a fresh look at the spectrum of space systems and determine if new STANAGs should be developed.

### Solvency---Inherency---AT: NATO 2022 Space Policy Solves

#### This is incoherent---the Space Policy just recognized space as a fifth domain---did nothing like the AFF.

Evgeniya Drozhashchikh 2-16. Ph.D. Student in the Faculty of World Politics at Lomonosov Moscow State University, RIAC Expert. “NATO’S Space Policy Ups the Stakes?” Modern Diplomacy. 2-16-2022. https://moderndiplomacy.eu/2022/02/16/natos-space-policy-ups-the-stakes/ //EM

Digging deeper into NATO’s approaches to space, the authors distinguish four key responsibilities that the Alliance associates itself with. They include integrating the space factor into the delivery of collective defence and crisis management tasks; conducing political-military consultations on space-related matters; providing space support to the members’ missions; ensuring interoperability between allies’ space products. To implement these roles, it is required to activate efforts in—at least—nine directions, embracing both technological advancements and measures to ensure political and military cohesion.

Generally speaking, the Space Policy is not at all about devising brand-new cooperation mechanisms, to which we can assign increasing joint space domain awareness, ensuring interoperability of space capabilities and converging approaches to deterrence, defense and resilience in space. Some of the proposed actions have already been in place—take the envisaged mutual trainings and exercises. For some 25 years, the U.S. has been initiating multiple wargames, the most well-known of which are Schriever games[1]. The latter are popular for three key reasons: wide geographic scope of participants including those from NATO, contribution to the analysis of key patterns of future conflicts in space, attraction of both allied military and commercial partners—all of those are reflected in the current Space Policy. Another example of NATO formalizing its previous experiences is the provision regarding application of space assets for solving other domain tasks. Actually, these were operations that NATO members conducted in the late 1990s till the early 2000s, and they have made the global community think of space as an integral component of military planning. Therefore, it may be assumed that the objective of the document was not only to explore new tracks of cooperation but also to officially accumulate the previous ones under the NATO umbrella, thus adding authority points to the organization.

All in all, with the Space Policy endorsed, NATO gained a feasible plan of how to transform space into the fifth operational domain. This domain may be “activated”, on the one hand, if there are attacks to, from, or within space, and on the other hand, if there is a need to increase the effectiveness of operations in other domains. Thus, there are almost no visible constraints for benefitting from space as the high ground.

### Solvency---Inherency---AT: NATO Document Solves

#### Nah bro.

Vivienne Machi 22. Reporter based in Stuttgart, Germany, contributing to Defense News' European coverage. She previously reported for National Defense Magazine, Defense Daily, Via Satellite, Foreign Policy and the Dayton Daily News. She was named the Defence Media Awards' best young defense journalist in 2020. “New NATO policy positions the alliance as a broker, not an owner, in space race.” Defense News. 1-20-2022. https://www.defensenews.com/global/europe/2022/01/20/new-nato-policy-positions-the-alliance-as-a-broker-not-an-owner-in-space-race/ //EM

STUTTGART, Germany – Amid the global race toward a militarized space domain, NATO sees its role firmly planted as a coordinator and interlocutor amidst its member states, but demurs from becoming a space-based actor itself, a recently released document shows.

For the past several years, leaders from the alliance and its 30 member states have declared space an operational domain, trumpeting the need for more holistic and coordinated technology investments. NATO’s “overarching space policy” – which was established in 2019 but made publicly available for the first time on Monday – represents a big step for the alliance to finally codify the importance of the space domain for its wider interests and activities. But certain vague language also makes clear that the partners still diverge in how NATO can concretely involve itself in space, observers said.

The document tries to strike “a balanced tone,” acknowledging the need for NATO to be an active player in the space domain, while shying away from the notion that the alliance is militarizing space, “given sensitivities among allies on this concept,” said Lauren Speranza, director of the Transatlantic Defense and Security program at the Center for European Policy Analysis (CEPA).

Over six pages, NATO describes itself as a point of contact for its members’ ambitions in the space domain, focusing on several “key roles” where it can serve a coordinating function and as a forum for discussion. The document says the alliance “requires” space systems in specific capability areas, but won’t become an “autonomous space actor,” or develop its own platforms for use in the domain.

Where’s the investment?

The capability areas include: space situational awareness; intelligence, surveillance, and reconnaissance (ISR); space-based monitoring of Earth-based domains; satellite communications; position, navigation, and timing; and shared early-warning assets.

A NATO official confirmed to Defense News on Wednesday that the alliance has no intent to collectively develop space-related capabilities for the foreseeable future, noting that it’s more affordable to pay for relevant services when needed.

That’s a missed opportunity, said Nicholas Nelson, a senior fellow with CEPA’s Transatlantic Defense and Security program. NATO has developed its own sovereign capabilities before – most notably its fleet of Boeing E-3A Airborne Warning and Control System (AWACS) aircraft.

The “vast majority” of NATO members don’t have access to sophisticated space equipment, and having access to a joint asset, such as a common satellite bus, would be “value-accretive, both for the cohesion of the alliance, as well as the capabilities,” he noted.

The document overall provides key insight into NATO’s collective thinking of the space domain, said Simona Soare, a research fellow for defense and military analysis at the International Institute for Strategic Studies.

“The focus on interoperability and sharing best practices is welcomed as key to the allies’ and the alliance’s ability to ensure its core tasks, most important of which remains collective defense, in a context in which an increasing number of allies and partners are considering developing their own space capabilities and assets,” she said.

The policy release follows the alliance’s concerted focus in recent years on seven so-called “emerging and disruptive technologies,” or EDTs. NATO has advocated for its 30-strong members to invest more holistically and strategically in these EDTs, and this year, the alliance released – or made public – three related policies, on artificial intelligence, on cyber, and now on space.

Where’s the red line?

The space policy is essentially the same document that the alliance agreed upon in 2019, the NATO official told Defense News. The main update comes toward the end of the document, in a section that describes how members agreed that attacks to, from, or within space on an ally could trigger an Article 5 decision on a “case-by-case basis.”

But the publicly released document still provides scant details about how NATO allies actually plan to respond to hybrid threats in and from space, likely because member-nations don’t completely agree on where the red lines should be, analysts noted.

“I think the possible response options are less fleshed out in space, and allies will be less comfortable reaching consensus and taking action,” Speranza said.

NATO has purposefully maintained ambiguity about its red lines in other operational domains. The alliance’s new cyber policy, released in June, revealed the decision to consider that certain “lower-level” malicious cyber attacks by the same threat actor can be as destructive as a single, large-scale cyber attack, and could, at least in theory, trigger the treaty’s Article 5 collective defense mechanism.

The document also avoids naming any specific state or non-state actors as threats in the space domain, and focuses instead on the types of capabilities and effects that could threaten allies in space. This could be related to differences of perspective among the allies when it comes to responding to these actors with either dialogue, or deterrence, Soare said.

More to come?

Parts of the new space policy make clear that NATO’s role in the domain is still a work in progress. A section involving “deterrence, defense, and resilience” states that the alliance “will consider” a range of “potential” options to counter threats against a member state in space, and that NATO “should develop” a common understanding of concepts “such as the role of space in crisis or conflict.” Certain guidelines “will need to be developed” on the way to secure NATO’s access to space data, products and capabilities, it adds.

It’s critical that NATO eventually establishes common terminology for its EDTs, but finding agreement there may be one of the biggest obstacles for the alliance to really define its collective space strategy, Nelson said. “The nomenclature they use for space – as well as cyber – still differs when you’re talking to different stakeholders.”

While individual member nations like the United States, France, and the United Kingdom have already developed their own defense-related space doctrines, a collective NATO strategy is still in progress, the alliance official explained. But this space policy is meant as a lasting policy, and the goal is to now implement that policy through concrete actions, like completing the nascent NATO Space Center at Ramstein Air Base in Germany and launching the future NATO space center of excellence in Toulouse, France, according to the official.

Analysts expect NATO to more concretely define its stance on space in future documents, and certainly in the lead-up to the 2022 summit, to be held in June in Madrid. There, leaders plan to unveil the alliance’s new “Strategic Concept” white paper, the first update since 2010.

“I am optimistic about the direction NATO is going,” Nelson said. “I would like them to move faster, … but with that said, this is a good first step.”

### Solvency---Inherency---AT: 2020 MoU Solves

#### This was just SATCOM NOT military integration---also proves the MoU can be between 4 countries.

NATO 20. “NATO begins using enhanced satellite services.” NATO. 2-12-2020. https://www.nato.int/cps/en/natolive/173310.htm?selectedLocale=en //EM

On Wednesday (12 February 2020) NATO held a ceremony to mark the conclusion of a Memorandum of Understanding between four nations for the provision of critical satellite communications services to NATO for the next 15 years.

The memorandum between France, Italy, the United Kingdom and the United States enables the four Allies to provide space capacity from their military satellite communications (SATCOM) programmes to NATO. Nations began delivering the capability on 1 January 2020.

At the ceremony, the Assistant Secretary General for Defence Investment Camille Grand said:

"NATO depends on space for a wide range of activities, from intelligence gathering and navigation, to tracking forces around the globe and detecting missile launches". Adding that space is essential for the Alliance's deterrence and defence, he said that "NATO also aims to serve as a forum for political-military consultations and information sharing on relevant deterrence and defence related space developments".

Last year, NATO authorized 1 billion EUR for satellite communications (SATCOM) services for the next 15 years. The NATO Communications and Information (NCI) Agency is responsible for operating the satellite communications capability to deliver services to NATO. The NCI Agency coordinated the agreement with the service-providing Nations. This landmark agreement will provide a greater, more resilient and more flexible space capability for NATO to conduct its operations and exercises. National experts will be embedded with the NCI Agency to deliver this critical capability.

# T

## Security Cooperation

### T-Security Cooperation

#### The AFF is enforced by the Space Force---which conducts security cooperation.

DCSA 21. Part of the United States Department of Defense, provides financial and technical assistance, transfer of defense matériel, training and services to allies, and promotes military-to-military contacts.“The Security Cooperation Enterprise.” Defense Security Cooperation Agency. September 2021. https://www.dsca.mil/50th-anniversary/the-security-cooperation-enterprise //EM [SC = security cooperation]

DSCA leads a Security Cooperation (SC) enterprise of more than 20,000 personnel and provides policy, legal, financial, legislative, programmatic, and weapons system expertise to stakeholders across the U.S. interagency. Here are other stakeholders in the SC process:

The Office of the Secretary of Defense (OSD) establishes military requirements and implements programs to transfer defense articles and services to eligible foreign countries and international organizations.

The Under Secretary of Defense for Policy (USD(P)), which DSCA falls under, serves as the principal staff assistant and advisor to the Secretary of Defense on SC matters.

The Defense Technology Security Administration (DTSA), an agency under USD(P), establishes DoD technology security policies related to the international transfer of defense-related goods, services, and technologies. DTSA reviews and provides expert recommendations on foreign access to U.S. military technology foreign purchases of U.S defense industry.

The Military Departments (MILDEPs) advise the Secretary of Defense on all SC matters for their respective departments. The MILDEPs also execute foreign sales and training as Foreign Military Sales (FMS) “Implementing Agencies” (IAs):

Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation (DASA (DE&C)) provides policy oversight for international affairs functions, including FMS.

U.S. Army Security Assistance Command (USASAC) provides management oversight of Army SC programs.

Office of the Deputy Assistant Secretary of the Navy (International Programs) (Navy IPO) provides policy oversight of Navy, Marine Corps, and Coast Guard SC Programs.

Office of the Deputy Under Secretary of the Air Force, International Affairs (SAF/IA), provides policy oversight for all Air and Space Force SC programs.

#### Space Force is under Title 10.

USC, ND (United States Code, No Date, accessed on 6-26-2022, 10 USC Ch. 908: THE SPACE FORCE, §9081. The United States Space Force, “Title 10—ARMED FORCES”, <https://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleD/part1/chapter908&edition=prelim>, HBisevac)

From **Title 10**—ARMED FORCES

Subtitle D—Air Force and Space Force

PART I—ORGANIZATION

CHAPTER 908—THE SPACE FORCE

Sec.

9081.The United States Space Force.

9082.Chief of Space Operations.

9083.Office of the Chief of Space Operations: function; composition.

9084.Office of the Chief of Space Operations: general duties.

9085.Regular Space Force: composition.

9086.Space Development Agency.

Editorial Notes

Amendments

2021—Pub. L. 117–81, div. A, title X, §1081(a)(33), Dec. 27, 2021, 135 Stat. 1921, redesignated item 9084 "Space Development Agency" as 9086 and transferred it to appear after item 9085.

Pub. L. 116–283, div. A, title IX, §§921(b), 922(e), title XVI, §1601(b), Jan. 1, 2021, 134 Stat. 3805, 3807, 4042, added items 9083, 9084 "Space Development Agency", 9084 "Office of the Chief of Space Operations: general duties", and 9085 and struck out former item 9083 "Officer career field for space".

§9081. The United States Space Force

(a) Establishment.—There is established a United States **Space Force** as an armed force **within** the Department of the **Air Force**.

(b) Composition.—The Space Force consists of—

(1) the Regular Space Force;

(2) all persons appointed or enlisted in, or conscripted into, the Space Force, including those not assigned to units, necessary to form the basis for a complete and immediate mobilization for the national defense in the event of a national emergency; and

(3) all Space Force units and other Space Force organizations, including installations and supporting and auxiliary combat, training, administrative, and logistic elements.

(c) Functions.—The Space Force shall be organized, trained, and equipped to—

(1) provide freedom of operation for the United States in, from, and to space;

(2) conduct **space operations**; and

(3) **protect** the **interests** of the United States in space.

#### Space Force is under the DoD---for reference.

Gov, ND (Gov, No Date, accessed on 6-26-2022, “Department of Defnese- Air Force”, <https://www.federalregister.gov/agencies/defense-department>, HBisevac)

[Department of the Air Force Homepage](http://www.af.mil/)

[Headquarters United States Air Force](http://www.af.mil/sites/usaf.html)

[Air Combat Command](http://www.acc.af.mil/public/index.html)

[Air Education and Training Command](http://www.aetc.randolph.af.mil/)

[Air Force Materiel Command](http://www.afmc.wpafb.af.mil/)

[Air Force Research Laboratory](http://www.afrl.af.mil/)

[Air Force Reserve Command](http://www.afrc.af.mil/)

[Air Force Reserve Officer Training Corps (AFROTC)](http://www.af.mil/sites/afrotc.html)

[Air Force Special Operations Command (AFSOC)](http://www.afsoc.af.mil/)

[**Air Force Space Command**: 14th Air Force Flying Tigers](http://www.spacecom.af.mil/hqafspc/)

[Air Force Mobility Command](http://www.amc.af.mil/)

[Air National Guard](http://www.ang.af.mil/)

[Pacific Air Forces](http://www2.hickam.af.mil/)

[U.S. Air Forces in Europe](http://www.usafe.af.mil/)

Field Operating Agencies

[Air Force Agency for Modeling and Simulation](http://www.afams.af.mil/)

[Air Force Audit Agency](http://www.afaa.hq.af.mil/)

[Air Force Base Conversion Agency](http://www.afbca.hq.af.mil/)

[Air Force Center for Environmental Excellence](http://www.afcee.brooks.af.mil/)

[Air Force Civil Engineer Support Agency](http://www.afcesa.af.mil/)

[Air Force Colonel Matters Office](http://www.colonels.hq.af.mil/)

[Air Force Communications Agency](http://public.afca.scott.af.mil/)

[Air Force Historical Research Agency](http://www.au.af.mil/au/afhra/)

[Air Force History Support Office](http://www.airforcehistory.hq.af.mil/)

[Air Force HQ Air Intelligence Agency](http://www.aia.af.mil/)

[Air Force Information Warfare Center](http://www.afiwc.aia.af.mil/)

[Air Force Inspection Agency](http://www-afia.saia.af.mil/)

[Air Force Logistics Management Agency](http://www.il.hq.af.mil/aflma/)

[Air Force Manpower & Innovation Agency](http://www.afmia.randolph.af.mil/)

[Air Force Manpower Readiness Flight](http://www.afmia.randolph.af.mil/afmia/index-afmrf.htm)

Requirements Determination & Utilization

[Competitive Sourcing](http://www.afmia.randolph.af.mil/afmia/about/cs.htm)

[Programs Integration Division](http://www.afmia.randolph.af.mil/afmia/mip/index.htm)

Technical Guidance, Modeling & Simulation

[Information Systems Division](http://www.afmia.randolph.af.mil/afmia/about/sys.htm)

[Air Force Medical Support Agency](http://usafsg.satx.disa.mil/)

[Air Force National Security Emergency Preparedness Agency](http://www-afnsep.forscom.army.mil/)

[Air Force News Agency (AFNEWS)](http://www.afnews.af.mil/)

[Air Force Office of Scientific Research](http://www.afosr.af.mil/)

[Air Force Office of Special Investigations](http://www.dtic.mil/afosi/)

[Air Force Office of Survivor Assistance](http://survivorassistance.afsv.af.mil/)

[Air Force Personnel Center](http://www.afpc.randolph.af.mil/)

[Air Force Safety Center](http://www-afsc.saia.af.mil/)

[Air Force Services Agency](http://www-p.afsv.af.mil/default.nav.asp)

[Air Force Studies and Analyses Agency](http://www.afsaa.hq.af.mil/)

[Air Force Technical Applications Center](http://www.aftac.gov/)

Air Force Weather Agency

[Air Force Intelligence Agency](http://www.aia.af.mil/)

[Air Force Reserve Personnel Center](http://www.arpc.org/)

[United States Air Force Academy](http://www.usafa.af.mil/)

### T-Security Cooperation---W/M---Title 10

#### Space force is under Title 10.

LII / Legal Information Institute 17. “10 U.S. Code § 9081.”12-12-2017. https://www.law.cornell.edu/uscode/text/10/9081 //EM

(a)Establishment.—

There is established a United States Space Force as an armed force within the Department of the Air Force.

(b)Composition.—The Space Force consists of—

(1)the Regular Space Force;

(2)all persons appointed or enlisted in, or conscripted into, the Space Force, including those not assigned to units, necessary to form the basis for a complete and immediate mobilization for the national defense in the event of a national emergency; and

(3)all Space Force units and other Space Force organizations, including installations and supporting and auxiliary combat, training, administrative, and logistic elements.

(c)Functions.—The Space Force shall be organized, trained, and equipped to—

(1)provide freedom of operation for the United States in, from, and to space;

(2)conduct space operations; and

(3)protect the interests of the United States in space.

## Cybersecurity

### T-Cyber Security

#### Cybersecurity is the protection and defense of both analogue and digital electronic devices and their communication channels---it can entail both defensive and offensive operations

RWCS ’20 [Real World Cyber Security; April 14; cyber analyst with deep expertise and extensive experience in embedded systems product development and product development security, including hardware security, secure boot, software and firmware security, network and protocol security, operating systems hardening, user interaction and user experience security, industrial design security, data protection and data privacy, cryptographic security, secure software development practices, security test and evaluation, government product security certifications and validation, intellectual property protection, import/export compliance, product liability, supply chain integrity, security in mergers and acquisitions, and corporate security governance; RWCS, “Defining Cybersecurity,” <https://medium.com/swlh/defining-cybersecurity-44cf1b1d6ae0>]

If You Can’t Properly Define Cybersecurity, How Can You Know What It Is?

It’s clear that the cybersecurity industry hasn’t been able to agree upon what cybersecurity is and isn’t. Even NIST, who is responsible for the definition of technical terms used by the U.S. Federal Government, has four different definitions of cybersecurity! At a minimum, there are dozens of different definitions of cybersecurity currently in use. Nearly all are incomplete in scope, some are horridly wrong, and nearly all fail to differentiate between cybersecurity and its information security cousin.

Background

If you look up the definition of “cybersecurity,” most of the answers you get are laughable. Most appear to be written by some “expert” with no actual concept of what cybersecurity is. Nearly all of those definitions sound as though they were written by an academic pontificating what he thinks cybersecurity theoretically should be, without himself ever having done any actual hands-on cybersecurity engineering.

Until July 2019, the sole “official” definition of cybersecurity (as defined by NIST) was: “The ability to protect or defend the use of cyberspace from cyber attacks.” Hyper-informative, wasn’t it? It’s about like telling a man who’s never seen a donut that, “A donut is a pastry shaped like a donut torus.” [See note 1.]

Then, just when you think it can’t get worse, it does. Now NIST can’t even agree within itself what cybersecurity is! It now four different definitions of cybersecurity! None of them tell you anything particularly useful about cybersecurity. Those definitions of cybersecurity are: [2]

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

The ability to protect or defend the use of cyberspace from cyber attacks.

The process of protecting information by preventing, detecting, and responding to attacks.

The prevention of damage to, unauthorized use of, exploitation of, and — if needed — the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

If you search online for a definition of cybersecurity, most definitions are just as bad — if not worse — than the definitions NIST provides. Here are some examples:

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. [3]

The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. [4]

May also be referred to as information technology security. [5]

The preventative techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access. [6]

The practice of protecting systems, networks, and programs from digital attacks. [7]

The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems. [14]

Notice the pattern? The definitions all talk about defending computers, networks, and data. That isn’t what cybersecurity is. That’s what information security is! Plus, the scope is strictly digital in many cases. Clearly, whoever wrote those definitions have no experience with industrial controls security, where even analogue devices can be at risk of attack. [8]

We have two problems here. First, we have failed to define what cybersecurity adequately or accurately is. Worse, we are trying to somehow shoehorn cybersecurity into being either the same as information security or some subset of information security. It isn’t, and I’ll go into detail why in a minute.

So, if we can’t even agree upon what cybersecurity is, how can we possibly expect to create reasonably secure systems and products that depend upon an in-depth understanding of cybersecurity?

Clearly, we can’t.

And, the problem is compounded by the mindset that the same tools and techniques used for information security are applicable to cybersecurity. Yes, most information security tools and techniques can be applied to cybersecurity, but cybersecurity requires tools and techniques which go far beyond those of information security.

How can we expect to secure our systems when we are using the wrong tools? Or, at best, an incomplete set of tools?

Again, clearly, we can’t.

In my professional opinion, the root of the problem we’re facing is that too many “cybersecurity experts” began their careers as “information security experts” and never have had actual hands-on cybersecurity experience beyond applying partial aspects of cybersecurity to information systems. Thus, we are left with information-centric definitions of cybersecurity, where the “experts” have tried to mold cybersecurity into the shape of information security.

Well, it’s time to break that mold!

Let’s get started with a few definitions.

Definitions

First, let’s define security:

Security is the protection of assets from threats.

That’s fairly clear, but let’s dissect it to ensure the subtleties are covered:

Assets are anything tangible or intangible that has value. In the context of security, usage of the word “asset” usually refers to a “protected asset.”

Protected Assets are any asset protected by a security service. Examples of protected assets could include: data or information (electronic or physical), network and computing infrastructure, software, products and associated intellectual property, people (employees, customers, vendors), real estate and personal property, and utilities and other critical infrastructure. That is, anything of value is a potential protected asset.

Security Services are any threat reduction capability provided by security. There are five generally recognized security services: Confidentiality, Integrity, Availability, Authenticity, and Access-Control. (See the blog post, What Are The Fundamental Services Provided By Security? Hint: CIA Is Not The Answer for additional details.)

Threats are anything with the potential to cause harm. For example, the potential for an attack to occur. Threats can be either intentional (e.g., sabotage) or accidental (e.g., aircraft bird strike), and they can be both man-made events (e.g., human errors, cyber attacks, power failures, and network outages) or natural events (e.g., fires, floods, earthquakes, hurricanes, and tornados). Also, see security threats, below.

Attacks are any action taken against an asset with the intention of causing harm.

Security Threats are anything that may cause harm to a protected asset and/or associated entities. For example, whereas a security threat that discloses personally identifiable information would most likely inflict minimal harm to the asset that held the disclosed information, the disclosure itself could do considerable harm to both the organization’s brand and to the individuals whose information was disclosed. There are seven generally recognized categories of security threats: Denial of Access, Forgery, Spoofing, Repudiation, Unauthorized Access, Unauthorized Disclosure, and Unauthorized Modification (see blog post referenced in Security Services for more details.).

Entities, in the context of security, are anything that attempts to use a protected asset. An entity can be a person, software, robot, or anything else that attempts to use a protected asset.

Okay, I lied: That definition has a lot of subtly buried within it. Hopefully, now the definition of security has a deeper meaning for you.

So, that’s the definition of the mission of security across all of the organization’s security domains. In most organizations, there should be three top-level security domains:

Corporate Security

Information Security

Cyber Security

Now, let’s define each of those security domains.

Corporate Security

Corporate Security is those aspects of an organization’s security not directly related to technology.

That is, in general, corporate security is those aspects of security that pre-date technology or technological security solutions, or are unrelated to technology. Falling under the corporate security domain would be aspects of security related to employee services, safety, environmental services, or facilities; or which are intellectual property, legal, or regulatory in nature. (This is not an all-inclusive list.)

In other words, much of what you would think of as an organization’s security before the advent of digital technologies falls into the corporate security domain.

Today, corporate security often makes extensive use of technology. But, corporate security’s technology is often not under the auspices of information security or cybersecurity. Without close collaboration between security groups, serious gaps in security defenses will occur.

Worse, there often isn’t a corporate security group in the organization. Instead, you often find aspects of corporate security disbursed between multiple (and, often non-communicating) groups, such as human resources, facilities, safety, plant protection, legal, risk management, and environmental.

I plan to discuss corporate security in more detail in an upcoming blog post, Corporate Security: The Forgotten Security Domain.

Information Security

Information Security is the protection of information in any form and at all times.

That’s pretty much the classic paragraph-long definition of information security, summarized into one sentence.

Now, let’s dissect it to get a deeper understanding of what that means.

Security is the protection of assets from threats.

Protection is the rendering safe from harm. Protection is passive security. That is, security that does not offer a response to an attack. It is equivalent to putting a lock on a door to secure your house.

In any form means it includes both physical (e.g., printed documents) and electronic (e.g., files and databases) information.

At all times means the information must be protected, whether it is at rest (i.e., in storage), in use, or in motion (e.g., electronic information sent over a network, or a printed document transported by a courier).

Thus, we define information security as the protection of information. Note that we didn’t place any constraints upon the scope of protection. That is, if we have to protect computers and networks to protect information, then that would be within the scope of information security. But, keep in mind that the objective is the protection of information. Nothing more. Nothing less.

Cyber Security

We’ve already shown that there isn’t a commonly agreed-to definition for cybersecurity. Now, I’m going to propose a definition for cybersecurity which covers all aspects of cybersecurity — something which is lacking from other definitions — while providing a clear distinction from information security. [10]

Cybersecurity is the protection and defense of both analogue and digital electronic devices, their communications channels, and their processing-and-control logic and algorithms.

Now, let’s dissect that definition to get a deeper understanding of what it means and its ramifications.

Security is the protection of assets from threats.

Protection is the rendering safe from harm. Protection is passive security. That is, security that does not offer a response to an attack. It is equivalent to putting a lock on a door to secure your house.

Defense is an action taken to resist an attack. Defense is active security. This means that you have dynamic security with ever-changing defenses — which can include offensive actions to stop an attack. It is the equivalent of confronting an intruder in your house with a loaded weapon.

Digital Devices are any electronic device that uses discrete data and processes for all its operations. This clearly includes computers, cell phones and tablets, routers, switches, WiFi access points, and firewalls, but it also includes all other digitally networked devices, such as all IoT devices, VoIP telephones, digital security cameras, smart badge readers, etc.

Analogue Devices are any electronic device that uses continuous data and processes for all its operations. This would include landline telephones, fax machines, most nuclear reactor control systems, older radar systems, older industrial controls, some satellite and other space systems controls, and literally thousands of other devices. In industrial controls situations, analogue devices often serve as failsafe backups to digital controls.

Communications Channels are the means by which a device is connected to other devices. For analogue device communications, this could be a simple wire or wire-pair, coax cable, analogue radio, or similar technologies. For digital device communications, it would include any type of wired or wireless network. For digital to analogue device communications, it could include any of the previously mentioned means of analogue device communications used to communicate to an analogue interface in the digital device.

Processing Logic and Algorithms are the means by which a device accomplishes its designated purpose. For analogue devices, this is all done in hardware. For digital devices, this includes both hardware and software (microcode, firmware, operating systems, applications, etc.).

Control Logic and Algorithms are the means by which a device regulates its processing. For analogue devices, this is all done in hardware. For digital devices, this includes both hardware and software (microcode, firmware, operating systems, applications, etc.).

Now, let’s put the phrases together and detail the bigger picture.

Is the protection and defense is cybersecurity’s first significant difference from information security. Cybersecurity not only offers protection like information security, but it also offers defense. In other words, cybersecurity can take the offensive actions necessary to defend systems.

Of both analogue and digital electronic devices is the next significant difference from information security, as information security’s tools seldom address analogue devices. It is also different in that information security offers protection of non-electronic information (e.g., printed), whereas cybersecurity only deals with electronic devices and their data. [11]

This definition means that protection and defense are also offered to the electronic devices (components) combined to construct a more complex electronic device. For example, protection and defense would be offered to CPUs, GPU, FPGAs, ASICs, NICs, DACs, memory, controllers, and all the other various analogue and digital components that comprise a modern end-purpose electronic device, such as a smartphone or a computer. In other words, cybersecurity protects and defends any security-sensitive electronic device, be it analogue or digital, and be it an end-purpose device or a component of such a device.

Their communications channels is again a difference between cybersecurity and information security. Cybersecurity provides both protection and defense of the electronic communications channels themselves, both analogue and digital. Whereas, information security only provides for the protection of the information conveyed over those communications channels.

Additionally, information security also provides for the protection of information communicated by non-electronic means (e.g., printed documents), which is outside the scope of cybersecurity.

And their processing-and-control logic and algorithms is the final difference between cybersecurity and information security. Cybersecurity offers protections to both hardware and software, and can take actions to defend both from attack. By contrast, information security only provides passive protection to information.

So, that is the definition of cybersecurity and an explanation of its scope.

To recap, cybersecurity provides security for all electronic technology, except for the information processed by such technology (information is protected by information security).

Or, another way to view the difference between information security and cybersecurity is that information security secures the information itself, and cybersecurity secures everything that creates, uses, processes, stores, or communicates that information.

Where Information Security Fails Us

In my blog introduction, I state that “trying to treat cybersecurity problems as though they are information security problems” is one of the fundamental mistakes we are making in security today. The lack of an understanding of the differences between information security and cybersecurity is the root cause of this problem.

As we have seen in the preceding definitions, information security is “data-centric,” and cybersecurity is “device-centric.” Trying to apply information security principals to “device security” creates two problems: First, you can’t adequately secure “hardware” using the same controls used to secure data; And second, there is nothing in information security that provides for an active defense.

Let’s look at some of the issues that the premises supporting information security fail to address. To do this, we’ll examine an example from product security.

The overwhelming insecurity of IoT products has filled the news recently. Why? Many would say that it’s a simple matter of companies trying to produce products on the cheap. However, I would argue that the issue is more likely the product’s designers’ failure to recognize the potential for security problems in their products.

I believe that fundamentally, such product failures are compounded by an incomplete view of security: a view driven by an information security focus. A focus that, for embedded systems products (such as IoT devices), is incomplete, at best. Why incomplete? Because most security issues with IoT devices are not information related. Rather the problems are with the devices themselves.

Let’s begin by listing some of the security questions that product designers should be asking, but are obviously not asking. And, with most product security practitioners coming from an information security background, those product security architects probably do not even know they should be asking these questions.

After all, why should they know better? Nothing they had learned in the scope of information security would indicate that these are issues with which to be concerned. The types of product security questions (that is, cybersecurity questions) which all product security architects should be asking include:

How do you prevent reverse engineering of the product?

How do you prevent tampering with the product?

How do you prevent the production of unlicensed clones of the product?

How do you prevent access to the hardware interfaces used for development debugging of the product?

How do you prevent access to the hardware interfaces used for manufacturing testing of the product?

How do you perform failsafe firmware updates of the product (such that a failed update does not brick the product)?

How do you prevent unauthorized modification of the product’s firmware?

How do you prevent your firmware from running on third-party devices?

How do you ensure the integrity of your supply chain?

How do you prevent unauthorized modification of the device itself?

How do you prevent misuse of the device from damaging the device itself (e.g., using a USB port on a device for other than its intended purpose, and drawing too much power)?

How do you prevent misuse of the device from creating a safety incident (e.g., using an aerosol can to create a vapor fog to trigger a motion detector to unlock a door)?

How can this device be abused by an attacker to cause harm?

How can we verify that our UI is always unambiguous to its intended audience?

How can we verify that our UX is always intuitive to its intended audience?

How can we verify that our UI creates neither security or safety issues?

How can we verify that our ID creates neither security or safety issues?

And this is just a very small sample of the questions that every product development organization should be asking, but which is clearly failing to occur.

Now, I can already hear the objections: “These are hardware engineering issues, not information security issues, and that’s why they’re not covered by information security.” Well, that’s half wrong and half right. Wrong, in that they are not hardware engineering issues; rather, they are hardware security issues. Right, in that they are not information security issues; rather, they are cybersecurity issues. [12]

These, and tens of thousands of other similar issues, are being left unaddressed during product development because information security doesn’t address these types of issues. Nor should it, as those issues are cybersecurity issues and not information security issues.

Nothing in an information security professional’s background or training would prepare them to even know that they should be asking the types of questions I posited. And, that’s what should be expected, because these are not information security issues and I would not expect an information security professional even to have half-a-clue that such problems exist. It’s for precisely this reason that cybersecurity exists and is different from information security.

The problem is really simple: Information security exists to protect information. Nothing in the fundamentals of information security was ever intended to secure anything other than information. Thus, we need to stop trying to use an information security mindset to secure “stuff” that isn’t information. We must recognize that cybersecurity’s scope is beyond that of information security, and thus apply cybersecurity principals to cybersecurity problems.

Defense

We also need to remember that cybersecurity allows for active measures to defend devices. There’s a reason that the military and intelligence agencies refer to their security operations as cybersecurity, and that’s because they take active countermeasures to attacks. You don’t do that when your objective is to secure information. In fact, that entire concept is an anathema to the information security principals and mindset.

Cybersecurity defense is a big rabbit hole I don’t plan to explore further in this posting, other than to remind you that cybersecurity’s objective is the protection and defense of assets.

Summary

There is an old saying, “When the only tool you have is a hammer, everything looks like a nail.” With no real cybersecurity experience, too many information security experts are trying to hammer cybersecurity into becoming an information security nail. We need to reset the thinking of those information security professionals and teach them that cybersecurity is more like a bolt than a nail, and that you use a wrench, not a hammer, when installing or removing a bolt.

Now, a quick review…

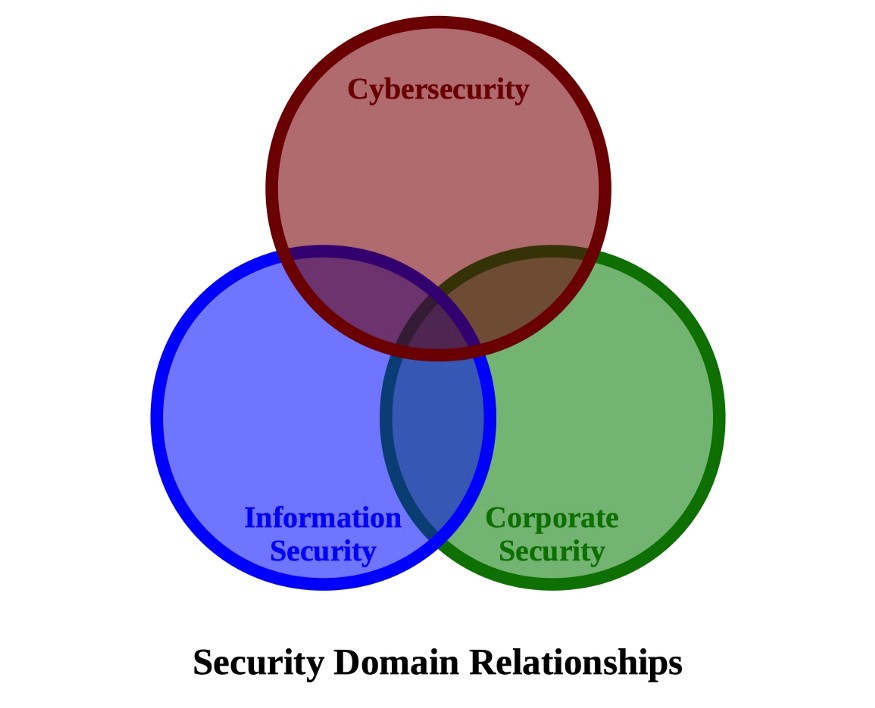
In most organizations, there are three security domains with which it must be concerned:

Corporate Security, which protects (and sometimes defends) people; and real, corporate, and intellectual property.

Information Security, which protects information (data).

Cybersecurity, which protects and defends: hardware, communications, and software.

The diagram below illustrates those relationships among the organization’s security domains.



We established the following definitions in support of those security domains:

Security is the protection of assets from threats.

Corporate Security is those aspects of an organization’s security not directly related to technology.

Information Security is the protection of information in any form and at all times.

Cybersecurity is the protection and defense of both analogue and digital electronic devices, their communications channels, and their processing-and-control logic and algorithms.

Trying to treat cybersecurity problems as though they are information security problems is one of the fundamental mistakes we are making in security today. We have to remember that information security is “data-centric,” and cybersecurity is “device-centric.” Trying to apply information security principals to “device security” creates two problems:

You cannot adequately secure “hardware” using the same controls used to secure data, and

There is nothing in information security that provides for active defense.

If you search the Internet, you will find that many so-called “information security experts” claim that cybersecurity is a subset of information security. But, compared to information security, cybersecurity has a substantially broader scope, addresses a more complex set of security threats, and offers active defenses not provided by information security.

If anything, we should view information security as a subset of cybersecurity. However, that’s not accurate either, as what those two domains are attempting to secure is different — data vs. hardware, software, and communications. Some overlap between the two is unavoidable, but at the most fundamental levels, they are attempting to solve different problems. [13]

Thus, we need clear, concise, unambiguous definitions of both cybersecurity and information security.

Hopefully, you will find the definitions provided here meet those criteria.

So, don’t let alleged information security experts try to tell you what is and is not cybersecurity! Those so-called “information security experts” are precisely that, and nothing more, because they clearly do not understand cybersecurity!

Please leave cybersecurity to actual cybersecurity practitioners.

Thank you!

# CP

## Advantage

### ADR CP---2AC

#### Widespread SSA abilities are a pre-requisite to ADR capabilities---we can’t collect something we can’t find!

Jason Forshaw et al., 20 (Jason Forshaw, Mike Lindsay, Charity Weeden, John Auburn, Chris Blackerby, 9-18-2020, accessedon 6-23-2022, Advanced Maui Optical and Space Surveillance Technologies Conference, “An Exploration of Space Situational Awareness (SSA) Needs for Active Debris Removal ADR) Operators”, https://amostech.com/TechnicalPapers/2020/Poster/Forshaw.pdf, HBisevac)

Comprehensive Space Situational Awareness (SSA) data allows users to accurately interpret and characterize the activity of satellites, improving operational safety and reducing the risk of collisions by increasing ability to recognize abnormal or off-nominal behavior. In the years since its origin, there have been increasing use cases for SSA, such as asset investment protection, insurance claims, and safety of flight. Now with the advent of new In-orbit Servicing (IOS) missions such as Active Debris Removal (ADR), SSA becomes an important part of operational services.

Astroscale is one of the few companies in the world proposing to aid in the removal of orbital debris through the provision of the following in-orbit services: end-of-life (EOL) targeting the LEO constellations, ADR targeting existing larger space debris, and life-extension targeting GEO satellites. As we grow our business, develop our capabilities, and become closer to fully operational services, Astroscale is developing a clearer understanding of SSA needs for its future ADR missions. This paper aims to address those specialized needs, understanding the key technical drivers.

2. SSA NEEDS FOR ADR

In a classical ADR mission, we have a servicer (the satellite doing the removal) and a client (the asset in space being removed). We will be using this terminology throughout the paper.

We break down our SSA needs into 5 categories:

(1) Pre-launch Assessment

Important data can be provided by SSA even before a servicer is launched, such as client position and, in some cases, client attitude and tumbling rate. ADR services in future will have inherent fixed tumbling rate servicing limits – if a client tumbling rate is too high, then a client may be unserviceable to begin with. Such information needs to be ascertained before a service commences, otherwise this places risk on the ADR provider if they launch a servicer only to find that they can’t perform the intended removal.

(2) Search and Approach

SSA is mandatory for future search and approach maneuvers. Generally, the client is defunct and the satellite has failed in a way such that it needs removal. In this case, absolute positioning systems on-board e.g. GPS are not functional and thus the client’s position can only be known through use of SSA services. One of the first steps in a servicer rendezvousing with a client is the “search and approach” phase (see CONOPS section below) which thus requires use of an SSA service.

(3) Failure Analysis

SSA services can provide some form of failure analysis capability to analyze the conditions surrounding the  failure of the client. For example, if the client is tumbling in a specific way, or has unusual trajectory motion,  this might indicate a GNC or propulsion failure. Understanding such information before rendezvous, could be  very valuable to the ADR service provider.

(4) Collision Analysis and CAM Alerts

CAM (Collision Avoidance Maneuver) alerts are a core stable of conventional SSA provision and are also needed in ADR missions. The servicer must be able to move out of the way of other satellites, or trackable debris.  However, depending on the accuracy of the SSA data, SSA providers may be able to provide independent tracking to help prevent collisions during Rendezvous and Proximity Operations (RPO).

(5) Independent Monitoring for Ensuring Transparency

Finally, regarding safety and security, SSA can provide independent monitoring for ensuring transparency for any regulatory and potential insurance compliance. In particular, tracking of the servicer during the course of the mission can provide confidence that no malicious behavior is being undertaken.

It is to be noted that the needs for SSA for ADR do differ than the broader needs of SSA for mass observation of satellites. In a conventional SSA scenario (e.g. government operational intelligence, general tracking of debris), SSA providers scan for, or track, a very large database of objects. SSA for ADR differs in that, specifically for Needs #1 to #3, ADR customers are looking for specific tracking of just 2 entities – the servicer and the client. Thus, high-quality data on 2 objects is far more valuable than low quality data on a very large number of objects.

#### It fails AND causes escalation because they are perceived as ASATs!

Leonard David 21. Author of Moon Rush: The New Space Race (National Geographic, 2019) and Mars: Our Future on the Red Planet (National Geographic, 2016). He has been reporting on the space industry for more than five decades. “Space Junk Removal Is Not Going Smoothly.” Scientific American. 4-14-2021. https://www.scientificamerican.com/article/space-junk-removal-is-not-going-smoothly/ //EM

A Space Age “tragedy of the commons” is unfolding right under our nose—or, really, right over our head—and no consensus yet exists on how to stop it. For more than a half-century, humans have been hurling objects into low-Earth orbit in ever growing numbers. And with few meaningful limitations on further launches into that increasingly congested realm, the prevailing attitude has been persistently permissive: in orbit, it seems, there is always room for one more.

After so many decades of the buildup of high-speed clutter in the form of spent rocket stages, stray bolts and paint chips, solid-rocket-motor slag, dead or dying satellites and the scattered fragments from antisatellite tests—all of which could individually damage or destroy other assets—low-Earth orbit is finally on the verge of becoming too crowded for comfort. And the problem is now poised to get much worse because of the rise of satellite “mega constellations” requiring thousands of spacecraft, such as SpaceX’s Starlink, a broadband Internet network. Starlink is but one of many similar projects: Another mega constellation from a company called OneWeb is already being deployed. And Amazon’s Project Kuiper is seeking to create a mega constellation of up to 3,200 satellites in the near future.

As the congestion has grown, so too have close calls between orbiting assets. The International Space Station, for instance, regularly tweaks its orbit to avoid potentially hazardous debris. Worse yet, there has been an uptick in the threat of full-on collisions that generate menacing refuse that exacerbates the already bad situation. Consider the February 2009 run-in between a dead Russian Cosmos satellite and a commercial Iridium spacecraft, which produced an enormous amount of debris.

Finding ways to remove at least some of all that space junk should be a top global priority, says Donald Kessler, a retired NASA senior scientist for orbital debris research. In the late 1970s he foretold the possibility of a scenario that has been dubbed the Kessler syndrome: as the density of space rubbish increases, a cascading, self-sustaining runaway cycle of debris-generating collisions can arise that might ultimately make low-Earth orbit too hazardous to support most space activities.

“There is now agreement within the community that the debris environment has reached a ‘tipping point’ where debris would continue to increase even if all launches were stopped,” Kessler says. “It takes an Iridium-Cosmos-type collision to get everyone’s attention. That’s what it boils down to.... And we’re overdue for something like that to happen.”

As for the Kessler syndrome, “it has already started,” the debris expert says. “There are collisions taking place all the time—less dramatic and not at the large size scale,” Kessler adds.

UP AND OUT

Kessler’s nightmare scenario has yielded no shortage of possible debris-flushing fixes: nets, laser blasts, harpoons, giant foam balls, puffs of air, tethers and solar sails—as well as garbage-gathering robotic arms and tentacles—have all been proposed as solutions for taking out our orbital trash.

A new entrant in grappling with this worrisome state of affairs is the just launched End-of-Life Services by Astroscale Demonstration (ELSA-d) mission. ELSA-d is a two-satellite mission developed by Astroscale, a Japan-based satellite services company: it consists of a “servicer” satellite designed to safely remove debris from orbit and a “client” one that doubles as an object of interest. The project aims to showcase a magnetic system that can capture stable and even tumbling objects, whether for disposal or servicing in orbit. Following a multiphase test agenda, the servicer and client will then deorbit together, disintegrating during their fiery plunge into Earth’s atmosphere.

ELSA-d is now circling in Earth orbit. The mission was lofted on March 22 via a Russian Soyuz rocket that tossed scads of other hitchhiking satellites into space. Following the liftoff, Astroscale’s founder and CEO Nobu Okada said ELSA-d will prove out debris-removal capabilities and “propel regulatory developments and advance the business case for end-of-life and active debris removal services.” The launch is a step toward realizing “safe and sustainable development of space for the benefit of future generations,” he said.

Although ELSA-d and other technology demonstrations of its ilk are unquestionably positive developments for clearing orbital debris, they should not be mistaken for cure-alls. Despite their modest successes, such missions are falling short of addressing the dynamic dilemma at hand, and the proliferation of space junk continues essentially unabated.

ONE-SIZE-FITS-ALL SOLUTION?

“From my perspective, the best solution to dealing with space debris is not to generate it in the first place,” says T. S. Kelso, a scientist at CelesTrak, an analytic group that keeps an eye on Earth-orbiting objects. “Like any environmental issue, it is easier and far less expensive to prevent pollution than to clean it up later. Stop leaving things in orbit after they have completed their mission.”

There simply is no “one-size-fits-all solution” to the problem of space junk, Kelso says. Removing large rocket bodies is a significantly different task than removing the equivalent mass of a lot more smaller objects, which are in a wide range of orbits, he observes. Meanwhile innovations by companies such as SpaceX are dramatically lowering launch costs, opening the floodgates for far more satellites to reach low-Earth orbit, where some will inevitably fail and become drifting, debris-generating hazards (unless they are removed by ELSA-d-like space tugs). “Many of these operators are starting to understand the difficulty and complexity of continuing to dodge the growing number of debris.”

Space junk ranges from nanoparticles to whole spacecraft such as the European Space Agency’s Envisat, which is the size of a double-decker bus and at the top of everyone's removal hit list, says Alice Gorman, a space archaeologist and space junk expert at Flinders University in Australia.

There are also objects such as despin weights, which are solid lumps of metal, and thermal blankets, which are paper-thin. “They’ll cause different types of damage and may need different strategies to remove. There is no way that a one-size-fits-all approach is going to do it,” Gorman says.

The most serious risks, she says, come from debris particles between one and 10 centimeters in size. “There’s far more of them than whole defunct spacecraft, and there is a far greater probability of collision,” Gorman says. “While debris this size might not cause a catastrophic breakup, collision with it can certainly damage working satellites and create new debris particles.”

Turning her attention to satellite mega constellations, Gorman worries about their effects in a low-Earth orbital environment that is already congested. “We also know that orbital dynamics can be unpredictable,” she says. “I want to see some of these mega constellation operators releasing their long-term modeling for collisions as more and more satellites are launched.”

There is no doubt that active orbital debris removal is technically challenging, Gorman says. “However, the big issue is that any successful technology that can remove an existing piece of debris can also be used as an antisatellite weapon,” she says. “This is a whole other can of worms that requires diplomacy and negotiation and, most importantly, trust at the international level.”

Indeed, the ability to cozy up to spacecraft in orbit and perform servicing or sabotage has spurred considerable interest from military planners in recent years, says Mariel Borowitz, an associate professor at the Georgia Institute of Technology’s Sam Nunn School of International Affairs. “These rapidly advancing technologies have the potential to be used for peaceful space activities or for warfare in space,” she says. “Given the dual-use nature of their capabilities, it’s impossible to know for sure in advance how they’ll be used on any given day.”

### ADR CP---Unilateral---2AC

#### Unilateral ADR is perceived as space mil---causes allies to alienate.

BrianWeeden 11**.** Brian Weeden, Secure World Foundation, Montreal, Canada Space Policy Volume 27, Issue 1, February 2011, Pages 38-43 Space Policy Overview of the legal and policy challenges of orbital debris removal https://www.sciencedirect.com/science/article/pii/S0265964610001268

Although ADR operations are not inherently ASAT activities, many of the technologies and techniques which are candidates for ADR operations could also be used to damage or destroy a spacecraft. In the past, some of these techniques have been included in ASAT programs, although most have not made it past the theoretical stage [22]. The development of ADR technologies and techniques by one state, particularly in classified programs, could be interpreted by other states as development of ASAT capabilities. This could prompt those states to develop their own ASAT capabilities or pursue other mechanisms to counter the perceived threat, which could in turn lead to an arms race or instability in the space domain. Actual ADR operations in orbit could also be a significant source of concern. Many states lack the SSA capacity to determine what is happening in orbit. Even among those states which do possess some SSA capacity, it can still be difficult to determine the exact cause of a spacecraft failure or malfunction. Thus, ADR operations carried out unilaterally by one state or covertly could create misperceptions and mistrust that could lead to instability, and potentially to conflict.

### ADR CP---Fails---1AR

#### The technical and legal challenges make it impossible.

Debra Werner 18. correspondent for SpaceNews based in San Francisco. “Debris removal missions face technical, legal and financial hurdles.” 4/23/18. <https://spacenews.com/debris-removal-missions-face-technical-legal-and-financial-hurdles/> //EM

Catching orbital debris will not be easy.

Once a spacecraft travels into orbit, it must detect and approach its target, which may be tumbling uncontrollably, grab onto it and drag it out of orbit without destroying or losing control of either spacecraft, said Marlon Sorge, senior project engineer for The Aerospace Corporation’s Space Innovation Directorate.

Luisa Innocenti, who heads ESA’s Clean Space Office, agrees active debris removal will be technically challenging, but she’s confident it can and will be done. After all, “ESA landed on a comet,” she said. “If we could do that, we can capture the object.

Then, there are the legal hurdles. Under the 1967 Outer Space Treaty, any spacecraft launched by a nation remains its property even decades after it stopped working.

“A U.S. company can’t go up and grab random debris,” said Theresa Hitchens, senior research associate at the University of Maryland’s Center for International and Security Studies. “If it’s Russian debris, a company has to have Russian permission to get it. And if it’s old debris in small pieces, how do you really know whose debris it is?”

Even if a company obtains government permission to collect a defunct satellite or spent rocket stage in orbit, the project raises legal questions. For example, what if the debris strikes another satellite in orbit or breaks up on reentry and damages property on the ground in a country that wasn’t involved in the mission? The liability issues need to be sorted out, Sorge said.

#### It's scientifically never been sorted out.

J.-C. **Liou 9**, NASA scientist in the Orbital Debris Program Office, “A sensitivity study of the effectiveness of active debris removal in LEO,” Volume 64, Issues 2-3, Jan-Feb 2009, pp. 236-243

Concepts for removing large debris from LEO have been proposed for more than 25 years. Early ideas for using the U.S. Space Shuttle, either directly or in conjunction with an orbital transfer vehicle, were found unattractive due to safety, availability, cost, and policy issues. Numerous independent robotic concepts, ranging from classical space-based garbage scows to momentum and electrodynamic tethers, drag augmentation devices, solar and magnetic sails, and other exotic techniques, have also been considered. However, reviews by panels of international experts have repeatedly failed to identify a single plan which is both technically feasible in the near-term and economically viable.

### Ban ASATs CP---2AC

Most of these answers will apply to an ‘arms control’ CP too.

#### Say no.

Robert Farley 1-9. Senior Lecturer at the Patterson School at the University of Kentucky. Dr. “Does a Space War Mean a Nuclear War?.” 19FortyFive. 1-9-2022. https://www.19fortyfive.com/2022/01/does-a-space-war-mean-a-nuclear-war/ //EM

No one has ever fought a nuclear war, and no two nuclear powers have engaged in a prolonged, high-intensity conventional conflict. Now that conventional systems have become implicated in space technologies for reconnaissance, targeting, and communications, leaders will have to make very difficult, very careful decisions on what enemy capabilities they want to disrupt. Acton and MacDonald propose a straightforward ban on attacks against nuclear satellite infrastructure, which would also require agreement to keep nuclear and conventional communications networks separate. This is the little ask; countries should plan to fight more carefully. The big ask is for a multilateral ban to prevent future anti-satellite weapons tests in space. This would reduce the danger that debris could close off, temporarily or permanently, human access to certain locations in earth orbit. But given that countries use satellites for the conduct of conventional military operations, it’s a lot to ask for warfighters to consider critical military infrastructure off-limits in any particular conflict.

#### Verification fails

Jinyuan **Su 17**, Professor, School of Law, Xi′an Jiaotong University; Erin J.C. Arsenault Fellow, Institute of Air and Space Law, Faculty of Law, McGill University, 1/1/17, “Space Arms Control: Lex Lata and Currently Active Proposals,” Asian Journal of International Law, Vol. 7, p. 61-93

The destabilizing effect of space weapons and their potential devastating threat to the benign space environment make them one of the most serious challenges to the peaceful exploration and use of outer space. As existing international law only prohibits certain categories of space weapons, urgent actions need to be taken to fill the lacuna. However, states disagree markedly, at the primary level, as to whether space-based weapons or terrestrial-based ASATs need to be addressed more imminently.6 Scholarly debates have addressed the question of at which points on the chain of "research, development, testing, placement and use" they should be prohibited.7 At the secondary level, the verification of compliance with primary-level obligations is immensely difficult in outer space.8 Highly intrusive verification measures, such as on-site inspections, do not seem to be a realistic option given the utmost confidentiality and sensitivity of space activities.9 Space arms control obligations at the primary and secondary levels are intertwined as the verifiability varies with respect to different aspects of prohibition, and verifiability would in turn affect states′ acceptance of primary-level obligations.

### Ban ASATs CP---Deficit---Say No

#### Russia and China have longstanding differences.

Paul Meyer 4-1. Adjunct Professor of International Studies at Simon Fraser University in Vancouver and a founding Fellow of the Outer Space Institute. Previously, he had a 35-year career in Canada’s Foreign Service including serving as Canada’s Ambassador to the UN and the Conference on Disarmament in Geneva. “Restraining an Arms Race in Outer Space, Survival”, Global Politics and Strategy Volume 64, 2022, pp. 81-94, 04-01-2022, <https://doi.org/10.1080/00396338.2022.2055825> //EM edited for grammar.

A ‘responsible’ way forward?

The apparent popularity of a ban on destructive ASAT testing and the related but less demanding goal of establishing rules for proximity operations could yield real substance from the new OEWG process if the participating parties are prepared to produce tangible results. Yet Russia and China have expressed reservations about this new forum and may take steps to disrupt it. Moving beyond an exchange of views to an actual negotiation is not often a straightforward process, and there are already signs of disagreement among participating states. The organizational meeting for the OEWG that took place on 7 and 9 February 2022 did not agree to hold the OEWG’s first substantive meeting that same month, so this was pushed back to mid-May. Despite these birthing pains, the OEWG on ‘Reducing Space Threats’ appears to be the most promising diplomatic avenue for progress in preventing an arms race and reducing the danger of actual armed conflict in outer space. The OEWG, as a functioning diplomatic process, has at long last provided a forum to discuss and take action on space security free from the straitjacket that the CD has imposed on this subject.

That said, a functional negotiating forum is a necessary but not a sufficient condition to ensure real progress. While much will depend on whether leading space powers opt for cooperation concerning space-security norms, it will also be important for other states and interested parties to advocate for negotiations on cooperative security measures. Civil-society organizations are becoming increasingly vocal on space security: in October 2021, a ‘Joint Statement on Outer Space’ prepared by civil-society actors called upon states ‘not to deliberately disrupt, damage or destroy space assets’ and urged them to consider an open letter signed by scores of former politicians, officials and civilian space experts exhorting the UN General Assembly to begin work on a treaty banning debris-causing ASAT tests.25

If and when serious negotiations on space security get under way, there will be a need for flexibility on the part of participating states as to whether the product of any negotiations will be legally binding. Given the longstanding differences among states on this issue, it might be prudent to set the status of any agreed measures to one side, to be determined at a later stage of negotiations. Establishing common ground on how to define and assess threats to space security will be necessary for the OEWG (or any other process) to succeed. In the absence of common understandings of what constitutes a threat to space operations or any collective commitment to reduce such threats, debates over defining ‘responsible’ behaviours in outer space may not yield meaningful results.

#### Russia says no---they have strategic incentives to avoid caving-in.

Jaganath Sankaran 18. Assistant professor at the LBJ School of Public Affairs at the University of Texas at Austin. “Russia’s Anti-Satellite Weapons: An Asymmetric Response to U.S. Aerospace Superiority.” ArmsControl. 3-7-2018. https://www.armscontrol.org/act/2022-03/features/russias-anti-satellite-weapons-asymmetric-response-us-aerospace-superiority //EM

Notwithstanding these assessments, most Russian analysts display a severe fear of U.S. and allied technological superiority. Although these fears may reflect an extreme worst-case scenario, many Russian military analysts share them. Therefore, they argue, the dependence of U.S. and NATO forces on space-based assets is a vulnerability of which Russia cannot fail to take advantage in a crisis. Russian military commentators claim ASAT and other counterspace weapons will deter aggression and offer war-fighting advantages if deterrence fails.26

These Russian motivations pose profound challenges to pursuing lasting space arms control measures. Several proposed nonbinding behavioral norms may stall the testing of ASAT weapons for the near term. For instance, U.S. Deputy Defense Secretary Kathleen Hicks recently argued for a global ban on ASAT tests that create debris.27 These norms can be diplomatically pursued through multilateral dialogues, including at the UN. Meanwhile, U.S. Secretary of State Antony Blinken reiterated a U.S. desire to develop informal norms to standardize acceptable behavior in space operations. In a speech at the UN Conference on Disarmament, he said the United States wants to engage in “developing standards and norms of responsible behavior in outer space.”28 He further noted, “[W]e should be reducing tensions in outer space, not making them worse.”29

Such diplomatic engagements would provide the United States and its NATO allies with some transparency into Russia’s ASAT and counterspace programs and motivations. Similarly, Russia would gain transparency into U.S. and NATO programs and concerns. Diplomatic engagements can also help communicate redlines and establish a shared understanding of pathways that could lead to conflict escalation in space.30

In the end, however, there are limits to what dialogue and voluntary behavioral norms can accomplish. Without mutual restrictions on aerospace weapons and combat operations, Russians will continue to argue that U.S. and NATO forces retain a significant war-fighting superiority that can be offset only with counterspace systems. Addressing Russia’s perceived vulnerabilities to modern aerospace campaigns will require deeper engagement and structured arms control, possibly with an instrument similar to the Intermediate-Range Nuclear Forces Treaty. Such binding agreements are a difficult proposition in the prevailing geopolitical environment, but they are essential to achieve comprehensive space security and strategic stability.

### Ban ASATs CP---Deficit---Say No---Ukraine

#### No chance Russia agrees---Ukraine ruined the existence of good faith space cooperation.

US specific version

Jeremy Grunert 5-26. Officer in the United States Air Force Judge Advocate General’s Corps. He currently serves as an Assistant Professor in the Department of Law at the United States Air Force Academy. “The Future of Western-Russian Civil-Space Cooperation.” War on the Rocks. 5-26-2022. https://warontherocks.com/2022/05/the-future-of-western-russian-civil-space-cooperation/ //EM

Russia’s Response to Space Sanctions and Short-Term Effects

Russia’s initial response to Western space-related sanctions constituted little more than Roscosmos head Dmitry Rogozin launching a furious Twitter tirade, threatening to cease Russian technological support to the International Space Station. But more concrete responses followed: Russia suspended its launch operations with the European Union; cut off rocket engine servicing and exports to the United States; and has held at least one previously contracted commercial satellite launch hostage in an attempt to extort a NATO member state. Along the way, the mercurial Rogozin has continued to bluster on social media and in the Russian press, threatening that the 500-ton International Space Station could be deorbited over the United States or Western Europe, that the loss of Russian rocket technology would force the United States and its allies to access space on “broomsticks,” that continued partnership in the International Space Station and other joint projects was contingent on the lifting of Western sanctions, and, several weeks later, that Russia would, in fact, leave its long-standing partnership in the International Space Station.

Russian President Vladimir Putin has been less strident than Rogozin, at least in terms of Russian space activities. Downplaying the effects of Western sanctions, Putin has insisted that Roscosmos will continue its civil-space missions — including the Luna-25 Moon mission (one of the lunar missions in which the European Space Agency canceled its collaboration), broadband-providing satellite services, and nuclear propulsion technology development — without international collaboration. Putin himself has not commented on the future of the International Space Station.

From the perspective of NASA and the United States, Russia’s counter-sanctions and threats have had little short-term impact. NASA announced its intent to continue partnering with Roscosmos on the maintenance of the station shortly after the invasion of Ukraine, and while Russia has symbolically canceled some joint space station experiments in retaliation for Western sanctions, most International Space Station operations are proceeding as normal. This has included (despite breathless articles about possible “stranded” astronauts) the return of U.S. astronaut Mark Vande Hei to Earth in a Soyuz crew capsule at the end of March and, at least until mid-May when some media outlets reported the cancellation of the agreement, plans to fly a Russian cosmonaut to the International Space Station on a SpaceX Crew Dragon capsule later this year. NASA Administrator Bill Nelson has consistently characterized Rogozin’s threats as mere bluster and stated that he “see[s] nothing that has interrupted [the] professional relationship” between NASA and Roscosmos in International Space Station operations. As a number of experts have noted, Rogozin’s comments concerning the space station do not signal Russia’s immediate intentions and recognize Roscomos’s obligation to provide at least a year’s advance notice prior leaving the International Space Station partnership — a notification that, to date, has not been provided. Additionally, Rogozin’s media statements are not significantly different from those of Russian government officials made prior to the invasion of Ukraine regarding Russia’s intention to potentially leave the partnership after the 2024 conclusion of the station’s current international operating agreement.

Unfortunately, the short-term effects of the Western sanctions campaign have been far more significant for Europe. The European Space Agency’s decision to cancel its joint projects with Roscosmos effectively ended almost 30 years of space collaboration between the two organizations. In addition to the canceled, suspended, or indefinitely postponed joint civil-space missions, the Russian embargo on Soyuz flights for European payloads has resulted in the cancellation of approximately 16 satellite missions between 2022 and 2024. This has left almost 200 satellites, including several Galileo geo-navigation satellites and a number of other high-profile European satellite missions, without an immediate method of reaching orbit. While a number of launch providers have attempted to adjust their launch schedules and manifests to accommodate these missions, it remains to be seen whether there will be sufficient space on current launches to undertake these missions in the short term. Furthermore, non-space related sanctions, particularly those targeting Russia’s oil, coal, gas, and energy exports, are already causing economic hardship to European economies.

Long-Term Effects

As sanctions and counter-sanctions between the West and Russia proliferate, and as the war in Ukraine grinds on in an ever more brutal fashion, it is difficult to predict exactly what long-terms effects these sanctions will have in the space domain. A number of factors will likely contribute to the long-term effects, including, at a minimum, the length and outcome of the Russo-Ukrainian war; whether Western sanctions are lifted when the conflict concludes; and the extent to which Russia is able to evade Western sanctions or find alternative sources of money and materiel, whether by seeking greater engagement with other international partners (China being the primary candidate) or through other means.

First, how will the Russian civil-space program be affected over the long-term by the current sanctions? The Biden administration has insisted that current sanctions will halve Russia’s high-tech imports and radically affect its defense and aerospace industries, particularly over a period of years. Others counter that such export controls are more likely to constitute a short-term “flesh wound” from which Russia will be able to recover over the long-term by shifting to other supply sources. It seems, however, that sanctions are already wreaking havoc within Russia’s industries: The loss of high-tech electronic and computer equipment imports has reportedly forced shutdowns of a number of military manufacturing plants, including tank factories and surface-to-air missiles production facilities. New military systems under development by the Russian defense industry were described as being “hostage to many new technologies and systems” as early as 2019. Now, with the bite of sanctions, it is unclear whether such systems can be produced in sufficient numbers to contribute to Russia’s military efforts in Ukraine. Additionally, reports out of Ukraine indicate that sanctions have already reduced Russian forces to jerry-rigging military equipment with semiconductors and computer chips from household appliances. While nothing has been publicly released concerning the effects of sanctions on Russia’s space activities, the apparent effects of sanctions throughout Russia’s military and technology production do not bode well for the long-term health of the country’s space industries.

Russia’s space program has suffered heavily over the past decade — particularly in the wake of previous Western sanctions imposed after Vladimir Putin’s annexation of Crimea. As space expert James Clay Moltz notes, since 2014, the Russian space program has “become less innovative and more militarily focused” and its “civil and commercial space technology has failed to keep up with world standards,” already drastically reducing its competitiveness. Even before the present crisis in Ukraine, the French Institute of International Relations theorized that the Russian space program was on a path of significant decline that might not be averted without Russian reengagement with the West and partnership with Europe. Such reengagement now seems impossible, with both the European Space Agency and individual European governments turning back toward the United States for space partnerships. Should these trends continue, Western sanctions and European disengagement may prove devastating to a Russian space program already weakened by pre-2022 sanctions, budget cuts, and aging technology.

With respect to long-term civil-space cooperation between the United States and Russia, there is no immediate threat (despite Rogozin’s bombastic statements) to the International Space Station partnership. However, between Russian officials’ publicly stated intentions to leave the International Space Station sometime in the next several years and the generally deteriorating geopolitical relationship between Russia and the United States, it is by no means clear that civil-space cooperation will continue in a meaningful way after the decommissioning of the space station. Russia has already sought civil-space partnerships with China, signing a five-year space cooperation agreement with the Chinese government and agreeing to jointly construct a lunar research station. A shift by Russia away from civil-space cooperation with the United States and Europe would further solidify the growing perception of “strategic competition” between the West and a Russian-Chinese bloc — a competition already widely seen as existing and growing in the context of military and intelligence-related outer-space operations.

### Ban ASATs CP---Deficit---Verification---1AR

#### It fails:

#### 1. DUAL USE---it makes loopholes inevitable.

Brian Britt 21. M.A. candidate at Georgetown University’s Security Studies Program studying space security, terrorism, and the changing Arctic environment. “The Space Review: Arms control in outer space won’t work.” Space Review. 11-15-2021. https://www.thespacereview.com/article/4336/1 //EM

Elusive definitions

Treaties that ban or control weapons must define what, exactly, they aim to ban or control. Without an ASAT definition that is simultaneously inclusive and precise, international regimes preventing the development, deployment, and use of ASATs are ineffective. Two obstacles make constructing a useful definition nearly impossible: weaponry diversity and the dual-use problem.

By the most literal interpretation of this PPWT language, almost everything can be classified as an ASAT and cannot be put into space.

The variety of potential ASAT weaponry presents a problem. ASAT weapons are any technology that can temporarily or permanently disable or destroy a satellite’s functionality. This means lasers and other directed energy weapons, air- and land-launched kinetic missiles, cyber uplink and downlink attacks, radiofrequency jamming attacks, attacks on ground stations, and maneuverable attack satellites are all ASAT weapons.

The diversity of ASAT weapons makes articulating a sufficiently comprehensive and precise definition impossible. Any attempt to do so will inevitably leave significant loopholes because each technology exists in a separate domain defined by unique operational requirements, norms, and expectations that require specific rules and regulations to control.

Controlling these technologies is especially difficult given most have legitimate, peaceful, or commonplace uses. Satellites are fragile. It takes little force to render them temporarily or permanently ineffective. When a target is defined by fragility, everything becomes a weapon, meaning innocent and commonplace technologies can be weaponized. Remotely operated repair satellites, for instance, are being developed to revitalize failing satellites.[5] But the same capabilities used to repair can be repurposed to destroy. Similarly, any satellite equipped with a radiofrequency antenna necessary to receive signals can also emit them with sufficient strength to jam the communications of nearby satellites.[6] This dual-use problem presents an obstacle for ASAT arms control by pitting legitimate and peaceful operational freedom against national security.

#### 2. VERIFICATION---it’s impossible to prevent development.

Brian Britt 21. M.A. candidate at Georgetown University’s Security Studies Program studying space security, terrorism, and the changing Arctic environment. “The Space Review: Arms control in outer space won’t work.” Space Review. 11-15-2021. https://www.thespacereview.com/article/4336/1 //EM

Verification problems

To identify and differentiate between compliance and disobedience, the international community must be able to identify and characterize objects in orbit. International arms control treaties cannot rely on goodwill alone. Verification capabilities must therefore be an inherent part of any agreement that restricts the use or deployment of weaponry.

But it won’t be in outer space—no reliable verification capabilities currently exist. Once an asset is deployed in orbit, it’s remarkably difficult to tell what it is and what it is capable of doing. For non-physical weapons, like cyber and jamming capabilities, there are no means to verify compliance. Any attempt to ban non-physical ASAT weapons would rely exclusively on trust. The PPWT seeks to bar signatories from placing “any weapons in outer space.”[8] It’s mere finger-wagging more than an enforceable rule without a means to verify compliance.

Effective verification mechanisms would be costly, complicated, and ineffective. And without verification capabilities, useful arms control agreements are hopeless.

Advocates for ASAT arms control would disagree, pointing to modern space situational awareness capabilities that can detect space launches and track the orbital inclination of their payloads through space-based infrared and infrasound monitoring systems.[9] Even if states can track objects that are placed into orbit, “verifying the function of a particular space object already in orbit is significantly more difficult.”[10] The “PAXSAT A” study demonstrated that uncovering the functionality of satellites in orbit is possible by utilizing a four-satellite constellation.[11] But this investigation method relies on the ability of the constellation to position itself near the object in question and the assumption that form follows function. Two problems are presented here. First, we do not have the infrastructure to conduct on-orbit investigations. Second, the logic that form follows function is fallible. Because space launches are expensive, advocates argue that the extra weight and cost needed to obscure the true function of an ASAT weapon in orbit with facade architecture is too expensive to be realistic. But basing arms control agreements on the predicted frugality of nation-states seems illogical, at best.

Even with perfect launch monitoring capabilities, significant unknowns remain. Many space-related armaments are ground-based, meaning these weapons can be developed and deployed outside of the scope of current ASAT monitoring systems. Also, for non-physical weapons, verification is simply impossible. No mechanism exists, for example, to verify compliance with moratoriums against developing or deploying cyberweapons or jamming capabilities.

#### 3. ATTRIBUTION---there’s no way to find who did it!

Brian Britt 21. M.A. candidate at Georgetown University’s Security Studies Program studying space security, terrorism, and the changing Arctic environment. “The Space Review: Arms control in outer space won’t work.” Space Review. 11-15-2021. https://www.thespacereview.com/article/4336/1 //EM

Attribution problems

Attribution, the ability to identify a violation and legitimately tie it to an actor, is a key ingredient of arms control agreements. The ability to attribute violations is key to justifying the invoking of punishments in accordance with international treaty law. Thus, attribution capabilities are the foundation of a deterrence mechanism that makes arms control agreements attractive and practical.

Attribution capabilities, or the lack thereof, present another problem for ASAT arms control. Some forms of ASAT attacks are attributable. Others are not. Non-physical threats, for instance, are particularly difficult to tie actions to national actors.

In the event a laser, for example, is used against a space asset, satellite operators would have a difficult time identifying the actor responsible for the attack. In the harsh environment of space, systems frequently fail without explanation. Unless the targeted satellite is equipped with sensors that could identify “a spike in thermal energy or sudden saturation of optical sensors,” there is no way to differentiate between a random satellite failure and a malicious laser attack.[12] And even if such capabilities exist, there is no guarantee one could attribute the laser’s use to a national actor.

Russia and China proposed the PPWT specifically because it satisfies the political hunger for ASAT arms control while permitting loopholes for a variety of ASAT possessions.

Jamming attacks are similarly difficult to attribute. Satellites use a narrow range of the electromagnetic spectrum to communicate. The crowded nature of orbits today means it is common for multiple space assets to use similar or identical frequencies and, as a result, routinely unintentionally jam the communications of a neighboring satellite.[13] Differentiating between intentional and unintentional jamming is difficult, if not impossible. In this environment, verification and compliance mechanisms are complicated to construct.

#### 4. ADVERSARIES---they won’t comply.

Brian Britt 21. M.A. candidate at Georgetown University’s Security Studies Program studying space security, terrorism, and the changing Arctic environment. “The Space Review: Arms control in outer space won’t work.” Space Review. 11-15-2021. https://www.thespacereview.com/article/4336/1 //EM

Adversarial interests

International participation is another key ingredient of effective ASAT arms control regimes. But many of America’s key space-capable competitors perceive ASAT weapon possession as a strategic necessity. In other words, the interests of America’s rivals decrease the likelihood of reaching an international consensus on an anti-ASAT treaty, which is a necessary ingredient for a successful ASAT arms control regime. The United States relies on its space assets for a “diverse array of political, military and economic activities” fundamental to its national security.[15] This overreliance is seen as a weakness, something America’s adversaries can reliably exploit when conventional American military capabilities outstrip theirs.

#### Ban fails

Michael **O’Hanlon 11**, Senior Fellow in Foreign Policy Studies at the Brookings Institution, 2011, “Balancing U.S. Security Interests in Space,” in Toward a Theory of Spacepower: Selected Essays, https://apps.dtic.mil/dtic/tr/fulltext/u2/a546585.pdf

Overall, space arms control should not be a top priority for the United States in the future, contrary to what many arms control traditionalists have concluded. Some specific accords of limited scope, such as a treaty banning collisions or explosions that would produce debris above a certain (low) altitude, and confidence-building measures such as keep-out zones near deployed satellites, do make sense. But the inability to verify compliance with more sweeping prohibitions, the inherent antisatellite capabilities of many missile defense systems, and the military need to counter efforts by other countries to use satellites to target American military assets all suggest that comprehensive accords banning the weaponization of space are both impractical and undesirable. That said, the United States should not want to hasten the weaponization of space and indeed should want to avoid such an eventuality. It benefits from its own military uses of space greatly and disproportionately at present. It should take unilateral action, such as by declaring that it has no dedicated antisatellite weapons programs, to help buttress the status quo as much as possible.

One type of arms control accord on activities in space would be quite comprehensive, calling for no testing, production, or deployment of ASATs of any kind, based in space or on the ground, at any time; no Earth-attack weapons stationed in space, ever; and formal, permanent treaties codifying these prohibitions. These provisions are in line with those in proposals made by the Chinese and Russian delegations to the UN Conference on Disarmament in Geneva. They also are supported by some traditional arms control proponents who argue that space should be a sanctuary from weaponization and that the Outer Space Treaty already strongly suggests as much.14

These provisions suffer from three main flaws. To begin, it is difficult to be sure that other countries' satellite payloads are not ASATs. This is especially true in regard to microsatellites, which are hard to track. Some have proposed inspections of all payloads going into orbit, but this would not prevent a "breakout," in which a country on the verge of war would simply refuse to continue to abide by the provisions. Since microsats can be tested for maneuverability without making them look like ASATs and are being so tested, it will be difficult to preclude this scenario. A similar problem arises with the idea of banning specific types of experimentation, such as outdoor experiments or flight testing.15 A laser can be tested for beam strength and pointing accuracy as a ballistic missile defense device without being identified as an ASAT. A microsat can be tested for maneuverability as a scientific probe, even if its real purpose is different, since maneuvering microsats capable of colliding with other satellites may have no visible features clearly revealing their intended purpose. Bans on outdoor testing of declared ASAT devices would do little to impede their development.

#### Banning one system is useless – adversaries shift

Michael **Krepon 12**, Co-Founder of the Stimson Center, 3/6/12, “Toward a Space Code of Conduct,” <https://www.worldpoliticsreview.com/articles/11680/toward-a-space-code-of-conduct>

Paradoxically, the reasons for prior restraint in the military space competition also have made space arms control very difficult. Because there are so many ways to interfere with, disable or destroy satellites -- including by means of launch platforms that are indispensable for other military uses -- a ban on all of these means is inconceivable. A ban on “dedicated” ASAT weapons specifically designed and intended for use against satellites is conceivable, but it is also not credible, since so many other ways to counter satellites will remain unconstrained.

A treaty banning space warfare, the use of ASATs or dedicated ASAT weapons therefore runs aground on a Catch-22: To be effective, the scope must be sufficiently broad as to be unrealizable, while a narrower scope would be unreliable. This Catch-22 becomes even more severe when effective verification standards are considered. What can be verified is insufficient, since bans on dedicated ASATs can be circumvented by hiding them in warehouses, while extant military capabilities with ASAT potential can be declared as intended for other purposes. These circumstances make it extremely difficult to engage in classical arms control treaty negotiations for the global commons of space. But the existence of considerable military capabilities with ASAT potential also makes it extremely unwise for major powers to strike first against each other’s satellites, since retribution and unintended escalation -- including escalation across the nuclear threshold -- might well follow.

### Ban ASATs CP---Turn---Verification---1AR

#### Arms control drives secret ASATs, avoiding detection and increasing weaponization.

Brian Britt 21. M.A. candidate at Georgetown University’s Security Studies Program studying space security, terrorism, and the changing Arctic environment. “The Space Review: Arms control in outer space won’t work.” Space Review. 11-15-2021. https://www.thespacereview.com/article/4336/1 //EM

Where arms control advocates go wrong

Despite these challenges, some argue that ASAT arms control agreements are a necessary aspect of a safe, secure, and stable space environment. Advocates for arms control maintain agreements could prevent an ASAT arms race. This is wrong. Arms control agreements will do more to shape the direction of, rather than prevent, an ASAT arms race. Because any agreement will be less than comprehensive, states will seek to develop ASAT weapons that fall outside of the agreement’s jurisdiction. If the agreement bans kinetic ASAT weapons, for instance, space-capable nations will push to develop more diverse, more effective non-kinetic weapons.

In addition, any agreement will likely increase the incentives to camouflage and disguise ASAT technology, worsening a problem that the arms control agreement initially set out to resolve. Any restrictions will inevitably force nations to make ASAT capabilities increasingly integrated with innocent infrastructure to avoid detection, furthering the dual-use problem, seeding doubt among the reliability of routine space assets, and incentivizing the weaponization of outer space.

### Build Satellites---2AC

#### It’s only a question of integrating existing, transatlantic satellites.

AT: Build Satellites CP

Stephen Ganote et al. 19 (Stephen Ganote is a Managing Director at Avascent where he serves clients in space communications and select defense tech markets and leads its commercial space practices, Janie Yurechko is a Strategic Development Specialist at Ball Aerospace and a MBA Candidate at Georgetown University, Diana Jack is a manager in Avascent's Space practice where she provides strategic guidance to major primes, New Space companies, and governments, Connor O’Shea is President and Co-Founder at Westgen Technologies Inc, a remote power generation and methane reduction technology company, 9-30-19, accessed on 6-19-2022, Atlantic Council Scowcroft Center for Strategy and Security, “Reenergizing Transatlantic Space Cooperation”, <https://issuu.com/atlanticcouncil/docs/reenergizing_transatlantic_space_cooperation>, HBisevac)

This congestion is increasingly causing harm: an Iridium satellite was destroyed by a collision with a defunct Russian satellite in 2016; Capella Space recently reported that one of its satellites narrowly avoided a catastrophic collision with a piece of space debris; and as noted above, debris from a 2019 Indian ASAT test now threatens the International Space Station. 21 Debris interference has even been suspected in the 2019 failure of Intelsat 29e.22 In addition to growing competition for physical space, more satellites are competing for finite (and crowded) radio-frequency spectrum. Space stakeholders express growing concern about coordinating transmissions from many thousands of new satellites reliant on similar or overlapping frequency bands, as to avoid jamming signals and degrading capabilities.23 The advent of 5G is further complicating this issue. This coordination is no trivial matter; the Department of Defense, the most sophisticated and well-resourced space actor in the world, inadvertently jams its own satellites dozens of times a month.24

#### There is a tradeoff---finite number of federal satellites presently multi-task and face competition for use---surveillance disrupts it, especially with nuclear test monitoring.

Rodney Carlisle 15, Professor Emeritus of History from Rutgers University, Encyclopedia of Intelligence and Counterintelligence, pg. 160-162 //EM

Satellites and microwaves.

The use of satellites for intelligence communication can be traced back to the dawn of the space age when the first satellite (Sputnik) was launched by the Soviet Union on October 4, 1957. Thousands of communication satellites have been launched since then for reconnaissance and intelligence-gathering. By the 2000s, the U.S. and global satellite industry are in rapid flux, with new technological innovations adding increased capability. For example, numerous new U.S. spy satellites now have measurement- and signature-intelligence sensors, designed to focus in on, track, and describe mobile or fixed targets. In 1995, the CIA and Department of Defense created a Central MASINT Office (CMO) in the Defense Intelligence Agency (DIA), subsequently upgraded in 1998 to a quasi-autonomous DIA organization; 1998 was also the year that the Defense Advanced Research Projects Agency (DARPA), the NRO and air force, moved ahead with plans to develop two satellites with synthetic-aperture radar (SAR) and moving-target-indicator (MTI) ability. This is for a planned constellation of 24-48 satellites in all, at 1-meter resolution for imaging of 29,000 square kilometers every hour, able to give the U.S. Air Force an all-weather surveillance capability. Another innovation in recent U.S. geostationary satellite technology is the development of the Kuvstur Global Positioning System (GPS) made for nuclear-targeting and navigation, as well as detection of nuclear explosions, in a constellation of 21 operational satellites and three active spares, deployed in six arrays of four satellites. Increasingly, GPS data is also being sold for commercial use in a host of areas, and has entered the consumer satellite-image market. Countries the United States is sharing or plans to share GPS satellite data with include Russia and Israel, though Israel is also launching its own satellites. The data will also be shared with NATO allies through the 270 LinkedOperations Intelligence Center, Europe (LOCE) terminals, servicing the United Kingdom, Canada, Norway, Greece, Belgium, France, and Spain. Data from the U.S. Space-Based Infrared System (SBIRS) High and Low, will go solely to allies cooperating with space-based military programs, such as Italy and Germany. Satellites are becoming ever more integral for a wide range of U.S. foreign policy tasks, including global power projection capability. As warfare and related intelligence becomes more capital-intensive and high-tech, demands for satellites are increasing. Yet with financial troubles within the commercial satellite industry in the early 2000s, the Pentagon faces a massive shortage of satellite-transmission bandwidth. The U.S. military estimated in the 1990s that by 2005 there would be some 1,000 new satellites for the Pentagon to draw on for weapons dependent on space-based wireless communications, and decided in 1996-97 to lease capacity from the then-burgeoning commercial satellite industry. Communication with satellites for intelligence purposes is usually handled by the National Security Agency (NSA), while communication with satellites for the exploration of space is within the brief of NASA. But both use the same microwave technology. Therefore the information on communication with satellites provided by NASA also may explain how the National Security Agency (NSA), working with the National Reconnaissance Office (NRO), must communicate with spy satellites. NASA's Deep Space Network (DSN) allows it to "acquire telemetry data from spacecraft, transmit commands to spacecraft, and track spacecraft position and velocity . . . measure variations in radio waves for radio science experiments, gather science-data [and) monitor and control the performance of the network." Translated into terms for intelligence, this means the NRO can gather intelligence data from spy satellites and transmit commands to them to change orbit or lower their orbiting altitude to focus on new targets of intelligence information. This is probably what was done in December 2002, when North Korea reactivated its nuclear reactor at Yongbyon. Such communication also controls the satellites and confirms that they are carrying out the intelligence mission they are tasked to perform.

### Build Satellites---Deficit---Tradeoff---1AR

#### Analysts are key and trade-off.

Carla Crandall 10, J.D. Candidate at the J. Reuben Clark Law School at Brigham Young University, “Why Aren't We Using that Intel Stuff? Using Reconnaissance Satellite Imagery in Domestic Disaster Prevention and Response”, Brigham Young University Law Review, 2010 B.Y.U.L. Rev. 1831, Lexis

n31. See Best & Elsea, supra note 26, at CRS-5. Obviously operating the nation's satellite program is expensive, but once launched for reconnaissance purposes, the cost is sunk and the satellites can thus be used for multiple purposes without many additional costs. Highlighting this point, Charles Allen has expressed, for instance, that ""we're not fully utilizing legal and lawfully authorized capabilities of the U.S. government, capabilities for which U.S. taxpayers paid over decades hundreds of billions of dollars.'" Hsu, supra note 6, at A8. The most significant additional cost associated with domestic collection would likely be the opportunity cost of diverting analytical resources from overseas intelligence missions to interpretation of domestic satellite imagery - a cost that would be incurred whether analysts were interpreting imagery from commercial or reconnaissance imagery.

#### CP’s too slow and expensive.

Richard A. Best 10, Defense Analyst with the Congressional Research Service, The Oxford Handbook of National Security Intelligence, Ed. Johnson, p. 431

From its inception in 1961, the NRO has in a variety of different ways come under the shared authority of the DCI/DNI and DOD/Air Force. In addition, given the nature of the space industry, it is difficult to conceive that current problems could be resolved, or even realistically addressed, if the NRO were essentially transferred from DOD to the DN1. It is noteworthy that a prominent group of experts on space issues recently took a diametrically opposite approach, recommending thai the NRO be removed from the Intelligence Community and placed under a national security space authority who would report to both the DNI and the secretary of defense and to whom would be assigned the functions currently assigned to the NRO, the Air Force Space and Missile Systems Center, and other organizations and possessed of authority to formulate and execute budgets for space efforts across the government. (Institute for Defense Analyses 2008,18,21). Furthermore, there is interest both in Congress and in DOD in providing the military services with separate operationally responsive space systems not launched or operated by the NRO. Separate satellites for DOD might be useful in some circumstances, but high costs would be involved and it is doubtful that such a move would facilitate the development of a comprehensive space architecture.

### Cyber CP---2AC

[AT: NCA plank]

#### Already exists!

The White House 2-17 (The White House, 2-17-2022, accessed on 6-26-2022, “Office of the National Cyber Director”, <https://www.whitehouse.gov/oncd/>, HBisevac)

The Office of the National Cyber Director was established by the **N**ational **D**efense **A**uthorization **A**ct for Fiscal Year 2021, as well as President Joe Biden’s nomination and Senate confirmation of John Christopher Inglis as the **first National Cyber Director**. The National Cyber Director serves as a principal advisor to the President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders.

[AT: set tech standards plank]

#### It fails and no one follows it.

Charles Mok 2-22 (Charles Mok is a visiting scholar at the Global Digital Policy Incubator, Cyber Policy Center, Stanford University, ✰ 2-22-2022 ✰, accessed on 6-26-2022, The Diplomat, “China and Russia Want to Rule the Global Internet”, <https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/>, HBisevac)

These acts of censorship and surveillance speak clearly about what kind of vision of **internet governance** **China** and **Russia** have in mind. Their interpretation of internet information security is about the **security** of their **regimes**, not of the security and privacy of users inside or outside of their countries. An internet governance framework with such toxic underlying values of censorship and surveillance should be extremely horrifying to anyone.

Particularly for China, however, such attempts to influence and indeed **dominate global techn**ology **standards** and governance are **nothing new**. Over the last few decades, China has invested heavily to participate in and influence global technology standard bodies. In November 2021, the Communist Party Central Committee and the State Council published the National Standardization Development Outline, spelling out goals and actions for “China Standards 2035.” These “China standards” are by all means meant to be made global.

The European Union has been on high alert about China’s ambition, and recently outlined a “**more aggressive approach**” to setting **global standards**, in order to ensure its leadership in development areas such as internet technologies, artificial intelligence and green technologies. To the Europeans, it was clear that China’s standard-setting exercises at the international level were meant to provide a competitive edge to China and its companies.

International technological standards-setting and internet governance frameworks are **complex** and **diverse**. It is also important to remember that traditionally standard settings are led by the **private sector** and **research communities**, **not by state actors**, for good reasons. Chinese and Russian representatives should have their seats at the table, but the world must be extremely cautious about such standard-setting processes being taken over by companies controlled by autocratic regimes, tasked with their governments’ political agenda. It would be even worse if such autocratic governments are to directly steer and dominate such processes.

### Cyber CP---NFU Plank---2AC

#### NFU fails

Keith Payne, 15 (Keith Payne, PhD, Professor and Head of the Graduate Department of Defense and Strategic Studies, Missouri State University, 2015, accessed on 6-26-2022, Air Force University, “US Nuclear Weapons and Deterrence”, <https://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-29_Issue-4/V-Payne.pdf>, HBisevac)

Realists in this regard are from Missouri, the “show me” state, and ask utopians to explain how, why, and when a powerful new cooperative international norm with corresponding international institutions will become a reality. Realists point to the unhappy history of the unmet claims and dashed hopes of the 1928 Kellogg-Briand Pact (intended to prevent offensive war by global legal agreement), the League of Nations, and the United Nations. To be sure, the future does not have to be bound by the past, but before moving further toward nuclear disarmament, realists want to see some clear evidence of the emerging transformation of the global order—not just the claim that it can occur if all key leaders are so willing, faithful, and visionary and can “embrace a politics of impossibility.”12 As the old English proverb says, “If wishes were horses, then beggars would ride.”

But has not everything changed in the twenty-first century? Has not the end of the Cold War ushered in a new global commitment to cooperation, the rule of law globally, and benign conflict resolution? The unarguable answer is no. Russian military actions against Georgia in 2008 and Ukraine since 2014 (the latter in direct violation of the 1994 Budapest Memorandum signed by Russia, Great Britain, and the United States) are sufficient empirical evidence to demonstrate that Thucydides’ stark description of reality is alive and well. China’s expansionist claims and military pressure against its neighbors in the East and South China Seas teach the same lesson.

Why is this reality significant in the consideration of nuclear weapons? Because in the absence of reliably overturning the powerful norm of raison d’État and Thucydides’ explanation of international relations, states with the capability and felt need will continue to demand nuclear capabilities for their own protection and, in some cases, to provide cover for their expansionist plans. To wit, if Ukraine had retained nuclear weapons, would it now fear for its survival at the hands of Russian aggression? Former Ukrainian defense minister Valeriy Heletey and members of the Ukrainian parliament have made this point explicitly, lamenting Ukraine’s transfer of its nuclear forces to Russia in return for now-broken security promises of the Budapest Memorandum.13

This lesson cannot have been lost on other leaders considering the value of nuclear weapons. Nor is it a coincidence that US allies in Central Europe and Asia are becoming ever more explicit about their need for US nuclear assurances under the US extended nuclear deterrent (i.e., the nuclear umbrella). They see no new emerging, powerful global collective security regime or cooperative norms that will preserve their security; thus, they understandably seek the assurance of power, including nuclear power. The Polish Foreign Ministry observed in a recent press release that “the current situation reaffirms the importance of NATO’s nuclear deterrence policy.”14 This reality stands in stark contrast to utopian claims that powerful new global norms and international institutions will reorder the international system, overturn Thucydides, and allow individual states to dispense with nuclear weapons or the nuclear protection of a powerful ally. As the Socialist French president Francois Hollande has said, “The international context does not allow for any weakness. . . . The era of nuclear deterrence is therefore not over. . . . In a dangerous world—and it is dangerous—France does not want to let down its guard. . . . The possibility of future state conflicts concerning us directly or indirectly cannot be excluded.”15 There could be no clearer expression of Thucydides’ description of international relations and its contemporary implications for nuclear weapons.

Opponents of the administration’s plan to modernize the US triad now double down on the utopian narrative by insisting that the United States instead lead the way in establishing the new global norm by showing that Washington no longer relies on nuclear weapons and does not seek new ones. Washington cannot expect others to forgo nuclear weapons if it retains them, they say, and thus it must lead in creation of the new norm against nuclear weapons by providing an example to the world. For instance, “by unilaterally reducing its arsenal to a total of 1,000 warheads, the United States would encourage Russia to similarly reduce its nuclear forces without waiting for arms control negotiations.”16 A good US example supposedly can help “induce parallel” behavior in others.17 If, however, the United States attributes continuing value to nuclear weapons by maintaining its arsenal, “other countries will be more inclined to seek” them.18

Nuclear realists respond, however, that the United States already has reduced its nuclear forces deeply over the last 25 years. America cut its tactical nuclear weapons from a few thousand in 1991 to a “few hundred” today.19 Moreover, US-deployed strategic nuclear weapons have been cut from an estimated 9,000 in 1992 to roughly 1,600 accountable warheads today, with still more reductions planned under the New START Treaty.20 The United States has even decided to be highly revealing of its nuclear capabilitiesto encourage others to do so,with no apparent effect on Russia, China, or North Korea.21 America has adhered fully to the reductions and restrictions of the 1987 Intermediate-Range Nuclear Forces Treaty—the “centerpiece of arms control”—but the Russians now are in open violation. As former undersec- retary of state Robert Joseph stated recently, decades of deep US reductions “appear to have had no moderating effect on Russian, Chinese or North Korean nuclear programs. Neither have U.S. reductions led to any effective strengthening of international nonproliferation efforts.”22 Utopians want the United States to lead the world toward nuclear disarmament by its good example, but no one is following.

### Cyber CP---NFU Plank---1AR

#### NFU doesn’t solve, but incentivizes gray zone aggression

**Kerttunen 2017** Dr. Mika Kerttunen (LTC (ret.) Finnish Army) is adjunct professor in military strategy at the Finnish National Defence University and Director of Studies at the Cyber Policy Institute in Tartu, Estonia. Chapter 1, “Looking for Stability: American and Russian Nuclear Doctrines and Arms Control” from the National Defense University “Arms Control in Europe:Regimes, Trends and Threats” National Defence University Series 1: Research Publications No. 16 2017 pg. 24 http://www.doria.fi/bitstream/handle/10024/144087/Arms%20control%20in%20Europe\_netti.pdf?sequence=1

The policy of no first use (NFU) would not necessarily reduce the risk of unintentional use or the likelihood of intentional use. On the contrary, no first use can, at best, be regarded as political lip service and, at worst, as destabilizing. Though widely supported within the disarmament community, deterrence advocates consider the no first use policy harmful, as following the need to maintain the risk of escalation, refraining from first use is considered to undermine deterrence. Moreover, NFU can encourage activities under assumed nuclear red-lines and umbrellas. The U.S. has systematically refrained from NFU and, as mentioned, although the Soviet Union declared it would not use nuclear weapons first, the Russian Federation abandoned this stance in 1993, leaving China as the only nuclear weapon state to subscribe to this policy.

#### Its just words, conventional thumps, and links worse

**Stanley 8** (Stanley Foundation – Stanford University’s Center for International Security and Cooperation, “A New Look at No First Use”, 4-4, http://www.stanleyfoundation.org/publications/pdb/NoFirstUsePDB708.pdf)

Some conference participants worried that adopting nfu might actually encourage proliferation by weakening security assurances or by suggesting a shortcut for a weak state to match our military capability. One participant speculated that this is a natural consequence of US conventional superiority and that we should consider how to redress those security imbalances. Other participants argued that the us nuclear posture is basically irrelevant as it relates to this problem: no matter what the us nuclear posture is, states will see nuclear weapons as a way of offsetting america’s conventional military superiority.

### Cyber CP---NFU Bad---2AC

#### No first use causes nuclear war.

Colby 16 (Elbridge, Director of the Defense Program at the Center for a New American Security, former U.S. Deputy Assistant Secretary of Defense for Strategy and Force Development, Foreign Policy, “Nuclear Weapons Aren’t Just For the Worst Case Scenario,” https://foreignpolicy.com/2016/08/04/nuclear-weapons-arent-just-worst-case-scenario-first-use-china-obama-trump/, 8/4/2016, 7/5/2019)

Recent reports suggest that Republican presidential nominee Donald Trump insistently asked an anonymous foreign-policy expert why the United States should not use nuclear weapons more readily. This has led to a chorus of voices decrying the way in which Trump is reported to have spoken about the nuclear option, with many insisting the United States should only ever employ nuclear weapons in retaliation after an opponent has used them first. It is certainly right that such terrible weapons should only be used in extreme circumstances (a point of view Trump appears to have expressed earlier this year), but the conventional wisdom is wrong in suggesting the United States should under no circumstances be the first to use nuclear arms. This controversy is not merely another spark of the campaign season, for, according to reports, President Barack Obama himself is considering implementing a “no-first-use” pledge regarding nuclear weapons — that is, a promise never to be the first to use nuclear weapons. Such a pledge would be exceedingly unwise. Nuclear weapons are horrible instruments of destruction, but they are also associated with the longest period of major-power peace in human history. And they only work because potentially ambitious states believe their use is plausible enough that starting a war or escalating one against a nuclear-armed state or its allies would just be too risky to countenance. The point of reserving the right to use nuclear weapons first (which, it must be emphasized, is different from a policy of preemption or heavy reliance on them) is not to convey a madman’s itchy trigger finger on the button. Rather, its purpose is to communicate clearly to any potential aggressor that attacking one’s vital interests too harshly or successfully — even without resorting to nuclear weapons — risks prompting a devastating nuclear response, something that, at scale, is far more costly than any realistic gains. A no-first-use pledge would undermine this pacifying logic. If the policy were believed, then it would make the world safe for conventional war. Since potential aggressors would write the risk of nuclear use down to zero, they would feel they could safely start and wage fierce conventional wars. Conventional wars can be small, quick, and decisive, which is why they can also be appealing — just ask Napoleon, James Polk, Otto von Bismarck, or Moshe Dayan. But they can also escalate dramatically and unpredictably, especially when major powers are involved. Thus, the most likely route to nuclear use is via a nasty conventional war, as happened in World War II. In such circumstances, high-minded pledges made in peacetime may well seem foolish or too burdensome. A believable no-first-use pledge would likely raise, rather than diminish, the likelihood of nuclear weapons being used by lightening the shadow of nuclear weapons over the decision-making of potential combatants. Better for everyone to think as carefully and clearly as possible about nuclear weapons before a war is underway. Alternatively, if the no-first-use pledge were not believed, what would the point of such a promise be other than diplomatic window dressing? It is for these reasons that the United States has never adopted a no-first-use policy. During the Cold War, the United States relied on its nuclear deterrent to compensate for perceived Soviet and Warsaw Pact conventional advantages in Europe. But even in the post-Cold War period of American military supremacy, when Washington sought to diminish its strategic reliance on nuclear weapons, it judged the future was too uncertain to dispense with the reserved right to go first. While other countries such as China and India have declared no-first-use policies (though there is a great deal of skepticism about how reliable Beijing’s pledge is), Washington and the allies that depend on its nuclear umbrella have always recognized that a no-first-use pledge by the United States would be unwise because of the breadth of defense commitments it has assumed. If the U.S. nuclear arsenal were solely designed to deter attacks on the continental United States, a no-first-use pledge might have more merit, as launching such an assault would be incredibly difficult. But Washington also seeks to deter attacks on its allies in areas like Eastern Europe and East Asia, where U.S. conventional superiority is far less assured. The main reason why a no-first-use pledge does not make sense for Washington, then, is the reality that the United States cannot always expect to maintain the military upper hand everywhere, and a no-first-use pledge is not the kind of commitment a nation can turn on and off without damage to its credibility and reputation. But can anyone plausibly challenge the United States in a conventional war in the near to medium term? The answer is yes; China might well be able to. Russia and North Korea are also very dangerous to the United States and its allies in their own ways, and Moscow could plausibly hope to take on the United States conventionally if it could localize a conflict in its “near abroad” and keep it short, but neither can reasonably expect to challenge the United States in a serious, prolonged conventional war and hope to prevail. But China at some point in the not-too-distant future might. A range of authoritative sources are showing that the conventional military balance of power between the United States and China with respect to points of contention in East Asia such as Taiwan and the South and East China Seas is, at the very least, becoming increasingly competitive. Beijing is fielding more and more highly capable forces in the Western Pacific that present a growing challenge to America’s ability to effectively project military power in the region. The days are therefore passing when the United States could easily swipe away any effort by the People’s Liberation Army at power projection in the Western Pacific. Instead, any future fight in the region between the United States and its allies on the one hand and China on the other would be hard and nasty. And the trend lines are not moving in a good direction. Indeed, within a decade, China might be in a position where it could reasonably expect to confront a U.S. ally or partner in the Western Pacific and hope to prevail if the conflict remained relatively limited. If the United States adds to this a credible guarantee that it would not use nuclear weapons first, it would strengthen China’s confidence that it could wage a short, sharp conventional war and gain from it, just as such confidence is rising and becoming more plausible to decision-makers in Beijing already contemplating the use of force in the region. According to a recent Reuters report, for instance, influential voices in the Chinese military establishment are already pushing for firmer security policies and even military action in the South China Sea — and this at a time when the United States still enjoys the conventional upper hand. These voices are likely to seem more credible and appealing in the councils of power in Beijing as Chinese military advantages grow, and they would only be emboldened by a U.S. statement that it will not use nuclear weapons first. A no-first-use pledge would therefore increase the chances of war in Asia. Indeed, rather than excluding the possibility of American nuclear first use, Washington should be emphasizing it. This does not mean the United States should ever use its nuclear weapons lightly. Rather, Beijing should simply understand that, even if it is able to gain conventional military advantages in the Western Pacific, Washington is prepared to seriously consider using nuclear weapons first to vindicate its own vital interests and those of its allies — for instance with respect to their territorial integrity. More than that, Beijing should understand clearly that if it pushes forward with its military buildup, it will spur the United States to rely even more on its nuclear forces to compensate — and, if that is not enough, the real possibility that U.S. allies will be impelled to pursue nuclear arsenals of their own. Communicating all this to Beijing does not require any Strangelovian contortions. But it does require the United States to firmly and consistently say (or otherwise communicate) that it is prepared to use nuclear weapons first if truly pressed; to build the forces, such as a next-generation standoff cruise missile and intercontinental ballistic missile, useful in making such a declaration credible; and to exercise and deploy its forces in ways that show Beijing its earnestness about such a declaration. Such a policy is more likely to contribute to peace and stability than a no-first-use pledge. China is very unlikely to turn away from its effort to achieve military dominance in East Asia and the Western Pacific based on appeals to goodwill or competitions in moral preening. What might actually work is persuading Beijing that succeeding in this effort is likely to backfire by resulting in little to no gain and a more menacing and dangerous set of opposing militaries. Does China want a U.S. defense posture for Asia that relies more on nuclear weapons? A proliferated Asia-Pacific? Washington must make Beijing understand that if it continues its military buildup, those are very real probabilities. A no-first-use pledge would suggest to Beijing just the opposite — that continuing to build up, and perhaps even using, its military power may not be sufficiently dangerous or costly after all. That would be far worse for Asia and America than a perhaps unfashionable reminder that there will be a grim nuclear risk if Beijing ever seeks to capitalize on its growing conventional military strength.

#### Lack of a credible, efficient first strike capability emboldens adversarial nuclear aggression.

Green ’19 [Brendan; assistant professor of political science at the University of Cincinnati; 7-9-2019; “Donald Trump and Presidential Nuclear Launch Authority: The More Things Change…“; War on the Rocks; https://warontherocks.com/2019/07/donald-trump-and-presidential-nuclear-launch-authority-the-more-things-change/; Accessed 7-1-2020; Camp-AI]

Many brave barrels of ink and intrepid pixels have gone to their fate to advance a better understanding of nuclear weapons. However, prior to 2016, few of these seriously grappled with the implications of a figure like Donald Trump in the Oval Office. His arrival has precipitated a reexamination of long-settled questions in nuclear analysis — most importantly the president having the **sole authority** to launch a nuclear weapon. Although such reconsideration of common wisdom is always welcome, the increasingly popular answer to the question of presidential nuclear authority is not: that the United States should adopt a policy requiring authorization from multiple actors to fire nuclear weapons. In fact, multiple authorization remains a bad idea, even if the alternative places formal control of America’s fate in hands of uncertain stability. The debate over how to authorize the use of nuclear weapons is one facet of the “always/never” problem that was identified by Peter Feaver: States want high assurance that nuclear weapons will always be used when directed and that they will never be used otherwise. The problem is that there tends to be a tradeoff between “always” and “never.” Measures that add safeguards against accidental or unauthorized use tend to reduce operational efficacy in situations where speed and tight control are crucial, while command-and-control arrangements that prioritize flexibility and speed tend to be more vulnerable to abuse and/or mishaps. The balance between “always” and “never” can be set in a number of different ways, and states can reasonably make adjustments depending on the circumstances. For instance, warfighting doctrines (either for a damage-limiting first strike or for battlefield use) are more operationally challenging, often depending on speed, coordination, and adaptability. By contrast, doctrines emphasizing retaliatory punishment do not necessarily depend on a quick response, though credibility may be more fundamental for deterrence. Likewise, in peacetime, the need to prioritize successful nuclear operations would appear to be less than during a crisis or war, while the threat of unauthorized use is also lower. The key policy question is, under what circumstances, if any, is making changes to the authority to launch nuclear weapons a good way to push the balance toward “never?” Several recent articles argue that such circumstances were created with Trump’s election. Whether referring to the president explicitly or not, they all express the fear of an unstable or irrational actor launching a nuclear war. These arguments for multiple authorization come in several flavors. More restrictive arguments aim to require the explicit approval of other constitutional actors — either the Supreme Court or a majority of a specially constituted congressional committee — or the uniformed military. Less restrictive arguments suggest that the president should be compelled to consult with other civilian and military actors, time and circumstances permitting, without actually giving them veto power. How Effective Are Legal Restrictions One problem with arguments like these is that the most effective restrictions on an irrational president’s nuclear authority are informal, not legal, and by and large already exist. In the case of a bolt-from-the-blue peacetime attack, resistance from the armed forces — perhaps even vigorous resistance — can probably be expected regardless of the legal situation. Jeffrey Lewis and Bruno Tertrais note that “captains of US SSBNs [ballistic missile submarines] are expected to make communications contact in the event of [an] unexpected launch order that seems out of place or character,” citing one former captain who is on record saying “that, in the event of a peacetime launch, he would insist on confirmation and a justification.” Similarly, at the height of the Watergate scandal, when President Richard Nixon was drinking heavily and talking bombastically about nuclear weapons, Secretary of Defense James Schlesinger famously gave orders that military commanders needed to double check with him or Secretary of State Henry Kissinger before executing any order for a nuclear launch. Personally, I think a bolt-from-the-blue attack order is more likely to precipitate a soft coup than it is actual nuclear use. In such a case, the constitutional fallout is likely to be significant and thus it ought to be the focus of our attention. At the same time, during a crisis or conventional war, legal requirements are not likely to stop a determined president, rational or otherwise. For instance, President Dwight Eisenhower noted in public that, regardless of Congress’ formal power to declare war, any president who didn’t act with alacrity to order a nuclear attack when needed to protect the American people “should be hanged.” He privately reassured members of Congress that “in the event of a real emergency,” he “would not come to Congress, but” would “go ahead” and act on his own. Even when America was at peace, Eisenhower circumvented the legal restrictions of the Atomic Energy Act, which forbade sharing custody of nuclear weapons with American allies. He set up a system where American controls over nuclear weapons in Europe were extremely loose. As Eisenhower put it, “we are willing to give, to all intents and purposes, control of the weapons. We retain titular possession only.” Congressional reports howled with outrage, but the policy was not changed until a new administration decided to change it. Eisenhower was an exceptional president in many ways, but not with regard to legal restrictions and foreign policy. In any event, requiring a president to consult with other actors prior to launching a nuclear weapon, as envisioned by less restrictive proposals, will probably take place anyway in the form of the chain of command pushing back during peacetime, as described above. More restrictive proposals for checking presidential nuclear authority would need to be aimed at very difficult, and rare, cases: situations where a determined but irrational president wants to launch a nuclear strike and is unsuccessfully opposed by military and perhaps other civilian authorities, likely during a war or crisis. The only way to stop nuclear use under these circumstances is to require multiple authorizations, with each party possessing an effective veto. This is the kind of command arrangement that was pursued by the Soviet Union during the Cold War and is still in place in Russia today. Tilting Too Far Toward “Never” However, this leads to a second problem, which is that proposals for multiple authorizations tilt the dial much too far toward “never” at the expense of “always.” The costs of such an approach should not be dismissed as fanciful, as there are many signs that the world could be headed for **increased nuclear competition**. Keir Lieber and Daryl Press point out that technological change has made nuclear arsenals more vulnerable than ever before. I argue that these technical trends, along with unstable beliefs about mutually assured destruction and domestic hurdles to arms control, have **heightened the global** **risks** of peacetime nuclear competition. Similarly, the 2018 Nuclear Posture Review highlights the increasing emphasis that American adversaries are placing on their nuclear forces. Analysts like Brad Roberts have made similar observations. Even states with historically stable nuclear force postures, like India, are moving toward counter-force competition. If these trends persist, requiring multiple levels of authorization could be **costly during war and crises**, as well as peacetime. In the event of a war, the time needed to surmount a congressional or Supreme Court veto could **spell doom in instances where a first strike might be justified**, such as an attempt to preempt a North Korean nuclear force about to fire. Moreover, additional veto concerns of any sort make retaliatory missions much more challenging, since they increase the demands on the secure communications capabilities and continuity of government procedures necessary to ride out an attack. During a crisis, adding veto power beyond the president could encourage American adversaries to take more nuclear risks in the belief that Washington will have a relatively lower risk tolerance. The result could be more nuclear crises with **worse outcomes**. In the end, almost the entire value of nuclear weapons comes from the (at least implicit) threat to use them. Standing up before the world and ostentatiously making them more difficult to use during a crisis sends exactly the wrong signal. A complex system requiring multiple authorizations could impose peacetime costs as well. The experience of the Soviets is instructive here. In the later part of the Cold War, Soviet military officers and civilian analysts alike were deeply pessimistic about the survivability of the Soviet nuclear command system. In part, this was a technical problem, but these worries were also caused by political decisions about Soviet command and control, including the multiple actors needed to authorize a launch. The command system necessitated buying heavily redundant nuclear forces and early warning capabilities to compensate for decapitation risks. It also caused a ferocious civil-military upheaval, with the General Staff of the Armed Forces of the U.S.S.R. pressing strongly for greater ability to launch on warning. Chief of the General Staff Marshal Nikolai Ogarkov was eventually removed in response, at least in part, to this controversy. Importantly, Soviet command arrangements did not go unnoticed in Washington. When the CIA learned of the Soviet multiple authorization system in 1977, National Security Adviser Zbignew Brzezinski flagged the issue for President Jimmy Carter. Brzezinski noted that a Soviet decision to retaliate was not “the choice…of a single individual.” Instead, it was “probably a three-man collegial decision.” Brzezinski concluded that consequently “it might be very difficult for the USSR to ‘launch from under attack’ unless the three men are kept constantly in touch — no separate vacations.” The Carter administration’s interest in Soviet command and control was part of a broader learning process that indicated that Soviet nuclear forces were much more vulnerable than policymakers had initially anticipated. In conjunction with other changes in the intelligence picture, these discoveries led to a **more aggressive American nuclear posture** during Carter’s last three years in office. Domestic Considerations A third problem with command and control based on multiple authorizations is its effects on domestic politics. Though some analysts claim to use Trump only as a foil to highlight structural risks that would exist in any administration, one cannot help but notice that there was a conspicuous dearth of interest in presidential control of nuclear weapons during the Barack Obama years. Whatever one thinks of Trump, it seems like a bad idea to change long-standing defense structures in response to displeasure with the current Oval Office occupant, however justified. Such a move would set a **bad precedent**, worsen political polarization, and be perceived as highly partisan. Some would defend the motives behind instituting a multiple authorization protocol as a reconstitution of congressional authority in national security matters. Congress is, after all, granted the sole power to declare war under Article I of the Constitution. One would think that Obama’s robust defense of presidential prerogatives over the use of force and Congress’ craven abdication on most national security issues of significance would have cured analysts of this particular anachronism. It has the air of special pleading about it — one doubts that any analysts calling to restore congressional dignity are really prepared to embrace a thorough-going originalist approach to the constitution, or even the kind of foreign policy that a legislature could manage. There is much to be said against the new understanding of the constitution that arose, largely without amendment, in the 20th century. But one of its great virtues is that is has provided a viable political order under modern conditions, including a global foreign policy, as well as a massive technological revolution in warfare. Together, these conditions increase the need for making speedy decisions about nuclear war while making those decisions largely immune to legislative oversight. For good or for ill, both Congress and the executive recognized this fact during the Cold War. Attempting to close our eyes to it now seems unwise. The romantic in me would like to enhance congressional authority in foreign policy, and much else besides. The realist in me, however, has learned to stop worrying and to love leviathan, who, as Hobbes promised us, at least provides the most promising route to survival. Moreover, I would argue that the president is optimally situated to provide domestic legitimacy to nuclear decision-making, insofar as such legitimacy is possible at all. The president owes his authority to victory in a nation-wide election, conducted according to the procedures mandated by the Constitution. No other elected official who might be included in the chain of command can claim as much, while the mandate of civilian appointments like the secretary of defense or the Supreme Court justices is even more tenuous. And, of course, military officers have no democratic mandate at all, their many other virtues notwithstanding. If democracy is to have the high national value it is generally accorded, surely decisions of national survival should be made by the one office elected by the majority of the entire nation. In the end, nuclear weapons force policymakers to face uncomfortable truths. No sane person wants to see these weapons used. But for America to be able to effectively deter its enemies, it must be prepared to use its arsenal in extreme circumstances and use it with speed and certainty. Eisenhower, again, put it best: In nuclear operations, “the United States would be applying a force so terrible that one simply could not be meticulous as to the methods by which this force was brought to bear.” America’s national interests and, indeed, its survival, require a clear chain of command headed by the only individual who has a democratic and constitutional claim to speak for the entire nation: the president. Even if that president is Donald Trump.

#### NFU undermines deterrence for future tech attacks---extinction

Eldridge Colby09. Fellow at the Center for a New American Security, JD from Yale Law. “Nuclear Weapons and Expanded Deterrence Against Catastrophic Attacks,” Chapter 15 in Part I: Deterrence of In the Eyes of Experts: Analysis and Comments on America’s Strategic Posture, US Institute of Peace Press, https://www.usip.org/sites/default/files/In%20the%20Eyes%20of%20the%20Experts%20full.pdf

Summary: The United States and its allies will face increasingly sophisticated and dangerous weapons of catastrophic destruction due to the accelerating advance and dissemination of technology. Nuclear weapons will play a key role in deterring the use of these weapons by state or non-state opponents as long as the United States continues credibly to threaten retaliation, to include nuclear usage, in response to catastrophic strikes. A “no first use” posture would be incompatible with an effective deterrent of this kind, and the Commission should consider stating so. Nuclear weapons will not, however, be sufficient to deter catastrophic attacks. Instead, the Commission should consider voicing support for the Administration’s commendable but poorly implemented policy of expanding deterrent threats to include those who enable or support catastrophic attacks against us or our allies. Text: Accelerating advances across science and technology, to include in computing, nanotechnology, biotechnology, as well as in the more mature nuclear field, combined with our staggering advantages in conventional warfare, make it a near certainty that the United States will in the coming decades face increasingly powerful, sophisticated, and dangerous weapons, tools, and systems. Though traditional state rivals will likely be the principal wielders of these new technologies, their dissemination outwards to marginal states and downwards to non-state actors means that the U.S. will confront threats from a variety of types and groupings of actors. While the parameters of these new technologies are uncertain, we can be confident that they will be not only tremendously powerful, disruptive, and damaging, but also supremely elusive and cost-efficient. Non- and counter-proliferation efforts will be a critical mitigant of these deleterious trends, but, given that they are the necessary obverse of the benefits of new innovation and that challenger powers will so clearly benefit from them, they cannot be halted. They instead must be managed. U.S. nuclear weapons should play a partial but central role in dealing with the rise of these threats. Our nuclear arsenal will do so because, so long as it is maintained at a sufficient level of quality and quantity and appropriately postured, it constitutes a decisive asymmetric retaliatory capability that ipso facto makes the use of any weapon of catastrophic consequence, however novel, against us or our allies more costly than beneficial. Further, by ensuring this decisive asymmetry they allow us and our allies the freedom not to have to match (either with similar weapons or defensively) every advance in weapons technology our opponents and rivals may make (though maintenance of an edge in some fields is advisable and even necessary). As with the NATO allies’ effective decision not to match Warsaw Pact capabilities after the failure of the Lisbon Treaty commitments and the formal decision to forswear chemical and biological weapons in the face of massive Soviet superiority (the latter clandestine) in those fields, the U.S. and its allies in the 21st century can reliably invest in maintaining an assured nuclear deterrent to render catastrophic acts of destruction irrational as such rather than seeking symmetry in armaments. This logic would counsel continuing to resist adopting a “no first use” doctrine and perhaps even considering, as our opponents and rivals begin to field disruptive new technologies, reminding them of our willingness to respond to catastrophic aggression of any kind with the tools most suited to our purposes. This would point towards restraining and perhaps walking back what has, in light of overwhelming conventional U.S. military superiority over the last two decades and an unusually calm international scene, become an informal “no first use” policy. More broadly, it would counsel shoring up the credibility of our threats to respond asymmetrically as we deem appropriate, whether with nuclear weapons or otherwise. This approach would have both direct deterrent as well as dissuasive benefits. Opponents facing the real prospect of firm and potentially severe retaliation by the U.S. will price the reality of this American commitment into their strategic calculations, thus rendering arms competitions less likely.

### Cyber CP---NFU Plank---AT: De-Alert

#### De-alert fails and undermines crisis stability

Peter Huessy 19 {Peter Huessy is Director of Strategic Deterrent Studies at the Mitchell Institute for Aerospace Studies and President of his own defense consulting firm, GeoStrategic Analysis. 8-9-2019. “A Dangerous Nuclear Agenda.” https://www.theepochtimes.com/a-dangerous-nuclear-agenda\_3035909.html}//JM

Should America Take Its Missiles Off Alert? Now another idea is to take American land-based missiles “off alert” (like unplugging an appliance) to lengthen the time between a crisis occurring, and when the United States commanders can actually launch our ballistic missiles. The idea is that in a crisis if the American President can’t quickly launch our land-based missiles, because the missiles are “unplugged” or de-alerted, the extra time it takes to put America’s missiles back on alert will be exactly the time needed for the crisis to be defused. (Since it takes only seconds to put a missile back on alert to be ready to fire, such an assumption is ridiculous.) Now such ideas as de-alerting has been proposed before. And such ideas have always been determined to be highly risky and dangerous. First, the “de-alerting” or unplugging of America’s missiles is not verifiable. Even if all nuclear powers de-alerted their missiles, the United States or its adversaries could place their own missiles back on alert in a matter of seconds and no one would be the wiser. We would not want American leaders to assume that Russian missiles could not be launched because they had been “de-alerted,” because America’s guard might be down, and our inaction assumed to reflect passivity. Second, the lack of any effective verification for such “de-alerting action” heightens uncertainty in a crisis. For example, in a crisis, Russia might assume the United States would rush to put our missiles back on alert to thus be able to launch them at Russia. But Russia could not verify whether our missiles were or were not on-alert and ready to launch or “turned off.” That uncertainty might easily pressure the Russian national leadership to decide it would be better to launch Russian missiles at the United States as soon as possible in order to “get the first punch in.” In short, given there is no way to verify whether a U.S. missile is on-alert or not on-alert, or can or cannot be launched, such uncertainty could easily lead a Russian leader to panic and during a crisis, make a rash decision to launch Russian missiles at America first. In doing so, the Russians would hope to destroy as many of our fixed, silo-based land based missiles as possible, under the assumption that even if the United States radars and early warning satellites see the Russian missiles coming at our silos, the American missiles will not have time to be put back in launch status because the United States “de-alerted” its own missiles and thus literally the American missiles will remain “sitting ducks.” So, in a crisis, because America will assume to have de-alerted, the Russians might then to decide to “go first” and launch its nuclear missiles and “hope for the best!” Such a “U.S. race to re-alert” is hardly reassuring.

### Cyber CP---NFU Plank---Turn---Aeterioids

#### Scrapping ICBMs makes asteroid deflection impossible – they’re the only thing that can do it

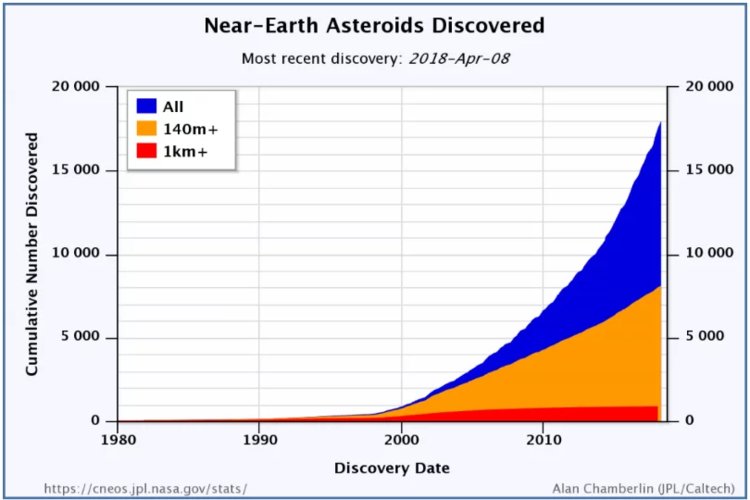
Amanda Buchanan 16, Assistant Astronomer @ Primland, "Is Blowing up an Asteroid with a Bomb Really a Good Idea?", Futurism, https://futurism.com/blowing-asteroid-bomb-really-good-idea

To clarify, ICBMs are the long-range nukes that the USSR and USA had pointed at each other during the Cold War (in fact, they still have some pointed at each other). Russian scientists argue that typical rockets are not good candidates for seizing asteroids because they require too much lead time to meet an asteroid that might be detected only days before impact. And true enough, typical payload rockets take several days to fuel. On the other hand, ICBMs can be launched at a moment’s notice.

#### Key to stop collision – otherwise extinction-level asteroids are coming

Peter Farquhar 18, "The White House is considering nuking asteroids, according to a NASA report", Business Insider, https://www.businessinsider.com/the-white-house-is-considering-plans-to-nuke-asteroids-2018-6?r=UK&IR=T

The US has an official strategy for dealing with Near-Earth Objects (NEOs) that threaten the planet — and yes, it involves nukes. You might know them as "asteroids", or "comets", but rocks and balls of ice and gas aren't the only objects that could potentially destroy a chunk of life on Earth. There's more detail on what an NEO is in the 20-page report prepared for the White House to look at, along with things like "procedural actions", "international cooperation" and "computational tools". But for now, let's cut straight to Goal 3 — "Develop Technologies for NEO Deflection and Disruption Missions". There are really only two options — deflection and disruption. "Multiple technologies may be suitable for preventing NEO impacts that are predicted well in advance," the report states. "While disruption via nuclear explosive device may be the only feasible option for NEOs that are very large or come with short warning time."Here are the technologies the White House is considering: Concepts for rapid response NEO reconnaissance missions. Including "mission concepts in which the reconnaissance spacecraft could also carry out deflection or disruption". International launch vehicle infrastructure to support planetary defense missions. Including "processes for accomplishing rapid response planetary defense space-lift". Identify technologies required to prevent NEO impacts. This is the one which includes "kinetic impactors, nuclear devices, and gravity tractors for deflection, and nuclear devices for disruption". Let's stop there, at "kinetic impactors, nuclear devices and gravity tractors". A kinetic impactor is simply smashing a spacecraft into the NEO in the hopes of deflecting it. A nuclear device is obviously your straightforward, "call Bruce Willis" case scenario. The gravity tractor is something NASA is a couple of years away from testing. It performs a little bit like this: [graphic omitted] Back in 2016, NASA announced its plan to target the 400-metre wide asteroid 2008 EV5 in 2021 with the gravity tractor technology. Another important part of its mission, which the NEO white paper alludes to, is to grab a boulder off the surface of EV5: [graphic omitted] Because if we're going to blow up asteroids, it's important to know exactly what it's made of. Best of all, we might not have to wait for a Armageddon-sized asteroid to threaten us before we get to blow it up. The White House paper also makes sure to mention that test runs on harmless NEOs are essential to make sure this type of action will work. It will, obviously, cost billions. But what are the chances of a decent ROI on all that spending and cooperation? For one, the NEO white paper mentions that any asteroid exploration and material testing can be done in partnerships with private industry, because asteroids can potentially be worth trillions. Fortunately for private industrialists, in 2015, US Congress passed the SPACE Act, giving US space firms the rights to own and sell natural resources they mine from bodies in space. But NASA has often referred to the fact there is "no record in modern times of any person being killed by a meteorite" and that even an asteroid 1.5 kilometres across only hits the Earth every million or so years. "In fact, as best as we can tell, no large object is likely to strike the Earth any time in the next several hundred years," it says. Here are a couple of reasons why the need for an official response playbook has escalated in the past few years. For starters, this is the damage an object the size of the Tunguska object could inflict on New York: [graphic omitted] The object that exploded over Tunguska and destroying 2,000 square kilometres of forest was 40-60 metres across. The asteroid that exploded over Chelyabinsk in Russia with the power of 20-30 atomic bombs, damaging 7,200 buildings and injuring 1,500 people, was just 20 metres across. Here's the rise in NEOs we've spotted larger than 140 metres since US Congress directed NASA to really start properly looking for them in 2005. We're up to 18,000 on just 3,500 since then:



NASA estimates there are over 10 million NEOs larger than the Chelyabinsk asteroid, and 300,000 objects larger than 40 metres, "that could pose an impact hazard and would be very challenging to detect more than a few days in advance". The big ones — larger than one kilometre across — are those that have the potential to severely disrupt life on Earth as we know it. The dinosaurs found out the hard way 65 million years ago when a 10-kilometre asteroid hit the Yucatan peninsula. But NASA says it's found and catalogued almost all of those, and none are on a collision course with Earth. NASA's NEOWISE survey, for example, has been tracking, and improved its ability to track, asteroids for four years now: That's where the other half of the report is focused — on improving tracking methods, data processing and processes for identifying hazardous asteroids and the best way to deal with them. Because while we are close to 100% certain that no extinction-level asteroids we've spotted are on a collision course with Earth, we're not 100% sure we've spotted all the extinction-level asteroids. As the NEO report admits, there is some chance that "large comets from the outer solar system could appear and impact the Earth with warning times as short as a few months".

### Hotlines CP---2AC

#### Hotlines fail and only increase miscalc

Dr. Simon J. A. Mason 13, Senior Researcher and Head of the Mediation Support Team at the Center for Security Studies, Doctorate in Environmental Science from ETH Zurich, and Matthias Siegfried, Project Coordinator of the Mediation Support Project at swisspeace, Holds an Executive Masters Degree in Business Administration, “Confidence Building Measures (CBMs) in Peace Processes” in Managing Peace Processes: Process Related Questions. A Handbook for AU Practitioners, Volume 1, African Union and the Centre for Humanitarian Dialogue, p. 64-75

• CBMs in the Security Sector

In the security sector, CBMs in inter-state conflicts can be differentiated from CBMs in intra-state conflicts. Classical military CBMs focus on avoiding escalation triggered by a misunderstanding of signals,16 In a highly hostile atmosphere, any behaviour of the other side is generally interpreted as being hostile, rather than as being a deterrent. The aim of these kinds of CBMs is to clarify the difference between an intended aggressive behaviour and the background noise of normal military activities, in order to avoid unintended escalation. Examples include communication hotlines, exchange of military maps, joint training programmes, information on troop movements, exchange of military personnel, establishment of a demilitarized zone, border tension reduction through joint patrolling, or no fly zones.17

In the context of peace processes between a government and an armed non-state actor, security issues can be dealt with simpty as technical questions, or they can be used in a CBM logic to build trust and a working relationship between former adversaries. Joint monitoring teams, for example, have a specific security goal as they verify ceasefire violations. At the same time, security personnel from both sides of the divide work together and can thereby build trust. From a mediator's point of view, joint monitoring teams, as well as other security arrangements, should not be seen as only increasing security. They have significant potential to create trust and help parties develop a working relationship across the conflict cleavage. Designed and used in a "CBM logic", they can have positive spillover effects into the political sector10 (see Box 4 on how the Joint Military Commission helped to create trust between the parties in the Nuba Mountains).

• Economic and environmental CBMs

Economic and environmental CBMs focus on joint economic endeavours or activities dealing with natural resource management and environmental challenges. Opening trade routes can help to ease tensions and benefit both actors. Co-operation over economic issues can often be a first step in collaborating across conflict lines. In Somalia, for example, actors from different clans and ideological inclinations are often very pragmatic about working together when it comes to doing business, for example trading in livestock across conflict lines. These economically-motivated collaborations can be seen as CBMs that could provide the building blocks for a bottom-up approach to a more comprehensive peace process. Other examples of economic CBMs include agreements to allow actors from different groups to access markets safely (for example, in the Kenya border area); agreements to open trade routes (for example, for pastoralists to access water points, or opening international transport routes to facilitate trade); joint economic development projects (such as the Korean Kaesong industrial region, or ideas for international pipelines); joint preparation against natural disasters; or peace parks (for example, in Southern Africa).20

• Social, humanitarian and cultural CBMs

Some of the very first CBMs used, even before negotiations begin, are typically humanitarian CBMs. If parties agree on some basic humanitarian principles, not using anti-personnel mines for example, they signal commitment to international norms and possibly their preparedness to also try political means to reach their goals. Such CBMs help the affected population, but also provide conflict parties with the fresh start that is needed if they seek to try negotiations. Through such CBMs, they can signal to the other side an intention to change the status quo, A prisoner exchange is another typical humanitarian CBM (for example, the Gilad Shalit Fall 2011 exchange between Israel-Palestine, even if the trust-building goal did not seem to be the main or only motivation). Humanitarian ceasefires, that often include CBMs, can indicate the readiness of both sides to test an alternative approach (see Box 4). The negotiations surrounding such CBMs also help prepare the parties for future political negotiations, as negotiators pick up the necessary skills and know-how when negotiating the CBMs. Some of the Southern Sudanese actors involved in negotiating the Operation Lifeline Sudan in 1989 gained negotiation expertise that proved very helpful later on in the Sudan North South CPA negotiations.22

Social CBMs can include the release of information on missing persons (for example, in Bosnia Herzegovina), or allowing family visits (see box 3 for the Western Sahara example and box 8 when it comes to North-South Korea). Joint cultural events or student exchange programmes are other opportunities that can be used at all levels of society to humanize the other and build relationships. Joint sports activities have also been used in numerous cases to ease frozen relations and pave the way for negotiations (for example, between China and the U.S., see Box 5), Agreements which allow minorities to have rights to their religion and language can also be used as CBMs. even if they often go further than normal CBMs in terms of addressing the root causes of a conflict. In the implementation phase, joint language and educational projects may help to create trust throughout the wider society.

Links between sectors: The links between sectors, and how CBMs in one sector relate to other sectors, is one of the most vital aspects for mediators to be aware of and consider. Synergies and traction can be created through these links. At the same time, links between the sectors have to be clarified to avoid doing any harm. Links can also be developed by cross-matching activities and actors. Examples would be to have military actors involved in economic activities or businessmen involved in security CBMs,23 Lists of CBMs are useful in showing how creative and diverse CBMs can be, but care is needed so as not to suggest that ideas can be copied and used on any given conflict. Template solutions and CBMs that are not developed with the parties will not tit the given case, not be owned by the parties, and will not build trust. Since a mediator is the hub that connects the various topics and experts in the peace process, he or she is responsible for making sure the links between the different CBMs are used well. Clustering different types of CBMs and learning from other cases can be useful to develop ideas, but in the end it is vital that mediators design CBMs with the parties to ensure they are tailored to the specific conflict.

3.6 When should CBMs be used?

CBMs can be used in all phases of a peace process, but their nature and function changes if they are used before, during or after peace negotiations.

Many processes today are more complex than the classical, linear phase model of peace negotiations (informal talks, pre-negotiations, negotiations and implementation) with dffferent actors being involved in different phases that take place at the same time. Nevertheless, the phases still give some orientation as to when to use CBMs:

• Before a peace process begins and during pre-negotiations

Even before a peace process begins, CBMs can be envisioned without necessarily focusing on using them to initiate a negotiation process. They can simply aim to build bridges between conflicting parties and minimize the damage of the conflict, even if the parties are not considering negotiations. In this early

phase, CBMs are likely to be non-binding, social and humanitarian, but could possibly also include partial steps in the security field (such as a non-binding cessation of hostilities to allow a market to happen or to allow a celebration to occur). It is hard for any conflict actor to disagree with minimal humanitarian principles and actions and this is the reason why simple humanitarian agreements can often be a starting point (for example, not using anti-personnel mines). Economic CBMs (such as allowing access to the market place in Wajir. Kenya), which build on an economic rationale, can also be useful. In the "pre-negotiation" phase, parties are starting to consider negotiations more seriously as a credible strategy to solve their conflicts, even if it is not yet clear how. when and under which mediation framework this will happen. In addition to humanitarian and economic CBMs, the importance of political and security CBMs increases in this phase. The aim is for the parties to signal to each other their intention of testing negotiations and to show a certain degree of goodwill to try and enter the negotiation process.

• During negotiations

During the negotiation phase, CBMs that increasingly address aspects of the conflict can help to push the process forward. Depending on the nature of the conflict and design of the meoSation process, CBMs will play a different role. In some cases, parties can agree to key fundamental principles in a very general manner at the outset of a negotiation process, before the "sticky' details are negotiated. Through the initial agreement on principles, some trust is created. In this scenario, CBMs may still be used and may be important but they are not the only, or main, way to build trust. The Sudan North-South process between 2002 and 2005 successfully used CBMs to "humanize" the negotiators and push the process forward, even if there was an agreement earty on about some of the key principles (see Box 6).

In other processes, which do not have such an initial framework agreement on basic principles, trust will be built more incrementally and they will thus rely more heavily on CBMs, In the incremental approach, a series of agreements are used to slowly tackle the more difficult core issues later on. In this approach, CBMs are used as stepping stones to create traction,-5 Agreements on CBMs early on help to build trust and interest in negotiating more complex agreements at a later stage. In this sense, CBMs represent opportunities for parties to collaborate on something that is not strategically important to them and, in so doing, build the trust needed to subsequently address the strategic issues. CBMs pull parties away from the obstacle they are blocked on. the rock they can't get off the road. Once there is confidence, it is then easier to later address this obstacle,1\* The metaphor of steps in the ladder also highlights the incremental nature of building trust which takes time and an accumulation of small steps. This is the reason why some practitioners speak about a confidence building process,-7 Once a first set of CBM has been established, more comprehensive undertakings can be developed. The peace process between Israel and Jordan illustrates the incremental use of CBMs (see Box 7).

• During the implementation

During the implementation phase, CBMs can also be useful to maintain and increase the level of trust. In addition to external guarantees, external force and clear implementation modalities, this trust is vital to implementing and reinforcing peace agreements. CBMs among the wider public are important as benefits from the peace agreement affecting the broader community may not be tangible immediately, CBMs that deliver something tangible to the parties can help the constituencies live with the consequences of a peace agreement.

As the peace process develops, the nature of CBMs generally moves from non-binding, to politically-binding and sometimes even to legally-binding. In a similar manner, unilateral signals of good intention should develop into reciprocal CBMs that are balanced between the parties.

3.7 Challenges and options

Five challenges need to be considered when planning to use CBMs in a peace process.

• Challenge 1: Avoid using CBMs when lack of trust is not a core problem

Mediators are often confronted with at least three major obstacles in their work: the parties lack trust between each other and in the mediation process; the parties lack the political will to change the status quo31; and the parties lack a common understanding of the conflict and how to address it.32 These three obstacles are strongly interdependent; for example, trust tends to increase the better the actors understand each other. At the same time, the greater the trust, the easier it is to listen and develop common understanding. An actor's will to change the situation can also develop hand-in-hand with an increase in trust and common understanding. Nevertheless, these three obstacles are also distinct from each other. In some conflicts, there is common understanding and even trust, but no political will to change the status quo. The UN-led peace talks on Cyprus seem partially to illustrate this dynamic, even if this dynamic was also greatly influenced by the incentives set by the European Union (Greek EU membership without agreement on Cyprus).33 In other cases CBMs can help to ease tensions and pave the way for negotiations (such as the U.S. - China rapprochement in the 1960s outlined in Box 5 or the Nuba Mountain Ceasefire Agreement outlined in Box 4).

This differentiation is important, because it only makes sense to use CBMs in cases where lack of trust is a key factor in hindering negotiations. In cases where trust exists, but there is lack of common understanding (which also includes factual knowledge, for example on technical issues) or will, CBMs are not the right tool. In such cases techniques such as capacity-building workshops, dialogue workshops seeking to clarify misunderstandings related to different perceptions, bringing in experts with technical expertise and bringing in moral authorities to discuss values that shape the will to change the status quo, may be more appropriate.

One way to deal with this challenge, is to assess how far lack of trust, lack of will and lack of common understanding are hindering the process, and then to design appropriate measures.

• Challenge 2: Take care that CBMs are not used as a stalling or cover-up tactic

Another aspect to assess when considering CBMs is the possibility that parties will use CBMs as a stalling tactic and as an excuse for not negotiating. CBMs can be used by parties to signal to the international community or their constituencies that "they are doing something'' even if, in reality, they have no intention of changing the status quo or listening to the other side. In this way, parties can jeopardize the very idea of CBMs - to build trust - if they only use them as a cover up for stalling. CBMs can also be used to deflect or postpone negotiations on more significant issues.34 In some cases, it seems CBMs were used to play for time, while in fact a military strategy to solve the conflict was pursued. For example, in the Ivory Coast in 2005, a so-called "Confidence Zone' had been established that ran across the country to separate the rebel-held north and the government-held south. The zone should have provided for basic security of ordinary citizens living in the zone. Over time the situation deteriorated and gave rise to citizens' feeling of insecurity, rather than increased confidence,35 In other cases, the actual negotiations of the CBMs took so long, that it stole away time for negotiating more substantive issues. For example, on numerous occasions in the Cyprus peace process this seemed to be the case, even if one can also argue that the parties may not have wanted to address the substantive issues and so working on CBMs was better than doing nothing.36

A mediator’s main option in dealing with this challenge is to clarify the motivations of the parties for using CBMs, whether bilaterally with the parties or together in plenary meetings.

• Challenge 3: Be aware of "overly successful" CBMs that can distract from real negotiations

Yet another consideration when thinking of using CBMs is to assess whether they will distract from negotiations because they are too successful. CBMs address symptoms of the conflict, rather than the root causes. If CBMs are overly successful, they may take the pressure away from the parties to address the key issues and they may no longer have an incentive to negotiate. In this case, mediators will seek enough successful CBMs to initiate negotiations or move the negotiations on the root causes forward, while avoiding so many CBMs that they can be misused for strong public relations purposes by the parties or they limit the negotiation process only to CBMs. Both having too many CBMs and only focusing on CBMs may take the pressure off the negotiations on substantive issues. Enough dissatisfaction with the status quo is needed to negotiate an agreement. Discussing this dilemma with the parties may be useful to assess the balance needed.

• Challenge 4: Watch out for unilateral, asymmetric and "false" CBMs

In some cases, it might be easier for the mediator to ask one of the parties to commence with a unilateral CBM to which the other party can respond in a positive manner. However, there is a risk that, in such a unilateral approach, one of the parties might lose face or might claim victory over the other side. In the Korean peninsula. South Korea felt the CBMs were not being sufficiently reciprocated, especially from 2008 onwards (see Box 8). Premature concessions that are not reciprocated can increase mistrust.3\*1 In cases where power asymmetry is significant, the more powerful actors can sometimes initiate a change in relationship through a unilateral CBM, and due to their relative power, not risk very much. Thus, in situations where it is the only way to break the deadlock, the mediator might (with the tacit agreement of all parties involved) ask one of the parties to make a unilateral gesture.

In most cases, however, CBMs are most effective if they are designed in a "symmetric manner", whereby all the parties agree to, and implement, a joint CBM at the same time. However, even symmetrical CBMs can lead to asymmetrical impacts, where generally the weaker party is disadvantaged. "False" CBMs are built to look like CBMs but only affect one side instead of both, or all, sides. Even if mediators seek to design balanced CBMs, they may end up as false CBMs, and mediators will end up being perceived as biased. Truly symmetric CBMs should have symmetric impacts, which make it impossible for any one side to either lose face or claim victory. This approach will also help the mediator to preserve impartiality as none of the parties is being seen as responding to a demand of the mediator.

For these reasons, mediators need to carefully plan and discuss the CBMs with the involved parties, and assess their impact on the ground. The timing and degree of commitment needed for the CBMs to work has to be negotiated with the parties.\*' Equality is a key principle in the design of CBMs. However, if equal CBMs lead to unequal impacts, CBMs must be designed in such a way that more is demanded from the party claiming superiority.41 As mediators take care of the process, and parties of the content, the final responsibility and decision on what type of CBMs will be chosen rests with the parties. Mediators can bring in experts and comparative experiences from other cases but, in the end. the parties need to decide how far they want to go and what risks they are willing to take.

• Challenge 5: Avoid unrealistic, fuzzy, non-verifiable and non-implementable CBMs

Agreements on CBMs often lack sufficient details on how they will be implemented and measured.12 The danger of CBMs that are not clear and not verifiable is that they are not implemented, or that they are asymmetrically implemented. This can lead to greater distrust than before. This is why CBMs need clarity on their implementation, including verification mechanisms such as implementation reviews or Joint Commissions. A modest CBM that has clear implementation modalities is preferable to ambitious CBMs that are unclear in terms of how they will be implemented, verification mechanisms can be integrated into the CBMs to help the parties measure and report on the implementation. These verification mechanisms ideally involve the parties as well as some acceptable third party.43

#### Compliance will be selective

Moonis Ahmar 1, Scholar of International Relations and Conflict Resolution from Pakistan, 2001, “Changing Relevance of Non-Military CBMs in South Asia,” 331, “The Challenge of Confidence-Building in South Asia,”

The differing working results of CBMs in both cases raises a critical question: why are they more effective in one case than another? The answer lies in the analysis of different conflict situation, perception of the leaders and their overall priorities. First, there is a problem of commitment. CBMs are seen as a political arrangement that does not entail legal binding or commitment. Thus, the contracting parties have selective compliance to CBMs and use them according to their needs. This argument is more relevant to Pakistan. Second, conflict environment in the India- Pakistan case is more complex than the India-China case. This undermines the effectiveness of CBMs. Third, when the contacting parties, mostly the weaker ones, perceive CBMs as a peaceful way to dilute their original conflict goal, they seek to undermine the agreed CBMs. Many India-Pakistan CBMs have become redundant or dysfunctional because of this perception held by the latter. Fourth, coupled with it is the feeling of one or both parties that CBMs are the ways to avoid or postpone finding a solution to their problem. This is more widespread in the minds of Pakistan; even India had the same feeling vis-à-vis China. Fifth, destabilizing vicissitudes of domestic politics often curtail the prospects of success of CBMs. This is demonstrated more in the India-Pakistan case than in the India-China case. Finally, CBMs fail because the states of the contracting parties remain suspicious of each other as they refuse to have mutual trust; at the same time, developing mutual understanding between their peoples is highly undesirable for them. In most cases, non-military CBMs suffer or fail because of this sort of politically motivated fixation.

### Hotlines CP---China---1AR

#### China will never use hotlines, especially in a crisis

Dr. Andrew S. Erickson 19, Professor of Strategy in the China Maritime Studies Institute at the U.S. Naval War College and Visiting Scholar at Harvard University’s Fairbank Center, PhD in International Relations and Comparative Politics from Princeton University, MA in International Relations with a Concentration in China Studies from Princeton University, BA from Amherst University, “U.S.-China Military-to-Military Relations: Policy Considerations in a Changing Environment”, Asia Policy, Volume 14, Number 3, July 2019, p. 131

It would be extremely regrettable if the MOUs regarding CBMs were one-way documents that limited the United States without ensuring Chinese participation. Beijing declines many opportunities to communicate during a crisis and reduce risk that Washington suggests. For example, the United States will immediately accept a call from anyone in China’s chain of command at any time; Chinese defense officials will not take an immediate call.17 Even though China is given 48 hours to take a call, there is no public evidence that the DTL has actually ever been used during a crisis. Before introducing new dialogues, the two sides need to make sure that existing mechanisms for communication can withstand a crisis—currently an unlikely prospect. When the Countering America’s Adversaries Through Sanctions Act went into effect in 2018, for example, China recalled Admiral Shen Jinlong from the International Seapower Symposium, withdrew General Wei Fenghe from the Diplomatic and Security Dialogue, canceled the Joint Staff Dialogue Mechanism (the premier communications path between the two countries’ joint staffs), and canceled the Ronald Reagan Carrier Strike Group’s visit to Hong Kong. While China later reversed two of these decisions, the situation reflected a decades-old problem: when tensions rise, which is precisely the most important time to talk, Beijing cuts communications. And when China is willing to communicate, it shuns the hotline that the two sides labored to establish in favor of going through the Defense Attaché Office at the U.S. Embassy in Beijing.

### Orbital-Use Fees CP---2AC

#### OUF won’t solve---does not remove existing debris, fails to deter collisions, AND would need to be global which is impossible---only the AFF can solve.

Ruth Stilwell 20. Senior Non-Resident Scholar at the Space Policy Institute of George Washington University and Adjunct Professor at Norwich University. “The Space Review: Orbital use fees won’t solve the space debris problem.” The Space Review. 6-22-2020. https://www.thespacereview.com/article/3971/1 //EM

When it comes to space debris, the numbers are repeated often: more than 21,000 objects ten centimeters across or larger, approximately half a million objects between one and ten centimeters in diameter. Across the space community, there is general agreement that space debris is an existing, and worsening, problem. Many point to the free and open access to space, while others argue that proposed “mega-constellations” will take low Earth orbit to the breaking point. In response, some argue that economic disincentives, like orbit fees or taxes, could be used to reduce demand by increasing the cost of a satellite in orbit. Some argue that additional satellites create additional debris risk solely based on the increase in the satellite population. But is this the problem we are trying to solve?

The principal sources of orbital debris are satellite explosions and collisions, including intentional destruction.

The problem of space debris and congestion is not one of operational satellites, but rather one created by non-maneuverable debris. Space situational awareness and conjunction alerting systems seek to prevent collisions by maneuverable objects, further reducing the risk they impose. It is not the operational satellite, but the behaviors associated with putting the satellite in orbit and removing it at end of life, that increases the debris risk.

In developing appropriate mitigation strategies for orbital debris, it is imperative to consider the primary causes of orbital debris and develop approaches that address those causes. The principal sources of orbital debris are satellite explosions and collisions, including intentional destruction. High-risk orbital behaviors are well known: old launch vehicle upper stages left in orbit with residual propellants and high-pressure fluids, defunct satellites that are not deorbited, and anti-satellite weapons testing. These are the primary contributors to orbital debris and should be the focus of debris mitigation strategies.

State, commercial, and non-government users of space have a shared interest in creating the long-term sustainability of space operations, and global progress requires international agreement. Proposers for an orbital use tax mention that it would need to be globally harmonized but fail to recognize the difficulty in reaching such an agreement—if such an agreement is even possible. The recent collapse of the OPEC pact and the subsequent oil price war illustrates the fragility of international economic collaboration. By contrast, international agreements on standards and regulation for international operators, as we see in the maritime and aviation industries, tend to endure. It is important to recognize that diplomatic resources are limited and efforts to reach international agreement should focus on areas that can provide the most benefit and have the greatest chance for success.

An orbital use tax would put an additional financial penalty on the user that is able to prevent the collision risk but do nothing to change the behavior that created the collision risk.

For the long-term sustainability of space, the answer is not to make space more expensive to use, but rather to ask the users, both civilian and military, to be responsible to the goal of sustainable use. This requires a focus in three critical areas: collision avoidance, limiting debris-generating behaviors, and debris removal. As we ask the space community to be more responsible, it is important to define what that means. As illustrated by recent anti-satellite missile tests, the community can be alarmed, but we are functionally unable to hold each other to standards of behavior if those standards do not exist. Efforts at international agreement should be focused on reaching agreement in these areas if we are to have a sustainable and accountable orbital domain.

#### Widespread SSA abilities are a pre-requisite to solving debris---we can’t stop collisions!

Jason Forshaw et al., 20 (Jason Forshaw, Mike Lindsay, Charity Weeden, John Auburn, Chris Blackerby, 9-18-2020, accessedon 6-23-2022, Advanced Maui Optical and Space Surveillance Technologies Conference, “An Exploration of Space Situational Awareness (SSA) Needs for Active Debris Removal ADR) Operators”, https://amostech.com/TechnicalPapers/2020/Poster/Forshaw.pdf, HBisevac)

Comprehensive Space Situational Awareness (SSA) data allows users to accurately interpret and characterize the activity of satellites, improving operational safety and reducing the risk of collisions by increasing ability to recognize abnormal or off-nominal behavior. In the years since its origin, there have been increasing use cases for SSA, such as asset investment protection, insurance claims, and safety of flight. Now with the advent of new In-orbit Servicing (IOS) missions such as Active Debris Removal (ADR), SSA becomes an important part of operational services.

Astroscale is one of the few companies in the world proposing to aid in the removal of orbital debris through the provision of the following in-orbit services: end-of-life (EOL) targeting the LEO constellations, ADR targeting existing larger space debris, and life-extension targeting GEO satellites. As we grow our business, develop our capabilities, and become closer to fully operational services, Astroscale is developing a clearer understanding of SSA needs for its future ADR missions. This paper aims to address those specialized needs, understanding the key technical drivers.

2. SSA NEEDS FOR ADR

In a classical ADR mission, we have a servicer (the satellite doing the removal) and a client (the asset in space being removed). We will be using this terminology throughout the paper.

We break down our SSA needs into 5 categories:

(1) Pre-launch Assessment

Important data can be provided by SSA even before a servicer is launched, such as client position and, in some cases, client attitude and tumbling rate. ADR services in future will have inherent fixed tumbling rate servicing limits – if a client tumbling rate is too high, then a client may be unserviceable to begin with. Such information needs to be ascertained before a service commences, otherwise this places risk on the ADR provider if they launch a servicer only to find that they can’t perform the intended removal.

(2) Search and Approach

SSA is mandatory for future search and approach maneuvers. Generally, the client is defunct and the satellite has failed in a way such that it needs removal. In this case, absolute positioning systems on-board e.g. GPS are not functional and thus the client’s position can only be known through use of SSA services. One of the first steps in a servicer rendezvousing with a client is the “search and approach” phase (see CONOPS section below) which thus requires use of an SSA service.

(3) Failure Analysis

SSA services can provide some form of failure analysis capability to analyze the conditions surrounding the  failure of the client. For example, if the client is tumbling in a specific way, or has unusual trajectory motion,  this might indicate a GNC or propulsion failure. Understanding such information before rendezvous, could be  very valuable to the ADR service provider.

(4) Collision Analysis and CAM Alerts

CAM (Collision Avoidance Maneuver) alerts are a core stable of conventional SSA provision and are also needed in ADR missions. The servicer must be able to move out of the way of other satellites, or trackable debris.  However, depending on the accuracy of the SSA data, SSA providers may be able to provide independent tracking to help prevent collisions during Rendezvous and Proximity Operations (RPO).

(5) Independent Monitoring for Ensuring Transparency

Finally, regarding safety and security, SSA can provide independent monitoring for ensuring transparency for any regulatory and potential insurance compliance. In particular, tracking of the servicer during the course of the mission can provide confidence that no malicious behavior is being undertaken.

It is to be noted that the needs for SSA for ADR do differ than the broader needs of SSA for mass observation of satellites. In a conventional SSA scenario (e.g. government operational intelligence, general tracking of debris), SSA providers scan for, or track, a very large database of objects. SSA for ADR differs in that, specifically for Needs #1 to #3, ADR customers are looking for specific tracking of just 2 entities – the servicer and the client. Thus, high-quality data on 2 objects is far more valuable than low quality data on a very large number of objects.

### Russian Arms Control CP---2AC

#### Russia says no---they have strategic incentives to avoid caving-in.

Jaganath Sankaran 18. Assistant professor at the LBJ School of Public Affairs at the University of Texas at Austin. “Russia’s Anti-Satellite Weapons: An Asymmetric Response to U.S. Aerospace Superiority.” ArmsControl. 3-7-2018. https://www.armscontrol.org/act/2022-03/features/russias-anti-satellite-weapons-asymmetric-response-us-aerospace-superiority //EM

Notwithstanding these assessments, most Russian analysts display a severe fear of U.S. and allied technological superiority. Although these fears may reflect an extreme worst-case scenario, many Russian military analysts share them. Therefore, they argue, the dependence of U.S. and NATO forces on space-based assets is a vulnerability of which Russia cannot fail to take advantage in a crisis. Russian military commentators claim ASAT and other counterspace weapons will deter aggression and offer war-fighting advantages if deterrence fails.26

These Russian motivations pose profound challenges to pursuing lasting space arms control measures. Several proposed nonbinding behavioral norms may stall the testing of ASAT weapons for the near term. For instance, U.S. Deputy Defense Secretary Kathleen Hicks recently argued for a global ban on ASAT tests that create debris.27 These norms can be diplomatically pursued through multilateral dialogues, including at the UN. Meanwhile, U.S. Secretary of State Antony Blinken reiterated a U.S. desire to develop informal norms to standardize acceptable behavior in space operations. In a speech at the UN Conference on Disarmament, he said the United States wants to engage in “developing standards and norms of responsible behavior in outer space.”28 He further noted, “[W]e should be reducing tensions in outer space, not making them worse.”29

Such diplomatic engagements would provide the United States and its NATO allies with some transparency into Russia’s ASAT and counterspace programs and motivations. Similarly, Russia would gain transparency into U.S. and NATO programs and concerns. Diplomatic engagements can also help communicate redlines and establish a shared understanding of pathways that could lead to conflict escalation in space.30

In the end, however, there are limits to what dialogue and voluntary behavioral norms can accomplish. Without mutual restrictions on aerospace weapons and combat operations, Russians will continue to argue that U.S. and NATO forces retain a significant war-fighting superiority that can be offset only with counterspace systems. Addressing Russia’s perceived vulnerabilities to modern aerospace campaigns will require deeper engagement and structured arms control, possibly with an instrument similar to the Intermediate-Range Nuclear Forces Treaty. Such binding agreements are a difficult proposition in the prevailing geopolitical environment, but they are essential to achieve comprehensive space security and strategic stability.

### Orbital-Use Fees CP---Deficit---Global---1AR

#### It fails if it does not go global.

Tibi Puiu 21. Science journalist and co-founder of ZME Science. He writes mainly about emerging tech, physics, climate, and space. In his spare time, Tibi likes to make weird music on his computer and groom felines. “Orbital 'littering' fee might solve our space junk problem.” ZME Science. 11-12-2021. https://www.zmescience.com/science/orbital-fee-space-junk-0523523/ //EM

However, like other forms of taxes, an orbital-use fee would only work if all countries and agents launching satellites would participate in the program. There are now nearly a dozen countries that perform satellite launches and about 30 that own satellites but rely on others to launch them.

But if one country refuses to participate, the whole scheme is dismantled, similar to how a tax haven attracts corporations, leaving their home countries with no revenue.

“There are many ways the orbital-use fees could be collected and used. In the paper, we outline one possible model based on the Vessel Day Scheme (an agreement which regulates use of a tuna fishery between a group of nations in the Pacific, the Parties to the Nauru Agreement). In this model, the fees would be internationally harmonized and nations with satellite operators would collect fees from the operators subject to their laws. The revenues could then be used as the collecting nation sees fit,” Rao said.

“So for example, if company A was launching from the US, the US could collect the internationally-harmonized orbital-use fees from company A and spend it domestically, invest it in debris cleanup R&D, refund it to US taxpayers, or find some other use for it. The nice thing about these kinds of fees (“Pigouvian taxes”) is that their effectiveness doesn’t hinge on what the revenue is used for,” he added.

### Solar Shield CP---2AC

#### The tech does not even exist yet!

Tony 1NC Phillips, 10 (Dr. Tony Phillips is a professional astronomer and science writer and received his PhD from Cornell, 10-26-2010, accessed on 6-25-2022, NASA, “Solar Shield--Protecting the North American Power Grid”, https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\_solarshield, HBisevac)

That is why a node-by-node forecast of geomagnetic currents is potentially so **valuable**. During extreme storms, engineers could **safeguard** the most endangered transformers by **disconnecting them** from the grid. That itself could cause a blackout, but only temporarily. Transformers protected in this way would be **available** again for **normal operations** when the storm is over.

The innovation of Solar Shield is its ability to deliver **transformer-level predictions**. Pulkkinen explains how it works:

"Solar Shield springs into **action** when we see a **c**oronal **m**ass **e**jection (CME) billowing away from the sun. Images from SOHO and NASA's twin STEREO spacecraft show us the cloud from as many as **three points of view**, allowing us to make a **3D model** of the CME, and predict **when** it will **arrive**."

While the CME is **crossing** the sun-Earth divide, a trip that typically takes 24 to 48 hours, the Solar Shield team prepares to **calculate ground currents**. "We work at Goddard's Community Coordinated Modeling Center (CCMC)," says Pulkkinen. The CCMC is a place where leading researchers from around the world have gathered their **best physics**-**based computer programs** for modeling space weather events. The crucial moment comes about 30 minutes before impact when the cloud sweeps past **ACE**, a spacecraft stationed 1.5 million km upstream from Earth. Sensors onboard ACE make in situ measurements of the CME's **speed**, **density**, and **magnetic field**. These data are transmitted to **Earth** and the waiting **Solar Shield** team.

"We quickly feed the data into **CCMC computers**," says Pulkkinen. "Our models **predict fields** and **currents** in Earth's upper atmosphere and **propagate** these **currents** down to the **ground**." With less than 30 minutes to go, Solar Shield can **issue an alert** to utilities with detailed information about GICs.

**<<<NEG ENDS HERE>>>**

Pulkkinen stresses that Solar Shield is experimental and has never been field-tested during a severe geomagnetic storm. A small number of utility companies have installed current monitors at key locations in the power grid to help the team check their predictions. So far, though, the sun has been mostly quiet with only a few relatively mild storms during the past year. The team needs more data.

#### The CP only gives 30 minutes of warning.

BFHR in GREEN

1NC NASA 10 [NASA, 10-26-2010, "Solar Shield," No Publication, https://science.nasa.gov/science-news/science-at-nasa/2010/26oct\_solarshield]/ISEE

That is why a node-by-node forecast of geomagnetic currents is potentially so valuable. During extreme storms, engineers could safeguard the most endangered transformers by disconnecting them from the grid. That itself could cause a blackout, but only temporarily. Transformers protected in this way would be available again for normal operations when the storm is over. The innovation of Solar Shield is its ability to deliver transformer-level predictions. Pulkkinen explains how it works: "Solar Shield springs into action when we see a coronal mass ejection (CME) billowing away from the sun. Images from SOHO and NASA's twin STEREO spacecraft show us the cloud from as many as three points of view, allowing us to make a 3D model of the CME, and predict when it will arrive." While the CME is crossing the sun-Earth divide, a trip that typically takes 24 to 48 hours, the Solar Shield team prepares to calculate ground currents. "We work at Goddard's Community Coordinated Modeling Center (CCMC)," says Pulkkinen. The CCMC is a place where leading researchers from around the world have gathered their best physics-based computer programs for modeling space weather events. The crucial moment comes about 30 minutes before impact when the cloud sweeps past ACE, a spacecraft stationed 1.5 million km upstream from Earth. Sensors onboard ACE make in situ measurements of the CME's speed, density, and magnetic field. These data are transmitted to Earth and the waiting Solar Shield team. "We quickly feed the data into CCMC computers," says Pulkkinen. "Our models predict fields and currents in Earth's upper atmosphere and propagate these currents down to the ground." With less than 30 minutes to go, Solar Shield can issue an alert to utilities with detailed information about GICs. Pulkkinen stresses that Solar Shield is experimental and has never been field-tested during a severe geomagnetic storm. A small number of utility companies have installed current monitors at key locations in the power grid to help the team check their predictions. So far, though, the sun has been mostly quiet with only a few relatively mild storms during the past year. The team needs more data. "We'd like more power companies to join our research effort," he adds. "The more data we can collect from the field, the faster we can test and improve Solar Shield." Power companies work with the team through EPRI, the Electric Power Research Institute. Of course a few good storms would help test the system, too. They're coming. The next solar maximum is expected around 2013, so it's only a matter of time.

#### That’s insufficient to solve---advanced detection through SSA is key.

Martin Weiss & Mathew Weiss 19. Researcher at American Jewish University; Analyst at the UCLA-Olive View Medical Center, “An assessment of threats to the American power grid”. *Energy, Sustainability and Society* volume 9, Article number: 18. October 2019. <https://doi.org/10.1186/s13705-019-0199-y> //EM thx Khirn

2. The 15–45 min warning time of a geomagnetic storm provided by space satellites (ACE and DSCOVR) will be insufficient for operators to confer, coordinate, and execute actions to prevent grid damage and collapse.

### SSA CP---Multilateral---2AC

#### Cooperation can’t overcome technical challenges---different data, uncontrollable variables, and classification standards.

Alexandra **Stickings 19**, research fellow for space policy and security in the Military Sciences Team at the Royal United Services Institute for Defense and Security Studies, MSc in international security and global governance from Birkbeck College, University of London, 8/29/19, “The Future of EU–US Cooperation in Space Traffic Management and Space Situational Awareness,” https://www.chathamhouse.org/sites/default/files/CHHJ7468-Cooperation-Space-Traffic-WEB-190816.pdf

The second set of challenges are technical and may be those that are most open to exploitation by STM providers hoping to establish or increase their contribution. Despite the number of sensors and actors, there are still significant difficulties in understanding and predicting the movements of pieces of orbital debris. One of these is related to the size of debris that can be tracked, although the US Air Force will have greater capability in detecting smaller objects following the completion of the Space Fence in 2021.27 Many of the models used to predict debris movements do not take into account the effects of solar radiation and internal dynamics, such as residual radiation pressure from power sources or whether the object is tumbling. As a result, while it is possible to detect objects over a certain size, it is not always possible to track them. Research is required to further understand the behaviour of certain materials when they are subjected to radiation and to how internal radiation and tumbling affect the orbit of a piece of debris. Technical challenges also relate to the sharing of information. Although more data sources used to create positional information increases reliability, there can be difficulty in incorporating data from these sources if they use different methodologies, lexicons and ways of characterizing objects.

#### Countries collect SSA for military purposes---which means classification is key---absent that, it opens a window for attacks.

P. J. **Blount 19**, Postdoctoral Researcher, University of Luxembourg; Adjunct Professor, LL.M. in Air and Space Law, University of Mississippi School of Law, Board of Directors, International Institute of Space Law, April 2019, "Space Traffic Management: Standardizing On-Orbit Behavior", <https://www.researchgate.net/publication/332115013_Space_Traffic_Management_Standardizing_On-Orbit_Behavior>

The first element of STM is data. In order to effectively manage space activities, it is essential to have information about what is in orbit, where it is at a given time, and who (if anyone) controls it. This information is known as Space Situational Awareness (SSA) data. Currently, SSA data are collected through a variety of systems and by a number of different actors, but the U.S. Space Situational Network (SSN) is the most comprehensive and accessible of these systems.7

The SSN system is a network of sensors that collect on-orbit data. It is managed by the Combined Space Operations Center (CSpOC), which is part of the U.S. military's Joint Force Space Component Command. The primary mission of the SSN system is to protect military space assets and assure military access to space. However, CSpOC has been statutorily authorized to share these data globally.8 This sharing is designed to protect national security by making available the most sensitive SSA data only to other U.S. government entities and allies. The most widely available data, on the other hand, only contain what is known as the Two-Line Element sets, which carry the most basic information on the location of an object in orbit, and are publicly available through Space-Track.org with the creation of a user account.9

While the SSN system is the most comprehensive source of SSA data, there are other states, notably Russia and China, that also collect SSA data. Some nonstate entities such as the Space Data Association (SDA) collect these data as well. SDA is an organization of satellite operators that share SSA data with each other. Notably, SDA has signed an agreement with CSpOC for bilateral sharing of data between the two. There is, however, no comprehensive data pool for SSA data, and much of the data is still considered sensitive and restricted.

Foundational to any proposed STM project are data, and the data must be standardized so that actors within the system can access them and contribute their own data. Further, data integrity must be maintained within the system to avoid mistakes. This means that a multilateral STM system will need to adopt data standards to integrate data from multiple sources and compile it into a single database. Since SSA data are currently collected by various entities using a variety of sensors, ensuring that the data are harmonized will be important. Additionally, STM will require an open data system so that data are public and verifiable. The need for openness is rooted in trust. STM will require some satellite operators to move their on-orbit assets in order to avoid conjunctions with other space objects. If the data underlying the decision-making process are unavailable to operators, then they may balk at requests to maneuver on orbit. The ability to verify data is implicit to trust in that system. Of course, this is not so easy to implement. Currently, most states collecting SSA data do so for national security reasons, and importantly the three major collectors—the United States, China, and Russia—all maintain adversarial positions in relation to the others. Additionally, the data that are publicly available are incomplete at best. An open data structure will need to find a way to balance between openness and national security concerns.

#### In fact, SSA becomes divided---solving none of the second advantage.

Asha **Balakrishnan 18**, Ph.D. in mechanical engineering from the Massachusetts Institute of Technology, researcher at the IDA Science and Technology Policy Institute, et al., 2018, “Future of the Space Situational Awareness Enterprise - Global Trends,” https://amostech.com/TechnicalPapers/2018/SSA/Balakrishnan.pdf

There is trend towards functional modularization of the SSA system: it is becoming more segmented such that different actors and organizations can service each part (data collection, data processing and the creation of data products) of the system. This is a significant departure from the current SSA system, in which the DoD performs all three parts; now, organizations providing sensor data do not need to process it, and organizations processing data or fusing different sources of data together do not need to be the ones collecting. This trend—which enables organizations, particularly in the private sector, to operate independently and innovate new products or services—is already occurring, particularly in private firms in Europe or the United States. In many cases, investors are funding certain aspects of the system (e.g., data collection companies), and firms are offering products and services on a subset of system. Experience in other industries that grew out of government investment (e.g., computing) has also shown that entrance of the private sector is a precursor not only to falling cost and greater innovation, but also to growing democratization. However, the case studies indicate that globally SSA activities will likely remain dominated by national security-oriented organizations, even as they collaborate with their civil and commercial space counterparts, domestically and internationally; as a result, SSA will likely be slower to democratize than other sectors.

### SSA CP---Russia & China---2AC

#### Russia and China say no---everyone collects SSA data for national security and adversarial relations make integrating and trusting shared data difficult

P. J. **Blount 19**, Postdoctoral Researcher, University of Luxembourg; Adjunct Professor, LL.M. in Air and Space Law, University of Mississippi School of Law, Board of Directors, International Institute of Space Law, April 2019, "Space Traffic Management: Standardizing On-Orbit Behavior", <https://www.researchgate.net/publication/332115013_Space_Traffic_Management_Standardizing_On-Orbit_Behavior>

The first element of STM is data. In order to effectively manage space activities, it is essential to have information about what is in orbit, where it is at a given time, and who (if anyone) controls it. This information is known as Space Situational Awareness (SSA) data. Currently, SSA data are collected through a variety of systems and by a number of different actors, but the U.S. Space Situational Network (SSN) is the most comprehensive and accessible of these systems.7

The SSN system is a network of sensors that collect on-orbit data. It is managed by the Combined Space Operations Center (CSpOC), which is part of the U.S. military's Joint Force Space Component Command. The primary mission of the SSN system is to protect military space assets and assure military access to space. However, CSpOC has been statutorily authorized to share these data globally.8 This sharing is designed to protect national security by making available the most sensitive SSA data only to other U.S. government entities and allies. The most widely available data, on the other hand, only contain what is known as the Two-Line Element sets, which carry the most basic information on the location of an object in orbit, and are publicly available through Space-Track.org with the creation of a user account.9

While the SSN system is the most comprehensive source of SSA data, there are other states, notably Russia and China, that also collect SSA data. Some nonstate entities such as the Space Data Association (SDA) collect these data as well. SDA is an organization of satellite operators that share SSA data with each other. Notably, SDA has signed an agreement with CSpOC for bilateral sharing of data between the two. There is, however, no comprehensive data pool for SSA data, and much of the data is still considered sensitive and restricted.

Foundational to any proposed STM project are data, and the data must be standardized so that actors within the system can access them and contribute their own data. Further, data integrity must be maintained within the system to avoid mistakes. This means that a multilateral STM system will need to adopt data standards to integrate data from multiple sources and compile it into a single database. Since SSA data are currently collected by various entities using a variety of sensors, ensuring that the data are harmonized will be important. Additionally, STM will require an open data system so that data are public and verifiable. The need for openness is rooted in trust. STM will require some satellite operators to move their on-orbit assets in order to avoid conjunctions with other space objects. If the data underlying the decision-making process are unavailable to operators, then they may balk at requests to maneuver on orbit. The ability to verify data is implicit to trust in that system. Of course, this is not so easy to implement. Currently, most states collecting SSA data do so for national security reasons, and importantly the three major collectors—the United States, China, and Russia—all maintain adversarial positions in relation to the others. Additionally, the data that are publicly available are incomplete at best. An open data structure will need to find a way to balance between openness and national security concerns.

### SSA CP---Russia & China---Turn---2AC

#### SSA data gives China sufficient military intel to strike first

**Cox 18** [Lieutenant Colonel Timothy Cox is an Instructor at the Joint Forces Staff College, has previously served as the Chief of the Space Control Division at Headquarters Air Force, Commander, 318th Recruiting Squadron, Director of Operations for the 20th Space Control Squadron, Chief of the Commanders Action Group at Air Forces Central Command, and the Air Forces Central Command, Deputy Chief of Staff, “What Problem is a US Space Force Trying to Solve?,” Oct 24, 2018, https://othjournal.com/2018/10/24/what-problem-is-a-us-space-force-trying-to-solve/]

The first problem that demands a US Space Force is the reality that adversaries are, or are becoming, more capable of space warfare than the United States. One will often hear that the US dominates in space. This is objectively true if one is measures the number of platforms deployed or the ability to find, fix, and track space objects. Neither provide a meaningful combat edge to the US on orbit. More platforms mean more dependency and more targets. While being able to watch satellites is extremely useful, it cannot be determinative if the adversary has the same ability. The Combined Space Operations Center’s (CSPOC) catalog of virtually all orbital objects is the envy of everyone else vested in space, whether government or commercial. This space catalog, which draws data for predictive surveillance from sensors located around the globe, allows anyone with a calculator to predict the location of almost every object in orbit at a chosen time. The US has made the catalog publicly available and is working through the Department of Commerce to share even better quality data across a wider commercial spectrum in the interest of responsible space traffic management. While a thoroughly commendable and wise policy choice from a safety of flight perspective, such data sharing reduces much of the US’s orbital military advantage enabling potential adversaries to target satellites for intelligence gathering, interference or destruction. Simultaneously, those same adversaries have recognized that the US, is deeply committed to utilizing space as a crucial domain for military support and commercial activities (communications, environmental monitoring, Intelligence, Surveillance, and Reconnaissance (ISR), Precision Navigation, and Timing (PNT), etc.). However, the US is not well prepared to conduct operations to prevent an adversary from using anti-satellite capabilities to deny the advantages derived from the US’s space assets. This makes space a potential Achilles heel for the United States (or at very least a center of gravity); lots of capability on which there is a great dependency, but not a lot of ability to protect it. This vulnerability put the US at greater risk to attacks on space assets. It is unlikely an enemy would allow another to maintain such a comparative advantage when it can be so easily negated. The US does not need a Space Force to enable or launch more capabilities into space. The US needs a Space Force to protect the capability it already has on orbit.

#### Transparency flips PLA decision calculus – sudden decision to build relations based on honest and open communication with China makes the US look vulnerable and encourages strike against US space assets

**Stone 15** [Christopher Michael Stone, M.S. from Missouri State in Defense and Strategic Studies, “Reversing the Tao: A Framework for Credible Space Deterrence,” Fall 2015, *MSU Graduate Theses*, 1505]

How does the PLA organize their concept for space deterrence? First, according to PLA writings, the integration of space with other military forces is important in order to form the most effective military force possible. By having the strongest military force possible, says Chinese authors, can a nation deter other nations from attacking it. 144 This view has been seen in recent orders by President Xi Jinping for space to become integrated in all aspects of Chinese military operations. 145 Second is having a credible counterspace capability to threaten other nation’s space assets in order to deter the opponent from using its counterspace capabilities. “In this way, both sides would be reluctant to attack the others space assets lest they also come under attack.”146 In addition to having a credible counterspace capability for effective space deterrence, the Chinese advocate that they should reveal “firm resolve to dare to and prepare to use this capability” in order to create “certain psychological pressure on and fear in the adversary, and [force] the adversary to dare not conduct space operations with initiative.” 147 This includes conducting “limited space operational activities with warning and punishment as goals” as a means of de-escalation of the crisis.148 This view of forcedependent deterrence reads more like a traditional deterrent model than even the present DoD space deterrence framework that purposely avoids a credible threat of counteraction in the event of an attack on U.S. space assets. As PLA writers state, the goal of deterrence is to “choose appropriate deterrence means to display the horribleness, severity, and urgency of the consequences.”149 If a “period of tension” arises, Chinese writers state that it is vital to achieving strategic objectives terrestrially to “deliver destructive strikes to the enemy using maximum power in order to fight rapidly, conclude the operation rapidly and to withdraw from the confrontation.”150 As seen in the Chinese strategic culture that views the world and the international system in a holistic manner, the same holds true with their view of the many “zones” that the space domain covers with respect to space deterrence. “[It] covers vast areas (zones) from the cosmos at tens of thousands of kilometers from the Earth to the Earth’s surface, with many areas [zones] forming an organic whole…space military struggle…[is] a synthesis of many types of correlated military activity, including space to space, space to ground, and ground to ground.” 15 The Chinese do not “share the same interests” in the space domain or a view of enhancing the status quo of a U.S.-dominated international order. They are, according to many scholars, on a “quest for wealth and power.” 152 As one author stated, the Chinese are “no longer guided by Maoist proletariat ideology, [and] now see [space]…technology as a major factor in its rise as a world power as it seeks increased influence and independence. China’s pursuit of spacepower is a reflection of this emphasis on technology and its grand strategy to “regain the nation’s former status as a great power that controls its own fate.” 153 Despite the NSSS’ goal of preventing the development, testing, and deployment of space weapons systems, the Chinese possess the most rapidly maturing space program in the world and are using on-orbit and ground based assets to support China’s national economic, military and political goals and objectives.154 China has, according to a recent Pentagon report, “invested in advanced space capabilities, with particular emphasis on satellite communications, intelligence surveillance and reconnaissance (ISR), satellite navigation, and meteorology, as well as…a vast ground infrastructure supporting spacecraft and space launch vehicle manufacture, command and control, and data downlink.”155 In addition to this supporting infrastructure, the PLA “continues to develop a variety of capabilities designed to…prevent the use of space…by adversaries during a crisis or conflict including the development of directed-energy weapons and satellite jammers.”156 In addition, since the ASAT test in January 2007, the Chinese have continued to develop and test ground launched kinetic interceptors for space attack, with testing since 2007 being non-destructive. The 2015 DoD Report to Congress on Chinese Military Developments discusses several tests of Low Earth Orbit (LEO) capable interceptors as well as tests that appear to highlight a Geostationary Earth Orbit (GEO) capable interceptor capable of reaching at least 22,300 miles. These test programs indicate that while the DoD space deterrence framework speaks to the DoD’s stated deterrence and dissuasion of testing of counterspace weapons systems, China has not given any indication of ceasing these tests or of PLA development of doctrine for space warfighting because of the four element approach of DoD space deterrence. Why would this be? According to Chinese military authors, testing and development of space and counterspace technology is important for effective space deterrence: “Even in a relatively peaceful period, under circumstances where a hostile relationship is unclear, the presence and development of one side’s space systems and the boosting of its space capability, still can potentially influence and constrain the military activity of other nations and generate a certain deterrent effect.” 157 As mentioned earlier, some DoD analysts believe that transparency of military space activities is vital for preventing the use of outer space for military engagements of either reversible or destructive means. However, given the very different worldview and strategic culture of Chinese decision makers to the space domain and their historical and long term view of the international order, this foundational view of the DoD Space Deterrence framework has not improved the security of American assets in space. The Western mindset sees “transparency and openness as the surest way to peace” and believes that “when one state can effectively monitor another, fears of surprise attack are mitigated, and the tendency to overestimate a potential opponent’s capacities and intentions are minimized. With transparency, the security dilemma is obviated and cooperation is possible.”158 However, this is not the way the Chinese see transparency and openness. As one author correctly describes: To a [Chinese] strategist, letting an opponent know precisely one’s strengths and weaknesses merely invites attack. The key to stability in this view is uncertainty-- not knowing how strong or how weak an opponent is and never, under any circumstances, revealing one’s own strengths or weaknesses. The more sure the knowledge, the more crafty the countervailing plan, the more likely its success. 159 Why should we shun transparency, embrace adaptability and unpredictability in our spacepower strategic support planning? Xi Jinping sums this view up when he stated that: Boasting a vast land of 9.6 million sq km, a rich cultural heritage and a strong bond among the 1.3 billion Chinese people, we are resolved to go our own way…. We must not blindly copy the…models of other countries nor accept their dictation…As a Chinese saying goes, “Standing firm when assailed by rain and wind from all directions, our confidence is supported by our core values” 160 Given the long history of “humiliation” and weakness at the hands of Western “unequal treaties” and the establishment of the current UN system (created without the Chinese Communist Party’s involvement) transparency is not something that can be assumed with the Chinese government. It goes against the Chinese strategic culture of secrecy and deception in negotiation style as mentioned earlier and would create an impression of weakness domestically and internationally of the CCP. Due to this the CCP may view the sharing of such information as detrimental to their survival as the keepers of the strategic culture, governance and the PLA’s power and not a mutually beneficial path toward preservation of a Western dominated status quo. If capabilities are shared with the potential “enemy” it would be to “selectively...reveal China’s space technology and space capability, and adopt an oppositional mode to reduce their expectations for space weaponization and to increase their degree of difficulty and costs in space weaponization.”161 During peacetime however, PLA strategic guidance on deterrence recommends a combination of hiding one’s capabilities and keeping a low profile with active actions for war preparations such as testing and escalation control to include low-intensity warfare “until our deterrence goal is realized.”162 This highlights the value of avoiding transparency as part of a long term stratagem ignoring the ineffective American course of action of transparency as part of the NSSS deterrence concept. Instead, the United States should utilize uncertainty like the Chinese, given uncertainty enables friction that can create foundational strategic impediments for the adversary. The current strategic situation in space and on Earth, due to American and allied inaction, enables the Chinese to gather information and offensive capabilities needed to shape the strategic environment to the PLA advantage while giving the U.S. leadership the perception that the United States is winning when in fact they are losing to complex Chinese deterrence activities imposing friction on US and allied space operations and terrestrial strategy. 163 Clausewitz describes this phenomenon well when he stated: Friction (which includes the intersection of many factors, such as uncertainty, psychological/moral forces and effects, etc.) impedes activity. Friction is the only concept that more or less corresponds to the factors that distinguish real war from war on paper.164 A more recent strategic theorist, Colonel John Boyd, USAF, stated: Operate inside adversary’s observation-orientation-decision-action loops to enmesh adversary in a world of uncertainty, doubt, mistrust, confusion, disorder, fear, panic chaos …and/or fold adversary back inside himself so that he cannot cope with events/efforts as they unfold. 165 Why would these two strategic thinkers focus on friction and uncertainty? Because the atmosphere of war is friction, friction is generated and magnified by menace, ambiguity, deception, rapidity, uncertainty, mistrust, etc. These are the actions that the Chinese are engaged in space and in their increasingly belligerent and expansionist activities in the Asia Pacific region. This friction in the strategic sense, is the opposite and de-stabilizing side of the strategic Tao, with harmony/initiative generated by “rapidity and variety” leading to strategic success for China using the Observation, Orient, Decision, Action loop or also known as the Decision Calculus Loop.166 As Sun Tzu was cited as saying, “Those who use arms well, cultivate the Way (Tao)…”167 Orientation, seen as a result, represents what Boyd referred to as “images, views or impressions of the world shaped by genetic heritage, cultural tradition, previous experiences, and unfolding circumstances.”168 In other words, Boyd is defining what is called strategic culture today and is defined by Kartchner as “that set of shared beliefs, assumptions, and modes of behavior, derived from common experiences and accepted narratives (both oral and written), that shape collective identity and relationships to other groups, and which determine appropriate ends and means for achieving security objectives.”169 Once the DoD strategists and policymakers grasp these important aspects of strategic context, understanding that the Chinese are doing the same thing as part of their analysis, they can take that information and orient the nation’s strategic posture based on the patterns discerned relating to adversary activities and at the same time denying our adversary the possibility of discerning patterns that match our activity as part of our strategy execution.170 A few examples of Chinese strategic patterns of behavior include their use of force within crisis situations over time. For example, surprise is a very important pattern of force projection within the PLA. In October 1962, China conducted operations against India due to territorial disputes. The Chinese launched major, rapid attacks, which succeeded immediately. After a short pause, “the Chinese renewed their attacks in midNovember” using the doctrines of the classic Chinese strategist, Sun Tzu. These include: “all warfare is based on deception….therefore, when capable, feign incapacity; when active, inactivity….Pretend inferiority and encourage [adversary] arrogance…Attack where he is unprepared; sally out when he does not expect you….These are the strategist’s key to victory. It is not possible to discuss them beforehand.”171 Thus in order to be victorious, it is not beneficial to achieve strategic success through TCBMs; rather surprise attacks and deception are key to strategic victory. Secondly, another pattern is achievement of psychological and political shock. While some commentators such as Michael Krepon may believe that Chinese offensive deterrence strikes are “unlikely,” this highlights the lack of real observational understanding of the strategic culture and doctrines of the PLA.172 Psychological or political shock of a pre-emptive strike may be the payoff that the PLA is looking for rather than simply trying to gain a complete military advantage over U.S. capabilities. As a result, a rapid, destructive, limited attack with kinetic energy anti-satellites (KE ASATs) could create conditions that lead the United States or its allies to “become disheartened and defeatist as a result of the unexpected reverse he has suffered and may be induced to reduce his war aims” or perhaps change U.S. policy objectives in the Pacific to the Chinese advantage.173 What is more, is that achieving such a psychologicalpolitical shock is magnified in the case of a military force that has limited forceprojection and sustainment capabilities, such as the current posture of the DoD space forces that only contains reversible means of counterspace operations. An example of psychological shock leading to policy changes for an adversary is again found in the 1962 India campaign where the PLA adopted a punishment strategy that undercut Indian self-confidence174. By doing so, “the Chinese achieved a more rapid and decisive change in policy than would likely have emerged from a long-drawn-out negotiation in which the Chinese tried to trade the captured territory for an Indian recognition of Chinese ownership of the territories they held before the border war began.”175 Some may argue that a Chinese attack on U.S. or allied space systems is unlikely because the [military] benefits would not outweigh the costs. However, a counterargument can be made that DoD strategists and policymakers lack sufficient understanding of the strategic culture needed to properly orient the American space posture to be prepared to decide and act when necessary to protect space systems. In addition, it is important to note that China has even used force not only to settle a crisis such as that with India, but also have “typically used force to create a crisis.”176 Understanding this unique strategic orientation of the PLA forces is vital to understand the strategic reality as it is, and not as some would like it to be, to ensure American strategic interests and homeland are properly secured in space and terrestrially. The view of having space weapons as a means of CCP survival and territorial integrity through robust military power is key to understanding the linkage that Chinese military writers have of spacepower with nuclear weapons as well. The Chinese view the nexus of spacepower and nuclear weapons not as separate domains of operations, but rather as “an integrated-whole composite strength for strategic deterrence.” 177 As one PLA author stated: The party that enjoys superiority in space will secure its survival by weakening the enemy’s nuclear deterrent capabilities, thereby increasing tremendously one’s nuclear deterrent power. Space forces constitute both a space shield and a space sword.178 This quote highlights another disturbing yet important reality for American strategic planners to grasp: the development of space attack systems and a credible deterrent threat against U.S. systems also include the attacking of nuclear command and control space support segments. As the same PLA author describes this in further detail: “Commanders should actively take the initiative to strike at an enemy’s vital targets because “only through active offensive operations and counter-attacks can one seize and maintain the initiative. Specifically, vital targets include information, command and support systems. Hitting these vital targets through concentrated strikes is especially recommended in cases where the PLA faces a “powerful enemy equipped with high technology weapons and equipment” rather than conduct wars of annihilation…the first targets of a campaign…are the detection, command and telecommunications information systems, whose degradation or destruction will negate or reduce the enemy’s ability to control information and create conditions for later combat.” 179 Chinese military strategists recommend attacking these key information and command and control nodes because PLA analysts assess that space-based information “…will become a deciding factor in future wars, that space will be the dominant battlefield, and that in order to achieve victory on Earth and preserve sovereignty control of Chinese territory and expanding core interests, the PLA must first seize the initiative in space. This will require China to achieve space supremacy, defined as the ability to freely use space and to deny the use of space to adversaries.” 180 Moreover, “the assessment that space is the dominant battlefield [emphasis added] has led PLA analysts to conclude that war in space is inevitable.” 181

### SSA CP---Russia & China---Say No

#### China says no.

Kentaro Tanaka 17. M.A. in International Science and Technology Policy, Space Policy Institute, Elliott School of International Affairs, George Washington University, “Applicability of remote sensing policies to space situational awareness,” *Space Policy*, Volume 42, November 17)

While the United States has been seeking to develop a US-centric SSA sharing plan internationally, it seems some countries, particularly Russia and China, would rather seek to build and expand their own SSA networks. Russia holds the second-most advanced SSA capabilities in the world. Just like the United States, the Russian Space Surveillance Systems (RSSS) was built as missile warning systems in the 1960s [21]. Thus, many radar systems were deployed along the periphery of the Soviet Union territory, some of which are now outside of Russian territory, such as Kazakhstan, Tajikistan, Azerbaijan, and Belarus [22]. Even after the collapse of the Soviet Union, Russia holds control over the radar networks by making a series of bilateral agreements with those countries [23]. Additionally, the Keldysh Institute of Applied Mathematics (KIAM), a part of the Russian Academy of Science, take the initiative in coordinating the International Scientific Optical Network (ISON). With 37 observation facilities in 15 countries, and 79 telescopes, ISON covers geostationary (GEO) belt as well as geostationary transfer orbit (GTO), highly elliptical orbit (HEO), and low-earth orbit (LEO) [24]. While the United States seeks to share SSA information bilaterally, Russia is proposing a centralized approach with the UN as the center. At the fifty-ninth session of the COPUOS in June 2016, Russia submitted its working paper on establishing a UN platform that is designed to collect the SSA information, maintain a database, and share the data internationally [25]. In addition to Russia, China has already developed and utilized a wide range of space applications. Although China has published little information on its SSA capabilities, considering the current space capabilities China has built, it is reasonable to assume that China has developed a considerable degree of SSA capabilities today. One study shows that China may have six ground stations within its territory, one in Pakistan, and one in Namibia [21, p. 8]. China also operates space surveillance tracking ships, although they are primarily to support its human space flights [23]. As China continues to build its space capabilities further, its reliance on space systems will also increase. Therefore, China will make more earnest efforts to expand its SSA networks globally. However, the outlook on building SSA information sharing between China and the United States is unclear. Unlike other US allies, the space cooperation between United States and China has been limited, particularly after Congress decided to restrict NASA's official activities with China in 2011 [26]. In fact, it is said that China is starting to expand its SSA network by partnering with some other Asia-Pacific Space Cooperation Organization (APSCO) member countries: Iran, Pakistan, and Peru [27].

#### China says no – it’s a low priority.

Michael J. Listner 12. Attorney and analyst and consults on matters relating to space law and policy. He serves as General Counsel for Space Safety Magazine and is a contributor to that publication. “Geopolitical Challenges to Implementing the Code of Conduct for Outer Space Activities” <https://www.e-ir.info/2012/06/26/geopolitical-challenges-to-implementing-the-code-of-conduct-for-outer-space-activities/>

China’s reluctance to participate in and support the negotiations for the Code of Conduct may also be due to the fact the Code of Conduct would implicate China’s national space policies. China does not have a specifically focused space policy such as the United States, but it has articulated a space policy of sorts in a public white paper released March 2011. [5] The policies within this white paper do not reach the specificity and transparency that the Code of Conduct would encourage. If China became a party to the Code of Conduct or otherwise participated in its negotiation, it would find itself in the position of releasing more internal details about its domestic space policies. This may prove unacceptable to the Chinese government and further hinders China’s participation in the Code of Conduct. Another concern for China has to do with the topic of space debris. Space debris mitigation was a cornerstone of the original Code of Conduct and figures even more prominently in the new effort. China has indicated in the past that space debris is a low national priority and therefore agreeing to abide by and exhibit the behavior encouraged by the Code of Conduct would seem to run contrary to current Chinese interests in regards to space debris mitigation.

#### Even if they say yes, SSA cooperation eventually fails – low trust and short term thinking.

Nancy Gallagher 10. Center for International and Security Studies at Maryland, May, “Space Governance and International Cooperation ,” Astropolitics, 8.2 Taylor and Francis

If proponents of greater space cooperation truly believe that collective action problems like debris mitigation are the most important reason for cooperation, and if they are satisfied with the rate of progress on improving launch, operation, and disposal practices that has occurred over the past fifteen years, then continuing to frame the case for cooperation in these terms is a fine strategic choice. But if they believe that progress towards sustainability in managing space as a global commons has been inadequate, then they need to reconsider the preference for informal self-regulation over more formal and fully developed regulatory arrangements. And if they were hoping to use major successes in relatively uncontroversial types of technical space coordination as a way to build momentum for more significant cooperation on politically difficult space security issues, then they should think about how those larger, more politically sensitive issues are impeding low-priority technical coordination. Strategic sensitivities impede cooperation because many people whose decisions affect space, especially from U.S. and foreign defense policy communities, resist doing what would make sense for the long-term sustainable management of space as a global commons because they do not think about space in the same way that environmentalists, international lawyers, or collective action theorists do. People who believe that access to and use of space can be controlled for strategic gains relative to potential competitors sometimes invoke the “space as a global commons” phrase as a way to assert their own right to use space without interference from others without acknowledging that other users have similar rights, and that all rights in space confer corresponding responsibilities. An extreme form of this view argues that the United States should become a space hegemon to police the shared environment, protect peaceful uses, and prevent anyone else from accessing or using space for hostile purposes.21 Less extreme forms of adversarial thinking also impede functional cooperation by limiting willingness to share space surveillance information and restricting exports of technologies that could help with debris mitigation, space traffic management, and the optimization of scarce resources. The more such adversarial logic dominates decisions about space, the less likely U.S. or foreign decision-makers will be to forego short-term gains and future flexibility in order to protect space from environmental degradation and to avoid social disapproval.

#### SSA cooperation doesn’t spillover into a better, honest relationship.

Clark 14 Colin Clark, writer for Breaking Defense China Reaches Out To US For Space Data: Air Force Space Commander on December 08, 2014 at 11:41 AM https://breakingdefense.com/2014/12/china-reaches-out-to-us-for-space-data-air-force-space-commander/

Of course, getting the PRC’s Ministry of Foreign Affairs to get the People’s Liberation Army to do something doesn’t always happen quickly — if at all. Observers of the fallout after the Chinese anti-satellite test will remember that Foreign Affairs appeared absolutely clueless about the test, both publicly and privately. And that anti-satellite test, ironically, was responsible for an enormous increase in the amount of space debris that may cause a collision. That the United States will play the responsible global citizen and provide conjunction data to the Chinese after the test only deepens the irony. Of course, for the Chinese it’s a win as the US catalogue and tracking of orbital data is considered the best there is and they are getting direct access to it should any of their satellites be threatened. But this also provides proof to the Chinese that playing by international rules and norms can provide tangible benefits, which surely played a key role in the sharing being approved. Several attendees at the space breakfast said the Chinese request marked an important step forward in US-Chinese military-to-military relations and welcomed it. One of the foremost US authorities on the Chinese military’s space efforts says in an email that the Chinese move demonstrates “first and foremost, that in the Chinese system the Ministry of Foreign Affairs is NOT a powerful entity. This is reflected in the basic reality that the Foreign Minister has not been a member of the Politburo since the days of Qian Qichen, in the late 1990s.” He believes that the PLA “is most likely acting, in the first place, to remove an unnecessary link in the chain of information, especially important since conjunction data is perishable. “Given China’s steadily improving space situational awareness system, my own guess is that they are accessing this data, first, to minimize the chances of a conjunction. There have been some interesting stories in the Chinese press about moving satellites to avoid collisions. It is unclear what data has been used to make that determination, whether it is primarily home-grown, from the US, from third parties, or a combination. Second, it may be to double-check their own data: What are the Americans seeing that we are not? This may be partly a matter of resolution, and partly a possible source of intelligence. There was a brouhaha a few years back where we were reporting in our space catalogs European satellites that the Europeans denied existed.” So what does America get out of this? “For the United States,” Cheng writes, “ideally this would be an opportunity for us to gain insight into what organizations play a role in China’s space situational awareness organization. Who gets this data (almost certainly the General Armaments Department)? Who else outside the military gets this data? How does it get incorporated into China’s SSA system? In particular, does the China National Space Administration (CNSA) get this data, and at what point? (I doubt the information is going from us to CNSA).” In the end, Cheng assesses this is not the beginning of a fundamental change to US-Chinese military to military relations. “What WON’T change is that Chinese space (and military, but I repeat myself) officials will NOT engage in direct, US-PRC communications. Certainly not in a crisis, and probably only minimally in peacetime, even with this new connection.”

## Inducements

### Inducements CP---2AC

#### Inducements fail.

Jon B. Alterman 3/21 (Jon B. Alterman holds the Zbigniew Brzezinski Chair in Global Security and Geostrategy, and is director of the Middle East Program at CSIS, 3/21/22, accessed 3/24/22, “U.S. Power and Influence in the Middle East: Part Three”, https://www.csis.org/analysis/us-power-and-influence-middle-east-part-three)

Jon Alterman: The United States’ experience with its economic toolkit in the Middle East hasn’t always led to the changes that the United States intended. Sanctions have had some impact, but most targets have been able to adjust to them—and even profit from them—undermining their long-term effectiveness. The number of times governments have rethought their core interests because of sanctions is low. In addition, sanctions tend to give repressive governments even more control over their economies, potentially strengthening them against internal challenges. Positive inducements haven’t been markedly more successful. They’ve generally been less effective than hoped in creating a virtuous circle of reforms that bring governments closer to the United States. When there has been success, it’s often hard to measure—and hard to demonstrate to publics in the Middle East.

#### Inducements can’t solve interoperability

Kunertova ’20 [Dominika; April 24; postdoctoral research fellow at the Center for War Studies in Denmark, with a Ph.D. in Political Science from Université de Montréal, she researches trans-Atlantic security and defense cooperation, NATO-EU relations, and military technology; War on the Rocks, “CAN THE NEW ‘MAGI’ SAVE NATO?,” https://warontherocks.com/2020/04/can-the-new-magi-save-nato]

You Can’t Buy Interoperability

In contrast to statistical engineering that aims to adjust numbers to fit the desired “fair share,” true burden-sharing would put emphasis on defense capabilities and operational readiness. Shifting the emphasis away from abstract macroeconomic numbers to practical cooperation based on strategic needs should inform the content (which capabilities to buy), not only the form (defense spending levels), of burden-sharing debates. This highlights the problem that allies cannot just buy interoperability, as it requires enhanced cooperation and coordination. Although interoperability is considered the alliance’s core business, it has not been systematically treated in the burden-sharing debate. In addition, burden-sharing that includes the mutual-aid dimension would further refine the cash, capabilities, contributions — or “three C’s” — framework regularly mentioned by the current NATO secretary-general.

The current defense spending narrative is thus a symptom of empty formalism in NATO that reflects a lack of clarity about the alliance’s purpose, and favors statistical deceptions over effectively implementing the mutual commitment to defend each other. A February 2020 poll by the Pew Research Center revealed a worrying trend: While NATO is generally seen in a positive light across publics within the alliance (a median of 53 percent view NATO positively, though with double-digit percentage point declines in Germany and France over the past 10 years), many in 16 surveyed NATO countries seem reluctant to fulfill Article V collective defense obligations. A median of 50 percent across 16 NATO member countries is against their country defending an ally, while only 38 percent express willingness to come to help a fellow ally.

Future Defense Spending in Peril right, especially in the context of the short- and long-term consequences of the ongoing COVID-19 pandemic. While the scope of the economic impact is still unclear, it is likely to reshuffle financial priorities in NATO countries. Defense ministries will find it more difficult to reach the 2 percent spending level by 2024 or even to maintain the current defense expenditures programs. Moreover, with economies put to halt and eventual drops in national GDP, even if countries fulfill the 2 percent pledge, they could end up spending less in real terms. If NATO members continue to frame fairness in terms of the 2 percent defense spending target, it will further aggravate the burden-sharing problem, seriously test NATO solidarity, and ultimately endanger the alliance’s ability to adapt to the increasingly unpredictable security environment and the changing nature of security threats.

Improving NATO’s cohesion and its political role will not happen overnight or through high-level political declarations. If there are any lessons to be learned from the Three Wise Men’s effort back in 1956, it is that perseverance, personal relationships and reputation, pragmatism, and humility matter a great deal.

to describe cyber “attack,” “information operations,” and attribution findings with different implicit assumptions or implications.

#### It’s only a question of integrating existing, transatlantic satellites.

AT: Build Satellites CP

Stephen Ganote et al. 19 (Stephen Ganote is a Managing Director at Avascent where he serves clients in space communications and select defense tech markets and leads its commercial space practices, Janie Yurechko is a Strategic Development Specialist at Ball Aerospace and a MBA Candidate at Georgetown University, Diana Jack is a manager in Avascent's Space practice where she provides strategic guidance to major primes, New Space companies, and governments, Connor O’Shea is President and Co-Founder at Westgen Technologies Inc, a remote power generation and methane reduction technology company, 9-30-19, accessed on 6-19-2022, Atlantic Council Scowcroft Center for Strategy and Security, “Reenergizing Transatlantic Space Cooperation”, <https://issuu.com/atlanticcouncil/docs/reenergizing_transatlantic_space_cooperation>, HBisevac)

This congestion is increasingly causing harm: an Iridium satellite was destroyed by a collision with a defunct Russian satellite in 2016; Capella Space recently reported that one of its satellites narrowly avoided a catastrophic collision with a piece of space debris; and as noted above, debris from a 2019 Indian ASAT test now threatens the International Space Station. 21 Debris interference has even been suspected in the 2019 failure of Intelsat 29e.22 In addition to growing competition for physical space, more satellites are competing for finite (and crowded) radio-frequency spectrum. Space stakeholders express growing concern about coordinating transmissions from many thousands of new satellites reliant on similar or overlapping frequency bands, as to avoid jamming signals and degrading capabilities.23 The advent of 5G is further complicating this issue. This coordination is no trivial matter; the Department of Defense, the most sophisticated and well-resourced space actor in the world, inadvertently jams its own satellites dozens of times a month.24

## New Alliance

### New Alliance CP---2AC

#### Working within existing institutions are key---otherwise, allies would say no---if not, disputes would delay and prevent collective action.

James Moltz 11. Chairman of the Department of National Security Affairs at the Naval Postgraduate School, where he also holds a joint faculty appointment in the Space Systems Academic Group. “Coalition Building in Space: Where Networks are Power.” Navy Postgraduate School. 2011. https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf //EM

These conditions create fundamental incentives for collective action that do not exist in other areas of international relations. Ironically, one of the primary obstacles to enhanced collective action to protect space security may be the thinking of the actors themselves, which still remains largely rooted in the unilateral traditions of security provision from past security frameworks. But, as Robert Keohane argues, "To pursue self-interest does not require maximizing freedom of action.

On the contrary, intelligent and farsighted leaders understand that attainment of their objectives may depend on their commitment to institutions that make cooperation possible."13 Working with allies, therefore, may represent the best security solution available at this point in space history, and perhaps may serve as a bridge to broader forms of international cooperation in the future. Alliance-based efforts could mitigate a variety of emerging space-related security concerns. The prior existence of allied military institutions- particularly established patterns of cost-sharing, integration, joint operations, and joint training-both in the case of NATO and in various bilateral arrangements with Asian countries (such as Australia, Japan, and South Korea) should reduce typical collective action problems in forming such new mechanisms for space.

## Agent---DoS

### DoS CP---Background

#### Only the DoD can do the AFF---even if the DoS can do some stuff in space, DoD is key to the AFF.

Georgetown Law, 20 (Georgetown University Law, 10-8-2020, accessed on 6-24-2022, “Other U.S. Government Agencies Involved in Space Policy & Regulation”, <https://guides.ll.georgetown.edu/c.php?g=1037047&p=7762102>, HBisevac)

U.S. Department of Defense

The Defense Department coordinates U.S. national security policy and overseas all branches of the U.S. armed forces.

Assistant Secretary of Defense for Homeland Defense and Global Security

The ASD is responsible for formulating national security strategy for outer space, among other matters.

U.S. Space Force

The newest branch of the U.S. armed forces was established on December 19, 2019, with the signing of the U.S. Space Forces Act, part of the Defense Authorization Act of 2020. It is organized as a military service branch within the Department of the Air Force and is directed by the Chief of Space Operations.

### DoS CP---2AC

#### Military exercises are essential towards integrated space capabilities.

Paul A. Tombarge 14. Bachelor of Arts degree in Political Science from the University of Minnesota, a Master of Arts degree in Public Administration from the University of Maryland-Europe, a Master of Arts degree in International Security Studies from the Naval Postgraduate School, and a Graduate Certificate in Space Systems from the Naval Postgraduate School. He was also a U.S. Senior Fellow at the George C. Marshall European Center for Security Studies from 2013-2014. “NATO Space Operations.” George C. Marshall: Euopean for Security Studies from 2013-2014. 12-2014. https://www.marshallcenter.org/en/publications/occasional-papers/nato-space-operations-0 //EM

Exercises

With the upcoming end of the International Security Assistance Force’s (ISAF) mission in Afghanistan, NATO is expected to shift its emphasis from operational engagement to operational preparedness through its CFI. CFI is intended to build on the Alliance’s recent experience in Afghanistan and ensure the Allies can work even more effectively together in the future.102 A key pillar of this initiative is increased exercises as “an essential means for forces to practice tactics, techniques and procedures, promote and gauge interoperability, validate training and, when required, certify headquarters, units and formations.”103

In order to ensure the Alliance is able to fully exploit space capabilities, space operations should be incorporated into a variety of tactical, operational, and strategic level exercises and war games. At the tactical level, this could include such things as a multi-national RED FLAG exercise. RED FLAG is a realistic combat training exercise involving the air forces of the United States and its allies. Conducted on the vast bombing and gunnery ranges of the Nevada Test and Training Range, RED FLAG was established in 1975 to maximize the combat readiness, capability and survivability of participating units by providing realistic training in a combined air, ground, space and electronic threat environment as well as a free exchange of ideas between forces.104 Participating units execute missions against an opposing “Aggressor” force specially trained to replicate the tactics and techniques of potential adversaries. While Red Flag originally developed a flyer's combat proficiency, the last eight years have slowly incorporated space and cyberspace capabilities.105 Previously segregated from the CAF participants, space and cyber operators are now fully integrated at the tactical level as a primary training audience.

At the operational level, NATO could participate in a BLUE FLAG exercise. BLUE FLAG is an U.S. Air Force “Air Combat Command-sponsored exercise program that provides doctrinally-correct air, space, and cyberspace crisis action planning (CAP) and command and control (C2) training for joint/coalition air components and operational-level headquarters at the operational level of war.”106 Just as RED FLAG is intended to increase the combat survivability of tactical forces, the goal of BLUE FLAG is to train commanders and staff officers at the operational level of war so “they can immediately participate in directing an air war and make smart decisions during the critical first days of an engagement.”107

#### Military-to-military interactions are key to redundancy AND signal.

James Moltz 11. Chairman of the Department of National Security Affairs at the Naval Postgraduate School, where he also holds a joint faculty appointment in the Space Systems Academic Group. “Coalition Building in Space: Where Networks are Power.” Navy Postgraduate School. 2011. https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf //EM

Notably, one option that has not been examined seriously enough in the current space debate is a possible middle-ground alternative for reducing spacecraft vulnerability: that of creating an allied space "network." Specifically, linking space capabilities first among formal U.S. military allies and then perhaps with other friendly nations could greatly reduce (if not eliminate) the risks of single-point failures to important space systems and create a new form of space deterrence by raising the stakes for adversaries considering launching attacks on space assets. That is, by spreading capabilities among allies in space through the creation of inter-operable, redundant networks of satellites, including in the military sector, space-based partnerships could reduce costs, lessen vulnerability, and raise the challenges facing would-be attackers, thus obviating the need for expensive and destabilizing space-based weapons. This could provide considerable benefits in terms of U.S. and allied space security and improve chances for developing norms of peaceful international behavior.

#### DoD classification destroys the ability of the DoS to do anything---hindering an integrated alliance.

Sean Carberry 22. Managing Editor at National Defense. “Over-Classification, Lack of Standards Stymies Allied Space Forces.” National Defense. 6-24-2022. https://www.nationaldefensemagazine.org/articles/2022/6/24/over-classification-lack-of-standards-stymies-allied-space-forces //EM

Being integrated with allies means more than processes and training, Gardiner added. It means recognizing the space community is small, and Australia has limited resources. “[That] enables us then to understand where those gaps are and where can we actually be putting our national treasure towards so that we’re meaningfully contributing to where it’s needed.”

There are several related barriers to integrating space capabilities. Allies do not communicate enough about capabilities and gaps to ensure they are not duplicating efforts or leaving gaps that a nation might have the resources to fill — something that Gardiner said could amount to “fratricide.” One of the major reasons that communication doesn’t take place is over-classification, leaders said.

“I’ve never come up against as much classification as I have in the space domain,” said Godfrey.

“Unfortunately, it doesn’t make it easy to understand if I’m looking to develop a capability that I’ve just classified, how can I then have the conversation with my colleagues here to understand whether they’re already developing that capability, and if I actually need to go and spend money somewhere else because they’ve got it,” he added.

“I think one of the challenges that we’re working each and every day … is how do we get to a more comprehensive sharing amongst allies and partners,” said Dickinson. “How do we declassify, reclassify documents and materials so that we’re able to share?”

#### Fiat causes Chinese first strike.

**Cox 18** [Lieutenant Colonel Timothy Cox is an Instructor at the Joint Forces Staff College, has previously served as the Chief of the Space Control Division at Headquarters Air Force, Commander, 318th Recruiting Squadron, Director of Operations for the 20th Space Control Squadron, Chief of the Commanders Action Group at Air Forces Central Command, and the Air Forces Central Command, Deputy Chief of Staff, “What Problem is a US Space Force Trying to Solve?,” Oct 24, 2018, https://othjournal.com/2018/10/24/what-problem-is-a-us-space-force-trying-to-solve/]

The first problem that demands a US Space Force is the reality that adversaries are, or are becoming, more capable of space warfare than the United States. One will often hear that the US dominates in space. This is objectively true if one is measures the number of platforms deployed or the ability to find, fix, and track space objects. Neither provide a meaningful combat edge to the US on orbit. More platforms mean more dependency and more targets. While being able to watch satellites is extremely useful, it cannot be determinative if the adversary has the same ability. The Combined Space Operations Center’s (CSPOC) catalog of virtually all orbital objects is the envy of everyone else vested in space, whether government or commercial. This space catalog, which draws data for predictive surveillance from sensors located around the globe, allows anyone with a calculator to predict the location of almost every object in orbit at a chosen time. The US has made the catalog publicly available and is working through the Department of Commerce to share even better quality data across a wider commercial spectrum in the interest of responsible space traffic management. While a thoroughly commendable and wise policy choice from a safety of flight perspective, such data sharing reduces much of the US’s orbital military advantage enabling potential adversaries to target satellites for intelligence gathering, interference or destruction. Simultaneously, those same adversaries have recognized that the US, is deeply committed to utilizing space as a crucial domain for military support and commercial activities (communications, environmental monitoring, Intelligence, Surveillance, and Reconnaissance (ISR), Precision Navigation, and Timing (PNT), etc.). However, the US is not well prepared to conduct operations to prevent an adversary from using anti-satellite capabilities to deny the advantages derived from the US’s space assets. This makes space a potential Achilles heel for the United States (or at very least a center of gravity); lots of capability on which there is a great dependency, but not a lot of ability to protect it. This vulnerability put the US at greater risk to attacks on space assets. It is unlikely an enemy would allow another to maintain such a comparative advantage when it can be so easily negated. The US does not need a Space Force to enable or launch more capabilities into space. The US needs a Space Force to protect the capability it already has on orbit.

#### Shared-military satellites are key to redundancy AND signal.

James Moltz 11. Chairman of the Department of National Security Affairs at the Naval Postgraduate School, where he also holds a joint faculty appointment in the Space Systems Academic Group. “Coalition Building in Space: Where Networks are Power.” Navy Postgraduate School. 2011. https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf //EM

Notably, one option that has not been examined seriously enough in the current space debate is a possible middle-ground alternative for reducing spacecraft vulnerability: that of creating an allied space "network." Specifically, linking space capabilities first among formal U.S. military allies and then perhaps with other friendly nations could greatly reduce (if not eliminate) the risks of single-point failures to important space systems and create a new form of space deterrence by raising the stakes for adversaries considering launching attacks on space assets. That is, by spreading capabilities among allies in space through the creation of inter-operable, redundant networks of satellites, including in the military sector, space-based partnerships could reduce costs, lessen vulnerability, and raise the challenges facing would-be attackers, thus obviating the need for expensive and destabilizing space-based weapons. This could provide considerable benefits in terms of U.S. and allied space security and improve chances for developing norms of peaceful international behavior.

## European Union

### EU CP---Deficit---Top Level

If they cooperate with China and Russia, insert ‘say no’ answers.

The following are EU-intrinsic answers.

### EU CP---Deficit---Entanglement---2AC

#### Shared threat understanding with NATO is key to avoid accidental escalation AND solving debris.

Sam Wilson & Colleen Stover 21. Senior policy analyst for the Center for Space Policy and Strategy at The Aerospace Corporation; Project manager and researcher at The Aerospace Corporation’s Center for Space Policy and Strategy. “Defense Space Partnerships: A Strategic Priority.” Aerospace Center for Space Policy and Strategy. 09-17-2020. https://csps.aerospace.org/papers/defense-space-partnerships-strategic-priority //EM

Coalesce Allied and Partner Thinking on Space Security Concepts.

As part of defense space partnerships, allies can more thoroughly discuss the threats to space systems and potential space conflict scenarios. If the United States wants to fully leverage its allies and partners in any future conflict in space, the United States would benefit from having more discussions with its allies about the possibility and nature of such a conflict: how it might emerge, how the respective allies can contribute, the capabilities the allies should pursue in advance, and the actions that might constitute “red lines” or cross thresholds that are more severe than others.

In recent years, the United States has taken important steps to collaborate with allies and partners on space threats and space conflict. International partners participate in military space exercises such as Space Flag, Global Sentinel, and the Schriever Wargame.22 The Five Eyes (the United States plus Australia, Canada, New Zealand, and the United Kingdom) along with France and Germany all are members of the Combined Space Operations initiative. 23 Experts we spoke to told us that the United States should continue and expand these efforts. Partner preparation for space conflicts could be valuable from an operational and geopolitical perspective. Todd Harrison, Director of the Aerospace Security Project at the Center for Strategic & International Studies, stated the following:

Rotating allies in the [Combined Space Operations Center as part of the Combined Space Operations initiative] is important because it gives those countries experts on space security issues. Let’s say Russia or China start interfering with our nuclear command and control and early warning satellites. Any allied country needs to have their own experts so they understand our response—they need folks who can say, “Yes, I understand why the Americans are escalating over this.”24

In a conflict in space, even if an allied country does not have significant defense space capabilities, it should have an understanding why the United States or other allied countries are taking the actions that they are. That understanding might help that country support the United States and allies politically and militarily in other domains.

The United States and its allies having a shared understanding of space threats and space conflict will help in peacetime too. General John Raymond, the Chief of Space Operations, has prioritized developing norms for operating in space.25 These could include something like taking steps to not create debris and announcing planned maneuvers into other orbits.26 With a similar understanding of the issues, the United States and its allies will be better equipped to develop common ideas for responsible behavior in space. This will also help with multilateral discussions, such as United Nations (UN) proposals on space security. Our partners have not always supported U.S. positions on UN space security proposals, including our negation of proposals made by Russia and China. For example, in the 2014 UN vote on Russia’s proposed draft resolution on No First Placement of Weapons in Outer Space, only three countries voted with the United States against the resolution and 125 voted for it with Russia.27 New and deeper partnerships will create more commonality in assumptions and objectives for fostering a safe and secure space environment.

#### Specifically, NATO collective defense results in overreactions.

Ethan Williamson, 19 (Ethan Williamson, Federal Contractor with GridIron IT as a Cyber Task Order Analyst at the Joint Service Provider, 5-13-2019, accessed on 5-29-2022, Charged Affairs, “NATO’s Expanding Role in Cybersecurity”, <https://chargedaffairs.org/natos-expanding-role-in-cybersecurity/>, HBisevac)

Through these organizations and agreements, NATO has improved and strengthened its unified cyber defense capability, seemingly positioning itself to be a standard bearer for cybersecurity. However, these commitments lack specifics and could hamper NATO’s ability to respond to an attack because of bureaucratic and security protocols. Following the inclusion of cyber attacks under Article 5, NATO and its allies could not agree on what kind of attack would trigger the collective defense response. Allies still use their own incident standards to define cyber incidents and in some cases do not make these standards public. This results in an uneven response and makes it difficult for NATO and its allies to provide a unified, Article 5 response to cyber incidents. Stoltenberg has defended this vague definition by stating that, “a clearly defined threshold only invites attacks immediately beneath it.” This clarification does not address the larger issue of which attacks would trigger an Article 5 response, as NATO already defends against low-level cyber attacks daily. Ambiguous guidelines could also cause NATO to misappropriate responses to cyber attacks, leading to potentially embarrassing overreactions to minor incursions or devastating slow responses to crippling attacks. Without a clear definition, NATO will struggle to respond to attacks. As stated earlier, NATO’s focus is on deterring attacks—to such an extent that the cost of an attack would outweigh any benefits. However, this focus has resulted in NATO lacking the offensive capabilities to respond in the same capacity as its allies, like the United States.

### EU CP---Deficit---Capabilities---2AC

#### EU fails---political tensions and weak military posture destroys deterrence.

Giovanna De Maio 21. Nonresident fellow in the Center on the United States and Europe at Brookings. She is currently a visiting fellow with George Washington University’s Institute for European, Russian, and Eurasian Studies. With a background on Russia and international security, as well as on Italy’s relations with Russia, EU and United States, De Maio’s research analyzes transatlantic relations vis-à-vis the challenges posed by the rise of China and Russia, with a particular focus on NATO and EU. “Opportunities to deepen NATO-EU cooperation.” Brookings. December 2021. https://www.brookings.edu/research/opportunities-to-deepen-nato-eu-cooperation/ //EM

The twin shocks of the U.S. troop withdrawal from Afghanistan and the AUKUS nuclear submarine deal — along with the heavy toll of President Donald Trump’s tenure — have triggered an ongoing discussion in U.S.-Europe security relations. In particular, given the United States’ increased focus on the Indo-Pacific region in tackling the China challenge, the European Union has been more concretely reflecting on how to increase its military capabilities in regions which are no longer security priorities for Washington. So far, the North Atlantic Treaty Organization (NATO) has been the key military organization responsible for security in the trans-Atlantic space; therefore, an increased military role for the EU raises questions about how the two organizations would relate to each other.

NATO and the EU do have a long track record of cooperation, from institutional cooperation to personnel exchange and joint exercises. Over the years the two organizations have also operated in tandem, with the EU’s Operation Althea taking over the capacity-building efforts of NATO’s Stabilization Force in Bosnia and Herzegovina in 2004 and with both deploying simultaneous counterpiracy missions off the Somalia coast — Operation Ocean Shield (2009-2016) and Operation Atalanta (2008-2022). Moreover, NATO and the EU seem to also have converged in their respective strategic thinking along the lines of countering Russia and China’s aggressive behavior and malign economic influence, as well as threats coming from disruptive technologies and disinformation. Pressed by these challenges, NATO and the EU have progressively expanded their traditional range of military and civilian activities so much that their missions now partially overlap, with NATO embracing capacity-building and cyberoperations and the EU stepping up on crisis management.

Yet NATO-EU cooperation remains somewhat limited because of political tensions between member states (which hinders intelligence sharing) as well as weak European military capabilities and inadequate defense spending. Over the past few years the EU has made important progress in this domain through the establishment of the European Defense Fund and several defense projects under the Permanent Structure Cooperation (PESCO) mechanism. Yet, according to several studies in the field, the state of European defense appears insufficient to tackle more serious military threats or to enable the EU to take initiatives in its neighborhood independently from the United States. In its “Strategic Compass” to be published in March 2022, the EU is supposed to adopt a bolder approach to its defense capabilities. In parallel, in a new strategic concept to be released in June 2022, NATO is supposed to tackle security throughout a widened angle, looking at domains that are not strictly defense-related.

As NATO and the EU progressively expand their scope and strategic thinking in the context of growing global challenges, this paper reflects on how the two organizations could engage in a deeper dialogue to leverage each other’s capabilities: the EU should rely on NATO’s experience with logistics and procurement to strengthen its own and the alliance’s military posture, while NATO should rely on the EU’s experience to counter disinformation, improve military mobility, and tackle hybrid threats stemming from malign economic influence and disruptive technolgies. Reaching such synergies is crucial to strengthening both NATO and EU security posture and to ensure readiness on a number of fronts, not necessarily tied to the military domain and perhaps beyond the trans-Atlantic space itself.

#### EU fails---cannot solve allied interoperability NOR training capabilities.

Stephen Ganote et al. 19. Managing Director at Avascent where he serves clients in space communications and select defense tech markets and leads its commercial space practices, Janie Yurechko is a Strategic Development Specialist at Ball Aerospace and a MBA Candidate at Georgetown University, Diana Jack is a manager in Avascent's Space practice where she provides strategic guidance to major primes, New Space companies, and governments, Connor O’Shea is President and Co-Founder at Westgen Technologies Inc, a remote power generation and methane reduction technology company. “Reenergizing Transatlantic Space Cooperation.” Atlantic Council Scowcroft Center for Strategy and Security. 09-30-2019. https://issuu.com/atlanticcouncil/docs/reenergizing\_transatlantic\_space\_cooperation //EM thx HBisevac

This first wargame was set in 2017, and envisioned conflict with a near-peer space adversary; the partnership is now confronted with technological threats well beyond what was likely contemplated at the time.35 There has been some halting progress: the Schriever exercises have in recent years come to include Germany and France, as well as the traditional “Five Eyes” participants (the United States, UK, Canada, Australia, and New Zealand); European officers are educated at the National Security Space Institute at Peterson Air Force Base; and the European Union Satellite Center provides some joint training on the other side of the Atlantic. These are positive first steps, but senior officials recognize that they do not yet meet the scale or interconnectedness required for growing global space-security challenges.36 Recommendation: Expand the scale and scope of cooperative space wargames, training, doctrine, and education by taking:. several concrete actions. Based on a complete assessment of NATO member-state space capabilities and requirements, defense planners should develop a NATO Space Policy document and accompanying structured space engagement, with guidance on how to meet those requirements through shared and interoperable assets. As part of this new space policy, defense planners should suggest a more regular allied training regime that includes updated doctrine. Recognizing the benefits of coordinated space warfighting, more allies should join in the US “Space Flag” exercises, making it equivalent to Red Flag in the air domain.37

#### Those essential towards shared understanding AND deterrence.

Paul A. Tombarge 14. Bachelor of Arts degree in Political Science from the University of Minnesota, a Master of Arts degree in Public Administration from the University of Maryland-Europe, a Master of Arts degree in International Security Studies from the Naval Postgraduate School, and a Graduate Certificate in Space Systems from the Naval Postgraduate School. He was also a U.S. Senior Fellow at the George C. Marshall European Center for Security Studies from 2013-2014. “NATO Space Operations.” George C. Marshall: Euopean for Security Studies from 2013-2014. 12-2014. https://www.marshallcenter.org/en/publications/occasional-papers/nato-space-operations-0 //EM

Exercises

With the upcoming end of the International Security Assistance Force’s (ISAF) mission in Afghanistan, NATO is expected to shift its emphasis from operational engagement to operational preparedness through its CFI. CFI is intended to build on the Alliance’s recent experience in Afghanistan and ensure the Allies can work even more effectively together in the future.102 A key pillar of this initiative is increased exercises as “an essential means for forces to practice tactics, techniques and procedures, promote and gauge interoperability, validate training and, when required, certify headquarters, units and formations.”103

In order to ensure the Alliance is able to fully exploit space capabilities, space operations should be incorporated into a variety of tactical, operational, and strategic level exercises and war games. At the tactical level, this could include such things as a multi-national RED FLAG exercise. RED FLAG is a realistic combat training exercise involving the air forces of the United States and its allies. Conducted on the vast bombing and gunnery ranges of the Nevada Test and Training Range, RED FLAG was established in 1975 to maximize the combat readiness, capability and survivability of participating units by providing realistic training in a combined air, ground, space and electronic threat environment as well as a free exchange of ideas between forces.104 Participating units execute missions against an opposing “Aggressor” force specially trained to replicate the tactics and techniques of potential adversaries. While Red Flag originally developed a flyer's combat proficiency, the last eight years have slowly incorporated space and cyberspace capabilities.105 Previously segregated from the CAF participants, space and cyber operators are now fully integrated at the tactical level as a primary training audience.

At the operational level, NATO could participate in a BLUE FLAG exercise. BLUE FLAG is an U.S. Air Force “Air Combat Command-sponsored exercise program that provides doctrinally-correct air, space, and cyberspace crisis action planning (CAP) and command and control (C2) training for joint/coalition air components and operational-level headquarters at the operational level of war.”106 Just as RED FLAG is intended to increase the combat survivability of tactical forces, the goal of BLUE FLAG is to train commanders and staff officers at the operational level of war so “they can immediately participate in directing an air war and make smart decisions during the critical first days of an engagement.”107

### EU CP---Deficit---Say No---Russia

#### No chance Russia agrees---Ukraine ruined the existence of good faith space cooperation.

EU specific version

Jeremy Grunert 5-26. Officer in the United States Air Force Judge Advocate General’s Corps. He currently serves as an Assistant Professor in the Department of Law at the United States Air Force Academy. “The Future of Western-Russian Civil-Space Cooperation.” War on the Rocks. 5-26-2022. https://warontherocks.com/2022/05/the-future-of-western-russian-civil-space-cooperation/ //EM

Russia’s Response to Space Sanctions and Short-Term Effects

Russia’s initial response to Western space-related sanctions constituted little more than Roscosmos head Dmitry Rogozin launching a furious Twitter tirade, threatening to cease Russian technological support to the International Space Station. But more concrete responses followed: Russia suspended its launch operations with the European Union; cut off rocket engine servicing and exports to the United States; and has held at least one previously contracted commercial satellite launch hostage in an attempt to extort a NATO member state. Along the way, the mercurial Rogozin has continued to bluster on social media and in the Russian press, threatening that the 500-ton International Space Station could be deorbited over the United States or Western Europe, that the loss of Russian rocket technology would force the United States and its allies to access space on “broomsticks,” that continued partnership in the International Space Station and other joint projects was contingent on the lifting of Western sanctions, and, several weeks later, that Russia would, in fact, leave its long-standing partnership in the International Space Station.

Russian President Vladimir Putin has been less strident than Rogozin, at least in terms of Russian space activities. Downplaying the effects of Western sanctions, Putin has insisted that Roscosmos will continue its civil-space missions — including the Luna-25 Moon mission (one of the lunar missions in which the European Space Agency canceled its collaboration), broadband-providing satellite services, and nuclear propulsion technology development — without international collaboration. Putin himself has not commented on the future of the International Space Station.

From the perspective of NASA and the United States, Russia’s counter-sanctions and threats have had little short-term impact. NASA announced its intent to continue partnering with Roscosmos on the maintenance of the station shortly after the invasion of Ukraine, and while Russia has symbolically canceled some joint space station experiments in retaliation for Western sanctions, most International Space Station operations are proceeding as normal. This has included (despite breathless articles about possible “stranded” astronauts) the return of U.S. astronaut Mark Vande Hei to Earth in a Soyuz crew capsule at the end of March and, at least until mid-May when some media outlets reported the cancellation of the agreement, plans to fly a Russian cosmonaut to the International Space Station on a SpaceX Crew Dragon capsule later this year. NASA Administrator Bill Nelson has consistently characterized Rogozin’s threats as mere bluster and stated that he “see[s] nothing that has interrupted [the] professional relationship” between NASA and Roscosmos in International Space Station operations. As a number of experts have noted, Rogozin’s comments concerning the space station do not signal Russia’s immediate intentions and recognize Roscomos’s obligation to provide at least a year’s advance notice prior leaving the International Space Station partnership — a notification that, to date, has not been provided. Additionally, Rogozin’s media statements are not significantly different from those of Russian government officials made prior to the invasion of Ukraine regarding Russia’s intention to potentially leave the partnership after the 2024 conclusion of the station’s current international operating agreement.

Unfortunately, the short-term effects of the Western sanctions campaign have been far more significant for Europe. The European Space Agency’s decision to cancel its joint projects with Roscosmos effectively ended almost 30 years of space collaboration between the two organizations. In addition to the canceled, suspended, or indefinitely postponed joint civil-space missions, the Russian embargo on Soyuz flights for European payloads has resulted in the cancellation of approximately 16 satellite missions between 2022 and 2024. This has left almost 200 satellites, including several Galileo geo-navigation satellites and a number of other high-profile European satellite missions, without an immediate method of reaching orbit. While a number of launch providers have attempted to adjust their launch schedules and manifests to accommodate these missions, it remains to be seen whether there will be sufficient space on current launches to undertake these missions in the short term. Furthermore, non-space related sanctions, particularly those targeting Russia’s oil, coal, gas, and energy exports, are already causing economic hardship to European economies.

Long-Term Effects

As sanctions and counter-sanctions between the West and Russia proliferate, and as the war in Ukraine grinds on in an ever more brutal fashion, it is difficult to predict exactly what long-terms effects these sanctions will have in the space domain. A number of factors will likely contribute to the long-term effects, including, at a minimum, the length and outcome of the Russo-Ukrainian war; whether Western sanctions are lifted when the conflict concludes; and the extent to which Russia is able to evade Western sanctions or find alternative sources of money and materiel, whether by seeking greater engagement with other international partners (China being the primary candidate) or through other means.

First, how will the Russian civil-space program be affected over the long-term by the current sanctions? The Biden administration has insisted that current sanctions will halve Russia’s high-tech imports and radically affect its defense and aerospace industries, particularly over a period of years. Others counter that such export controls are more likely to constitute a short-term “flesh wound” from which Russia will be able to recover over the long-term by shifting to other supply sources. It seems, however, that sanctions are already wreaking havoc within Russia’s industries: The loss of high-tech electronic and computer equipment imports has reportedly forced shutdowns of a number of military manufacturing plants, including tank factories and surface-to-air missiles production facilities. New military systems under development by the Russian defense industry were described as being “hostage to many new technologies and systems” as early as 2019. Now, with the bite of sanctions, it is unclear whether such systems can be produced in sufficient numbers to contribute to Russia’s military efforts in Ukraine. Additionally, reports out of Ukraine indicate that sanctions have already reduced Russian forces to jerry-rigging military equipment with semiconductors and computer chips from household appliances. While nothing has been publicly released concerning the effects of sanctions on Russia’s space activities, the apparent effects of sanctions throughout Russia’s military and technology production do not bode well for the long-term health of the country’s space industries.

Russia’s space program has suffered heavily over the past decade — particularly in the wake of previous Western sanctions imposed after Vladimir Putin’s annexation of Crimea. As space expert James Clay Moltz notes, since 2014, the Russian space program has “become less innovative and more militarily focused” and its “civil and commercial space technology has failed to keep up with world standards,” already drastically reducing its competitiveness. Even before the present crisis in Ukraine, the French Institute of International Relations theorized that the Russian space program was on a path of significant decline that might not be averted without Russian reengagement with the West and partnership with Europe. Such reengagement now seems impossible, with both the European Space Agency and individual European governments turning back toward the United States for space partnerships. Should these trends continue, Western sanctions and European disengagement may prove devastating to a Russian space program already weakened by pre-2022 sanctions, budget cuts, and aging technology.

With respect to long-term civil-space cooperation between the United States and Russia, there is no immediate threat (despite Rogozin’s bombastic statements) to the International Space Station partnership. However, between Russian officials’ publicly stated intentions to leave the International Space Station sometime in the next several years and the generally deteriorating geopolitical relationship between Russia and the United States, it is by no means clear that civil-space cooperation will continue in a meaningful way after the decommissioning of the space station. Russia has already sought civil-space partnerships with China, signing a five-year space cooperation agreement with the Chinese government and agreeing to jointly construct a lunar research station. A shift by Russia away from civil-space cooperation with the United States and Europe would further solidify the growing perception of “strategic competition” between the West and a Russian-Chinese bloc — a competition already widely seen as existing and growing in the context of military and intelligence-related outer-space operations.

## Unilateral

### Unilateral CP---2AC

#### Shared threat military integration with NATO is key to avoid accidental escalation AND solving debris.

Sam Wilson & Colleen Stover 21. Senior policy analyst for the Center for Space Policy and Strategy at The Aerospace Corporation; Project manager and researcher at The Aerospace Corporation’s Center for Space Policy and Strategy. “Defense Space Partnerships: A Strategic Priority.” Aerospace Center for Space Policy and Strategy. 09-17-2020. https://csps.aerospace.org/papers/defense-space-partnerships-strategic-priority //EM

Coalesce Allied and Partner Thinking on Space Security Concepts.

As part of defense space partnerships, allies can more thoroughly discuss the threats to space systems and potential space conflict scenarios. If the United States wants to fully leverage its allies and partners in any future conflict in space, the United States would benefit from having more discussions with its allies about the possibility and nature of such a conflict: how it might emerge, how the respective allies can contribute, the capabilities the allies should pursue in advance, and the actions that might constitute “red lines” or cross thresholds that are more severe than others.

In recent years, the United States has taken important steps to collaborate with allies and partners on space threats and space conflict. International partners participate in military space exercises such as Space Flag, Global Sentinel, and the Schriever Wargame.22 The Five Eyes (the United States plus Australia, Canada, New Zealand, and the United Kingdom) along with France and Germany all are members of the Combined Space Operations initiative. 23 Experts we spoke to told us that the United States should continue and expand these efforts. Partner preparation for space conflicts could be valuable from an operational and geopolitical perspective. Todd Harrison, Director of the Aerospace Security Project at the Center for Strategic & International Studies, stated the following:

Rotating allies in the [Combined Space Operations Center as part of the Combined Space Operations initiative] is important because it gives those countries experts on space security issues. Let’s say Russia or China start interfering with our nuclear command and control and early warning satellites. Any allied country needs to have their own experts so they understand our response—they need folks who can say, “Yes, I understand why the Americans are escalating over this.”24

In a conflict in space, even if an allied country does not have significant defense space capabilities, it should have an understanding why the United States or other allied countries are taking the actions that they are. That understanding might help that country support the United States and allies politically and militarily in other domains.

The United States and its allies having a shared understanding of space threats and space conflict will help in peacetime too. General John Raymond, the Chief of Space Operations, has prioritized developing norms for operating in space.25 These could include something like taking steps to not create debris and announcing planned maneuvers into other orbits.26 With a similar understanding of the issues, the United States and its allies will be better equipped to develop common ideas for responsible behavior in space. This will also help with multilateral discussions, such as United Nations (UN) proposals on space security. Our partners have not always supported U.S. positions on UN space security proposals, including our negation of proposals made by Russia and China. For example, in the 2014 UN vote on Russia’s proposed draft resolution on No First Placement of Weapons in Outer Space, only three countries voted with the United States against the resolution and 125 voted for it with Russia.27 New and deeper partnerships will create more commonality in assumptions and objectives for fostering a safe and secure space environment.

#### Specifically, Article V results in overreactions.

Ethan Williamson, 19 (Ethan Williamson, Federal Contractor with GridIron IT as a Cyber Task Order Analyst at the Joint Service Provider, 5-13-2019, accessed on 5-29-2022, Charged Affairs, “NATO’s Expanding Role in Cybersecurity”, <https://chargedaffairs.org/natos-expanding-role-in-cybersecurity/>, HBisevac)

Through these organizations and agreements, NATO has improved and strengthened its unified cyber defense capability, seemingly positioning itself to be a standard bearer for cybersecurity. However, these commitments lack specifics and could hamper NATO’s ability to respond to an attack because of bureaucratic and security protocols. Following the inclusion of cyber attacks under Article 5, NATO and its allies could not agree on what kind of attack would trigger the collective defense response. Allies still use their own incident standards to define cyber incidents and in some cases do not make these standards public. This results in an uneven response and makes it difficult for NATO and its allies to provide a unified, Article 5 response to cyber incidents. Stoltenberg has defended this vague definition by stating that, “a clearly defined threshold only invites attacks immediately beneath it.” This clarification does not address the larger issue of which attacks would trigger an Article 5 response, as NATO already defends against low-level cyber attacks daily. Ambiguous guidelines could also cause NATO to misappropriate responses to cyber attacks, leading to potentially embarrassing overreactions to minor incursions or devastating slow responses to crippling attacks. Without a clear definition, NATO will struggle to respond to attacks. As stated earlier, NATO’s focus is on deterring attacks—to such an extent that the cost of an attack would outweigh any benefits. However, this focus has resulted in NATO lacking the offensive capabilities to respond in the same capacity as its allies, like the United States.

#### Allied satellites serve as force multipliers---inevitably causing draw-in.

Antonio Carlo & Nikolaos Veazoglou 20. Previous analyst at the European Space Agency, Sapienza University of Rome; Researcher at the National and Kapodistrian University of Athens “ASAT Weapons: Enhancing NATO’s Operational Capabilities in the Emerging Space Dependent Era.” In: Mazal, J., Fagiolini, A., Vasik, P. (eds) Modelling and Simulation for Autonomous Systems. J. Mazal et al. (Eds.): MESAS 2019, LNCS 11995, pp. 417-425, 03-20-2020. Springer, Cham. //EM edited for grammar.

2 The Applications of Space Platforms

Since the dawn of the space age, outer space has been regarded as the ultimate high ground, which could provide a decisive military advantage to the State that retains superiority over it [2]. In the context of NATO operations space-based assets play an essential role, providing a multitude of services for more than 35 years. Some of the most advanced space-faring States are part of the alliance [3]. It is highly anticipated that in the next leaders’ summit taking place in London NATO will recognize space as a domain of warfare [4].

Since NATO does not own any satellites in orbit, it relys on services provided by governments, military, civilian and commercial entities. NATO has terrestrial SATCOM capabilities and units (terrestrial SATCOM anchor stations, transportable satellite ground terminals and equipment). The C2 for SATCOM is managed by NATO Communication and Information Agency (NCIA) and operated by NATO CIS Group (NCISG) [5].

Space-based assets function as force multipliers, providing support and crucial information during the strategic, operational and tactical levels of war. According to the Allied Joint Doctrine for Air and Space Operations, space capabilities provide a wide range of applications such as: global, strategic and intra-theatre satellite communications (SATCOM); positioning, navigation, and timing (PNT) services; terrestrial and space environmental monitoring; space situational awareness (SSA); intelligence, surveillance, and reconnaissance (ISR); NATO Shared Early Warning [6].

#### Integrated capabilities are key to redundancy AND signal.

James Moltz 11. Chairman of the Department of National Security Affairs at the Naval Postgraduate School, where he also holds a joint faculty appointment in the Space Systems Academic Group. “Coalition Building in Space: Where Networks are Power.” Navy Postgraduate School. 2011. https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf //EM

Notably, one option that has not been examined seriously enough in the current space debate is a possible middle-ground alternative for reducing spacecraft vulnerability: that of creating an allied space "network." Specifically, linking space capabilities first among formal U.S. military allies and then perhaps with other friendly nations could greatly reduce (if not eliminate) the risks of single-point failures to important space systems and create a new form of space deterrence by raising the stakes for adversaries considering launching attacks on space assets. That is, by spreading capabilities among allies in space through the creation of inter-operable, redundant networks of satellites, including in the military sector, space-based partnerships could reduce costs, lessen vulnerability, and raise the challenges facing would-be attackers, thus obviating the need for expensive and destabilizing space-based weapons. This could provide considerable benefits in terms of U.S. and allied space security and improve chances for developing norms of peaceful international behavior.

### Deficit---NATO---1AR

#### Shared coordination with NATO is key to avoid escalation.

Aaron Bateman, 20 (Aaron Bateman is pursuing a Ph.D. in the history of science and technology at Johns Hopkins University and previously served as a U.S. Air Force intelligence officer, 4-29-2020, accessed on 6-11-2022, War on the Rocks, “AMERICA NEEDS A COALITION TO WIN A SPACE WAR”, https://warontherocks.com/2020/04/america-needs-a-coalition-to-win-a-space-war/, HBisevac)

Therefore, it is vital for Washington to work with its allies to establish what specific space behaviors will be considered unacceptable and to communicate — and enforce — such standards with aggressive spacefaring nations like Russia and China. The United States and its allies should work collectively to prevent the testing of weapons in space. The debris generated from these tests poses a threat to the satellites of all spacefaring nations. If more nations begin testing anti-satellite weapons, military space systems could be inadvertently damaged. This situation could lead to an overall escalation in preexisting tension. The United States and its allies providing a clearly defined code of conduct for national security space activities is a feasible and necessary step to take in the immediate term. Certainly, though no one wants a war to begin in or extend into outer space, ignoring this possibility would be extremely negligent. The United States possesses highly sophisticated national security space systems that will be a prime target for capable spacefaring adversaries if a conflict should arise. In the past, the United States has presumed it can and will fight alone in space — but that is no longer necessary. Washington can better ensure its dominance in space if it more fully embraces its allies. Washington would be wise to build a coalition that creates a more robust system for monitoring the space domain, reacting to space threats, and prevailing in a war that extends into outer space. Building a space coalition — especially one that includes allies from Europe, the Middle East, and Asia — is no simple task. But, working towards systems integration and also a common space doctrine is positive step forward towards increased resiliency of the space systems that are essential for precision warfighting. Of course, technical systems cannot be the only focus of the coalition; it should also devote attention to the development of norms for military space activity. Hyten has stated that “trying to fight alone in space would be a mistake” — a mistake that we cannot afford to make.

### Deficit---Redundancy---1AR

#### Allies are key to prevent attacks from escalating.

James Moltz 11. Chairman of the Department of National Security Affairs at the Naval Postgraduate School, where he also holds a joint faculty appointment in the Space Systems Academic Group. “Coalition Building in Space: Where Networks are Power.” Navy Postgraduate School. 2011. https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf //EM

Getting from Here to There: Building a Layered Framework for Policing Space

Despite the risks facing U.S. space assets, the challenges for an adversary seeking to carry out a sustained campaign against space assets in multiple orbits in a noncooperative context are still difficult, thus making redundancy and reconstitution strategies potentially very effective against limited attacks. To the extent that a group of allied spacefaring countries could create a network of interactive satellites and develop policies for mutual support in a time of crisis, such efforts could greatly reduce even the risk of individual attacks on satellites) since any gaps could be quickly filled in and therefore rendered pointless. However) the United States and its allies are a long way from establishing this capability. This raises two related questions: what countries should be involved and what capabilities should be linked?

# DA

## Toolbox

### Thumper---2AC

#### Recent Space Force action thumps any DA BUT doesn’t solve the AFF.

Sandra Erwin, 6-22 (Sandra Erwin, Senior Staff Writer at SpaceNews, 6-22-2022, accessed on 6-24-2022, SpaceNews, “DoD Satcom: Big money for military satellites, slow shift to commercial services”, <https://spacenews.com/dod-satcom-big-money-for-military-satellites-slow-shift-to-commercial-services/>, HBisevac)

The Pentagon plans to spend nearly $13 billion over the next five years to develop and acquire military communications satellites. According to U.S. Department of Defense budget documents, this large investment supports growing demands for connectivity and secure data networks across the U.S. armed forces and national security agencies. The 2023-2027 spending plan includes funding for the Pentagon’s first-ever low Earth orbit broadband constellation and smaller numbers of bespoke communications satellites to augment or replace existing systems. These procurements of bespoke satellites, analysts and industry executives told SpaceNews, appear to run counter to government claims that DoD is poised to transition away from traditional satellite procurements toward greater reliance on commercial space services. “I think it’s fair to say that this budget doesn’t reflect a pivot to a greater adoption of commercial capabilities in lieu of government-owned and operated capabilities,” said Mike Tierney, industry analyst at the defense and aerospace consulting firm Velos. Unlike satellite acquisitions, commercial satcom services are funded through revolving accounts on a year-to-year basis and are not forecast in budget line items, Tierney noted, so it’s difficult to predict future buys. Lt. Gen. Michael Guetlein, commander of Space Systems Command, which oversees Space Force satellite procurements, said he is pushing for change in a culture that favors building systems in-house. The goal is to “buy what we can and only build what we must,” he said. “You will start to see that shift, year to year, as we go forward.” The satellite acquisitions funded in the Space Force budget, he said, reflect priorities vetted and approved by the Joint Chiefs of Staff. “The one thing that is always needed is more comm,” he said. “We never have enough comm to get after what we need to do. We need more comm to support the fight.” Guetlein said the satellite industry could expect more commercial satcom opportunities in the coming years. The U.S. Space Force’s Commercial Satellite Communications Office (CSCO) said it plans to award nearly $2.3 billion in commercial satcom contracts over the next two years. CSCO buys commercial satcom capacity and services for the U.S. armed forces and allies. The largest of the commercial opportunities is an $875 million multiple-award deal for low Earth orbit satellite broadband services over 10 years. The Space Force, in a 2020 vision document, said satcom should be an “integrated enterprise” of military and commercial systems. According to the document, “for those frequency bands, coverage areas or specialized capabilities not offered by the commercial satcom industry, purpose-built constellations and payloads will be acquired.” Making these buy-vs-build decisions “requires a little bit of calculus,” said Guetlein. “We’ve got to really understand how that capability is going to be used in the future, in a time of crisis or time of conflict. And can I depend on that capability?” “If I cannot guarantee that it will be there when I need it, then I probably need to own it, not lease it,” Guetlein said. “If industry can guarantee that that capability will be there in times of crisis or conflict, then I can probably buy those services. And I would rather buy those services than have to go build something myself.” One reason to buy commercial satcom services is that it adds layers of resilience, he said. “In a conflict, it gives us proliferation. It gives us redundancy across our networks.” At a time when U.S. adversaries are stepping up cyber attacks that threaten terrestrial and satellite-based networks, said Guetlein, the Space Force and its satcom suppliers will be taking a “holistic approach to cybersecurity and not just look at it in stovepipes.” NEW SATELLITE PROCUREMENTS The projected $13 billion worth of satellite procurements in the 2023-2027 defense budget pay for a mix of strategic and tactical communications systems. The lion’s share is for the Evolved Strategic Satcom, or ESS, program. The Space Force plans to spend $5.5 billion over five years to continue the development of three proposed payloads and ground system concepts from Boeing, Lockheed Martin and Northrop Grumman. The companies are expected to complete prototype designs by 2025 and conduct in-space demonstrations. The Space Force said it plans to field ESS in the early 2030s. The ESS will provide highly secure communications lines for the most sensitive national security operations, including nuclear command and control. Another big-ticket item in the budget is $2.2 billion for narrowband satellites. The Space Force is looking to buy two more Mobile User Objective System (MUOS) satellites that provide Ultra High Frequency (UHF) communications. The U.S. Navy acquired four MUOS satellites — made by Lockheed Martin — plus an on-orbit spare launched in 2016. The program has since been transferred to the Space Force. MUOS supports mobile users with voice and low-rate data transfer. Because the satellites are oversubscribed, DoD wants to buy two more. The Space Force is conducting an analysis of alternatives before it decides whether to buy two more MUOS or opt for a new design. A Lockheed Martin spokesperson said the company has kept its production line warm and is “ready for the next acquisition.” For secure tactical communications, DoD is budgeting $2.5 billion for Protected Tactical Service (PTS) satellites and a ground system called Protected Tactical Enterprise Service (PTES). Boeing and Northrop Grumman are developing PTS payloads and Boeing is also the PTES prime contractor. Both companies are expected to launch prototype payloads in 2024 for on-orbit demonstrations. The ESS and PTS constellations are intended to augment and eventually replace the Advanced Extremely High Frequency (AEHF) satellites made by Lockheed Martin. The sixth and final AEHF satellite was launched in March 2020. The AEHF satellites carry strategic payloads, which must be able to operate in a nuclear war environment, and tactical payloads for battlefield use. The plan is to disaggregate the capabilities of AEHF into the ESS for strategic communications, and the PTS for tactical users. The Space Force said the ESS satellites will provide polar coverage, which AEHF does not. The military today relies on two Northrop Grumman-developed Enhanced Polar System satellites to extend the AEHF network over the North Pole. While military satellites have mostly operated from geostationary orbits, the Pentagon is now for the first time building its own broadband constellation in low Earth orbit that will connect users across the world. The Space Development Agency, which is overseeing the project, is budgeting $2.7 billion over five years for the Transport Layer, a mesh network expected to have hundreds of small satellites. Even though there are commercially available broadband services, DoD’s requirements are unique, said SDA Director Derek Tournear. The Transport Layer satellites, for example, have to be interoperable with the Link 16 tactical data link protocol that is only used by the U.S. military and allies. “There’s no commercial market for Link 16 as far as I know. So that’s one of the areas where it is mission specific to the DoD,” said Tournear. INTEGRATION OF MILITARY AND COMMERCIAL The five-year budget plan includes $257 million for “commercial satcom integration,” a funding line Congress created in 2019 in response to backlash from the commercial satcom industry after appropriators funded a new Wideband Global Satcom (WGS) satellite that DoD did not request. Congress added $600 million in 2018 for WGS, arguing that the Air Force at the time was not providing sufficient satcom capacity to meet user demand. The integration line “is not huge dollars, and it’s not to buy commercial capacity, it’s just to develop standards and interfaces for the department to plan the architecture,” said Tierney, the industry consultant. So far, it is not clear that the desired hybrid networks are any closer to becoming a reality, he said. The priorities in the budget suggest that DoD remains heavily invested in military satcom and will rely on commercial services as a “relief valve” when it needs additional capacity. “The giant pivot people were hoping for is just not happening, at least not as quickly as commercial operators would have liked,” Tierney added. During a panel discussion at an Air & Space Forces Association conference in March, Guetlein said there’d been a running dialogue on how DoD should operate with commercial space systems during a conflict. “When we were in Afghanistan and Iraq, it was clear to us what was military, what was intelligence, what was commercial, what was allied,” he said. But the lines between government and commercial could become more blurred if DoD starts buying more commercial services, Guetlein said. “As we start going into the space fight and seek space superiority, there are those in a camp that says the government has to own all the capability on orbit,” he said. Some factions in DoD perceive commercial systems as being less cyber-secure than government-owned systems, but that thinking will change as the commercial sector continues to develop novel solutions to protect networks, said Keith Alexander, founder and chairman of IronNet, a cybersecurity consulting firm. Alexander, a retired Army general and former director of the National Security Agency, said satcom providers have to gradually build trust with government customers much like commercial cloud providers Amazon Web Services and Microsoft Azure did more than a decade ago when they started to pursue military and intelligence contracts. Questions about the security of commercial systems “was a big issue that we had with the cloud,” said Alexander. The government eventually warmed to the idea that it could have a “top secret cloud with a commercial vendor. I think showing that we can do the same thing with commercial satellite communications will get us to the same place.” COMMERCIAL SATCOM INVESTMENTS Peter Hoene, president and CEO of SES Government Solutions, said the industry is investing billions of dollars in new capabilities and DoD should be taking advantage of them. SES, an operator of geostationary and medium-Earth-orbit communications satellites, will be adding 11 high-capacity broadband satellites to its MEO constellation between 2022 and 2025. “Commercial satcom will likely never be a significant player in nuclear command and control and some other high-end missions,” Hoene said, but for the bulk of its satcom needs, DoD should be using commercial systems. The Space Force procurement office, CSCO, needs to “explore effective ways to adopt longer term contracts, purchasing commercial satcom more like fiber,” he added. CSCO so far “has not met industry expectations to explore deeper partnerships to ensure critical capacity is available to the warfighter when and where they need it,” Hoene said. “The acquisition process and the way the department procures commercial satcom is not where we believe the DoD needs to be.” SES in March made a major move to expand its military business with the $450 million acquisition of satcom integrator Leonardo DRS Global Enterprise Solutions, one of the largest providers of commercial services to the U.S. government. Hoene said this acquisition allows SES to partner with other companies in order to meet DoD demands for multiorbit satcom. “The satellite communications market is becoming increasingly competitive, particularly with the entrance of low Earth orbit providers like Starlink, OneWeb, Telesat and Amazon Project Kuiper,” he said. “We see the importance of integrated GEO-MEO-LEO and managed service solutions for DoD customers.” CULTURE IS HARD TO CHANGE Craig Miller, president of Viasat Government Systems, said the industry would have liked to see in the 2023 budget an “increased focus on commercial satellite communications, although we are seeing some motion in that direction.” “For many years, we’ve been talking to the Air Force when they were in charge of this, and now with the formation of the Space Force, we’re working very hard to get them to understand the value of commercial,” said Miller. Viasat is a global provider of satellite broadband and is looking to sign up military customers for its new Viasat-3 geostationary constellation of three highcapacity satellites. The first ViaSat-3, projected to launch in early 2023, will cover the Americas, to be followed later in the year by a second satellite to service Europe, the Middle East and Africa. A third satellite will cover Asia. DoD could save money by using high-capacity commercial satellites for tactical communications instead of buying systems like PTS, said Miller. “ViaSat-3 absolutely can meet the requirements of that system and the anti-jam requirements that are associated with that.” There are other commercial LEO, MEO and GEO systems coming online that could meet the PTS mission, Miller added. For narrowband L-band communications, there is Iridium and Inmarsat, although they couldn’t replace MUOS because the military uses the UHF frequency band, and that spectrum is owned and operated by governments. A spokesman for Iridium said the company’s mobile communications network could supplement MUOS coverage in the polar regions. The company in 2019 won a seven-year $738.5 million DoD contract for unlimited usage of Iridium narrowband devices for an unlimited number of subscribers. “Since users are already on the contract, it’s an affordable option for the Iridium network to complement MUOS with Iridium narrowband services,” said the spokesman. “We have already tested the capabilities of voice-to-voice calls from Iridium devices to MUOS.” One problem facing commercial vendors is that DoD buyers often are not aware of what the market offers, Miller said. “We’re really optimistic that they’ll open their eyes to the value of commercial satcom and they use it because they’ll see how effective it is. I think part of it is that they don’t quite know what it’s capable of yet.” “Culture change is really hard,” Miller said. DoD doing “more of the same rather than doing something new is normal. But all in all, I think that we will see more adoption of commercial.” DoD’s strategy to build a global network known as “joint all-domain command and control” requires massive communications pipelines for data sharing that can’t be achieved only with government systems, Miller noted. “When you think about a future peer conflict with China,” Miller said, “we have to be in a position where we can leverage our commercial technological advantage and then spend our defense dollars on the things that absolutely need defense dollars, and not duplicate things that are being developed in the commercial market.”

## DoD

### DoD DA---Resources Turn---2AC

#### TURN. The DoD will allocate resources for ASATs NOW---OR no link!

---We get that you are going to say this takes out the AFF---no, this is about only KINETIC attacks, disregarding NON-KINETIC attacks which is the AFF’s internal link

Kris Osborn 22. Previously served at the Pentagon as a Highly Qualified Expert with the Office of the Assistant Secretary of the Army - Acquisition, Logistics& Technology. “The United States is Preparing to Counter Anti-Satellite Weapons.” National Interest. 1-13-2022. https://nationalinterest.org/blog/reboot/united-states-preparing-counter-anti-satellite-weapons-199444 //EM

Here's What You Need to Know: Space war strategy continues to receive very large amounts of attention from the Pentagon and U.S. Space Command.

If a Russian or Chinese Anti-Satellite (ASAT) weapon streamed into space and exploded U.S. military satellites, friendly forces would instantly become very vulnerable to significant and extremely destructive enemy attacks….-- space-based infrared missile detection could be destroyed, GPS communications could be knocked out, guided weapons could jam and derail before hitting their targets and war-critical command and control could simply be “taken out.”

Any, all or part of this could happen in as little as 10 to 15 minutes once a satellite attacking missile is launched from the ground. Lives will hang in the balance as alerts are sent through U.S. command and control and decision-makers scramble to determine the best countermeasure with which to protect its space assets. Space war is no longer a distant prospect to envision years down the road --- it is here.

Recognizing the seriousness of this vulnerability, the Pentagon, U.S. Space Command, Missile Defense Agency and industry are moving quickly to integrate Machine Learning and AI into space-based systems and technology. The intention is to of course accelerate threat detection and get crucial information to decision-makers.

#### The plan shares the resource burden with NATO---solving tradeoff.

Sam Wilson & Colleen Stover 21. Senior policy analyst for the Center for Space Policy and Strategy at The Aerospace Corporation; Project manager and researcher at The Aerospace Corporation’s Center for Space Policy and Strategy. “Defense Space Partnerships: A Strategic Priority.” Aerospace Center for Space Policy and Strategy. 09-17-2020. https://csps.aerospace.org/papers/defense-space-partnerships-strategic-priority //EM

Additionally, space capabilities and operations are expensive. A clear advantage of military space partnerships is that they generate opportunities for sharing the financial burden of operating in space. As an example, the United States putting its security payloads on the Norwegian satellite will reportedly generate up to $900 million in savings.17 Hosting U.S. payloads on foreign systems, like this example, represents an area in which the United States could leverage allied and partner capabilities more so than it does currently. Hosted payloads offer affordable means to expand protected communications satellites; position, navigation, and timing satellites; and space situational awareness capabilities, among other systems. Rather than host payloads, partners can also simply contribute to the cost of a satellite system. For example, through multilateral agreements, Canada, Denmark, Luxembourg, the Netherlands, and New Zealand provided funding for the U.S. Wideband Global SATCOM-9 satellite that launched in March 2017.18 Or the United States can use partners’ satellites. For example, the United States partners with Japan and Europe to obtain weather information from space-based sensors, providing accurate weather information to warfighters around the world and avoiding the need to field additional U.S. systems.19 And it is not just satellites and payloads. Partners have terrestrial infrastructure and user equipment, including for position, navigation, and timing and satellite communications, that can be used collectively to achieve needed capabilities more efficiently. Leveraging allied systems can offer technological insights, system improvements, and capability expansions at lower costs.

### DoD DA---No Tradeoff---2AC

#### AFF uses the Space Force AND comes from a completely different pool of resources.

Sandra Erwin, 6-22 (Sandra Erwin, Senior Staff Writer at SpaceNews, 6-22-2022, accessed on 6-24-2022, SpaceNews, “DoD Satcom: Big money for military satellites, slow shift to commercial services”, <https://spacenews.com/dod-satcom-big-money-for-military-satellites-slow-shift-to-commercial-services/>, HBisevac)

The U.S. Space Force’s Commercial Satellite Communications Office (CSCO) said it plans to award nearly $2.3 billion in commercial satcom contracts over the next two years. CSCO buys commercial satcom capacity and services for the U.S. armed forces and allies.

## Politics---Agenda

### No Link---2AC

#### No link---the overwhelming importance of satellites quashes initial backlash.

Richard M. Harrison 22. Contributor at TheHill. “Space: One important thing that might retain bipartisan focus.” Hill. 1-7-2022. https://thehill.com/opinion/technology/588708-space-one-important-thing-that-might-retain-bipartisan-focus/ //EM

These days, despite the hyper-partisan atmosphere in Washington, there still seem to be two issues that both Democrats and Republicans can agree on. One is the pervasive threat posed by the People’s Republic of China. The other is the overarching importance of space.

When Vice President Kamala Harris chaired the Biden administration’s first National Space Policy Council meeting last month, her comments — along with the simultaneously released U.S. Space Priorities Framework — largely echoed the space policy launched by the Trump administration. That was not necessarily a given, since a continuation of policy is never a guarantee during presidential transitions. But the Biden administration’s acknowledgement is great news for the rekindling of America’s space program and strategy.

The emphasis is logical. Although news about space is all too often dominated by headlines of the latest Russian anti-satellite test or milestone in China’s space program, the domain is already ubiquitous — and essential — for daily life. We rely on space for our financial transactions, daily navigation, weather notifications, TV services, and telecommunications. Today, the global space economy is estimated at $450 billion annually — a figure that has doubled over the previous decade. This, however, is just the beginning. The economic value of space is poised to soar, entering the trillions annually over the course of the next two decades.

#### There is overwhelming, bipartisan support for space cybersecurity.

Martin Matishak 22, senior cybersecurity reporter for The Record, 1/19/2022, “Bipartisan bill would boost satellite cybersecurity,” https://therecord.media/bipartisan-bill-would-boost-satellite-cybersecurity/, Marsh

Bipartisan bill would boost satellite cybersecurity

A bipartisan pair of senators on Wednesday introduced legislation that would require the Homeland Security Department’s cybersecurity branch to supply commercial satellite owners and operators with tools to better protect against hackers.

The Satellite Cybersecurity Act from Sens. Gary Peters (D-Mich.) and John Cornyn (R-Texas) would mandate that the Cybersecurity and Infrastructure Security Agency (CISA) develop voluntary satellite cybersecurity recommendations to help companies better understand how to secure their systems.

The measure would also require CISA — which last year [launched a Space Systems Critical Infrastructure Working Group](https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group) — to create a publicly available online repository in order to give companies access to satellite-specific cybersecurity resources, as well as network security recommendations.

## Intel Backlash

### Intel Backlash DA---2AC

#### No backlash---NGA recommends the plan!

1NC Theresa Hitchens, 4-29 (Theresa Hitchens is the Space and Air Force reporter at Breaking Defense and a senior research associate at the University of Maryland’s Center for International and Security Studies at Maryland, 4-29-2022, accessed on 6-23-2022, Breaking Defense, “NATO considers buying commercial imagery, irking US spy sat agencies”, <https://breakingdefense.com/2022/04/nato-considers-buying-commercial-imagery-irking-us-spy-sat-agencies-sources/>, HBisevac) NRO = National Renaissance Office, NGA = National Geospatial-Intelligence Agency

GEOINT 2022: NATO is mulling a new, and somewhat surprising, effort to directly **buy imagery** from commercial providers in a move that industry sources say appears to have irked the **US spy satellite agencies** that have **traditionally** filled that **role**. Interested companies have until the close of business today to respond to NATO’s request for information (RFI).

Alliance member nations, too, have been asked to identify “**emerging** and/or existing” **remote sensing capabilities** that could help **NATO’s military command** produce “imagery intelligence,” or IMINT. IMINT is provided primarily by satellites, as well as by aerial photography.

The US is the largest operator of **military** intelligence, surveillance and reconnaissance (**ISR**) satellites, and is **outwardly supportive** of the effort, which an IC official said could improve NATO’s production of geospatial intelligence (GEOINT) products.

“We want NATO to produce timely, relevant, and trusted GEOINT that can be easily shared with the Alliance, and we work with NATO towards that end,” Melissa Planert, deputy director for international affairs at the National Geospatial-Intelligence Agency (**NGA**), said in an email.

“NGA’s position is that we also strongly recommend NATO seek diverse imagery sources, products and services from across the Alliance and from commercial vendors,” she added. “A diverse selection of imagery and analysis providers will only benefit GEOINT contributions to NATO intelligence requirements, and strengthen NATO policymakers’ understanding of the complex security situation.”