# Round 1 Myers Park 1AC

#### I affirm the resolution; The appropriation of outer space by private entities is unjust.

## Util FW

#### My value is justice

#### The standard is maximizing expected wellbeing.

#### Prefer:

#### 1] States must use util – they seek practical benefits for constituents and aren’t unified agents so they don’t have intentions.

#### 2] Death is bad and outweighs – a) agents can’t act if they fear for their bodily security which constrains every ethical theory, b) it destroys the subject itself – kills any ability to achieve value in ethics since life is a prerequisite which means it’s a side constraint since we can’t reach the end goal of ethics without life

#### Pleasure and pain are the only things intrinsically valuable.

Moen 16 [Ole Martin Moen, Research Fellow in Philosophy at University of Oslo “An Argument for Hedonism” Journal of Value Inquiry (Springer), 50 (2) 2016: 267–281] SJDI

Let us start by observing, empirically, that a widely shared judgment about intrinsic value and disvalue is that pleasure is intrinsically valuable and pain is intrinsically disvaluable. On virtually any proposed list of intrinsic values and disvalues (we will look at some of them below), pleasure is included among the intrinsic values and pain among the intrinsic disvalues. This inclusion makes intuitive sense, moreover, for there is something undeniably good about the way pleasure feels and something undeniably bad about the way pain feels, and neither the goodness of pleasure nor the badness of pain seems to be exhausted by the further effects that these experiences might have. “Pleasure” and “pain” are here understood inclusively, as encompassing anything hedonically positive and anything hedonically negative.2 The special value statuses of pleasure and pain are manifested in how we treat these experiences in our everyday reasoning about values. If you tell me that you are heading for the convenience store, I might ask: “What for?” This is a reasonable question, for when you go to the convenience store you usually do so, not merely for the sake of going to the convenience store, but for the sake of achieving something further that you deem to be valuable. You might answer, for example: “To buy soda.” This answer makes sense, for soda is a nice thing and you can get it at the convenience store. I might further inquire, however: “What is buying the soda good for?” This further question can also be a reasonable one, for it need not be obvious why you want the soda. You might answer: “Well, I want it for the pleasure of drinking it.” If I then proceed by asking “But what is the pleasure of drinking the soda good for?” the discussion is likely to reach an awkward end. The reason is that the pleasure is not good for anything further; it is simply that for which going to the convenience store and buying the soda is good.3 As Aristotle observes: “We never ask [a man] what his end is in being pleased, because we assume that pleasure is choice worthy in itself.”4 Presumably, a similar story can be told in the case of pains, for if someone says “This is painful!” we never respond by asking: “And why is that a problem?” We take for granted that if something is painful, we have a sufficient explanation of why it is bad. If we are onto something in our everyday reasoning about values, it seems that pleasure and pain are both places where we reach the end of the line in matters of value.

## 1 – Cyber

#### Public entities such as NASA have standards they can follow and clarity – other state programs to model. Private actors have no unified cyber guidelines due to lack of transparency and commercial motives – regulations key.

Shadbolt 21 -- Luke Shadbolt, Technical Study Satellite Cyberattacks and Security July 2021, HDI Global Specialty SE, <https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf>, //arav

Despite industry efforts to improve cybersecurity in many areas of critical infrastructure, there has been little focus on cybersecurity for space systems. Space systems are more complex than other forms of critical infrastructure from a technology development, ownership and management perspective as has been previously noted (see Figure 3). This has historically led to a lack of guidance in the form of international standards that govern space system security, and ultimately, policies that enforce these standards [6]. It is only recently that certain cybersecurity policies, such as the NIST Cybersecurity Framework, have started to be considered in the frame of the commercial satellite industry [25]. Among the space industry community the lack of attention to cybersecurity is acknowledged; however the responses to cybersecurity threats have been variable. An audit of NASA in 2015 revealed the need for a revamping of their cybersecurity standards and protocols, citing several attacks that were not publically disclosed. NASA’s efforts are not necessarily representative of the broader space industry’s cybersecurity awareness and efforts, however smaller organisations working on satellites look to NASA for standards and best practices. More established private space companies such as SpaceX or Blue Origin have no public comments on their cybersecurity posture [6]. Neither public nor private space asset organisations are at a complete standstill concerning their cybersecurity efforts; however there remain considerable gaps in the space asset security posture compared with other critical infrastructure sectors, and these must be addressed. V.1 Existing standards and regulation The International Telecommunication Union (ITU), a United Nations agency, regulates frequencies of satellite communications to prevent communication interference and registers the orbits of satellites; but beyond these areas there are currently few standards. In 2007 the ITU created a “global cybersecurity agenda” intended as “a framework for international cooperation in cybersecurity”; however it seems there have not been considerable updates to this agenda since 2007 despite the changing landscape of cybersecurity. At this point, there are no agencies that restrict the use of satellites and there is no overarching governing body that monitors the specific use of satellites. Even if one did exist, there are currently no mechanisms for enforcing any treaties / standards / governance [16]. Research by Chatham House has described these deficiencies on a global scale in relation to the North Atlantic Treaty Organisation (NATO) and the need for a NATO Space Policy [22]. General IT-based cybersecurity standards or frameworks however are widely available, and most space system security could benefit from adopting these. One of the best examples is the NIST CSF (Cybersecurity Framework). A draft paper recently published by NIST in June 2021, “Introduction to Cybersecurity for Commercial Satellite Operations”, is intended to introduce the CSF to commercial space businesses [25]. This includes describing a specific method for applying the CSF to commercial satellite operations; creating an example CSF set of desired security outcomes based on missions and anticipated threats; and describing an abstracted set of cybersecurity outcomes, requirements, and suggested cybersecurity controls. Another example is the CNSS (Committee on National Security Systems) Instruction 1253F (see Figure 4). While efforts are being made to mould these frameworks for space systems, uniformity is lacking, and updated standards and guidelines for spacecraft are likely warranted [7]. There are pockets of initiatives across the space community that are addressing cybersecurity for space systems, however most work in this area to-date has focused on the ground segment with little research or guidance on securing the space segment (i.e. spacecraft). Figure 4 outlines some of the known initiatives and standards that have been published relating to cybersecurity within the space domain. These range from high-level compliance controls to low-level communication protocol standards but are not overarching engineering principles for a spacecraft. HDI Study\_Satellite Cyberattacks and Security HDI Global Specialty SE Organization Title of Standard Applicability/ Scope Link to Standard Description of Standard CNSS CNSSI 1200 National Information Assurance Instruction for Space Systems Used to Support National Security Missions Ground and spacecraft for National Security System (NSS) only https://www.cnss.gov/CNSS/ issuances/Instructions.cfm This standard elaborates on how to appropriately integrate information assurance (IA) into the planning, development, design, launch, sustained operation, and deactivation of those space system V.2 Public space asset organisations NASA has taken several steps to improve security around space assets as follows: • First, NASA has begun implementing stricter access control policies across their providers and engineers in order to help guard against the phishing attacks that have been used in the past to steal credentials and access intellectual property. • Secondly, NASA has created teams across their space asset development centres that specifically work with the security of their missions systems. NASA’s Jet Propulsion Laboratory (JPL) has created the Cyber Defense Engineering and Research Group (CDER) whose goal is specifically to address mission systems (e.g. the Mars Science Lab) which often have unique cybersecurity requirements. Some of CDER’s work aims to develop tools and methodologies that apply across multiple mission systems to reduce costs and security operations. • Finally, NASA has begun encrypting data while it is stored and during transfer. At the end of 2016 AT&T encrypted NASA’s Deep Space Network (DSN), which is the foundation of communication infrastructure for interplanetary spacecraft missions. Somewhat ironically however this encryption was only performed after a report on how to hack into the Mars rover Curiosity appeared on the internet [6] [16]. NASA JPL’s CDER Group is also working with university researchers at the Massachusetts Institute of Technology (MIT) to conduct penetration tests on mission system software. Increasing engagement with the broader security research community will considerably improve mission system security for space assets. V.3 Private space asset organisations Like NASA the private space asset industry is currently improving its security, but as previously mentioned, it is impossible to evaluate many private sector companies who are not transparent regarding their cybersecurity efforts. SpaceX, Virgin Galactic or other space asset developers, owners and operators do not make their technology readily available for security researchers to test. This is probably because they are concerned that their sensitive code or information will fall into competitors’ hands. Despite this, penetration testers, ethical hackers and security researchers are constantly finding holes in various satellite network systems and asking the responsible party to fix the vulnerabilities. Unfortunately these vulnerability notifications often go ignored due to manufacturers’ lack of bandwidth to address the issues or mistrust of the hackers. The lifecycle complexities and associated liability questions discussed earlier (Figure 3) further complicate fixing vulnerabilities. If ignored, the ethical hackers generally follow responsible reporting procedures and expose the vulnerability to the public following a period of time after notifying the vendor. By publicly announcing the threat, the ethical hackers intend to garner large-scale attention to the problem and force the vendor to fix the issue. This was the case with the Iridium satellite owners who asserted their systems were extremely difficult to hack [23]. Only after ethical hackers announced their vulnerabilities and embarrassed the company did Iridium take steps to improve the security of their communication network [6].

#### Private companies are cutting corners – action is key

Akoto 20-1 -- William Akoto, **FEBRUARY 12, 2020, “Hackers could shut down satellites -- or turn them into weapons”,** [**https://gcn.com/cybersecurity/2020/02/hackers-could-shut-down-satellites-or-turn-them-into-weapons/291164/**](https://gcn.com/cybersecurity/2020/02/hackers-could-shut-down-satellites-or-turn-them-into-weapons/291164/)**, William Akoto is an assistant professor of international politics at Fordham University.  He studies the political economy dynamics of cyber conflict, international trade and military coups. He has a Ph.D in Political Science from the University of South Carolina. // arav**

Last month, SpaceX became the operator of the [world’s largest active satellite constellation](https://www.theverge.com/2020/1/14/21043229/spacex-starlink-satellite-mega-constellation-concerns-astronomy-space-traffic). As of the end of January, the company had [242 satellites orbiting the planet](https://spacenews.com/spacex-launches-fourth-batch-of-starlink-satellites-tweaks-satellite-design/) with plans to launch 42,000 over the next decade. This is part of its ambitious project to provide internet access across the globe. The race to put satellites in space is on, with Amazon, U.K.-based OneWeb and other companies chomping at the bit to place thousands of satellites in orbit in the coming months.

These new satellites have the [potential to revolutionize](https://www.ucsusa.org/resources/what-are-satellites-used) many aspects of everyday life -- from bringing internet access to remote corners of the globe to monitoring the environment and improving global navigation systems. Amid all the fanfare, a critical danger has flown under the radar: the lack of cybersecurity standards and regulations for commercial satellites, in the U.S. and internationally. As a [scholar who studies cyber conflict](https://scholar.google.com/citations?user=dQgC9-gAAAAJ&hl=en&oi=ao), I’m keenly aware that this, coupled with satellites’ complex supply chains and layers of stakeholders, leaves them highly vulnerable to cyberattacks.

If hackers were to take control of these satellites, the consequences could be dire. On the mundane end of scale, hackers could simply shut satellites down, denying access to their services. Hackers could also jam or [spoof](https://www.computerhope.com/jargon/s/spoof.htm) the signals from satellites, creating havoc for critical infrastructure. This includes electric grids, water networks and transportation systems.

Some of these new satellites have thrusters that allow them to speed up, slow down and change direction in space. If hackers took control of these steerable satellites, the consequences could be catastrophic. Hackers could alter the satellites’ orbits and crash them into other satellites or even the International Space Station.

**Commodity parts open a door**

Makers of these satellites, particularly small CubeSats, use [off-the-shelf technology](https://www.nbcnews.com/technolog/space-all-small-cheap-satellites-may-one-day-do-your-6C10488674) to keep costs low. The wide availability of these components means hackers can analyze them for vulnerabilities. In addition, many of the components draw on open-source technology. The danger here is that hackers could insert back doors and other vulnerabilities into satellites’ software.

The highly technical nature of these satellites also means multiple manufacturers are involved in building the various components. The process of getting these satellites into space is also complicated, involving multiple companies. Even once they are in space, the organizations that own the satellites often outsource their day-to-day management to other companies. With each additional vendor, the vulnerabilities increase as hackers have multiple opportunities to infiltrate the system.

[Hacking some of these CubeSats](https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think) may be as simple as waiting for one of them to pass overhead and then sending malicious commands using specialized ground antennas. Hacking more sophisticated satellites might not be that hard either.

Satellites are typically controlled from ground stations. These stations run computers with software vulnerabilities that can be exploited by hackers. If hackers were to infiltrate these computers, they could send malicious commands to the satellites.

**A history of hacks**

This scenario played out in 1998 when [hackers took control](https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders/) of the U.S.-German ROSAT X-Ray satellite. They did it by hacking into computers at the Goddard Space Flight Center in Maryland. The hackers then instructed the satellite to aim its solar panels directly at the sun. This effectively fried its batteries and rendered the satellite useless. The defunct satellite eventually [crashed back to Earth](https://www.bbc.com/news/science-environment-15466361) in 2011. Hackers could also hold satellites for ransom, as happened in 1999 when [hackers took control](http://content.time.com/time/magazine/article/0,9171,20673,00.html) of the U.K.‘s SkyNet satellites.

Over the years, the threat of cyberattacks on satellites has gotten more dire. In 2008, hackers, possibly from China, reportedly [took full control](https://www.itworld.com/article/2734574/two-u-s--satellites-pwned-in--07---08--new-report-blames-china.html) of two NASA satellites, one for about two minutes and the other for about nine minutes. In 2018, another group of Chinese state-backed hackers reportedly launched a [sophisticated hacking campaign](https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html) aimed at satellite operators and defense contractors. Iranian hacking groups have also attempted [similar attacks](https://www.thedailybeast.com/iranian-hacking-group-targeted-us-satellite-companies?ref=scroll).

Although the U.S. Department of Defense and National Security Agency have made [some efforts to address space cybersecurity](https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/), the pace has been slow. There are currently [no cybersecurity standards for satellites](https://www.satellitetoday.com/cybersecurity/2019/11/14/satellite-providers-stymied-by-lack-of-cyber-standards/) and no governing body to regulate and ensure their cybersecurity. Even if common standards could be developed, there are no mechanisms in place to enforce them. This means responsibility for satellite cybersecurity falls to the individual companies that build and operate them.

**Market forces work against space cybersecurity**

As they compete to be the dominant satellite operator, SpaceX and rival companies are [under increasing pressure to cut costs](https://www.nsr.com/smallsat-growth-on-shaky-foundations/). There is also pressure to speed up development and production. This makes it tempting for the companies to cut corners in areas like cybersecurity that are secondary to actually getting these satellites in space.

Even for companies that make a high priority of cybersecurity, the costs associated with guaranteeing the security of each component could be prohibitive. This problem is even more acute for low-cost space missions, where the cost of ensuring cybersecurity could exceed the cost of the satellite itself.

To compound matters, the complex supply chain of these satellites and the multiple parties involved in their management means it’s often not clear who bears [responsibility and liability for cyber breaches](http://dx.doi.org/10.15779/Z38CR6N). This lack of clarity has bred complacency and hindered efforts to secure these important systems.

#### It’s Coming Now - Space is the new frontier for cyberattacks.

Shin 21 -- John Shin, Forbes Councils Member**,** [**Forbes Technology Council**](https://www.forbes.com/sites/forbestechcouncil/), Managing Director at [RSI Security](https://www.rsisecurity.com/), helping organizations achieve cybersecurity and compliance success., Aug 20, 2021,07:45am EDT, “**Why Space Is The Next Frontier For Cybersecurity”,** [**https://www.forbes.com/sites/forbestechcouncil/2021/08/20/why-space-is-the-next-frontier-for-cybersecurity/?sh=608c654041b1**](https://www.forbes.com/sites/forbestechcouncil/2021/08/20/why-space-is-the-next-frontier-for-cybersecurity/?sh=608c654041b1) **//arav**

**With projects like Blue Origin and SpaceX, private-sector innovators like Jeff Bezos and Elon Musk are pursuing outer space endeavors at seemingly breakneck speed. These projects give us a glimpse of what's possible, making outer space travel and industry seem reachable within our lifetimes.**

**But with the digital technology and software required to make that happen, it's time to start assessing things from a cybersecurity perspective. In fact, both the** private **and public** sector**s are already** beginning to tackle **what** cybersecurity **means** in **the context of** outer space**.** Satellites **already** transmit **sometimes sensitive** data **to and from Earth,** making **them** a[**potential** target for **hackers or malicious** actors](https://www.wired.com/2011/10/hackers-attack-satellites/)**. Also, just because a satellite is in orbit doesn't mean that ground station facilities aren't already a target for cybercriminals.**

**Making space technology infrastructure and communications as safe as possible will require innovative thinking and new partnerships. Recognizing the challenges,** building uponcurrent cybersecurity **efforts and implementing space-oriented regulatory frameworks are the** key **factors for the final frontier.**

**Unique Cybersecurity Challenges Facing Space**

**In many ways, space industry and technology rely on the same infrastructure and carry out many similar functions of our terrestrial digital world. But the main challenges arise from scale, distance and the criticality of systems and equipment functioning. If a hacker were to penetrate earth-based systems and provide false information to a satellite, for instance, it**[**could cause an inter-space collision**](https://www.scientificamerican.com/article/hackers-could-shut-down-satellites-or-turn-them-into-weapons/)**and potentially take out major communications systems globally.**

**Secondly,** more **governments and** privateorg**anization**s **are becoming more**[involvedwith space **projects**](https://hbr.org/2021/02/the-commercial-space-age-is-here)than ever **before. While this lowered barrier to entry increases innovation and discovery, it also** enhances **the number of potential** access points for hackers**. NASA is no longer the main player to be safeguarded.** Malicious actors **now** have **many** more options **to target, from other governments to equipment manufacturers along the supply chain.**

**The** riseof **advanced** tech**nology that can be used for hacking — such as**[**quantum computers**](https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html)**— also** poses **a** significant cybersecurity threat **to the space-based ecosystem. As things like space tourism and militarization grow, so will the focus of** hackers **that** recognize **the potential monetary** value of **ransomware and other** attacks**. Combine this with the severe lack of international cybersecurity cooperation with space technology, and we see a** plethora of hurdles **that need to be overcome in the next few decades.**

**What The Industry Can Do To Make Space Safe**

**The good news is that companies and governments across the board are beginning to take a forward-thinking stance at emerging cybersecurity threats to space equipment, software and communications. Space equipment manufacturers Boeing and Northrup Grumman even hosted a recent webinar discussing**[**how to lower cybersecurity risk**](https://www.flightglobal.com/space/space-industry-worried-that-cyberattacks-could-spread-off-earth/144571.article)**in the design of space-bound equipment.**

**I completely agree with one of the main points made by these two companies:** We needupfront cybersecurity accountability **from the very beginning. This doesn't just go for equipment and hardware, but for operating systems and software that will be used by shuttles, rockets and satellites. It's easy for engineers or globally distributed software developers to take a product- and functionality-first approach, but emphasizing security at all phases of the process is paramount.**

**Finally, the private and public sectors need to collaborate and conduct as many real-world cybersecurity scenarios and exercises before equipment gets sent into orbit. Things like penetration testing and breach response need to be drilled exhaustively. Because once the equipment is sent into space, it becomes extremely difficult to adjust on the fly if gaps crop up.**

**The Role Of Regulatory Bodies And Frameworks**

**Governments and international bodies need to implement global standards for hacker-proofing technology along the entire space supply chain. In addition, there are existing cybersecurity standards that can be tweaked and implemented to make the space industrial ecosystem more secure.**

One such solution that is already being discussed is the [zero trust](https://searchsecurity.techtarget.com/definition/zero-trust-model-zero-trust-network) architecture. With zero trust, devices and equipment are hermetically sealed from a system's access standpoint, limiting unauthorized user access even within an organization. Zero trust reduces operational risk because even if a hacker gains access to systems on earth, gaining additional access is almost impossible due to zero trust architecture's decentralized nature.

**The National Institute of Standards and Technology (NIST) in the United States could also play a pivotal role in pushing standardized cybersecurity frameworks. Just last month, NIST introduced a reference document for how cybersecurity standards may be**[**introduced for commercial satellite operations**](https://csrc.nist.gov/publications/detail/nistir/8270/draft)**. Once NIST receives industry feedback, more concrete recommendations should emerge.**

**With the private sector making even more daring endeavors into orbit, it's undeniable that more of our terrestrial-based economy will be intertwined with space technology and activity. The challenge of safeguarding that infrastructure from hackers is unparalleled, but not impossible. By building on existing private-public partnerships and formulating innovative frameworks that all organizations can adopt globally, we can securely explore the final frontier free from cybercrime.**

#### Cyberattacks on the grid spiral to all-out nuclear conflict.

Klare 19 [Michael; November 2019; Professor emeritus of peace and world security studies at Hampshire College; “*Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation*,” Arms Control Association, <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>]

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.12 The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.13 The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

#### Now Private company satellites launching soon will be the new target.

 Heilweil 21 -- [Rebecca Heilweil](https://www.vox.com/authors/rebecca-heilweil), Rebecca Heilweil is a reporter for Open Sourced, covering emerging technologies, artificial intelligence, and logistics. Her Twitter handle is @rebheilweil., Jul 29, 2021, 7:00am EDT, <https://www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force>, “For hackers, space is the final frontier”, <https://www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force>, //arav

From [offering joyrides for the ultra-rich](https://www.vox.com/recode/22589197/space-travel-tourism-bezos-branson-rockets-blue-origin-virgin-galactic-spacex) to [beaming the internet](https://www.vox.com/recode/22431261/starlink-spacex-elon-musk-fcc-satellite-internet) down to Earth, private space companies are very much open for business.

But some cybersecurity experts say this emerging industry is a giant target for hackers. Amid the surge in commercial rocket launches and a recent spike in [ransomware attacks](https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices), cyberattacks aimed at space systems could disrupt internet access, interfere with the Global Positioning Satellite (GPS) system, and even turn satellites into [weapons](https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932).

“We should be worried about that if we’re worried about people hacking into our navigation systems. We should be worried about that if we care about our electric grid staying online,” Gregory Falco, [a civil engineering professor](https://engineering.jhu.edu/case/faculty/gregory-falco/) at Johns Hopkins University, told Recode. “These space systems enable all of this other critical infrastructure that we have, and we don’t even realize it.”

The United States is not currently facing a large proliferation of cyber attacks in space, but satellites have [been hacked in the past](https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932#:~:text=A%20history%20of%20hacks,panels%20directly%20at%20the%20sun.). For instance, two American satellites used by the US Geological Survey and NASA to monitor climate and terrain were broken into [four times over the course of 2007 and 2008](https://www.reuters.com/article/us-china-usa-satellite/china-key-suspect-in-u-s-satellite-hacks-commission-idUSTRE79R4O320111028). Intrusions and physical attacks on satellites, their connection systems, and the stations on Earth that control them have increased in recent years “probably due to the advancement of the tech being used and the space race,” according to Maher Yamout, a senior security researcher at the Russia-based cybersecurity company Kaspersky.

Back in April, the head of the Space Development Agency, which is a branch of the Department of Defense meant to boost the military’s space capabilities, [warned](https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/) that cyber attacks against satellites posed more of a threat than missiles. The Space Force, which is in charge of [overseeing the military’s satellites](https://www.politico.com/news/2021/02/03/space-force-explained-465799) and GPS, is also boosting [its cybersecurity investments](https://www.fedscoop.com/space-force-cybersecurity-contract-silicon-valley-xage-security/). The military is now preparing for the likelihood that there could be more cyberattacks in space, while the federal government urges the growing number of commercial space companies to [beef up their cybersecurity](https://www.space.com/trump-signs-space-cybersecurity-policy-directive.html), especially as they look to launch more satellites.

SpaceX, Amazon, OneWeb, and [others](https://www.businessinsider.com/spacex-starlink-amazon-oneweb-companies-compete-satellite-internet-2021-4#viasat-3) have already launched hundreds of satellites in order to sell [internet access around the world](https://www.vox.com/recode/2020/9/26/21457530/elon-musk-spacex-starlink-satellite-broadband-amazon-project-kuiper-viasat) — and are planning to send [thousands more](https://www.theverge.com/2021/4/19/22391508/amazon-ula-rocket-launches-internet-satellites-kuiper) into orbit. Those will join the [thousands of satellites](https://www.ucsusa.org/resources/satellite-database) we rely on for everything from telephone service to weather reports to [agricultural research](https://www.nasa.gov/feature/goddard/2021/nasa-at-your-table-the-space-agency-s-surprising-role-in-agriculture). While most people associate satellites with navigation apps, satellites also transmit crucial timing data that’s used to run the electric grid and banking transactions, according to Travis Langster, the vice president of the [space situational awareness startup Comspoc](https://spacenews.com/comspoc-embraces-startup-metality-after-agi-spinoff/).

Our increased reliance on this tech makes the threat of hacking especially worrisome. A hacker could try to access a satellite by targeting a company’s ground systems, and once inside, the attacker could manipulate the communications or controls, download unwanted software, or even tell the satellite to change its course, according to [Iain Boyd](https://www.colorado.edu/aerospace/iain-boyd), the director of the University of Colorado Boulder’s Center for National Security Initiatives.

“It’s the same kind of thing where people are getting into your computer system and behaving badly,” Boyd told Recode. He added that hackers might also attempt to overwhelm a satellite with false signals or impersonate a satellite’s communication — a process called spoofing — to confuse vehicles on Earth’s surface.

These cyberattacks on space systems have been disruptive, but their impact could be catastrophic. For instance, in 2014, US **officials** blamed China for a cyberattackthatforced **the National Oceanic and Atmospheric Administration (**NOAA**)** to[cut off **public** access](https://www.usatoday.com/story/weather/2014/11/12/china-weather-satellite-attack/18915137/)to **imagery** data **from a satellite** network used for weather forecasting. Russia has [reportedly used](https://www.businessinsider.com/gnss-hacking-spoofing-jamming-russians-screwing-with-gps-2019-4) GPS spoofing to confuse ships about their actual locations. And in the future, a worst-case scenario could involve a hacker tricking a satellite into crashing into other space infrastructure, according to William Akoto, an [international politics professor](http://willakoto.com/) at Fordham University, who studies cyber conflict.

“You can’t just walk down to the server room and apply a patch to something that’s in orbit,” explained Matthew Scholl, who leads the computer security division of the Information Technology Laboratory at the National Institute for Standards and Technology (NIST).

To address the impending threat of cyberattacks on space systems, the US military earlier this year transferred [more than 2,000 cybersecurity experts](https://www.fedscoop.com/space-force-cybersecurity-professionals-guardians/) to [the newly formed Space Force](https://www.vox.com/policy-and-politics/2019/12/21/21032757/trump-space-force-signs-ndaa-military-pay-family-leave). The Air Force, meanwhile, has begun [hosting competitions](https://www.fedscoop.com/air-and-space-forces-hack-a-sat-2021-second-year/) encouraging hackers to break into satellites, with the hope of learning more about potential vulnerabilities. But cybersecurity experts warn that the private space industry hasn’t been transparent about how it’s managing security threats.

“From a commercial standpoint, we have to hope that they’re doing something,” said Falco, the Johns Hopkins professor. “But most commercial companies working on satellite systems have given zero details about anything that they have regarding the security of their space systems.”

Some of these companies are currently hiring cybersecurity professionals. Blue Origin, for instance, has been looking for an information system security officer to find vulnerabilities in the company’s systems, while SpaceX is searching for [an information security assurance analyst](https://boards.greenhouse.io/spacex/jobs/5247874002?gh_jid=5247874002) to investigate the physical and cybersecurity of the company’s supply chain.

None of the companies Recode contacted — Virgin Galactic, Blue Origin, OneWeb, and SpaceX — responded to a request for comment about the state of their cybersecurity.

But as commercial space companies try to staff up their security teams, the federal government is also stepping in to help.

Last year, then-President Donald Trump signed an executive order [recommending principles](https://history.nasa.gov/SPD-5.pdf) for cybersecurity and space systems, encouraging private companies to [take precautions](https://history.nasa.gov/SPD-5.pdf) like boosting protections for control systems in their rockets and satellites and deploying antivirus software to protect their ground stations. NIST has [developed](https://csrc.nist.gov/publications/detail/nistir/8270/draft) cybersecurity resources for commercial space operations, including satellites.

In June, Reps. Ted Lieu and Ken Calvert proposed legislation that would classify space as [critical infrastructure](https://lieu.house.gov/media-center/press-releases/reps-lieu-and-calvert-introduce-bill-designate-space-critical) to boost collaboration between private space companies and the government on cybersecurity matters. The Federal Aviation Administration also helped create the Space Information Sharing Analysis Center (Space ISAC), a collaboration that coordinates with companies across the space industry to share information about potential threats and attacks to their cybersecurity.

“Infrastructure that is distributed globally means that there’s a very broad attack surface,” Erin Miller, Space ISAC’s executive director, told Recode. “We need to be building in and designing cybersecurity capabilities into every single one of our space systems.”

For now, that means that ensuring national security and addressing the cybersecurity challenges of the emerging space industry are one and the same. After all, the growing number of attacks against all sorts of private companies, whether they’re [oil pipelines](https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices) or [meat distributors](https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers), makes it clear that when firms don’t protect themselves from hackers, the American public can feel the consequences. As more of the tech that powers our everyday lives heads to space, so should the country’s increased focus on cybersecurity.

#### Independently, GPS loss threatens large economic loss

Graff 18 (Garrett M., former editor of Politico Magazine, editor-in-chief of Washingtonian magazine in Washington, D.C., and instructor at Georgetown University in the Masters in Professional Studies Journalism and Public Relations program, WIRED contributing editor, “The New Arms Race Threatening to Explode in Space,” WIRED, August 26, 2018, https://www.wired.com/story/new-arms-race-threatening-to-explode-in-space)

For decades, America’s satellites had circled Earth at a largely safe remove from the vicissitudes of geopolitics. An informal global moratorium on the testing of anti-satellite weapons had held since 1985; the intervening decades had been a period of post–Cold War peace—and unquestioned American supremacy—high overhead. During those decades, satellites had become linchpins of the American military apparatus and the global economy. By 2007, ships at sea and warplanes in the air had grown reliant on instant satellite communications with ground stations thousands of miles away. Government forecasters relied on weather satellites; intelligence analysts relied on high-­resolution imagery to anticipate and track adversaries the world over. GPS had become perhaps the single most indispensable global system ever designed by humans—the infrastructure upon which the rest of the world’s infrastructure is based. (Fourteen of the 16 infrastructure sectors designated as critical by the Department of Homeland Security, like energy and financial services, rely on GPS for their operation.) Now, Shelton feared, all those satellites overhead had become so many huge, unarmored, billion-dollar sitting ducks. In the decade since China’s first successful anti-satellite missile test, Shelton’s premonition has largely come true: Everything has changed in space. A secretive, pitched arms race has opened up between the US, China, Russia, and, to a lesser extent, North Korea. The object of the race: to devise more and better ways to quickly cripple your adversary’s satellites. After decades of uncontested US supremacy, multinational cooperation, and a diplomatic consensus on reserving space for peaceful uses, military officials have begun referring to Earth’s orbit as a new “warfighting domain.” On the ground, the military is starting to retrain pilots, ship captains, and ground troops in fail-safe forms of navigation that don’t rely on GPS—like celestial navigation. The US military must relearn how to fight “unwired” and defend itself in space. “We knew how to do that, and somehow we forgot,” General John E. Hyten, the head of US Strategic Command, said in 2015. When former director of national intelligence James Clapper left office at the end of the Obama administration, he told me that the increasing sophistication of America’s adversaries in space was one of the top three strategic threats he worried about. Clapper’s successor, Dan Coats, warned last spring that “Russia and China remain committed to developing capabilities to challenge perceived adversaries in space, especially the United States.” Since he took office, President Trump has dropped numerous hints of the warnings he’s evidently getting from military and intelligence leaders. During a spring livestream with astronauts aboard the International Space Station, he alluded, obliquely and without context, to the “tremendous military applications in space.” And he has repeatedly floated the idea of creating a new branch of the armed forces specifically for celestial combat—culminating last week with a speech out-and-out ordering the Joint Chiefs of Staff to begin developing plans for a new “Space Force.” But if space is indeed becoming a war-­fighting domain, it’s important to understand the stakes, not just for America’s strategic standing but for the species. A Russo-Sino-American space war could very well end with a [destroyed] crippled global economy, inoperable infrastructure, and a planet shrouded by the orbiting fragments of pulverized satellites—which, by the way, could hinder us all on Earth until we figured out a way of cleaning them up. In the aftermath of such a conflict, it might be years before we could restore new constellations of satellites to orbit. Preparing for orbital war has fast become a priority of the US military, but the more urgent priority is figuring out how to prevent it. Growing up in Oklahoma City, William Shelton dreamed of becoming a pilot. He got as far as the Air Force Academy before he discovered his eyes weren’t good enough. So instead he became an astronomical engineer. In 1976 he began serving as a launch facility manager at Vandenberg Air Force Base, the military’s oldest space and missile launch base, perched on the California coast north of Santa Barbara. He arrived just as the Air Force was beginning to understand how crucial space would be to its future: The nation’s first early-warning satellites had been put in orbit with the intention of tracking Soviet missile launches, and satellite imagery was becoming increasingly critical to intelligence gathering. Shelton’s poor eyesight, it turned out, had led him to the center of the Air Force’s new frontier. In August 1990, Shelton, then a young lieutenant colonel, took command of the 2nd Space Operations Squadron in Colorado. When he arrived at his post, the Air Force was busy building a new constellation of satellites—launching new ones from Cape Canaveral in Florida every few months to help fill out what he was told would ultimately be a global system aimed at helping the US improve its navigation and increase the precision of its bombs and missiles. This was the new Global Positioning System, and one of Shelton’s first duties at “2Sops” was to build support and enthusiasm for the new effort. To impress visitors (including the brass), he carried around a demo GPS unit that weighed 10 pounds, cost $3,000, and could tell America’s soldiers, sailors, airmen, and Marines exactly where they were on the surface of the planet. The power of the new system that 2Sops ran was proven faster than anyone imagined. The Gulf War caused a rush of final preparations to get GPS ready for battle. Around 2:30 am on January 17, 1991, GPS-equipped helicopters snuck into Iraq, using the technology to guide themselves through the darkened desert and knock out air defense radars. The first bombing campaign of the war had begun. Reporters marveled at precision-­guided bombs zeroing in on their targets and cruise missiles appearing to turn street corners to hit the right buildings. Shelton had a front-row seat to this transformation. As the technology has improved, so has the precision of GPS. The system originally provided accuracy to within 17 yards; with it, you could pinpoint a specific copse of pine trees. Today, if you’re using a smartphone, it can generally locate an object to within five yards—a resolution fine enough to locate a pair of pine trees within that copse. Soon it could be able to zero in on a pine cone: Research from UC Riverside has demonstrated that the latest tech is reliable to within an inch. And research has shown that 1-millimeter accuracy might be eventually possible—which means that the system could locate an individual seed inside that pine cone. Today, troops on the ground use GPS to navigate foreign streets; drone pilots can program a flight plan from thousands of miles away. And because GPS satellites also house America’s detection system for nuclear detonations, we rely on them to tell us if North Korea launches a nuclear weapon, and to tell our missiles and bombs where to find their targets. “When you look at our American way of war, the strategy is largely underpinned by space assets—navigation, early warning, timing,” Shelton says. And that’s just the military. The creators of GPS probably never intended for the system to become the backbone of daily life, but it has. I visited Colorado while reporting this story and tried to keep tabs on everything I did that relied on GPS. There were the obvious navigational moments—my Uber ride to the airport, my American Airlines flight to Denver, my own Google Maps–guided drive in a rental car to Schriever Air Force Base, outside Colorado Springs. But there were also less obvious instances, like the phone calls I made along the way (cellular networks rely on GPS data to keep their stations synchronized), my stop at the ATM (banks use GPS to track deposits and withdrawals), and the fill-up at the gas station (the credit card system also relies on GPS). Moreover, GPS is no longer the world’s sole geolocating mechanism. Russia, China, and the European Union have now all either deployed or begun working on their own full constellations of navigation satellites, ensuring that they won’t have to rely on the US system. It also means that, in the early moments of a war, it’s a fair bet that satellites—the other guy’s satellites—could be among the first targets. During the Cold War, a US army mountain outpost in the Fulda Gap, the shortest route between East and West Germany, served as an early warning trip wire for a Soviet invasion of Europe. If Russian tanks ever made a surprise attack, NATO planners knew that the soldiers there would likely be the first to find out. Today, the members of 2Sops play a similar role. Deep inside the squat, beige, windowless Building 400 at Schriever Air Force Base—the destination I had plugged into Google Maps during my trip to Colorado—10 people at a time remotely operate the heavenly constellation of GPS satellites that guide Tomahawk cruise missiles to their targets, deliver Lyft passengers to their destinations, and help farmers cultivate their crops. They also watch out for any shocks or attacks on the system. The average GPS operators are in their mid-twenties. During one recent shift, the entire Global Positioning System was being operated by two 19-year-old airmen (who, the Air Force emphasizes, are rigorously trained). Their commander, US Air Force lieutenant colonel Peter Norsky, is in his mid-thirties. Together, they watch over the roughly three dozen GPS satellites, troubleshooting the geolocation system and minding the quirks of each orbiting craft—this one’s damaged solar panels, that one’s balky communications links—as if they were remotely tending a stable full of temperamental horses. As integral as GPS is to daily life, the way it actually works is little understood by most people outside of Schriever Air Force Base. Fundamentally, the function of GPS is to provide the globe with a shared clock. GPS satellites allow phone companies to keep their systems in sync, battleships to chart open waters, and ATMs to time-stamp their transactions by triangulating signals from overhead and measuring how long it takes those signals from different satellites to reach a GPS receiver. The system works by making daily calculations, employing Newtonian physics and Einsteinian relativity, to minutely tweak the time broadcast from each GPS satellite as it moves through space—the high-tech version of tuning your grandfather clock to within 100-­billionths of a second. Time is, after all, relative; as of January, the time in space was 18 seconds ahead of Earth’s “Coordinated Universal Time,” since space doesn’t recognize the leap seconds that scientists add to terrestrial time to account for the planet’s slowing rotation. Additionally, the time-keeping device on each satellite gives a subtly different reading, the result of variations in their atomic clocks, which tell time by measuring the precise oscillations of an atom. (Some GPS satellites use rubidium atoms, which are highly accurate day to day; some use cesium, which is more accurate over long stretches.) Any malfunction in the GPS system threatens to plunge the global economy into chaos. Fortunately those glitches are rare, but they’re not unheard of. On January 25, 2016, one of 2Sops’ flight commanders, Captain Aaron Blain, was awoken by a call from work in the middle of the night. User reports from around the country suggested that the system’s precision had “wobbled,” making measurements increasingly inaccurate. Blain raced to Schriever in his Ford pickup and found that the constellation’s timing was off by about 13 microseconds. It was an infinitesimal number—over 25,000 times shorter than the blink of an eye—but for the finely tuned GPS it was a yawning crevice. Left uncorrected, the glitch could have ricocheted through the global economy, corrupting not just driving directions but stock trades too. Alongside the rest of his team, Blain worked through the night, chugging Mountain Dew. It took about six hours to locate the problem—a single corrupted measurement—and then individually reset the affected satellites. (Russia’s GPS equivalent, known as Glonass, has suffered even more serious issues. In 2014 it went down for 10 hours, but many Glonass receivers can also use GPS as a backup, so the systemic chaos was limited.) 2Sops averted a benign catastrophe that night, but it seems increasingly worried about what China and Russia are doing up in the heavens, out of sight. It recently doubled the number of airmen who oversee the satellites, so one team can run the GPS constellation while another trains to face worst-case scenarios—what the Pentagon refers to as “a contested, degraded, and ­operationally limited environment.” That is, a space war. The New Satellite Arms Race Threatening to Explode in Space In one respect, space is already like a war zone: It’s increasingly shot through with flying shrapnel. By some estimates, there are more than 100 million pieces of debris zipping around in Earth’s orbit. China’s 2007 anti-satellite test is estimated to have created some 150,000 new ones, many too small to be tracked. In 2013, some of those fragments hit a Russian satellite—threatening to add still more debris to the orbital mix. And as commercial ventures like SpaceX and Blue Origin ramp up their space tourism plans, Earth’s orbit is about to get even more crowded with both junk and spacecraft. Scientists say there could be a point at which the density of objects spinning around the planet reaches a threshold—called the Kessler effect—that triggers a runaway cascade of collisions: an entire orbit, in other words, set to Blend. Another tricky thing about space debris is that sometimes it isn’t just debris. A US military program called the Space Surveillance Network carefully tracks and monitors every piece of space junk that’s larger than a softball. That currently amounts to some 20,000 objects—everything from old satellite parts to discarded rocket boosters to a pair of pliers lost during an astronaut’s spacewalk. In 2014, a piece of presumptive space junk known to the US military as Object 2014-28E began to behave strangely. The object, known to be of Russian origin, started to perform complicated maneuvers. “That’s concerning—when you see something that appears to be debris come to life,” Shelton says. Object 2014-28E was, in fact, an autonomous spacecraft capable of veering off course and sidling up to other objects, including American commercial communications satellites. In the years since, Object 2014-28E has been joined by similar space objects of Russian provenance. Analysts fear that they might mark the revival of a Russian program known as Satellite Killer, which was shut down after the Cold War. But it’s difficult, even for US government analysts, to know for certain whether that fear is warranted. The secrecy that surrounds nearly everything space-related makes it hard to assess any adversary’s capabilities. Discerning intentions is especially difficult. “If I wanted to build a satellite that looked very different from its actual mission, that’s not hard to do,” Shelton says. A satellite that maneuvers close to another could be doing a repair job or squaring up for an attack—and it might use the same tools for both. “Small satellites with small grappling arms—they have both military and nonmilitary uses,” says Dean Cheng, who studies China’s military capabilities at the Heritage Foundation. “If I manipulate a satellite’s bits and pieces, I can also rip something out.” The US has also been secretive in developing what may or may not be weapons in space. Last May, the Air Force announced that an unmanned space-shuttle-like vehicle that appears to be classified had completed 718 days orbiting Earth, doing who knows what. As of this May, another OTV was circling the globe, more than 200 days into its mostly classified mission. Todd Harrison, director of the Aerospace Security Project at the Center for Strategic and International Studies in Washington, explains that there are effectively four categories of space weapons: kinetic (aimed at destroying a satellite), nonkinetic (aimed at disabling a satellite without touching it), electromagnetic (aimed at interfering with a satellite’s signals), and cyber (aimed at corrupting the data sent to a satellite). The US tested its own anti-satellite missile in 2008, shooting down an errant spy satellite as it was falling out of orbit. Russia has repeatedly flight-tested a so-called direct ascent weapon, the PL-19 Nudol ballistic missile, which could strike objects in orbit, although it hasn’t conducted a live attack on an orbiting satellite. And in the decade since China shot down its weather satellite in 2007, Beijing has launched multiple ballistic missile tests that extended into orbit. In addition, a trio of Chinese satellites have practiced “close-proximity operations,” similar to those performed by the Russian Object 2014-28E. Anti-satellite weapons form just one part of what China calls shashoujian, or “assassin’s mace” systems, which can be used at the start of an attack to achieve a surprise, decisive advantage over a technologically superior foe. There’s also the growing challenge of cyberattacks on satellites: Chinese hackers have reportedly infiltrated the US weather satellite system, and a Romanian hacker announced that he had accessed the server of one of NASA’s space flight centers. In the past decade, at least two nonmilitary US satellite systems have experienced brief, unattributed glitches tied to hacking attacks. Some actors have begun to exploit the fragility not of satellites themselves, but of the signals they broadcast. By the time the radio signals from a GPS satellite reach Earth from thousands of miles up, they can be easily overridden by a stronger signal broadcast on the same frequency. Simple GPS jammers sell online for $119, but they have a short reach. Militaries appear to be acquiring much more powerful jamming technologies. In 2016, roughly 1,000 planes and 700 vessels at sea reportedly experienced problems with their GPS signals near North Korea, which is believed to have purchased Russian jammers that can be mounted on trucks. Those devices have an effective radius of 30 to 60 miles. The US seems to possess similar technology; a test that went awry near a Navy base in San Diego in 2007 knocked out GPS signals to cell phone network operators for at least two hours. More troubling than simple jamming, though, is the rise of “spoofing,” which overrides correct GPS data with a more powerful localized signal that delivers false information to a receiver. In 2013 a team of researchers from the University of Texas at Austin successfully led astray an $80 million yacht in the Mediterranean, overpowering its GPS receivers and sending it onto a new course. The dirty truth about spoofing is that secure channels are no defense against it. “Even our encrypted military GPS receivers can be spoofed,” Harrison says. Shelton, who retired in 2014 after 38 years in the Air Force, lives not far from 2Sops in Colorado; these days he chairs an educational and advocacy nonprofit called the Space Foundation. He still expends a lot of energy worrying about what is happening in the heavens. “We as a nation have been too slow to respond to this threat,” he says. He’s particularly troubled by the failure of the US to procure new space systems. Some GPS satellites are older than the people running them. “Our systems are archaic,” Shelton says. “Because space assets are so expensive, we deploy ‘just enough’; there’s no backup or excess capability.” (The Air Force noted that the GPS constellation consists of more than 30 satellites, which provides some redundancy.) China, by contrast, is investing heavily in its space program, seeing it as a symbol of its growing prominence. As soon as this year, it could land a craft on the never-before-touched far side of the moon. And China’s global navigation satellite system, known as BeiDou, has some capabilities that outmatch even the United States’ GPS. In 2015, China created a new space-­focused military service, known as the People’s Liberation Army Strategic Support Force. Meanwhile, the US relies entirely on Russian rockets to get its astronauts to the Space Station (although NASA has awarded contracts to Boeing and SpaceX to fix that). As Cheng says, “Today China is one of two countries that can put a person into space—and the other country isn’t the United States.” Many of America’s space warriors, as they call themselves, share Shelton’s sense that the US isn’t responding nearly quickly enough to the threat of orbital war. “We needed to be marching faster,” says Deborah Lee James, who served as President Obama’s secretary of the Air Force. “Why aren’t there more space and cyber officers at the top of the Air Force?” Addressing these issues, as James’ question suggests, is not just about throwing money at the space-industrial complex. It involves organizational changes too. The Air Force is building what it calls the nation’s first Space Mission Force, made up of airmen trained to respond to the demands of an orbital war. On the same base as the 2Sops command center, the military has established the National Space Defense Center, which puts representatives from various military and intelligence offices focused on space under a single roof. And the defense authorization bill is full of upgrades to the Air Force’s space-­fighting capabilities, including the creation of an additional Air Force unit responsible for space warfighting operations. Not content to tinker with the Air Force, a growing number of people in Washington—including the commander in chief—have to come to favor creating an entire new military branch dedicated to space operations. In May, during a ceremony honoring West Point’s football team, President Trump told his audience, “We’re getting very big in space, both militarily and for other reasons, and we are seriously thinking of the Space Force.” The comment sounded to many listeners like yet another oddball Trumpian tangent. But then, after reportedly meeting resistance from the Air Force, Trump escalated. At a mid-June meeting of the newly constituted US Space Council, he announced—much to the surprise of his own advisors and the military itself—that he was ordering the Pentagon to move forward. As he said, “I’m hereby directing the Department of Defense and Pentagon to immediately begin the process necessary to establish a Space Force as the sixth branch of the Armed Forces. That’s a big statement. We are going to have the Air Force and we are going to have the Space Force—separate but equal. It’s going to be something.” The Space Force is, of course, not a fait accompli. Any military reorganization has to be approved by Congress—which is not necessarily an easy path. (Last year, a bill that included the creation of just such a new branch of the military passed the US House of Representatives, but that provision was taken out of the Senate version.) And the establishment of a new branch of the military involves a vast set of logistical and structural questions. Yet Trump’s push may speed up a natural evolution toward an independent space branch by years, if not a decade. Space, the president said, was “going to be important monetarily and militarily. We don’t want China and Russia and other countries leading us. We’ve always led.” But where—and to what—are we leading? Part of the challenge in figuring out how to think about space conflict is the sheer complexity of the orbital environment—an arena that has long belonged to nation-states, but that is increasingly becoming a domain of commerce and tourism. How do countries protect their interests up above—and down here? Right now, countries appear to be racing to build their military capabilities—but an arms race isn’t the only answer. The last time an arms race appeared poised to overtake space, the world’s superpowers banded together to sign the 1967 Outer Space Treaty, which banned weapons of mass destruction in space and held that “the moon and other celestial bodies” should be reserved for peaceful purposes. The Outer Space Treaty is still in force, but it is by now full of holes. Legal scholars had a hard time proving that China’s 2007 anti-­satellite test, for instance, violated the agreement. That’s because the missile that China fired was not technically addressed in the 50-year-old treaty. Part of what makes space such volatile terrain right now is that it’s hard even to apply the existing laws of war to it. No country can claim sovereignty in orbit, and it’s impossible to occupy territory there. So what counts as an act of territorial aggression? What qualifies as a proportional response? It’s even difficult to say, with certainty, what the physics of war in space will look like. We don’t well understand, for instance, how a kinetic attack on a satellite constellation might spill over into a spiraling Kessler effect. Humans have “millennia of experience in blowing up things on land,” says Laurie Blank, a law professor at Emory University and a specialist in the laws of armed conflict. “We’re still learning the consequences of all these things in space.”

## 2 - Conflicts

#### Unchecked Commercial Appropriation causes Space Conflicts.

Perez 21 Veronica Delgado-Perez. 12/14/21. Argument | The Commercialization of Space Risks Launching a Militarized Space Race. <https://www.theintlscholar.com/periodical/12/14/2020/analysis-commercialization-space-risk-international-law-military-space-race> [Veronica Delgado-Perez is a Staff Writer at The International Scholar.] // CVHS SR

Fundamentals of the Final Frontier It is a geopolitical imperative to determine what, if any, commercial activities and use of extraterrestrial resources are permitted within the confines of international law. Without clear-cut agreements on what activity is recognized by international law, the world will undoubtedly see states push the boundaries ever further in an attempt to gain the edge over geopolitical competitors — even more-so in an era of renewed great power competition. Yet to date, there exists no comprehensive treaty or legal reference to commercial activity in space. However, this should come as no surprise. It has only been since the turn of the century that technology and markets have progressed to the point where commercial space exploration and exploitation has become possible. Only recently have experts and analysts of geopolitics and international law begun to seriously examine questions surrounding the legal framework that would govern extraterrestrial resource-mining and other commercial activities. In the last decade, the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) dealt with commercial aspects in outer space. In one of their last reports, the Committee expressed that the era of the commercial utilization of outer space’s resources is intrinsically linked to the escalation of international competition over resources, which could threaten international peace and security. By encouraging the international community to engage in outer space’s activities for the benefit of humankind as a whole, “some delegations” have expressed that states should avoid the promotion of laws and regulations related to the commercialization of outer space, arguing that it should be considered the heritage of all humanity. In that regard, states must then ensure that domestic law on the use of outer space complies with international space law, which means that states should respect the principles outlined in the Outer Space Treaty and ensure that national regulations do not contravene international provisions. Even though the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies (which entered into force in 1967), refers to the exploration and use of outer space, it does not address questions of a commercial nature, which compromises the ability of states and international actors to address new challenges to extraterrestrial activities. In several provisions, the treaty highlights that these activities may be carried out for peaceful purposes and the benefit of all people, reaffirming that outer space is not subject to national appropriation. Were outer space not considered a global commons, that would imply that the resources and results of commercial exploration may fall within the jurisdiction of a country. It is thus incumbent upon Washington — and its commercial enterprises — to demonstrate how American commercial exploration of space benefits other countries and complies with international space law, or otherwise to adhere to the spirit of past treaties which emphasize the impartiality of outer space until such time as the law is clarified. International Law is Adrift in Space The potential benefits of commercial space exploration cannot be ignored. From an economic standpoint, the space industry would generate a significant economic boon for both states and private companies, due to the abundance and variety of resources — particularly scarce minerals that are difficult to extract on Earth. As one example of the vastness of resources held in outer space, one asteroid has the potential to contain more than the total supply of platinum extracted throughout the history of mankind. It may very well open the door to an advanced era of space navigation, building extraterrestrial infrastructure that facilitates the exploration and use of space’s resources, and extra-planetary human habitation. Inevitably, there are significant drawbacks to the commercialization of space exploration. These can vary, for instance, from the commercial dominance of space’s natural resources only by those states with the technical and financial capital to support space missions, to geopolitical competition over extraterrestrial resources that threatens world peace and security, to the potential for the monopolization of extraterrestrial resources by states and private companies. As was the case during the Cold War, the Soviet Union and the United States began a Space Race in which they struggled to achieve supremacy in space exploration and domination of science. Today, the number of space powers has increased thanks to continual advancements in flight, combustion, and fueling technologies. In the three decades since the end of the Cold War, technologically advanced countries like China, Japan, and France which previously had no space program have successfully navigated to the top tier of space-faring agencies and programs. In 2018, the U.S. allocated $41 billion to space programs, followed by China at $5.8 billion, and Russia at $3.1 billion. Collectively, the three major space powers control almost 65% of the global industry, showing space powers are monopolizing space and reinforcing the inequality gap between states that do not have sufficient economic and technological capacity to invest. With new actors on the game stage, conflicts of interest may arise. There is a risk that each actor adopts a kind of short-term Realist approach to space policy — one which is driven by self-interest in reaping the greatest benefits of extraterrestrial exploration and commercialization while controlling access to others. If unmitigated, states may choose to militarize outer space to gain a strategic edge over competitors and adversaries. This process has already begun. Under the Trump administration, the Pentagon established the U.S. Space Force as a new branch of the Armed Forces to protect the country and allied interests in space. Already, Delta 4 — one of the U.S. Space Force’s missions — conducts strategic and theater missile warnings, manages weapon systems, and provides information to missile defense forces. The measure shows that for the U.S., outer space is not only a domain of scientific exploration but has the potential to become increasingly securitized. With the impending expiration of the Strategic Arms Reduction Treaty (START) between the U.S. and Russia on February 5, 2021, a number of security dilemmas could arise. If the world’s two largest nuclear powers do not edge toward extending the treaty, Washington and Moscow risk returning to the era of unrestricted expansion of launch platforms and strategically-deployed nuclear warheads — potentially with the aid of military infrastructure in space. Although President-elect Biden has expressed his interest in negotiating an extension of New START, how Moscow and Washington might proceed remains an open question. Bilateral progress towards a new arms-control regime would require establishing limits on the number and range of long- and mid-range missiles, establishing measures to limit the expansion of traditional missile deployment to space, and banning the deployment of nuclear weapons and weapons of mass destruction in outer space. More than the risk of the securitization of space, state, and private actors could begin to claim exclusive legal rights over the resources they discover. Indeed, the U.S. Commercial Space Launch Competitiveness Act, which came into force in 2015, expressly recognizes the right of U.S. Citizens to possess, own, transport, use, and sell space resources. By this means, domestic law already acknowledges the legal claim to property by individuals, which is prohibited by international law. Under the Outer Space Treaty, states renounced any traditional form of acquisition of territories and agreed not to foray unilaterally into space to extend their national policies on Earth or to exercise any kind of sovereignty over celestial bodies or resources. The absence of a modern international treaty that addresses these issues should be received with grave concern, as there is significant potential for risk to become reality. Existing UN treaties lack the technological context and foresight to address legal questions regarding the potential for commercial exploration and exploitation of outer space or its resources. During the sixties and seventies, when international instruments like the Outer Space treaty were conceived, the principal aim of states was to support and expand the scale of the state’s national capacity for operation in space and the development of legal instruments to guide state’s international cooperation in the peaceful exploration of outer space. These instruments were never designed to respond to commercial questions over mining or tourism in space, private investment in space activities, or the emergence of non-state private enterprises operating in space. As a result, private enterprises operating in the vacuum of space also float in an unstable legal vacuum which threatens to implode in geopolitical competition. Beyond Stars and States In an increasingly commercial outer space in which there are no set limits to the exploitation of resources or claim to property, states and private companies will inevitably pursue the development of new extraterrestrial industries to suit their geoeconomic interests. If unchecked, the legal protection of outer space as a domain of exploration for the benefit of all humanity would functionally fail. To protect investments and profit from national space industries, states would likely resort to military force to protect and secure private assets. Over time, space would ultimately become a fourth border domain over which states claim, exercise, and defend sovereignty — including through the use of force. The challenge is thus to prevent the circumstances that could lead to space-borne conflict before it is made possible. Notwithstanding, commercial exploration and the use of natural resources need not lead to predation among actors involved in space. The potential rewards — both technological and environmental — that could come from investment in the harvesting of resources in space are immense. International law cannot afford to wait for the security dilemma posed by commercial activity in space to manifest before addressing it but must anticipate and proactively adopt measures to address future issues that govern extraterrestrial human activity. The only remedy for the lack of legal governance over commercial activity in space is the creation of new international laws through a comprehensive international treaty on commercial operations in space. The new treaty must expressly regulate commercial activities by states and private companies, enshrine an international liability and compensation regime covering damages caused with workable sanction provisions, and reinforce norms that restrict any militarization of outer space. The international community should focus its efforts on establishing a legal regime, with mandatory provisions (rather than non-binding resolutions, observations, commentaries, and conclusions) which generate both international responsibility and provide enforceable sanctions in the event of violations. The effort should be borne out by expanding the scope and strengthening the oversight powers of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), rather than creating a new organ with redundant bureaucracy. Beyond the tasks of encouraging space research programs, studying space activities, and addressing legal questions, COPUOS should be granted the necessary powers to perform control and oversight monitoring functions. Experience has taught the international community that cooperative arrangements between states and international organizations can prevent competition for resources from escalating to kinetic conflict. Through cooperation, there is a chance to preserve extraterrestrial resources for future generations, secure an equitable allocation of resources and benefits with a mind to each country’s specific needs, and prevent the expansion of geopolitical conflict to the domain of space. Space powers must recognize the value in partnering with other states to advance the development of space programs more efficiently. It should be clear now that all nations could reap the benefits of collective action, exploration, and commercialization of resources from beyond Earth’s atmosphere while preventing a drawn-out international conflict to the final frontier. The will of states not to jeopardize the fundamental basis of international law must be reflected in coordination and surveillance efforts to ensure that the advantages derived from space exploration allow humanity to continue evolving.

#### Space War cause Nuclear War.

Gallagher 15 “Antisatellite warfare without nuclear risk: A mirage” <http://thebulletin.org/space-weapons-and-risk-nuclear-exchanges8346> (interim director of the Center for International and Security Studies in Maryland, previous Executive Director of the Clinton Administration’s CTBT Treaty Committee, an arms control specialist at the State Dept., and a faculty member at Wesleyan)//Elmer

In recent decades, however, as space-based reconnaissance, communication, and targeting capabilities have become integral elements of modern military operations, strategists and policy makers have explored whether carrying out antisatellite attacks could confer major military advantages without increasing the risk of nuclear war. In theory, the answer might be yes. In practice, it is almost certainly no. Hyping threats. No country has ever deliberately and destructively attacked a satellite belonging to another country (though nations have sometimes interfered with satellites' radio transmissions). But the United States, Russia, and China have all tested advanced kinetic antisatellite weapons, and the United States has demonstrated that it can modify a missile-defense interceptor for use in antisatellite mode. Any nation that can launch nuclear weapons on medium-range ballistic missiles has the latent capability to attack satellites in low Earth orbit. Because the United States depends heavily on space for its terrestrial military superiority, some US strategists have predicted that potential adversaries will try to neutralize US advantages by attacking satellites. They have also recommended that the US military do everything it can to protect its own space assets while maintaining a capability to disable or destroy satellites that adversaries use for intelligence, communication, navigation, or targeting. Analysis of this sort often exaggerates both potential adversaries’ ability to destroy US space assets and the military advantages that either side would gain from antisatellite attacks. Nonetheless, some observers are once again advancing worst-case scenarios to support arguments for offensive counterspace capabilities. In some other countries, interest in space warfare may be increasing because of these arguments. If any nation, for whatever reason, launched an attack on a second nation's satellites, nuclear retaliation against terrestrial targets would be an irrational response. But powerful countries do sometimes respond irrationally when attacked. Moreover, disproportionate retaliation following a deliberate antisatellite attack is not the only way in which antisatellite weapons could contribute to nuclear war. It is not even the likeliest way. As was clearly understood by the countries that negotiated the Outer Space Treaty, crisis management would become more difficult, and the risk of inadvertent deterrence failure would increase, if satellites used for reconnaissance and communication were disabled or destroyed. But even if the norm against attacking another country’s satellites is never broken, developing and testing antisatellite weapons still increase the risk of nuclear war. If, for instance, US military leaders became seriously concerned that China or Russia were preparing an antisatellite attack, pressure could build for a pre-emptive attack against Chinese or Russian strategic forces. Should a satellite be struck by a piece of space debris during a crisis or a low-level terrestrial conflict, leaders might mistakenly assume that a space war had begun and retaliate before they knew what had actually happened. Such scenarios may seem improbable, but they are no more implausible than the scenarios that are used to justify the development and use of antisatellite weapons.

## 3- India

#### Private space appropriation discourages cooperation in space and triggers militarization

Claire Finkelstein, 2018, Claire Finkelstein is the Algernon Biddle Professor of Law and Professor of Philosophy, and director of the Center for Ethics and the Rule of Law at the University of Pennsylvania. Mark Nevitt is the Sharswood Fellow at University of Pennsylvania Law School. Trump risks leading the world into a space arms race thehill.com/opinion/national-security/402640-trump-risks-leading-the-world-into-a-space-arms-race.

**A motive might be sought in the potentially profitable** commercial ventures **in outer space, such as asteroid mining**, for which the president has voiced support. The president may imagine that a Space Force is the way to gain control over and protect the valuable assets involved. **However, this way of thinking is** risky**.**

Currently**, outer space is “militarized” but not yet “weaponized.” Militaries around the globe make heavy use of satellite technology** — such as surveillance and global positioning **— but so far they have refrained from placing weapons on satellites in outer space or using them directly for warfighting**. The administration’s **ad hoc push for space dominance risks upsetting a delicate balance: space now hovers precariously at the brink of weaponization and it would take only one major country defecting from the current system of peaceful self-constraint to drive us into a major arms race in outer space.**

**The current peaceful equipoise is largely because of the remarkable success of the 1967** Outer Space Treaty**, an international agreement with which more than 100 signatory countries have been compliant. Under this treaty, space is considered a “province of mankind” that is not owned or controlled by any single nation**. **Article IV of the treaty provides that celestial bodies be used “for peaceful purposes only,” and objects in orbit carrying nuclear or weapons of** mass destruction are strictly prohibited**. Article II of the treaty makes clear that outer space “is not subject to national appropriation by claim of sovereignty.”**

Seeking military dominance in space, coupled with encouraging appropriation of space for commercial purposes**, puts us at loggerheads with our traditional allies,** upsets stable **and well-established treaty** obligations**, and** moves the world closer to a highly dangerous arms race **in outer space.**

It is important to distinguish the idea of a Space Force from the pursuit of military and economic superiority in space. There may not be anything intrinsically wrong with the idea of a Space Force, or in somewhat more moderate form, a “Space Corps,” similar to the Marine Corps, or a “Space Command,” as Congress has called for in the 2019 National Defense Authorization Act, which President Trump signed into law last Monday. The merits of a stand-alone space unit depend on how its mission is conceived and how it fits into broader U.S. policy objectives in outer space, but a thoughtful, coherent and measured inter-agency space policy has yet to emerge. The danger comes from the aim of dominance, not the particular way in which dominance is sought. In addition to potentially touching off an arms race of planetary proportions, there could be an economic race over space resources, comparable to the emerging fight over the Arctic or over deep-sea fishing rights. The combination of space weaponization and space commercialization easily could thrust us into a new cold war (or worse). A hot war in outer space is unthinkable, and we cannot let it occur.

#### Private Sector supports militarism in space

Shamas & Holden**, 20**19, Victor Shamas &, Oslo Metropolitan University, Work Research Institute (AFI), Oslo, Norway; Thomas Holden, Independent scholar, Oslo, Norway, 2019, Palgrave Communications, One giant leap for capitalistkind: private enterprise in outer space, https://www.nature.com/articles/s41599-019-0218-9

**One** novel element **in this phase** of cap**italism-**in-space is **the inter**relationshipbetween **Silicon Valley, NewSpace, and the** state (see, e.g., Vance, 2015). **Silicon Valley’s capitalist class,** including Amazon’s Jeff Bezos, **play an outsize role in NewSpace. Behind and** aroundthese **figures, however,** remains the state**—**through **its weighty fiscal, regulatory,** military**, and symbolic investment. s.Footnote**15 To take but one example: In June 2018, SpaceX won **a** $130mil**lion** contractwith **the U.S. Air Force** to launch **an ‘Air Force Space Command'** sat**ellite** on**board a** Falcon Heavy rocket(Erwin, 2018).

#### Indian space mil causes regional war and arms races

Khan & Imam 19 [Sameer Ali Khan a and Irteza Imamb a Center for International Strategic Studies (CISS), Islamabad, Pakistan; b South Asian Strategic Stability Institute (SASSI), Islamabad, Pakistan. Astropolitics. "Outer Space and Strategic Stability in South Asia." https://www.tandfonline.com/doi/full/10.1080/14777622.2019.1578936]

A forthcoming study identifies various differences between the Cold War and South Asian context of strategic and deterrence stability and determines that key determinants of stability in the South Asian region include: “(1) absence of surprises from the adversary; (2) non-existence of ‘use it or lose it’ dynamics; and (3) no technological or political developments creating temptations for one side to go first.” 23 Indian developments in the areas of BMD, ASAT, and outer space auger negatively in all the three domains mentioned here. An increased capacity for identification of enemy targets is likely to create temptation for a surprise first strike by India. This is likely to force Pakistan to adopt either higher alert levels or expand its nuclear arsenal.24 Likewise, if India adopts a first-strike strategy facilitated by advanced spacebased capabilities, a use-it-or-lose-it dilemma is created for Pakistan. Further, availability of such offensive capabilities can potentially favor Indian adoption of an offensive political outlook and military doctrines. Pakistan, on the other hand, is likely to remain dependent on its nuclear deterrent until it has developed its own adequate space-based capabilities.

#### Keeping space weapon free solves South Asian crisis stability

Arif 19 [Misbah Arif Lecturer in the Department of Defence and Diplomatic Studies at Fatima Jinnah Women University, Rawalpindi, Pakistan. Rawalpindi, Pakistan. "Strategic Landscape of South Asia and Prevention of Arms Race in Outer Space." https://www.tandfonline.com/doi/abs/10.1080/14777622.2019.1578934?journalCode=fast20]

South Asia is in part volatile because of the historical rivalry between India and Pakistan. After non-conventional and conventional military buildups in the past, an arms race in the domain of outer space is now a possibility. Space is an advantageous frontier for military uses. In this context, the consensus in international law defines space as a global commons to be used for peaceful purposes. Nonetheless, space powers, including India, engage in space militarization, which can lead to the weaponization of space. India is motivated in this regard by aspirations of regional hegemony and to balance its capabilities with respect to China in an effort to counter China’s increasing influence in South Asia. These developments posit adverse effects on the strategic equation in South Asia, leading to strategic instability, and can undermine nuclear deterrence and bring about a South Asian arms race in space. Moreover, the security dilemma in South Asia has prompted defensive and offensive reactions from rival states in the region, exacerbating repercussions on the South Asian strategic landscape. Analysis of the issues suggests that keeping space free from weaponization can alleviate strategic instability in South Asia.