# Cyber - Negative

## Cyber War Advantage impact defense

### No Escalation

#### No risk of nuclear escalation from cyber attacks

Lonergan & Yarhi-Milo 22 [Erica, senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace, Keren, Professor of War and Peace Studies at Columbia Univ, “CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS,” 04/21/22, <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>, accessed 07/09/22, GDI-JCR]

But all of this focus on cyber operations causing nuclear escalation may be misplaced and, more importantly, distract policymakers from the dangers of a more plausible scenario: the use of ambiguous cyber signals during nuclear crises. Specifically, the nature of cyber operations reduces their inherent escalatory potential, particularly when compared to other ways a state could attack an adversary’s nuclear forces or command, control, and communications systems, like a direct counterforce strike or employing anti-satellite weapons. But their misuse as a signaling tool could do more harm than good. First, successfully conducting cyber operations against strategic targets, like nuclear systems, is harder than the conventional wisdom might suggest. It requires a means of gaining access to a particular system and developing an exploit to cause a desired effect — and then maintaining persistent (and stealthy) access to be able to conduct an offensive operation at the desired time. Moreover, the overall outcome may be unpredictable and net less-than-desirable results. Second, even if a state is able to conduct these kinds of operations, they typically prefer to do so in secret — and this mitigates some escalation concerns. That’s because, to cause an escalatory response, a state like Russia would have to uncover a cyber operation during a particular time period — such as while the Ukraine conflict is unfolding. For example, Russia would have to detect a cyber operation against a nuclear command and control system to cause Putin to perceive a “window of vulnerability,” perhaps assessing that it is part of a U.S. or NATO counterforce strategy to disable Russia’s ability to retaliate with nuclear weapons. But the likelihood of these circumstances arising is low because — unless a state is trying to signal with a cyber capability — it will try to keep these kinds of sensitive operations secret. Therefore, the chances of such an operation being discovered at a particular time period are relatively small. Finally, even if, hypothetically, Russia was to discover a cyber operation taking place, the likelihood of it leading to escalation is low. This is due to the virtual nature of cyber “weapons” — they rarely cause destruction in the physical world, let alone permanent damage. For example, even Russia’s 2015 cyber attack against Ukraine’s power grid, an important example of a strategic cyber attack against civilian critical infrastructure, only resulted in service disruptions for a few hours. During the current conflict, Russia-linked actors have so far been stymied in using cyber operations for strategic impact, such as the failed cyber attack by the group Sandworm against Ukraine’s power grid. Taken together, this reasoning suggests that, in practice, cyber operations may not rise to a level that would cause a state like Russia to actually fear the integrity of its nuclear command, control, and communications systems, creating few reasons to escalate to the level of nuclear employment.

## GNSS Impact Defense

### System Resilient

#### The impact is wildly overstated – GPS is safe and resilient

Davenport & Ganske 19 [Brandon, Combat Operations Division Space Cell Chief at the US Air Force Central Command Combined Air and Space Operations Center, Rich, editor at the Strategy Bridge & founding member of the Military Writers Guild, “‘Recalculating Route’: A Realistic Risk Assessment for GPS,” 3/11/19, *War on the Rocks*, <https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/>, 07/09/22, GDI-JCR]

Several recent articles have predicted calamity in the future relevance of space systems like the Global Positioning System (GPS). This growing trend includes articles with ominous headlines including, “Spoof, Jam, Destroy: Why We Need a Backup for GPS,” “The GPS Wars Are Here,” and “The Death of Precision in Warfare.” Each of these articles highlights vulnerabilities of GPS without offering realistic context or caveat to properly scope or provide scale to the actual threat. In fact, while friction exists in any endeavor of warfare, GPS remains resilient in the face of vulnerabilities, and — outside of the most total of wars — will remain so. GPS skeptics sometimes mistakenly conflate technology that is GPS-aided and that which is GPS-dependent. Moreover, by failing to appropriately caveat their claims, these articles suggest GPS’s vulnerabilities to jamming, spoofing, widespread disruption, and even destruction are unlimited. These articles also make little or no distinction between vulnerabilities of civilian systems and military systems, often concluding GPS should be replaced outright with a supposedly more resilient but unexplained substitute that would suffer from the same nuisances. A more realistic characterization should clarify just how vastly different the risks are between civilian and military GPS use and take more seriously the numerous unmentioned advantages in retaining GPS. We spent nearly a decade as U.S. Air Force weapons officers and have instructed, developed tests, tactics, and realistic exercises and informed the technical designs of future planning tools and weapon systems. The analyses offered by skeptics breaks drastically from our technical understanding and experience in examining threats against GPS. We seek to buck the trend of overwhelming presumption of danger to GPS and other space capabilities that overstates vulnerability while treating the technical challenge of threats too vaguely. We also reject the conclusion that GPS is too fragile to be reliable in warfare regardless of its scale or scope. Rather than sweeping claims of impending disaster, in this article we assert a more measured understanding of GPS’s vulnerabilities for civilian and military users, and a more reasonable expectation for how both sets of users can respond to denial attempts and disruption. After that, we proceed to the broader geopolitical relevance of GPS, responding to suggestions of these systems’ vulnerability to widespread kinetic and cyber attack by emphasizing just how important the system is to vital national interests. Finally, we consider whether deterrence safeguards GPS capabilities against extensive disruption or even complete destruction.

#### GPS is safe – disruptive attacks are implausible

Davenport & Ganske 19 [Brandon, Combat Operations Division Space Cell Chief at the US Air Force Central Command Combined Air and Space Operations Center, Rich, editor at the Strategy Bridge & founding member of the Military Writers Guild, “‘Recalculating Route’: A Realistic Risk Assessment for GPS,” 3/11/19, *War on the Rocks*, <https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/>, 07/09/22, GDI-JCR]

Worst Case Scenarios: Broad Disruption of GPS via Kinetic or Cyber Attack Now consider the possibility of even worse disruption to GPS than mere spoofing or jamming. One GPS skeptic suggests, “The 24 [sic] satellites that keep GPS services running in the US aren’t especially secure; they’re vulnerable to screw-ups, or attacks of the cyber or corporeal kind.” The idea here is that while jamming or spoofing cannot obtain widespread effect, theoretical attacks against the ground control system, the software, or even the satellites could still have a disastrous global impact. While these threats are worthy of consideration, they are less plausible than assumed. How would a widespread attack against military GPS systems play out? To completely deny GPS, an attacker would be forced to physically attack its critical command and control nodes or render inoperable most of the satellites. Such suggestions of widespread destruction or disruption almost always misrepresent the reality of how GPS functions as a system. Given the semi-autonomous nature of GPS and its gradual failure design feature, the effects of any ground site attack would be realized only after a protracted lapse of time. Given the location of GPS satellites in medium Earth orbit and the realities of accumulated physical attack on individual satellites, any kinetic attack against the system as a whole would likely evolve over a multi-day period. An adversary could launch several co-orbital systems to disrupt or destroy the constellation of GPS satellites, but this would either require numerous launches or conspicuous orbital transfers and would likely be detected given the extent of space situational awareness available to all the major world powers. Cyber risks to the control of GPS are clearly on the minds of U.S. defense officials and have resulted in the enactment of stringent protections. Here again, however, GPS skeptics overstate the scope of the threat. This concern may be, in part, the result of popular plot presumptions more akin to a novelized portrayal of the next world war than to real-world threats. Against the threat of cyber attack, a defender has the option to harden systems against access or use the system in a manner mitigating the threat. Regarding GPS, the U.S. military has opted to do both. While imprudent to claim a 100-percent secure system, the Department of Defense is working to make GPS as hardened a target as possible. Cyber attacks seeking to control the satellites themselves would require individually updating each of the satellites within the constellation with malicious code. Any upload to the whole system would take significant time, at least tens of hours, due to how contact is made with each satellite in their medium Earth orbits. In the meantime, the overwhelming scrutiny the GPS signal is under from U.S. military and civil monitoring stations, as well as from commercial augmentation services, surveyors, academic institutions, and others, could note any degradation or oddity in near real-time long before any aggressor attack could create widespread impact. And when a cyber attack is noted on one satellite, the control center stops subsequent contacts with other GPS satellites — precluding the spread of malicious code through the system. Realistically, because of the orbits of the GPS satellites and practical process, any disruption via this tactic would be obvious after the first few uploads and likely thwarted far before culmination. Our point is not to suggest a widespread attack on all 31 satellites in the GPS constellation is impossible. If a satellite can be put into orbit an anti-satellite weapon can reach it. If cyber controls GPS satellites then vulnerabilities must exist. Instead, the question is how to exploit these at such a scale, with such surprise, to obtain a widespread result without time to respond. Complete denial of GPS — via kinetic or cyber attack — while maybe technically possible, is implausible as it would connote an enormous, perhaps even apocalyptic, escalation. Instead of assuming complete denial of GPS, we recommend — and have taught — Western forces to learn necessary variety in tactics that allows for overmatch when GPS is available and how to retain an advantage should adversaries degrade it. Additionally, the Department of Defense has undertaken and considered an expansion of its complement of proficiencies with GPS as a core capability; such redundancy is far preferable to supplanting GPS with a replacement that would still be subject to most of the nuisances noted in the aforementioned articles.

#### System is resilient and impact would be minimal

Davenport & Ganske 19 [Brandon, Combat Operations Division Space Cell Chief at the US Air Force Central Command Combined Air and Space Operations Center, Rich, editor at the Strategy Bridge & founding member of the Military Writers Guild, “‘Recalculating Route’: A Realistic Risk Assessment for GPS,” 3/11/19, *War on the Rocks*, <https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/>, 07/09/22, GDI-JCR]

Conclusion While the potential for disruption of the dual-use GPS system continues to be a nuisance to both civilian life and military operations, an assessment of the facts and contexts shows the end is not actually so near for GPS. The system is more resilient than pessimists allow, and replacing a proven investment with thin promises of alternative resilience is bad advice. Further, nuisance and vulnerability are not the same thing. Finally, this article has explored what could happen if GPS’s widespread disruption or destruction is followed to a logical conclusion. A day without GPS, while perhaps possible, is implausible given how reliably well the system performs even under stress and how widespread destruction would be an escalation toward the extreme against a vital interest — an interest which all the major powers now share given their own equivalently vulnerable systems. Ultimately, a day without GPS is unlikely not because of the technology, but because of the human capacity to overcome nuisance in daily life and fight back using clever tactics.

#### The military has a backup ready in case of GPS disruption

Dawson 19 [Linda, Senior Lecturer Emeritus at UW Tacoma in Statistics and Physical Science, Aeronautical Flight Controller on the Space Shuttle Program at NASA, Navigation and Guidance Engineer for the Boeing Space Center, *War in Space: the science and technology behind our next theater of conflict*, p.7-8, GDI-JCR]

The US military requires reliable backup capabilities that allow it to be less dependent on satellite data. To do so, it must find new and comprehensive ways to identify threats to US timing systems. This means developing network operations that create, maintain, and improve timing sources and precision. There are many ways of measuring and distributing timing that do not rely on GPS or navigation systems. Examples include DARPA’s Chip-Scale Atomic Clock and palm-sized Atomic Clock with Enhanced Stability (ACES).11 Before GPS, Long Range Aids to Navigation (LORAN) was used to aid navigators around the world. LORAN is a ground-based system of receivers and transmitters that was first developed during World War II. By the mid-1990s, LORAN tower networks were able to provide coverage for North America, Europe, and some other regions, primarily in the US and Canada. As GPS became available for civilian use in 1995, LORAN’s popularity declined. GPS was more accurate and widely available. However, The US Coast Guard continued to work on an improved version of LORAN, called the “Enhanced” LORAN, or eLORAN. The enhanced system would be able to provide position accuracy comparable to GPS. In addition, the signal was designed to be resistant to jamming, broadcasting at hundreds of thousands of watts. Unlike GPS, eLORAN could even receive signals indoors, underwater, and in cityscapes or natural canyons or valleys.12

### No Attack

#### Our nuclear deterrent solves GPS attack

Davenport & Ganske 19 [Brandon, Combat Operations Division Space Cell Chief at the US Air Force Central Command Combined Air and Space Operations Center, Rich, editor at the Strategy Bridge & founding member of the Military Writers Guild, “‘Recalculating Route’: A Realistic Risk Assessment for GPS,” 3/11/19, *War on the Rocks*, <https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/>, 07/09/22, GDI-JCR]

Finally, it is important to examine two other factors: escalation control and unintended collateral damage to vital interests. Again, to be clear, temporary nuisances are not a vital threat and the distinction between jamming or spoofing and widespread destruction of GPS is crucial. But what would happen to society if a frustrated adversary chose, despite the difficulty, widespread destruction of the GPS constellation? The positional and timing aspects of the system play an important role in 14 of the 16 sectors classified as critical infrastructure according to the U.S. Department of Homeland Security. One assessment states the “[t]otal economic impact of GPS is virtually the size of the whole [U.S.] economy.” Another report suggests the global economic impact of GPS is over $2 trillion dollars per year and growing, with most of that benefiting the West. This is why other major and regional powers are seeking GPS-like parity with indigenous systems (which share the same vulnerabilities as GPS). Because GPS has such a far-ranging impact on society, any total countervalue attack creating a lasting effect on the system would likely be seen as a vital threat to Western society. Such a concern crosses the boundary into subjective considerations of conflict escalation. While banking delays, glitches in some power grids, and other awful outcomes might occur from complete denial of GPS, there is no guarantee it would wreck civilization. But any major power sophisticated enough to accomplish a widespread counter-GPS operation cannot be certain precisely how it would unfold. There will be many knock-on effects outside the scope of military conflict. Here arise concerns of escalation and geopolitical risk, especially as potential adversaries open themselves to similar risks to their own versions of GPS. Just as the major powers are constrained in using nuclear weapons for limited means, any widespread attack against GPS would be viewed as disproportionate. The signal in escalation would not only occur slowly as noted but also directly against vital interests. The United States would, at the least, respond in kind. Taking all of this into consideration, it is reasonable to believe GPS is protected against widespread attack under the same aegis of deterrence protecting other vital interests: the possibility of nuclear escalation.

### Alt Causes

#### Too many alt causes of GPS disruption to solve

Dawson 19 [Linda, Senior Lecturer Emeritus at UW Tacoma in Statistics and Physical Science, Aeronautical Flight Controller on the Space Shuttle Program at NASA, Navigation and Guidance Engineer for the Boeing Space Center, *War in Space: the science and technology behind our next theater of conflict*, p.9-10, GDI-JCR]

In 2012, the Department of Homeland Security (DHS) performed a GPS risk estimate. It was determined that the system’s weak signals are problematic, allowing interference to happen rather easily. Disruption can originate from ground-based sources in several different ways. Possible hackers could feed incorrect data into critical resource equipment, causing power outages and location errors. Signal jammers could disable cell phone service and emergency communication, leaving fire, police, and emergency medical to conduct business using older methods. Transactions would be limited to cash, which could be difficult to access without ATM services. The longer it takes to locate the jamming devices, the more systems are affected, causing confusion and chaos.16 A more complex disruption device is called a “spoofer.” Equipment in these spoofing systems produces mimicked signals that trick GPS receivers to lock onto them. The spoofed systems cause altered time and position data to be transmitted to unaware users. There is no associated alarm that indicates that anything is wrong. There has been evidence that Russia is testing a new GPS spoofing device. In 2017, the GPS on a ship in the Black Sea reported the ship’s position as 20 miles inland at a nearby airport. The navigation equipment was verified as working properly. To investigate the problem, the captain contacted other nearby ships. Their GPS signals also placed them at the same airport. Although the incident has not been confirmed, it is believed that about 20 ships were affected. Experts think that this is the first known case of GPS spoofing.17 In addition to location errors, spoofing can cause communication breakdowns and market failures. It is a real threat that can be activated almost entirely with software code. It was thought that the biggest threat to GPS was jamming it by masking the satellite signal with noise. Although this can create confusion, jamming is easy to detect, causing GPS receivers to sound an alarm when the signal is lost by this method. Spoofing is a stealthier technique, generating a false signal from a ground station that mimics a real signal and fools the satellite receiver. “Jamming just causes the receiver to die, spoofing causes the receiver to lie,” says consultant David Last, former president of the United Kingdom’s Royal Institute of Navigation.18 The US Department of Homeland Security has focused on GPS disruption for the past several years. It has listed both the intentional and unintentional threats to the satellite system. The unintentional list includes space weather, space debris, faulty software, and human error, among other things. Space weather is potentially the most devastating threat. Solar flares erupting high energy radiation from the Sun have already disabled satellites in the past. Figure 1.3 is an image of an active region on the Sun emitting a mid-level solar flare in 2014. Harmful radiation from large flares is capable of passing through the layer of the Earth’s atmosphere where GPS and communications signals travel, even though it cannot pass completely through the atmosphere to affect humans on the surface.19

## OCOs Answers

### OCOs – escalation

#### OCOs undermine norms and increase risk of escalation – defensive policy solves best

Valeriano 19 (Brandon - Donald Bren Chair of Armed Politics at the Marine Corps University & Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” 1/15/19, <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>, accessed 07/09/22, GDI-JCR)

We demonstrate that, while cyber operations to date have not been escalatory or particularly effective in achieving decisive outcomes, recent policy changes and strategy pronouncements by the Trump administration increase the risk of escalation while doing nothing to make cyber operations more effective. These changes revolve around a dangerous myth: offense is an effective and easy way to stop rival states from hacking America. New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game. Cyberspace to date has been a domain of political warfare and coercive diplomacy. An offensively postured cyber policy is dangerous, counterproductive, and undermines norms in cyberspace. Many have promoted the idea of a coming “Cyber Pearl Harbor,” but instead the domain is littered with covert operations meant to manage escalation and deter future attacks. Cyber strategy and policy must start from an accurate understanding of the domain, not imagined realities. Senior leaders throughout the federal government should consider a more prudent and restrained approach to cyber operations. We argue for a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation. At the same time, the United States should focus on protective measures to make U.S. systems less vulnerable and on sharing intelligence with allies and partners. A policy of restraint that maintains control over the weapons of cyber war is strategically wise.

#### SQ has avoided cyber escalation – increasing offensive capabilities would create unique risk for great power conflict spirals

Valeriano 19 (Brandon - Donald Bren Chair of Armed Politics at the Marine Corps University & Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” 1/15/19, <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>, accessed 07/09/22, GDI-JCR)

Contrary to observed patterns of limited disruption and espionage, Cyber Command sees cyberspace as a domain fraught with increasing risk, where great powers such as China and Russia will undermine American power. The only solution, from this perspective, is to go on the offense. Yet, the benefits of an offensive posture, especially in cyberspace, are mostly illusory to date. Instead, the cyber domain tends to be optimized for defense and deception, not decisive offensive blows. Not only is offense likely the weaker form of competition in cyberspace, it also risks inadvertent escalation. The fear, suspicion, and misperception that characterize interstate rivalries exacerbate the risk of offensive action in cyberspace. Cyber Command’s 2018 persistent-action strategy aims to “expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.”44 Put in simple terms, the best defense is a good offense: get on adversary networks and stop cyber operations targeting the United States before they occur. Under this strategy, offensive cyber operations will also be preemptive in that they are designed to “contest dangerous adversary activity before it impairs [U.S.] national power.”45 To use another sports metaphor, come out swinging. Go on the offense first and establish escalation dominance (that is, demonstrating such superior capabilities over the target state that it can’t afford to escalate in response).46 According to Cyber Command, preemptive strikes will “impose . . . strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.”47 Whether through punishment, risk, or denial strategies, offensive actions theoretically alter the target’s behavior by increasing the expected costs of targeting U.S. interests.48 Offensive action, according to this thinking, deters future aggression by signaling resolve and establishing escalation dominance. Yet, there are well-established reasons to doubt that offensive options produce the intended results in cyberspace. The rationale behind persistent action—that the best defense is a good offense—is deeply flawed. In fact, most military and strategic theory holds that the defense is the superior posture.49 For example, Sun Tzu describes controlling an adversary to make their actions more predictable, and hence easy to undermine, by baiting them to attack strong points.50 The stronger form of war is a deception-driven defense: confusing an attacker so that they waste resources attacking strong points that appear weak. This parallels cybersecurity scholars Erik Gartzke and Jon Lindsay’s claim that cyberspace is not offense dominant, but deception dominant.51 Rather than persistent action and preemptive strikes on adversary networks, the United States needs persistent deception and defensive counterstrikes optimized to undermine adversary planning and capabilities. New policy options proposed by Cyber Command and the Trump administration risk exacerbating fear in other countries and creating a self-reinforcing spiral of tit-for-tat escalations that risk war even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. Shifting to a policy of preemptive offensive cyber warfare risks provoking fear and overreaction in other states and possibly producing conflict spirals. Even limited-objective cyber offensive action defined as “defending forward” can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, “intrusions into a state’s strategically important networks pose serious risks and are therefore inherently threatening.”54 More worryingly, with a more offensive posture, it will be increasingly difficult for states to differentiate between cyber espionage and more damaging degradation operations.55 What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, “in the [aggressor] state’s own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective.”56 The new strategy risks producing a “forever cyber war” prone to inadvertent escalation because it implies all cyber operations should be interpreted as escalatory by adversaries.57

## Space War Impact Defense

### No Space War

#### Virtually zero risk of space war. Satellite systems are redundant. The impact is a lie hyped by defense experts to justify military expenditures

Johnson-Freese & Hitchens 16 edited for language [Joan, Prof of National Security Affairs at US Naval War College, Theresa, Senior Research Scholar at the Center for International and Security Studies at Maryland, former Director of the U N Institute for Disarmament Research, “Stop the Fearmongering Over War in Space: The Sky’s Not Falling, Part 1,” *Breaking Defense*, 12/27/16, <https://breakingdefense.com/2016/12/stop-the-fearmongering-over-war-in-space-the-skys-not-falling-part-1/>, accessed 07/09/22, GDI-JCR]

In the last two years, we’ve seen rising ~~hysteria~~ [hype] over a future war in space. Fanning the flames are not only dire assessments from the US military, but also breathless coverage from a cooperative and credulous press. This reporting doesn’t only muddy public debate over whether we really need expensive systems. It could also become a self-fulfilling prophecy. The irony is that nothing makes the currently slim possibility of war in space more likely than fearmongering over the threat of war in space. Two television programs in the past two years show how egregious this fearmongering can get. In April 2015, the CBS show 60 Minutes ran a segment called “The Battle Above.” In an interview with General John Hyten, the then-chief of U.S. Air Force Space Command, it came across loud and clear that the United States was being forced to prepare for a battle in space — specifically against China — that it really didn’t want. Gen. John Hyten: It’s a competition that I wish wasn’t occurring, but it is. And if we’re threatened in space, we have the right of self-defense, and we’ll make sure we can execute that right. David Martin: And use force if necessary. Gen. John Hyten: That’s why we have a military. You know, I’m not NASA. It was explained by Hyten and other guests that China is building a considerable amount of hardware and accumulating significant know-how regarding space, all threatening to space assets Americans depend on every day. If viewers weren’t frightened after watching the segment, it wasn’t for lack of trying on the part of CBS. Using terms like “offensive counterspace” as a 1984 NewSpeak euphemism for “weapons,” it was made clear that the United States had no choice but to spend billions of dollars on offensive counterspace technology to not just thwart the Chinese threat, but control and dominate space. While it didn’t actually distort facts — just omit facts about current U.S. space capabilities — the segment was basically a cost-free commercial for the military-industrial complex. In retrospect though, “The Battle Above” was pretty good compared to CNN’s recent special, War in Space: The Next Battlefield. The latter might as well have been called Sharknado in Space – because the only far-out weapons technology our potential adversaries don’t have, according to the broadcast, seems to be “sharks with frickin’ laser beams attached to their heads!” First, CNN needs to hire some fact checkers. Saying “unlike its adversaries, the U.S. has not yet weaponized space” is deeply misleading, like saying “unlike his political opponents, President-Elect Donald Trump has not sprouted wings and flown away”: A few (admittedly alarming) weapons tests aside, no country in the world has yet weaponized space. Contrary to CNN, stock market transactions are not timed nor synchronized through GPS, but a closed system. Cruise missiles can find their targets even without GPS, because they have both GPS and precision inertial measurement units onboard, and IMUs don’t rely on satellite data. Oh, and the British rock group Pink Floyd holds the only claim to the Dark Side of the Moon: There is a “far side” of the Moon — the side always turned away from the Earth — but not a “dark side” — which would be a side always turned away from the Sun. More nefariously, the segment sensationalized nuggets of truth within a barrage of half-truths, backed by a heavy bass, dramatic soundtrack (and gravelly-voiced reporter Jim Sciutto) and accompanied by sexy and scary visuals. Make no mistake there are dangers in space, and the United States has the most to lose if space assets are lost. The question is how best to protect them. Here are a few facts CNN omitted. The U.S. has all of the technologies described on the CNN segment and deemed potentially offensive: maneuverable satellites, nano-satellites, lasers, jamming capabilities, robotic arms, ballistic missiles that can be used as anti-satellite weapons, etc. In fact, the United States is more technologically advanced than other countries in both military and commercial space. That technological superiority scares other countries; just as the U.S. military space community is scared of other countries obtaining those technologies in the future. The U.S. military space budget is more than 10 times greater than that of all the countries in the world combined. That also causes other countries concern. More unsettling still, the United States has long been leery of treaty-based efforts to constrain a potential arms race in outer space, as supported by nearly every other country in the world for decades. Indeed, under the administration of George W. Bush, the U.S. talking points centered on the mantra “there is no arms race in outer space,” so there is no need for diplomat instruments to constrain one. Now, a decade later, the U.S. military – backed by the Intelligence Community which operates the nation’s spy satellites – seems to be shouting to the rooftops that the United States is in danger of losing the space arms race already begun by its potential adversaries. The underlying assumption — a convenient one for advocates of more military spending — is that now there is nothing that diplomacy can do. However, it must be remembered that most space-related technologies – with the exception of ballistic missiles and dedicated jammers – have both military and civil/commercial uses; both benign — indeed, helpful — and nefarious uses. For example, giving satellites the ability to maneuver on orbit can allow useful inspections of ailing satellites and possibly even repairs. Further, the United States is not unable to protect its satellites, as repeated during the CNN broadcast by various interviewees and the host. Many U.S. government-owned satellites, including precious spy satellites, have capabilities to maneuver. Many are hardened against electro-magnetic pulse, sport “shutters” to protect optical “eyes” from solar flares and lasers, and use radio frequency hopping to resist jamming. Offensive weapons, deployed on the ground to attack satellites, or in space, are not a silver bullet. To the contrary, U.S. deployment of such weapons may actually be detrimental to U.S. and international security in space (as we argued in a recent Atlantic Council publication, Towards a New National Security Space Strategy). Further, there are benefits to efforts started by the Obama Administration to find diplomatic tools to restrain and constrain dangerous military activities in space. These diplomatic efforts, however, would be undercut by a full-out U.S. pursuit of “space dominance.” This includes dialogue with China, the lack of which Gen. William Shelton, retired commander of Air Force Space Command, lamented in the CNN report. Given CNN’s “cast,” the spin was not surprising. Starting with Ghost Fleet author Peter Singer set the sensationalist tone, which never altered. The apocalyptic opening, inspired by Ghost Fleet, posited a scenario where all U.S. satellites are taken off-line in nearly one fell swoop. Unless we are talking about an alien invasion, that scenario is nigh on impossible. No potential adversary has such capabilities, nor will they ever likely do so. There is just too much redundancy in the system. General Hyten, now head of U.S. Strategic Command, has perfected his sound bites regarding the threats. Other military officials – and of course a DoD contractor – gave what should be expected as their (worst case) perspectives. But theirs is not the only perspective. And no alternate views were offered. The whole show reached its crescendo when “the answer” was revealed toward the end. The U.S. military needs more of everything. It needs to have such overwhelming “stuff” that nobody would dare attack U.S. assets. It needs an offensive arsenal. It needs more money. CNN certainly did its part in scaring the bejesus out of the American public and Congress – and thus helping the Pentagon make its case. In Part II of this article, out tomorrow, we’ll explain how US policy went down this alarmist rabbit hole and how to get it back on track.

### No Space War – China

#### Low risk of US/China nuclear escalation over ASATs

Acton 18 [James, Jessica T. Mathews Chair and co-director of the Nuclear Policy Program at the Carnegie Endowment for International Peace, “Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,” *International Security*, <https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00320>, accessed 07/09/22, GDI-JCR]

The risk of the United States' misinterpreting Chinese nonnuclear strikes against dual-use U.S. C3I assets as preparations for nuclear use would probably be lower than in the case of Russia for two reasons. First, in contrast to Moscow, Beijing has adopted a no-first-use pledge. Second, unlike their Russian counterparts, Chinese leaders can have absolutely no doubt that nuclear first use would do nothing to meaningfully limit the damage their country would suffer in a nuclear war with the United States. As a result, Washington would be unlikely to interpret Chinese nonnuclear strikes as preparations to fight and win a strategic nuclear war.

#### China avoiding conflict involving space assets – they’re too invested and it would be lose-lose

**Pollpeter 15** (Kevin, Eric Anderson Research Analyst on the Study of Innovation and Technology in China for the Institute On Global Conflict And Cooperation. Institute On Global Conflict And Cooperation, China Dream, Space Dream China’s Progress in Space Technologies and Implications for the United States. http://origin.www.uscc.gov/sites/default/files/Research/China%20Dream%20Space%20Dream\_Report.pdf)

Moreover, what is unwritten in Chinese analyses is that as China becomes more invested in space capabilities it takes on the same vulnerabilities as the United States. Although China would not have the same asymmetries as the United States in a conflict in the Western Pacific, the goal of having a global, 24- hour, all-weather remote sensing capability and spending nearly $1 billion per year until 2020 to establish a global satellite navigation system and associated technologies indicates that China is devoting significant effort and resources to establish a system that is similar in architecture to that of the U.S. military’s space program. With this trajectory, China will have as much to lose as it has to gain from the management or mismanagement of the outer space global commons. It is in this vein that some sort of strategic accommodation that ameliorates the worst effects of competition could be achieved.

#### The US and China are avoiding miscalc and escalation with a communications hotline for space activities.

**Schouten 15** (Lucy. Christian Science Monitor Rapid Response Team Writer. CSM. Conflict resolution in space: First hotline since the Cold War. http://www.csmonitor.com/Science/2015/1125/Conflict-resolution-in-space-First-hotline-since-the-Cold-War)

The two governments have set up a direct hotline to communicate about space operations. The countries are supposed to use the hotline to discuss any collisions or plans that might impact the other nation's space operations, Sam Jones for the Financial Times reports. "We’ve also made it clear that we will do what is necessary to protect the space assets of the United States," US Assistant Secretary of State Frank Rose told the Times. "We all have a lot to lose." The hotline shortens communication between Washington and Beijing by several steps. Officials previously routed messages through the Chinese Ministry of Foreign Affairs. This meant they sent messages from the Joint Space Operations Center "to the Pentagon to the state department, to the US embassy in Beijing, and then on to a contact there," Mr. Rose told the Times. Then the process would begin again on the Chinese side. Shortening that line of communication by cutting out the middlemen is a step forward for the solar system, as the US will now have structures in place to handle problems that may arise with China, a growing power in the space industry. It marks a move to try and prevent conflict in explored space, which would cause significant damage to the US economy and military operations. "Our societies are becoming more and more dependent on space," Patricia Lewis, research director at Chatham House international affairs think-tank in London, told the Times. Establishing a special hotline between aeronautical powerhouses is not without precedent. The US kept a direct line of communication open with the Soviet Union even during the tense moments of the Cold War to prevent a mistake from becoming a crisis. Such a development is a long time coming, as an incident occurred back in 2007 that revealed the problems resulting from conflicts in space. China conducted its first successful test of an anti-satellite weapon and blew up a satellite. The US had previously been the only nation with this kind of weapons capability, and it was a shock not only because the satellite was destroyed but also because it increased space debris dangerously, the BBC reported. A hotline such as this is a step in the "settling" process of near space, says Bruce MacDonald, who led the Council on Foreign Relations study of China, space weapons, and US security and is adjunct faculty with the John Hopkins School of Advanced International Studies.