# AFF – Cyber Space Assets

#### Big thanks to Aayan Ali, Billy Blechman, Sanjith Geevarghese, Brandon Lin, Win Neubarth, Lauren Nieto, Dani Roos, Stephen Yang and Steven Yu for their help on this file.

## 1AC – Cyber Space Assets

### 1AC – China Advantage

#### Ukraine completely shifted NATO priorities towards Russia---failure to readdress Chinese advancements opens the door for Chinese adventurism AND security threats.

Liselotte Odgaard 22, professor at the Norwegian Institute for Defense Studies, 2/24/2022, "NATO’s China Role: Defending Cyber and Outer Space," *Washington Quarterly*, 45(1), pp 175-180, https://doi.org/10.1080/0163660X.2022.2059145, sg

NATO’s vague recognition in 2021 that China constitutes a challenge to the transatlantic alliance reflects an institution that has failed to take on the security threats emanating from Beijing. Russia’s invasion of Ukraine on February 24, 2022 highlights the reasons why this omission is problematic. The war in Ukraine has reignited transatlantic unity of purpose in addressing threats from Moscow toward European security. The existential shock that Europe is facing now that a Russian regime has shown itself willing to go to war against European countries carries with it the risk that China will be forgotten when NATO discusses its future priorities. During the war, China is walking a tightrope between maintaining its commitment to sovereignty and territorial integrity and keeping up cooperation with Russia. The future strength of the Chinese-Russian partnership is likely to be determined by the continued usefulness of Moscow in China’s efforts to carve out more space for a Sinocentric international order based on authoritarian regimes. Meanwhile, China will continue to engender threats to the US and Europe in all domains and across geographical regions.

With the summit statement of the North Atlantic Council released June 14, 2021, NATO extended a commitment to “engage China with a view to defending the security interests of the Alliance,” since “China’s stated ambitions and assertive behavior present systemic challenges to the rules-based international order and to areas relevant to Alliance security.”1 China’s coercive policies, nuclear arsenal, military modernization, military cooperation with Russia, lack of transparency, and use of disinformation are listed as main areas of concern for the alliance. NATO takes the China challenge seriously but has yet to devise a strategy to address it.

Compared to the United States, Europe took a long time to acknowledge its stake in managing security challenges from China. As Beijing pushed beyond its traditional zones of interest in East and Southeast Asia toward the Indian Ocean in the 2000s, US security policies began to focus more on China as Washington sought a new geopolitical equilibrium in Asia.2 Since 2014, France and the UK have spearheaded Europe’s naval diplomacy to counter the displays of force and increasing tensions in maritime Asia to which China contributes. This engagement has focused on regular exercises with the US and its Asian allies, operations in support of freedom of navigation, and base-sharing agreements.3 In 2021, the EU recognized that these geopolitical dynamics directly impact its security and announced the establishment of supportive mechanisms in its Indo-Pacific strategy.4 However, NATO has been conspicuously absent in these transatlantic endeavors designed to counter challenges to US and European security. Reflecting NATO’s absence from the main arena of US-China strategic competition, the alliance is hardly ever mentioned in off-the-record conversations on Indo-Pacific security between diplomats and think tank personnel.

NATO’s reluctance to take on the China challenge is perhaps not surprising, given its inherent assumption that the European continent is the jewel in the crown of the US alliance system, which is thought to guarantee US assistance in the event of a military threat against Europe. This assumption was challenged during the Trump administration, which openly questioned the US commitment to Article Five’s collective defense obligation. The invasion of Ukraine has given NATO a new lease on life and put it at the frontlines of transatlantic cooperation on deterring Russia from further military action in future. However, NATO’s focus on its eastern frontline carries the risk that the alliance turns into a Russia-focused European institution and ignores that China is a global great power competitor which also constitutes a major challenge to the security of all NATO member states.

Washington increasingly looks to the EU rather than NATO for guidance on Europe’s future security policy. One reason is that NATO’s toolbox is lagging in domains such as cyber and outer space, although cyber and outer space operations are key enablers of actions in all domains including air, sea, and land. One indication of this is the US-EU negotiations surrounding a common response to cyber threats which took place during the first US-EU Trade and Technology Council (TTC) meeting in Pittsburgh in September 2021. In addition, during Trump’s presidency, longstanding US dissatisfaction with Europe’s modest defense spending threatened to put NATO on the backburner in transatlantic security debates.5 Since then, Russia’s invasion of Ukraine has elicited a sea change in German defense policy with the announcement in February 2022 that defense spending will increase to more than 2 percent of its gross domestic output annually.6 While this may be a convincing signal that Europe will finally devote the resources required for its own defense and revive NATO’s central role in transatlantic security, there is also a risk that China will be moved to the periphery of the alliance’s agenda.

On February 11, 2022, during the runup to the Russian-Ukrainian war, the Biden administration published its Indo-Pacific strategy as US Secretary of State Anthony Blinken was in the midst of a Pacific trip to Australia, Fiji, and Hawaii.7 This US prioritization signaled that despite Moscow’s war in Europe, Washington remains committed to strengthening its presence in the Indo-Pacific and competing with China. If the US drops the ball on the Indo-Pacific, Washington is concerned that China might use force against Taiwan.8 Consequently, the key question for the US is how many resources can be tied up in Europe without losing sight of the long-term goal: deterrence of China. As US strategic competition with China increases while NATO is sitting on the fence, failure to develop a transatlantic defense policy that addresses China will leave Europe vulnerable to China’s ability to exploit the weak links in European defense arrangements, which are newly fragmented by the Russian invasion of Ukraine.9

EU efforts to build an independent regional defense profile and nurture cooperation between Europe’s defense industry and national defense communities reflect a growing recognition that the region needs to become a self-reliant defense actor. However, Europe still needs to demonstrate that self-reliance does not imply merely focusing on Europe’s periphery. Otherwise, the industrial challenges from China may outcompete Europe’s defense industry. Shipbuilding is a case in point. By 2021, China built 50 percent of all existing ships in the world. Through design collaboration agreements, cyber espionage, and acquisitions, China has copied advanced innovative ship designs. Enormous financial resources from the state allow Chinese companies to enjoy economies of scale by building dual-use factories which not only outcompete Western companies in the commercial shipbuilding industry, but also threaten the production of navy vessels. If not taken seriously, Europe and the US may soon have no choice but to buy frigates from China.10 This example demonstrates the centrality of China for global economic and security developments and should encourage Europe to manifest a position of unified strength in defending NATO member states against Chinese security challenges. This realization will help convince the US and its adversaries that Europe continues to be a credible partner in countering common threats against transatlantic security, whether they appear in or beyond the European region.

China’s challenges to US and European security constitute such common threats across a broad range of sectors. These include gradual reinterpretations of principles of international law, the subversion of universal liberal market economic practices, and cyber insurgencies targeting a wide range of civilian and military entities. These Chinese policies all have major military implications because they are related to developments in the operating principles, capabilities, and priorities of China’s armed forces. Only NATO can offer an integrated transatlantic response to the military aspects of Chinese policies that threaten those sectors across the globe, including European actors. NATO’s involvement is essential if the credibility of the alliance’s security guarantees is to be preserved and an effective response to China’s encroachments on a liberal rules-based order is to be established.

NATO’s involvement is essential to establish an effective response to China

The omnipresent character of the China threat demonstrates that it is long overdue for NATO to position itself as a significant player in addressing Beijing’s challenges to transatlantic security. NATO is key to keeping US and European security policies coordinated when applying mechanisms of deterrence and defense against Chinese challenges. If transatlantic unity of purpose is lost, both the US and Europe are far less likely to succeed in addressing China sufficiently.

#### Non-kinetic attacks on space based assets are the most likely – NATO collective defense is key to deterrence

Madeline Moon 20, a member of the UK Delegation to the NATO Parliamentary Assembly, Vice-Chairperson of the Sub-Committee on Transatlantic Defence and Security Cooperation from 2012 to 2015, rapporteur of the Sub-Committee on Future Security and Defence Capabilities “THE SPACE DOMAIN AND ALLIED DEFENCE,” NATO Parliamentary Assembly, https://www.nato-pa.int/document/2017-space-domain-and-allied-defence-moon-report-162-dscfc-17-e-rev1-fin, p. 1-10 /BL

42. Non-kinetic means, for example, cyber hacking, laser dazzling, or the emission of electromagnetic pulses, can also be used to interrupt or disable rather than destroy satellites. While considered less damaging to the space environment and potentially less traceable, many forms of non-kinetic attacks are very difficult to attribute, stirring fears of quick escalation and questions of proportionality of response in a near future conflict where space-assets would likely be involved. Russia and China are already heavily invested in this domain, ultimately seeking the means to disrupt US hegemony in space (Pellegrino, Stang, 2016).

Non-kinetic means: cyber-attacks, jamming, spoofing, and dazzling

43. Because of the resulting debris, which can have a mutually destabilising impact, destroying satellites with kinetic force is not an ideal method for damaging satellite capability. Non-destructive and covert methods, such as cyber-attacks, jamming, spoofing, or dazzling are alternative means to disrupt and deny access to satellite capabilities. In fact, space warfare is more likely to involve the denial of vital information flows supporting command and control of an enemy’s forces, rather than the exoatmospheric destruction of its space-based assets.

44. By attacking a satellite’s control system, or mission package, an actor could take over control of the satellite, shut it down, change its orbit, put it on collision course with other space objects, or destroy its solar panels by exposing it to damaging levels of radiation. In addition, a satellite’s global network of ground stations might be subject to attack with potential serious consequences. 45. Rather than ASAT weaponry, cyber-attacks can instead be used to take control of a satellite or the whole communication network, including the ground stations (Suzuki, 2016). As implied above, cybersecurity and space security are inherently linked. As satellite technologies and space assets are sourced from a broad international supply base they require regular security upgrades to their software systems via remote, distributed connections, which make them vulnerable to cyber-attacks (Livingstone and Lewis, 2016).

46. Due to the nature of their missions, the military pays more attention than commercial operators to the defence of their space systems. As a result, commercial satellite telecommunications are more often than not less resilient than military ones. Still, as commercial satellites are increasingly co-opted or leased for military communications or other civilian mission-critical functions such as air traffic control, train rail traffic, electrical grid management, and other critical civilian infrastructure, commercial satellites can be considered high-value soft targets for adversaries (Suzuki, 2016). In addition, radio frequencies for satellite communications are limited and the increase in the number of commercial and private satellites puts pressure on scarce resources. Some operators are therefore using less secure frequencies, which are easier to hack (Suzuki, 2016).

47. As such, it is clear a range of cyber threats exists against space-based systems. The large amount of data transmitted through satellites presents an opportunity for adversaries to corrupt accuracy and reliability with a relatively low probability of discovery. Examples could be: States seeking a military advantage via the theft of intellectual property; organised criminal elements with sufficient resources seeking financial gain; amateur or professional hackers showing off their skills; or even capable terrorist groups wishing to disrupt services provided by space-based assets or inflict damage on the space environment. Of course, any combination of these threats is also imaginable depending on the adversaries’s assets and capabilities (Livingstone and Lewis, 2016).

48. Satellite feeds can also be jammed via the intentional interference in signal transmission and reception through the deliberate use of radio noise and electromagnetic signals. In particular, global navigation satellite system (GNSS) signals are vulnerable to jamming attacks because civil applications have not always been designed with security in mind. Often, jamming of GPS signals or other radio telecommunications can even be carried out using simple, commercially-available tools (Suzuki, 2016). By way of example, North Korea has carried out a series of coordinated jamming attacks against the Republic of Korea, which affected GNSS signals in the Seoul area and led to the degradation of infrastructure such as mobile phone networks (Livingstone and Lewis, 2016).

49. Spoofing allows an adversary to manipulate the information about the location, position and condition of a satellite. Spoofed data is relatively hard to detect. If successful, the spoofing attack could damage critical infrastructure, such as the national power grid, by introducing false timing signals, or cause economic damage by targeting trading systems in the financial services sector (Livingstone and Lewis, 2016). Spoofing could also confuse the coordination of command and control of a nation’s armed forces in a time of crisis.

50. Dazzling is a way of blinding a satellite with a laser. If the laser is powerful enough, it can even burn satellite sensors and disable them (Airbus Space briefing). Docking and rendez-vous methods are alternative ways of damaging a satellite by using electronic or kinetic force. While docking would have the benefit of not producing space debris, it would expose the attacker to detection. To mitigate the potential consequences of a docking attack, the United States and its allies are developing a programme of Space Situational Awareness, which monitors any objects approaching existing space assets (Suzuki, 2016).

51. The trend toward the development of increasingly disruptive and non-attributable non-kinetic means puts the long-term stability of the space environment at risk. Increasing dependence on space-based architecture coupled with hybrid and asymmetrical disruption tactics will create a space environment ripe for rapid escalation and instability.

V. NATO AND THE SPACE DOMAIN

A. WHY SPACE MATTERS FOR NATO

52. As is clear from above, improvements in space technology drive the development of advanced military systems; they are important force multipliers when integrated into joint operations. Therefore, a clear and mutual understanding of how military, civil, commercial, national and multinational space capabilities contribute to military operations in order to achieve Alliance security objectives is essential. Increased awareness about the potential for adversaries seeking to exploit their own access to space for military purposes to the detriment of Allied assets and capabilities is vitally important (NATO Allied Joint Doctrine for Air and Space Operations, 2016).

53. At the strategic level, NATO is well positioned to strengthen deterrence in space. NATO’s collective defence and economic prosperity rely on space-based infrastructure, and an attack on the space assets of one Ally would impact the security of all. As such, NATO needs a whole-of-alliance approach to protect its interests in space to enhance resilience and deter any threat to its space-based capabilities. At the operational level, space needs to be incorporated in NATO planning and command structures. At the tactical level, relevant training should be provided to personnel and NATO exercises should reflect space warfare scenarios wherein Allied space-assets are denied or temporarily disabled (Schulte, 2012).

54. Today’s modern operational environment relies heavily on guaranteed access to space-based architecture – Allied forces' daily training, and maintenance and execution of ongoing operations are all made capable by a vast network of shared space assets. Allied space capabilities provide a number of products and services, including: global, strategic and intra-theatre satellite communications; positioning, navigation and timing services; terrestrial and space environmental monitoring; real-time space, geological, meteorological and oceanographic situational awareness; advanced intelligence, surveillance and reconnaissance capabilities; as well as NATO Shared Early Warning and transponder tracking such as Friendly Force tracking and maritime tracking (NATO Allied Joint Doctrine for Air and Space Operations, 2016).

55. NATO’s most advanced military systems are dependent upon space-based assets in order to execute missions successfully, particularly Airborne Warning and Control Systems (AWACs), the Alliance’s Ballistic Missile Defence programme, and the Alliance Ground Surveillance System (AGS), set to become operational in 2017. The AGS system consists of air, ground and support segments and will perform all-weather and persistent terrestrial and maritime surveillance in near real-time, contributing to a range of missions1 , providing military commanders with a comprehensive picture of the situation on the ground (GovSat, 2016).

56. Space capabilities contributing to the Alliance’s mission planning and execution at all levels of warfare come from government, military, civilian and commercial providers. NATO does not currently own any orbit spacecraft. It does, however, own and operate several terrestrial elements (e.g. SATCOM anchor stations and terminals). The United States provides the majority of space support NATO currently uses. However, in 2013, there were approximately 39 ‘military or government’ satellites owned by NATO Member States other than the US providing communication, imagery and automatic identification system detection.

57. The primary European NATO Member States who have space capabilities are France, the United Kingdom, Germany, and Italy: The availability of a space capability in support of NATO operations, however, is determined exclusively by the nation or company that owns the satellite. It should be noted that France, Germany, Italy, and the United Kingdom have advanced and capable observation systems supporting their conventional forces today: they are the Pléiades; SAR-Lupe (radar) and Helios 2 (optical, infrared); COSMO-SkyMed; and Skynet 5 respectively.

58. Currently the SATCOM Post-2000 programme provides the Alliance with satellite communications capabilities. The British, French, and Italian governments work in concert to provide the Alliance with advanced SATCOM capabilities. Under the signed Memorandum of Understanding between the three governments, the Alliance is allowed access to the French SYRACUSE 3, the Italian SICRAL 1 and 1Bis, and the British Skynet 4 and 5 military networks (Briefings NATO officials).

59. The current contract negotiated by the consortium is for a 15-year period, scheduled to end in 2019. The NATO Communications and Information Systems Services Agency (NCSA) needs a contract upgrade, however, as the Alliance’s current satellite bandwidth requirements have outpaced what is available under the current contract. Among other deficiencies, the current arrangement does not include EHF-/Ka-band capabilities, which will be critical to future Alliance SATCOM needs (De Selding, 2016).

60. To contract the necessary upgrade of its SATCOM capacity, NATO can look to eight Allies currently developing or in possession of the satellite capacity necessary for military communications; France, Germany, Italy, Luxembourg, Spain, Turkey, the United Kingdom, and the United States (De Selding, 2016). In November 2016, NATO awarded a contract to support the operational phase of the above mentioned AGS system to Luxembourg’s GovSat, an affiliate of satellite operator SES. Launching in 2017, the GovSat-1 satellite will provide an end-to-end service including the delivery of satellite capacity in commercial Ku-band and sensor data communications between the NATO Global Hawk UAVs and ground segment over the AGS operational area. With this contract, Luxembourg Authorities and the NCI Agency as procurement executive agent acquire and manage these services.

61. While the centrality of space is also recognised in NATO’s Strategic Concept, which mentions technological trends that could potentially impede access to space (NATO, 2010), NATO has not issued any policy or military strategy for space operations. So far, only the Allied Joint Doctrine for Air and Space Operations provides some guidelines on the role of space support in operational planning. In 2013, NATO also released the NATO Space Handbook, which explains space fundamentals for commanders and their staff.

B. NATO AND THE SPACE DOMAIN: A WAY FORWARD

62. NATO should renew its focus on space cooperation. Every NATO country relies on safe and reliable access to space assets for both commerce and military operations. However, NATO doctrine and planning have lagged and the Alliance has not issued any military strategy or policy for space operations. For example, the Joint Airpower Competence Centre (JAPCC) has proposed a narrow framework for a NATO Space Policy concentrating on the employment, coordination, and defence of space capabilities used to support NATO operations and core business (JAPCC, 2012). Any NATO policy should furthermore be coherent with existing policies, such as those of the EU and the US. The JAPCC proposes five guiding principles:

#### China is increasing their technological advancements in space – an attack on NATO’s system would rapidly degrade alliance military capabilities and lead to miscalculation

Madeline Moon 20, a member of the UK Delegation to the NATO Parliamentary Assembly, Vice-Chairperson of the Sub-Committee on Transatlantic Defence and Security Cooperation from 2012 to 2015, rapporteur of the Sub-Committee on Future Security and Defence Capabilities “THE SPACE DOMAIN AND ALLIED DEFENCE,” NATO Parliamentary Assembly, https://www.nato-pa.int/document/2017-space-domain-and-allied-defence-moon-report-162-dscfc-17-e-rev1-fin, p. 1-10 /BL

2. NATO forces depend greatly on the use of space-based systems for essential communications, navigation, tracking, and targeting capabilities, as well as weather forecasting. Space-based system coordination plays a vital role in all current NATO key pillars of defence; allowing for the effective management of conventional forces at home and abroad, nuclear deterrent systems, and the evolving ballistic missile defence system. Rapid development, use, and dependency on space, however, imply growing risks.

3. Renewed attention to kinetic anti-satellite (ASAT) capabilities as well as other forms of non-kinetic space denial capabilities such as jammers and lasers is increasingly bringing space to the forefront of security policy planning and debate. As great power strategic competition rises again in Europe and Asia-Pacific, the ability to deter and defend space assets is more important than ever due to the rising costs associated with a space denial campaign.

4. While the costs of disruption to space-based architecture are high, the arena inherently lends itself to collaboration rather than confrontation, largely due to the difficulty of verification mechanisms for space-related activities. As a result, many governments continue to push for a space code of conduct to enhance the prospects for peaceful space cooperation by reducing the opportunities for miscommunication, misperception, and misuse of the domain. To date, the Alliance has no official space policy, though it does have the recently published Allied Joint Doctrine for Air and Space Operations. Given its critical dependence on space, NATO Allies must look for a way to consolidate their approach to and understanding of defence and deterrence in space.

5. This report will examine the rapid evolution and increasing necessity of space-based systems security. It will seek to demonstrate the role space-based systems play at all levels in Alliance security. It will then highlight steps parliamentarians can take to push for an effective NATO space policy.

II. WHY A DEFENCE COMMITTEE REPORT ON SPACE?

6. The 21st century will prove to be the race for space. Space-based systems are the key enablers of national and international infrastructures of today and tomorrow. The current speed of technological developments indicates the pace of diffusion of technology with some form of dependence on space-related hardware will only accelerate. Accordingly, outer space is becoming increasingly congested, contested, and competitive.

7. The benefits to investing in space-based assets are clear: Space-based infrastructure provides data for global positioning, navigation and timing; enables communication systems via large-scale data relay; guarantees the accuracy and efficacy of global financial transactions and trade; supports a wide range of private and public scientific research; as well as oversees environmental monitoring and forecasting. As such, satellite constellations are vital for the efficient functioning of modern aviation, maritime navigation, and ground transportation (both civil and military).

8. As dependence on space-based infrastructures grows, the costs associated with the disruption, denial, or even destruction of such assets will have increasingly distributed and devastating effects. In military operational terms, space-based assets allow for critical manoeuvre of forces, strategic and situational awareness, and precision-strike capabilities. The loss of space assets would significantly hamper any modern military’s ability to respond to not only defend vital assets and populations, but also to respond quickly and efficiently in a crisis.

9. As a result, understanding the evolution of the space security environment is critical for the NATO PA Defence and Security Committee (DSC). As the scale of impact of space denial scenarios grows, it is clear the disruption, denial, or destruction of any Ally’s space assets will have an Alliance-wide resonant effect. Just as NATO forces require freedom of action in the land, air, and sea of their territories, so do they require the freedom from interference with their space-based assets.

A. MILITARY USES OF SPACE

10. Throughout the Cold War the United States and the Soviet Union utilised a range of satellites in conjunction with their strategic nuclear forces: to both link together their respective command and control systems and to monitor and track the other side’s movements. The first Gulf War in 1991 put the benefits of space-enabled systems on dramatic display; even television audiences could witness the tracking and elimination of Iraqi military assets by US precision-guided weaponry. In the ensuing quarter of a century, the centrality of space-based assets to modern militaries is undeniable.

11. Today, space-based assets are essential strategic enablers of modern forces. Since the advent of net-centric warfare during the US invasion of Afghanistan in 2001, NATO military forces depend on satellite services to link and integrate information into land, air, and sea platforms. Effective and real-time inter-services integration enhances decision-making and facilitates navigation. As a result, space-based assets are serious force multipliers for today’s militaries.

B. SPACE PROLIFERATION: MANY NEW ACTORS

12. Technological advances over the last two decades have greatly expanded the breadth and depth of possibilities for space access. As a result, a proliferation of actors hoping to have a stake in space is changing the nature of the three principal geocentric orbits. The flood of new actors is making these orbits increasingly congested and dirty.

13. Currently almost every country either owns a satellite or has a stake in space. There are approximately 1,100 operational satellites in orbit around the Earth, causing some orbital planes to be severely overcrowded. The recent advent of new, dynamic commercial actors has renewed public interest and ignited a second space race (UK Parliament Briefings). Companies such as SpaceX and Virgin Galactic are providing competition between service providers to build, launch, and operate new space systems: the outcome being a steady decline in the cost barrier to space entry and the proliferation of new systems operators (Insinna, 2016).

14. As entry costs continue to fall, the space domain is becoming more easily and more widely accessible, not only to the military and the commercial sector, but also to ordinary citizens due to the development of a range of new, increasingly smaller satellites from mini to micro, and even nano, pico, and femto-satellites – which range from over 500kg to less than 100g. While providing many of the capabilities of current satellites, they will be cheaper to produce and easier to launch, but harder to track and regulate (Lewis and Livingstone, 2016).

15. The scope of the challenge of the growth of satellites in space will only continue to grow because of this relative democratisation of space entry and use. In 2016, the Federal Communications Commission of the United States alone, for example, had received over 8,700 filings for launches of Non-Geosynchronous Orbit (NGSO) communications satellites (Messier, 2016). If these projects are completed, along with the thousands of other projects planned by nations around the globe, Low Earth Orbit congestion will pose a significant regulation challenge.

III. GREAT AND RISING POWERS IN SPACE

16. New actors are changing the geostrategic space environment and will shape space policies in the 21st century. The United States and Russia are still the world’s leading space powers; other countries, however, are steadily advancing their space capabilities, particularly China, which has developed successful launch capabilities and a multifaceted space programme over the last decade (Robinson and Romancov, 2014).

17. The United States is still widely considered the world leader in space. It has the largest space budget, a vast network of military and commercial satellites, and a burgeoning commercial space sector. The rise of the commercial sector’s involvement in space has spurred on a second space race, with companies such as SpaceX and Blue Origin racing to see who can get to Mars first (Briefings UK Parliament). European space and defence sector giant Airbus Defence and Space is working on the ExoMars rover to explore the surface of that planet (Briefings Airbus Defence and Space).

18. As noted above, the rapid pace of commercial development of space launch, control, and satellite assets is changing the nature of space access and exploration. A clear benefit to the United States’s growing commercial space sector is the competition’s cost reduction effect and the added resiliency to the US military’s vital assets in space. The US military has used Boeing-Lockheed Martin’s United Launch Alliance to launch its payloads, but the recent certification of SpaceX’s Falcon 9 rocket to launch US national security payloads is adding price-lowering competition to the market. In addition, Blue Origin and Virgin Galactic are competing to supply the US Space Agency with a reusable spaceplane for its Defense Advanced Research Projects Agency (DARPA) (Insinna, 2016). The continued growth of US involvement in space at both the governmental and private sector levels has allowed it to remain the clear leader in space.

19. Second to the US presence in space is Russia. Moscow owns a massive constellation of military satellites. Most provide the Russian military with globe-spanning communications capabilities (Luzin, 2016). In 2014, the Russian government announced it would increase funding for the Russian Federal Space Agency to modernise and expand infrastructure and capabilities by 2020 (World Economic Forum, 2016). However, international sanctions following Russia’s annexation of Crimea have crippled the Russian space industry by depriving it of the advanced components needed to build many new communications and navigation satellites (Luzin, 2016).

20. Despite recent tensions and growing strategic competition in Europe and the Middle East, Russia and the United States maintain relatively strong levels of space cooperation. The long tradition of US-Russia space cooperation, dating back to the earliest era in space exploration in the 1950s and 60s, continues today with the countries’ use of the International Space Station (ISS). The ISS is the cooperative project supported by the United States, Canada, Europe, and Russia; the ebb and flows of the US Space Agency has made the US dependent at times on Russia’s shuttle capacity, and the United States currently depends on the Russian-made RD-180 engines for its Atlas rockets, which launch US payloads into space.

21. After years of investment and strategy, China is on its way to becoming a space superpower. While China’s estimated space budget is still dwarfed by the US, in 2016 it had 19 successful space launches — the second-highest number for the year behind Russia’s 26, and ahead of America’s 18. China has put up sophisticated communications and intelligence satellites, offered cheap launch services to other nations, and launched manned mission initiatives. In addition, China developed a “quantum satellite” designed to transmit quantum-encrypted information from space, which is theoretically hack-proof and ensures any attempt to intercept or tamper with the transmission would alert both sender and receiver (Dillow et al., 2016).

#### Lack of dialogue to clarify intentions in emerging conflict spheres like the outer space-cyberspace intersection escalates crises on earth by creating use-or-lose pressures for all space-enabled military assets

Laura Grego 20, senior scientist in the Global Security Program at the Union of Concerned Scientists, 1/8/20, “The New U.S. Space Force Will Make Space More Dangerous, Not Less,” https://www.worldpoliticsreview.com/articles/28452/why-the-trump-space-force-will-make-space-more-dangerous

But keeping space secure also requires reducing the threats to satellites. On this score, the Space Force is likely to make space a more contentious and dangerous environment, not less. It’s not just Trump’s rhetoric about dominance in space that is harmful; resources for the new military service will be provided to “deter aggression in, from, and to space.” This will create incentives within the national security bureaucracy to hype the threat of space weapons, and to then build new weapons to counter them.

In a speech last spring outlining his priorities for space, Gen. David L. Goldfein, the chief of staff of the U.S. Air Force, stated that, “It’s not enough to step into the ring and just bob and weave… At some point, we’ve got to hit back.” What Goldfein failed to mention is that the U.S. already has more sophisticated anti-satellite technology than potential adversaries like Russia and China. In fact, having anti-satellite weapons actually does very little to keep one’s own satellites safe from attack. Yet military leaders appear to believe that reserving the option to deny the use of space to potential adversaries is more important than the benefits that come with a less weaponized space.

What’s more, unconstrained development of space weapons will make space more dangerous, costly and unpredictable to use. It will make conflict on Earth riskier, too. A space environment that is perceived as threatening may create an incentive to “use or lose” satellite-enabled military capabilities as a crisis approaches, potentially speeding up conflict. Goldfein underscored this point in remarks following a series of space conflict simulations conducted by the Air Force last month. “In every war game,” he said, “we determined that if you move first in space, you’re not guaranteed to win. But if you move second, you’re likely to lose.”

In the absence of robust international agreements to protect satellites and the outer space environment—the 1967 Outer Space Treaty does not specifically ban non-nuclear weapons from being tested in space or put into orbit—more countries are developing weapons that can destroy satellites in orbit, leaving fast-moving bits of debris that can stay in space for decades and later damage other satellites. When India obliterated its own satellite with an anti-satellite weapon last March, Prime Minister Narendra Modi expressed pride afterward that it had joined an “elite club of space powers.” Testing anti-satellite weapons, much less engaging in an actual conflict in space, can have profound and lasting effects on space. For example, the destruction of a single large satellite in low-Earth orbit would more than double the amount of dangerous debris in these important orbits.

Sensible constraints on this kind of behavior, and limits on dangerous space weapons technologies, would go a long way to augmenting stability, preserving the space environment and avoiding an arms race. But attempts to hammer out such constraints have seen little success. The United Nations Conference on Disarmament has been deadlocked for decades. Negotiations over the European Union’s proposed International Code of Conduct for Outer Space Activities—which would require signatories to resolve not to damage or destroy any satellite except for reasons of safety, self-defense or to avoid debris production—foundered in 2015. Last year, a group of U.N.-convened governmental experts looking at space arms control concluded their deliberations without coming to consensus recommendations.

Still, the outlook is not all bleak. Even without binding legal instruments, no state has ever intentionally destroyed another’s satellite. And in 2018, 87 U.N. member states agreed to voluntary guidelines to protect the long-term sustainability of the space environment.

However, despite the United States having the most investment in space—nearly half of operational satellites are American—it has put very little effort into space-related diplomacy. While the Space Force is big news for the Pentagon, the State Department is nowhere to be seen. Russia and China have repeatedly submitted drafts of their preferred arms control arrangement to the U.N. Conference on Disarmament, most recently in 2014. Their proposed treaty would include binding prohibitions on placing weapons in space and using force or threatening the use of force against satellites. The United States repeatedly rejects these proposals as flawed but declines to provide its own alternative vision.

Despite, or perhaps because of, the deep ideological divides between the world’s great powers, it is critically important that they keep engaging with each other, if only to avoid miscalculation. Information about potential adversaries’ technical capabilities is plentiful, especially in a highly visible domain like space. But assessing their intentions is notoriously difficult. The U.S. and Russia have built some shared understandings over the course of decades of diplomatic engagement, but Washington has little such common ground with China. As a result, the world’s two largest economies risk misinterpreting each other in potentially very serious ways.

Understanding an adversary’s intentions brings more clarity to decision-making in a complex operating environment and may help manage or resolve a conflict more successfully. In 2010, Lincoln P. Bloomfield Jr., a veteran U.S. national security official, warned that without a history of bilateral understandings or crisis management in conflicts involving emerging domains like outer space and cyberspace, there would be “no credible basis for anyone around the president to attribute restraint to the adversary, no track record from which to interpret the actions by the adversary.”

Those risks have not faded in the ensuing decade. If anything, they have multiplied. Doubling down on new space weapons and creating a dedicated Space Force while neglecting to vigorously pursue sensible negotiated constraints seems a sure path to a dangerous future, after having wasted billions of dollars.

#### China non-kinetic satellite attacks escalate quickly – the US is more vulnerable than adversaries

Nicholas Wright et al 18, Georgetown University, Dean Cheng (Heritage Foundation), Col Peter Garretson (USAF), Namrata Goswami (Independent Analyst), James Lewis (Center for Strategic and International Studies), Bruce W. MacDonald (Johns Hopkins University School of Advanced International Studies), Kazuto Suzuki (Hokkaido University, Japan), Brian C. Weeden (Secure World Foundation) and Nicholas Wright (Georgetown University) 7-2018, “Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation”, (SMA) Periodic Publication /billy

Information is the lifeblood of US military strength, making the space assets that create and/or transmit this information to distant forces extraordinarily appealing targets. The US economy increasingly depends on space-enabled information services (SEIS) as well. China is also becoming more space dependent, but most scenarios for possible military space operations would occur much closer to China (e.g., Taiwan, East/South China Sea) than to the US mainland, allowing China to be less space-asset dependent than the US. The space and cyber domains are closely intertwined, and in their essence deal with information and share a number of similarities. The importance of both the space and cyber domains to strategic planning and crisis management is matched by the lack of much real-world crisis management experience in these domains. These incentives exist for Russia as well. In a crisis, both China and the US would likely face an unstable, high-stakes environment that is neither familiar nor well understood. In this environment, China in particular would likely be tempted to escalate quickly in both space and cyber domains to disrupt US military forces and operations if it could, ideally before they could even arrive (Miller & Fontaine, 2017). Being somewhat less space dependent, China would be less vulnerable to US space offense and might be more emboldened to escalate in space than the US. Both countries seem likely to conduct offensive operations in cyberspace during the early stages of a crisis, though they would want to exercise some caution in the extensiveness of their operations because of escalatory risks. Understanding space escalation dynamics in the context of crisis stability requires grasping its strategic landscape, including how deterrence functions or fails in a crisis and what factors strengthen or weaken that deterrence. Interdependencies between and among space and other domains are enormously complicated, and their exploration is essential to understanding twentyfirst century strategic crisis dynamics. In the late stages of a crisis that threatens to transition into conflict, adversaries would be likely to engage in limited space and cyber actions designed both to send a signal of intention to escalate if conditions are not met (could be either a real threat or a bluff) and to put themselves in a more advantageous position should major conflict break out. Space asset vulnerabilities provide an adversary with dangerously attractive incentives to escalate and preemptively attack in a crisis (MacDonald, Blair, Cheng, Mueller, & Samson, 2016). In such a scenario, each side would confront the choice of striking first with all its assets in place, knowing that a conflict is beginning; or ceding the initiative, absorbing a first strike, and making a ragged retaliation against an opponent fully expecting such a response. As a crisis progresses and becomes more intense, each side must wrestle with the prospect that the chances for full-scale conflict are increasing. While neither side may wish for a full-scale war, neither side wishes to receive a major first strike. instability, where pre-emption pays far greater benefits than retaliation (Colby & Gerson, 2013). The weaker or more disadvantaged country in a crisis may find this line of thinking irresistible, or at least preferable to the alternatives. Countries sometimes go to war not because they want to, but because doing so appears less risky than not doing so. Any space power would want to avoid being in an unstable use-or-lose situation. In addition, a major feature of the space and particularly cyber domains is that major attacks can be initiated with little advance warning—and in the case of cyber— with almost no warning. In the space and cyber domains, there is nothing comparable to the stabilizing threat of an assured second-strike capability like that represented in the nuclear domain by sea-based ballistic missiles. For the United States, there are greater risks if conflict escalates into space. Given our greater dependence on space both militarily and economically, the US will want to emphasize deterrence of conflict in space. This can be achieved not just by having space offense, though this would be a necessary component, but also through cross-domain pre-eminence. Conflict is unlikely to be confined to space; cyber and conventional domains will also be involved. Even if the US prevailed in a space-only conflict, the victory would likely be Pyrrhic unless it was overwhelming—China and Russia are unlikely to engage their forces far away from their shores, unlike the US. Thus losing our space capabilities would be more damaging to us than it would be to Russia or China (Morgan, 2010). Until we have a much more survivable and resilient space architecture, we should not want to put our space assets at risk unless absolutely necessary. This 'vulnerability/dependence gap' can be addressed through cross-domain advantages that the US has, particularly in the cyber domain

#### US-China nuclear war causes nuclear winter---guarantees extinction

Nicole S. Lovenduski et al. 20. PhD, Department of Atmospheric and Oceanic Sciences, University of Colorado, Boulder; Cheryl S. Harrison, PhD, Institute of Arctic and Alpine Research; Holly Olivarez, Environmental Studies Program, University of Colorado; Charles G. Bardeen, PhD, Atmospheric Chemistry Observations and Modeling Laboratory, National Center for Atmospheric Research; 6 , Owen B. Toon, PhD, Laboratory for Atmospheric and Space Physics; Joshua Coupe, PhD Department of Environmental Sciences at Rutgers; Alan Robock, PhD, Department of Environmental Sciences at Rutgers; Tyler Rohr, Water Power Technologies Office, Department of Energy, and Samantha Stevenson; Bren School of Environmental Science and Management. “The Potential Impact of Nuclear Conflict on Ocean Acidification”. Geophysical Research Letters. 47, e2019GL086246. https://doi.org/10. 1029/2019GL086246

Nuclear warfare could have devastating impacts on millions of people, yet it has been suggested that regional or global nuclear conflict may be possible in the future (Toon et al., 2019). In addition to the calamitous impacts of nuclear conflict on a local level, research conducted with a range of climate models finds a global cooling in response to various conflict scenarios (Coupe et al., 2019; Malone et al., 1985; Mills et al., 2014; Pausata et al., 2016; Robock et al., 2007; Turco et al., 1983). This global cooling is driven by fires started by the nuclear weapons. These fires inject smoke into the upper troposphere, where rapid lofting can spread the sunlight-absorbing soot particles into the stratosphere (Turco et al., 1983). Recent research implies that even a small nuclear conflict may have impacts on the global climate system, affecting the state and circulation of the atmosphere (Robock et al., 2007), increasing the sea ice extent in both hemispheres (Mills et al., 2014), and reducing plant productivity and crop yields in regions far from the conflict location (Özdogan et al., ˘ 2013; Toon et al., 2019; Xia & Robock, 2013). While less studied, the potential impacts of nuclear conflict on the ocean are many. Numerous physical, chemical, and biological processes in the ocean are temperature dependent, and sunlight is a critical ingredient for photosynthesizing phytoplankton at the base of the marine food web. Using a climate model with an interactive ocean, Mills et al. (2014) evaluated the ocean physical response to a potential India/Pakistan nuclear war that lofts 5 Tg of black carbon particles into the stratosphere; they find a 0.8◦ C decrease in globally averaged sea surface temperature, with smaller temperature reductions at depth. Recently Toon et al. (2019) used an Earth system model that includes a representation for phytoplankton to evaluate the ocean biological response to nuclear conflict; they report a 5–15% decrease in phytoplankton productivity under a range of conflict scenarios. Such findings prompt further investigation into how nuclear conflict and the resulting global cooling may alter the chemical state of the ocean. Perturbations in the ocean's carbonate chemistry are of particular interest, owing to their importance for ocean acidification. Ocean acidification is an ongoing, large-scale environmental problem driven by fossil fuel emissions of carbon dioxide (CO2). Cumulatively since the preindustrial era, the ocean has absorbed 41% of the carbon emitted by human industrial activities (McKinley et al., 2017). While this ocean absorption of carbon has partially mitigated anthropogenic global warming, it has fundamentally altered the carbonate chemistry of the ocean, increasing the concentration of hydrogen ions ([H+]) while decreasing the concentration of carbonate ions ([CO2− 3 ]). Observations collected at time series sites across the global ocean find statistically significant reductions in the potential hydrogen (pH = −log([H+])) and the saturation state of the calcium carbonate mineral aragonite (Ωarag, which is proportional to [CO2− 3 ]) over the past few decades (Bates et al., 2014). These changes are a direct consequence of the ocean absorption of anthropogenic carbon; carbonate chemistry dictates that the excess carbon will react with water and CO2− 3 to decrease ocean pH and Ω (Feely et al., 2004). Both of these changes may have negative consequences for marine organisms, in particular for those that precipitate calcium carbonate shells (e.g., coccolithophores, pteropods, foraminifera, corals, molluscs, and echinoderms), as the precipitation is hindered by low pH, and because decreases in Ω favor shell dissolution (Doney et al., 2009). To date, there have been no studies of the effects of nuclear conflict on ocean acidification, though past modeling studies on the ocean's response to volcanic forcing and to proposed geoengineering schemes have intimated that ocean carbonate chemistry is highly sensitive to these types of external forcings. Using a fully coupled carbon-climate model, Frölicher et al. (2011) find that volcanic-induced cooling following the 1991 Mt. Pinatubo eruption led to immediate increases in the flux of carbon from atmosphere to ocean and consequently, increases in the total dissolved inorganic carbon (DIC) concentration in the surface ocean. Eddebbar et al. (2019) demonstrate that air-to-sea CO2 fluxes are significantly enhanced following the eruptions of Agung, El Chichón, and Pinatubo in a large ensemble of simulations with an Earth system model. Matthews et al. (2009) conduct solar radiation management climate engineering simulations with an intermediate complexity model of the coupled climate-carbon system; they find changes in ocean pH and Ωarag as a result of the anomalous cooling. Similarly, Lauvset et al. (2017) indicate that radiation management geoengineering leads to changes in North Atlantic pH in a fully coupled Earth system model, but they do not explore changes in Ωarag. While these studies are suggestive of the carbonate chemistry response to nuclear conflict, the external forcing perturbations are of a different magnitude and duration than those imposed by nuclear conflict. Further, it is difficult to mechanistically understand the ocean carbonate chemistry response to such external forcing perturbations in fully coupled models, where the terrestrial response to forcing additionally influences the atmospheric CO2 concentration. Here, we use a state-of-the art Earth system model to simulate the ocean carbonate chemistry response to a range of nuclear conflict scenarios. We decouple the ocean carbon cycle from that of the terrestrial carbon cycle via a direct prescription of the atmospheric CO2 boundary condition used for air-sea CO2 flux, that is, changes in the terrestrial biosphere have no influence on the atmospheric CO2 that the ocean sees. As we will demonstrate, we find large perturbations in ocean pH and Ωarag as a result of nuclear conflict. These perturbations have relatively long duration (order of 10 years) and are driven by decreases in temperature and subsequent increases in the ocean carbon inventory. 2. Methods We analyse output generated by the Community Earth System Model (CESM) version 1.3, a state-of-the-art coupled climate model consisting of atmosphere, ocean, land, and sea ice components (Hurrell et al., 2013). The atmosphere component of CESM in our simulations is the Whole Atmosphere Community Climate Model (WACCM; Marsh et al., 2013) with nominal 2◦ resolution, 66 vertical levels, and a model top at ∼145 km; it uses the Rapid Radiative Transfer Model for GCMs (RRTMG; Iacono et al., 2000) for the radiative transfer. The Community Aerosol and Radiation Model for Atmospheres (Bardeen et al., 2008) is coupled with WACCM to simulate the injection, lofting, advection, and removal of soot aerosols in the troposphere and stratosphere, and their subsequent impact on climate (Coupe et al., 2019; Toon et al., 2019). The ocean component of CESM is the Parallel Ocean Program version 2 (Danabasoglu et al., 2012) with nominal 1◦ resolution and 60 vertical levels. The biogeochemical ocean component of CESM is the Biogeochemical Elemental Cycling model that represents the lower trophic levels of the marine ecosystem, full carbonate system thermodynamics, air-sea CO2 fluxes, and a dynamic iron cycle (Doney et al., 2006; Moore et al., 2004, 2013; Moore & Braucher, 2008; Long et al., 2013; Lindsay et al., 2014). LOVENDUSKI ET AL. 2 of 9 Geophysical Research Letters 10.1029/2019GL086246 The ocean in the coupled CESM simulation is initialized from rest with World Ocean Circulation (WOCE) temperature and salinity (Gouretski & Koltermann, 2004). Biogeochemical tracers are initialized to observationally based climatologies where possible (Lauvset et al., 2016); where these were not available (such as dissolved iron and phytoplankton biomass), the model is initialized with fields interpolated from an existing CESM simulation. The new, fully coupled simulation was spun up for 4 years to an approximate steady state with a constant atmospheric CO2 mixing ratio of 370 ppm, representative of the mixing ratio in the year 2000. Due to the relatively short spin-up period, the globally integrated air-sea CO2 flux is not in steady state (drifting at a rate of 0.14 Pg C year−2) when the perturbation forcing is applied. We therefore present our results as anomalies from the drifting control integrations. Three control simulations of 20-year duration are generated using round-off level differences in atmospheric initial conditions. As each of these control simulations has different phasing of internal variability (e.g., El Niño-Southern Oscillation), we use the standard deviation across this ensemble to identify statistically significant perturbations due to nuclear conflict. We report on the anomalies generated from four simulations of nuclear conflict with varying amounts of soot injection: three India/Pakistan conflict scenarios that inject 5, 27, and 47 Tg of soot, respectively, and one US/Russia conflict scenario that injects 150 Tg of soot. The initial soot injection amounts are generated from plausible scenarios for nuclear conflict following advice from a number of military and policy experts; the reader is referred to Toon et al. (2019) for further details on scenario development. In each case, we prescribe that the conflict begins on 15 May of the 5th year of the first control simulation, and we integrate the model for a 15-year period following the injection. We assume that the smoke generated by mass fires from nuclear conflict is injected into the upper troposphere above the target sites (in the U. S./Russia case, smoke is spread evenly over the two nations), as in Toon et al. (2019). WACCM lofts much of this smoke higher into the stratosphere via solar heating of black carbon aerosols in the smoke, where the black carbon aerosols persist for about a decade. The resulting annual mean, post-conflict (May to the following April) anomalies in aerosol optical depth are shown in Figure 1a. These optical depth changes result in a 10–40% reduction in incoming solar energy (Toon et al., 2019). While we discuss the anomalies generated from all four of these conflict simulations, we describe two in greater detail throughout this manuscript: the U. S./Russia case, as it is the largest climate perturbation overall, and the India/Pakistan 47-Tg case, as it is the largest climate perturbation generated by a regional nuclear conflict. Ocean biogeochemistry in the version of CESM used for our simulations has been extensively validated in the literature (Brady et al., 2019; Freeman et al., 2018; Harrison et al., 2018; Krumhardt et al., 2017; Lindsay et al., 2014; Lovenduski et al., 2015, 2016; Long et al., 2013, 2016; Moore et al., 2013; McKinley et al., 2016; Negrete-García et al., 2019). Of particular note for our study, the simulated surface ocean carbonate ion concentration from a long, preindustrial control simulation of CESM compares favorably with reconstructed observations, albeit with lower interannual variance than has been measured at subtropical time series sites (Lovenduski et al., 2015). In Figure S1 in the supporting information, we illustrate the comparison between observationally based estimates of surface ocean pH and Ωarag (from GLODAPv2; Lauvset et al., 2016) and the CESM control ensemble mean. In this comparison, we note that the observational estimates have been extensively interpolated and are intended to represent year 2002 carbonate chemistry parameters, whereas CESM has been integrated under an atmospheric CO2 mixing ratio that corresponds to year 2000 forcing. We find high correspondence between the spatial patterns of modeled and observed pH and Ωarag, giving us confidence that CESM is capable of representing the mean state of these two variables. 3. Results Globally averaged surface ocean pH increases in response to each of the nuclear conflicts, where the magnitude of the pH anomaly scales with the amount of soot injected (Figure 1b). In each case, the pH anomaly exceeds the interannual standard deviation of pH in the control ensemble mean (gray shading in Figure 1b). We observe the largest increases in surface ocean pH in response to the U. S./Russia 150-Tg case; here the globally averaged surface ocean pH anomaly exceeds 0.05, corresponding to a ∼10% decrease in the global mean hydrogen ion concentration. Under each scenario, the pH anomaly peaks 2–4 years after the conflict and persists for ∼10 years. With the exception of the high-latitude oceans, the pH increase following the nuclear conflict is pervasive across the surface ocean (Figures 2a– 2c). In the 47-Tg India/Pakistan scenario, we observe local pH anomalies exceeding 0.06 units on average in years 2–5 post conflict (Figure 2c); the anomalies are largest in the North Atlantic, North Pacific, and Equatorial Pacific. These large, abrupt changes in surface ocean pH may have important consequences for calcifying organisms, as shell precipitation can be affected by the ambient hydrogen ion concentration in seawater (Kroeker et al., 2013). Since the beginning of the industrial revolution, global ocean pH has dropped by an estimated 0.1 units (Ciais & Sabine, 2013). The anomalies in pH generated by our simulations exceed 50% of this historical change and occur over a much shorter time period. Whether and how organisms respond to the initial and rapid alleviation of low pH, followed by an immediate return to the current pH state in the global ocean, is as yet unknown (see, e.g., Haigh et al., 2015). In contrast to our results for pH, we observe decreases in surface ocean Ωarag following nuclear conflict (Figure 1c), which should tend to inhibit the maintenance of shells and skeletons in calcified organisms. While minimal changes in Ωarag are simulated for the 5-Tg India/Pakistan case, the other three cases produce large decreases in saturation state, on the order of 0.1 to 0.3 units (Figure 1c). In each of these three cases, the anomalies exceed the interannual standard deviation of Ωarag in the control ensemble mean (gray shading in Figure 1c). The peak response in these three cases occurs 3–5 years post conflict, a year or so later than the pH response. While for pH the globally averaged anomaly is negligibly small, 10-years post conflict; anomalies in globally averaged Ωarag persist beyond our 15-year simulation time frame for all conflict scenarios. The decreases in aragonite saturation state span the tropics and subtropics, with the exception of the central and eastern Equatorial Pacific region (Figures 2d– 2f). Local decreases in saturation state exceed 0.5 units in the western North Atlantic and western North Pacific under the 47-Tg India/Pakistan scenario (Figure 2f). Importantly, the simulated decreases in saturation state are highly pronounced in regions that host diverse coral reef ecosystems (for instance, the western and southwestern Pacific and the Caribbean), and like pH, the changes in saturation state occur fairly rapidly. Projections from climate models suggest that coral reef ecosystems across the world will experience aragonite saturation state declines from their preindustrial value of 3.5 to 3.0 by the end of the century (Ricke et al., 2013); alarmingly, our simulations project similar Ωarag declines over a 3- to 5-year period, which then persist for years after the initial forcing dissipates. The opposite-signed anomalies in pH and Ωarag induced by nuclear conflict seem puzzling at first, as for "typical" anthropogenic ocean acidification scenarios, both of these variables simultaneously decrease. Why would nuclear conflict cause opposing responses in pH and saturation state? To understand these opposing responses, we need to consider the carbonate chemistry system in seawater and its sensitivity to changing temperature. Gaseous CO2 reacts with seawater to form carbonic acid (H2CO3), which then dissociates to form H+ and bicarbonate (HCO− 3 ). The hydrogen ion then reacts with CO2− 3 to form additional HCO− 3 , CO2 + H2O− ↽−−−−−−⇀−H2CO3. (1) H2CO3− ↽−−−−−−⇀−H+ + HCO− 3 . (2) H+ + CO2− 3 − ↽−−−−−−⇀−HCO− 3 . (3) The equilibrium constants for these reactions (typically expressed as K0, K1, and K2, respectively; Sarmiento & Gruber, 2006) are sensitive to changes in temperature, for example, the cooling induced by nuclear conflict. We need to also consider the dissolution reaction for mineral calcium carbonate (CaCO3) in seawater, CaCO3(s)− ↽−−−−−−⇀−Ca2+ sat + CO2− 3,sat, (4) where [Ca2+]sat and [CO2− 3 ]sat are the concentrations of dissolved calcium and carbonate in equilibrium with mineral CaCO3, and the solubility product (Ksp) for this reaction is also sensitive to temperature (Sarmiento & Gruber, 2006). Further, the saturation state for a calcium carbonate mineral in seawater (here: aragonite), can be expressed as Ωarag = [Ca2+][CO2− 3 ] Ksp , (5) where both [CO2− 3 ] and Ksp are affected by changes in temperature (Ca2+ is highly abundant in seawater, and thus changes in temperature do not affect its concentration enough to matter for CaCO3 dissolution; Emerson & Hedges, 2008; Sarmiento & Gruber, 2006). Thus, we can decompose the anomalies in pH and Ωarag into the component driven by temperature-induced changes in the carbonate chemistry equilibrium constants (K0, K1, K2, and Ksp) and the component driven by all other changes to the carbonate chemistry system, such as changes in the DIC concentration, the alkalinity, or the salinity. We approximate the temperature sensitivity of the equilibrium constants using a program developed for CO2 system calculations (CO2SYS; van Heuven et al., 2011) via finite difference approximation. The component driven by all other changes to the carbonate system is computed as the residual of the other two terms. The pH response to nuclear conflict is the sum of two opposing drivers: an increase in pH driven by a decrease in sea surface temperature that alters the carbonate chemistry equilibrium constants and a decrease in pH driven by an increase in the DIC concentration of the upper ocean. Figure 1b illustrates the temporal evolution of the components of the global pH anomalies from the India/Pakistan 47-Tg simulation driven by changes in the equilibrium constants versus all other changes in the carbonate chemistry system. The equilibrium constant-driven pH anomaly is positive, peaking 2–3 years after the conflict, whereas the “other” component of the pH anomaly is negative, peaking 3–5 years after the conflict. The resulting total pH anomaly is positive, indicating that it is more strongly influenced by changes in the equilibrium constants than other changes. In the India/Pakistan 47-Tg case, globally averaged temperature reaches a minimum 2 to 3-years post conflict; the model initially produces 3.5◦C–4◦C anomalies at the surface that rewarm toward pre-conflict values for the duration of the simulation (Figure 3a). In contrast, surface ocean salinity-normalized DIC anomalies peak 3 to 5-years post conflict (Figure 3b), mainly as a result of the enhanced solubility of CO2 in colder seawater. While decreasing biological export production also contributes to increased DIC in the surface ocean, this signal is small relative to the change driven by enhanced air-to-sea CO2 flux (e.g., Figure S2). The delay in DIC relative to temperature anomalies is a result of the long (order months to years) timescale for CO2 to fully equilibrate with the surface mixed layer (Emerson & Hedges, 2008). The cold, high DIC surface anomalies slowly propagate into the global ocean thermocline; we observe 1◦ C and 10 mmol m−3 anomalies in temperature and DIC, respectively, at a depth of 300 m that persist beyond the length of our simulation (Figure 3). As there are no significant anomalies in global mean alkalinity or salinity post conflict (not shown), we conclude that the DIC perturbation drives the “other” component of the pH anomalies. We find similar behavior for these components in the other conflict scenarios (not shown). The negative Ωarag anomalies post conflict are driven by a combination of lower temperatures and higher DIC concentrations. Colder surface temperatures tend to increase Ksp, while higher surface DIC concentrations tend to decrease [CO2− 3 ], resulting in lower Ωarag values post conflict. Figure 1c illustrates that the DIC (other) component dominates the total Ωarag anomaly for the India/Pakistan 47-Tg simulation. As for pH, the equilibrium constant component peaks earlier than the other component; this is due to the timing of the temperature and DIC perturbations (Figure 3). The spatial patterns of the post-conflict surface pH and Ωarag anomalies in the India/Pakistan 47-Tg scenario (Figures 2c and 2f) result from perturbations in local surface ocean temperature and DIC (Figure S3). Negative temperature anomalies and positive DIC anomalies are pervasive in the tropics and extratropics, with the exception of the eastern Equatorial Pacific, where a large and long-lasting El Niño-like event develops following the conflict (Coupe, et al., manuscript in review). This strong reduction in the equatorial trade winds greatly weakens upwelling in the cold tongue region, producing near-zero surface temperature anomalies and a reduction in vertical DIC supply here (Figure S3). In the Southern Ocean, temperature and DIC are not much affected by the nuclear conflict, likely a result of enhanced upwelling of warm water from the subsurface (Harrison, et al., manuscript in preparation). Taken together, the aforementioned changes in temperature and DIC lead to increases in pH and decreases in Ωarag over most of the ocean surface (Figure S4). The changes in surface ocean pH that we simulate for nuclear conflict resemble the simulated response of pH to volcanic eruptions, but are an order of magnitude larger. Figure S5 illustrates the anomaly in surface ocean pH in the first year following the eruptions of Agung, El Chichón, and Mt. Pinatubo, as estimated by the CESM Large Ensemble (Kay et al., 2015), which uses the same physical and biogeochemical ocean components as in our nuclear conflict simulations. The ensemble mean isolates the evolution of the Earth system under historical external forcing, including the aerosol loading following volcanic eruptions (Eddebbar et al., 2019), and averages across the various representations of internal variability (Deser et al., 2012; we note that ensembles are not necessary for the nuclear conflict scenarios since the much larger magnitude of forcing provides a higher signal-to-noise ratio). The anomaly in the ensemble mean shown here thus cleanly captures the response of surface ocean pH to volcanic eruptions. Here we show the anomaly in preindustrial pH (pH anomalies in equilibrium with preindustrial atmospheric CO2, which is computed simultaneously with contemporary pH at model run time), as the contemporary pH anomalies include also the response to increasing atmospheric CO2 from one year to the next. The similarity in the spatial patterns of volcanically induced pH anomalies and those produced under nuclear conflict is striking (cf. Figures S5 and 2c), suggesting that volcanic forcing produces similar temperature, DIC, and thus pH anomalies (including the El Niño-like response to volcanic forcing in the eastern Equatorial Pacific, described in Eddebbar et al., 2019). However, the eruption-driven pH anomaly is both smaller (an order of magnitude) and of shorter duration (∼2 years) than in the India/Pakistan 47-Tg simulation. Unfortunately, a similar analysis of volcanic Ωarag anomalies in the CESM Large Ensemble was not possible as preindustrial [CO2− 3 ] was not saved to disk. 4. Conclusions and Discussion We report on the surface ocean pH and Ωarag anomalies generated from four simulations of nuclear conflict using the CESM with full ocean carbonate system thermodynamics. Globally averaged surface ocean pH increases in response to each conflict, with the largest increases in the North Atlantic, North Pacific, and Equatorial Pacific Ocean. The pH anomalies persist for 10 years post conflict and are primarily driven by changes in the carbonate chemistry equilibrium constants as a result of decreases in sea surface temperature. In contrast, CESM simulates globally averaged decreases in surface ocean Ωarag in response to nuclear conflict, with the largest decreases in the tropics and subtropics. The Ωarag anomalies persist beyond the length of our 15-year simulations and are driven by a combination of changes in the carbonate chemistry equilibrium constants and the solubility-driven increases in DIC. We further demonstrate that the surface pH anomalies induced by nuclear conflict resemble those induced by volcanic eruptions in the same modeling system. The simulated changes in global and regional pH and Ωarag as a result of nuclear conflict are large and abrupt. In the most extreme forcing scenario (U. S./Russia 150 Tg), over a period of ∼5 years, global surface ocean pH increases by 0.06 units, and Ωarag decreases by 0.3 units. To put these numbers into perspective, this simulated rate of change of pH is 10 times larger than the rate of change we have observed over the past two decades as a result of ocean acidification (−0.0018 year−1; Lauvset et al., 2015). Worryingly, surface ocean Ωarag decreases more than six times faster than has been observed in the open ocean over the past three decades (−0.0095 year−1 at the Bermuda Atlantic time series; Bates et al., 2014). While the cooling associated with nuclear conflict rapidly and briefly alleviates the decline in pH associated with ocean acidification, the increase in solubility causes the ocean to absorb ∼11 Pg of excess carbon in a 10-year period, leading to a rapid drop in Ωarag. Whether and how calcifying organisms might respond to such rapid and opposing changes in pH and Ωarag is as yet unknown. In order to measure organism response to ocean acidification, a majority of laboratory studies perform CO2 bubbling perturbation experiments, which simultaneously decrease the pH and Ωarag in the surrounding seawater solution (Pörtner et al., 2014). This simultaneous change in two carbonate chemistry parameters challenges our ability to isolate the organism response to changes in pH or changes in Ωarag alone. A recent laboratory sensitivity study of marine bivalve larvae used chemical manipulation experiments to decouple these two parameters; they found that larval shell development and growth were negatively impacted by decreasing Ω and unaffected by changes in pH (Waldbusser et al., 2014). If these sensitivities are sustained in other organisms, we might conclude that calcifying organisms would be severely affected by nuclear conflict. Our findings shed light on the ocean biogeochemical response to other forms of extreme external forcing, such as volcanic eruptions (Eddebbar et al., 2019; Frölicher et al., 2011) and solar radiation management climate engineering (Lauvset et al., 2017; Matthews et al., 2009). They may further inform the study and understanding of the role of ocean acidification in marine extinction following the Chicxulub impact event (Henehan et al., 2019). Importantly, our results suggest that even a regional nuclear conflict can have an impact on global ocean acidification, adding to the list of the many, far-reaching consequences of nuclear conflict for global society.

#### Specifically, cyber-attacks on space-based sensors cause total failure of missile defense systems

Beyza Unal 19, Ph.D., senior research fellow with the International Security Department at Chatham House, July 2019, “Cybersecurity of NATO’s Space-based Strategic Assets,” <https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets/2019-06-27-Space-Cybersecurity-2.pdf>

Missile defence relies heavily on early warning capabilities otherwise known as integrated threat warning and threat assessment (ITW/TA): US space-based infrared sensors detect the hot plumes of ballistic missile launches and communicate the information to the service component command.

Theatre missile defence, which includes the Patriot missile defence system – a long-range surface-to-air missile system used by the US and NATO allies – and standard missile defence systems, and which is part of the naval component of the integrated Aegis weapon system, also serves as part of overall missile defence capability.45 The Aegis combat system operates in the maritime domain, using radar to track and guide weapons to destroy targets; its elements – which include a space tracking and surveillance system, the AN/SPY-1A radar, a command and decision system and a display system – could all potentially be exposed to cyberattacks.

The US Department of Defense conducted an auditing exercise in 2018 for the internal controls of its ballistic missile defence systems (BMDS). The aim of the audit was to ensure that systems and programmes were functioning as intended. The findings indicated that there were ‘internal control weaknesses related to protecting networks and systems that process, store, and transmit BMDS technical information’.46 These weaknesses could be exploited through insider threat and/or cyber means.

Missile defence systems may fail, or they may be activated due to false information sent from communication systems (such as ground-based radars) to the command unit. The Israeli anti-missile defence system Iron Dome, for example, is claimed to have a 90 per cent accuracy rate when intercepting targets. Yet there have been cases where a faulty response within the system has activated the launch of interceptor missiles erroneously, such as occurred in Gaza in March 2018, when it was triggered by machine gun fire.47 Thus the battle management and weapons control system was proved at that time to be unable to make proper threat assessments. Similar outcomes could result if the threat assessment control system is interfered with via cyber means; the consequences could be much higher, including the loss of civilian life. In the Israeli case, it was reported that Rafael Advanced Defense Systems, a supplier of technology to the Iron Dome system, together with Israel Aerospace Industries and the Elisra Group, both of which were also involved in the project, faced persistent cyberattacks during the period of October 2011 to August 2012. This resulted in the loss of sensitive data that was believed to include the specifications of the Arrow 3 missile, developed jointly by the US and Israel.48 Vulnerability to cyberattacks within the supply chain is not unique to NATO, and NATO and its allies should address this type of risk. Supply chain integrity (in terms of both hardware and software) is imperative for reliable military systems.

One of the core elements of a missile defence system is that it relies on the reception of near real-time information by a command centre to be able to identify and project the trajectory of an incoming missile. Through automated response it calculates the speed, velocity and location of the target in order to be able to intercept the incoming missile in a short time frame. Any deliberate interference with the information, for instance from the radar, could mean that the defence missiles fail to intercept an incoming threat, or could lead to a faulty decision based on falsified or spoofed information. Thus, for example, a defence missile could fail to hit the correct target and strike well beyond the intended target zone. In order to detect deliberate interference or cyber intrusion, it is important to put preventive measures in place. One such measure could be to conduct organized, simulated cyberattacks on a system to assess its performance: this is known as penetration testing. In the future, detection of anomalies could be possible through ML and AI, especially in closed networks.49

#### Missile defense is key to deter North Korea – failure of missile defense causes North Korean nuclear attack

Vince A. Manzo AND John K. Warden 21, a Research Analyst with the Strategic Initiatives Group at the Center for Naval Analysis (CNA); a Senior Policy Analyst on the Strategic Analysis & Assessments team at Science Applications International Corporation (SAIC). AUGUST 29, 2017 “WANT TO AVOID NUCLEAR WAR? REJECT MUTUAL VULNERABILITY WITH NORTH KOREA”; War On the Rocks; https://warontherocks.com/2017/08/want-to-avoid-nuclear-war-reject-mutual-vulnerability-with-north-korea/

The North Korea policy of the Donald Trump administration has been mired in a morass of contradiction and bluster. But there might be a silver lining: There is an indication that the administration will follow its predecessors and attempt to deny North Korea the ability to hold the United States at risk with nuclear weapons. If effectively implemented as a part of a comprehensive deterrence strategy, this approach would give the United States and its allies the best chance of containing a nuclear-armed North Korea and avoiding nuclear war.

In their attempts to formulate an effective strategy, the previous two administrations articulated an important strategic principle: The United States will attempt to deny North Korea the ability to hold the U.S. homeland at risk with nuclear-armed intercontinental ballistic missiles (ICBMs). This is not, however, the same as saying that the United States will prevent North Korea from testing an ICBM or deploying an operational ICBM force, a goal that does not seem possible without paying an unacceptable cost. Rather, the principle is a signal of U.S. intent to deny North Korea the ability to use the threat of nuclear strikes against the U.S. homeland as coercive leverage.

The most visible and expensive element of this policy is the U.S. Ground-Based Midcourse Defense (GMD) system. Initiated under President George W. Bush’s administration in 2002 and expanded by President Barack Obama in 2013, the GMD system is designed to defend against North Korean and Iranian ICBMs. The U.S. decision to deploy this system demonstrates that, from a strategic planning perspective, the United States saw a North Korean ICBM as a distinct possibility and took steps to ensure that extended deterrence to Japan and South Korea would remain viable even if North Korea deployed a nuclear-capable missile that could range the continental United States.

By seeking to reduce vulnerability to a North Korean nuclear attack on the U.S. homeland, the United States has placed North Korea in a different category than Russia. (Where China should fit is a matter of debate.) Washington accepts that “mutual vulnerability” to nuclear attack is an enduring reality of its relationship with Moscow. In other words, the United States assesses that neither it nor Russia has the ability to disarm a considerable portion of the other’s nuclear weapons capability and prevent a significant retaliatory strike. Furthermore, as a matter of policy, the United States does not seek to develop strike and missile defense capabilities that would deny Russia a survivable nuclear second-strike capability.

Part of the reason the United States has accepted mutual vulnerability with Russia is that it wants to avoid first-strike instability. The traditional concept of first-strike instability reasons that a nuclear-armed country would have a strong incentive to launch a first strike against its nuclear-armed adversary in a crisis if, first, doing so would enable it to generate an advantage by destroying a significant portion of its adversary’s nuclear forces and, second, its adversary also has an incentive to strike first and limit damage before its own forces are degraded or destroyed. In other words, nuclear deterrence could fail in a crisis if one or both sides were to perceive that both the potential payoff of attacking and the risk of delaying or restraining are high.

Importantly, the use-them-or-lose-them logic of classical first-strike instability does not apply to the U.S.-North Korea nuclear relationship. In a crisis or conflict, North Korea would certainly fear for the survivability of its nuclear forces and potentially its regime. But even once North Korea’s nuclear force grows larger and more sophisticated, Pyongyang could not conceivably hope to generate an advantage by conducting a damage-limiting nuclear first strike against the United States. Such a strike would not significantly degrade U.S. nuclear forces or overall war potential and would ensure the end of the Kim regime. This is in no way a “dominant strategic move” for North Korea.

How then, could the United States fail to deter North Korean nuclear use? Pyongyang knows that it cannot use nuclear weapons and other capabilities to defeat U.S. and allied military forces. Instead, Kim Jong Un’s more plausible theory of victory is a strategy that attempts to use nuclear coercion to persuade the United States that the costs and risks of overthrowing the Kim regime are too high. In this sense, North Korea’s initial attempt at asymmetric escalation using nuclear weapons is more likely to be a limited strike against regional military targets than a massive strike against the continental United States. Pyongyang would attempt to degrade the ability of the U.S. to flow forces to the Korean Peninsula, while demonstrating a propensity for controlled risk-taking. But critically, North Korea would retain a survivable reserve nuclear force to threaten destruction of major U.S. population centers if the United States does not back down.

From this perspective, accepting U.S. vulnerability to North Korean nuclear forces would improve the credibility of North Korea’s coercive strategy and increase the risk of both war and nuclear use. If Kim Jong Un is confident that North Korea can maintain a survivable reserve force that can threaten U.S. cities, he may be tempted to use nuclear weapons in a limited, coercive fashion to try to terminate a conventional conflict with the United States and its allies. Rather than use-or-lose, the logic driving North Korean first use would be, use some because you will not lose the rest. Even more unsettling, if Pyongyang became confident in its ability to use nuclear coercion as a war termination mechanism, it might conclude that it has leeway to initiate violent provocations and even war.

Thus, rather than accepting North Korea’s ability to cause significant destruction to the United States with a nuclear strike, the United States should field damage limitation capabilities, a combination of strike and missile defense armaments that would allow the United States to disarm the majority of North Korea’s nuclear weapons capability and prevent significant retaliatory strikes against U.S. cities. If the United States has a credible damage limitation option, the Kim regime is more likely to calculate that crossing the nuclear threshold would be a strategy for suicide, not survival, because North Korea would lack a reliable second-strike capability to deter regime change.

In order for U.S. damage-limitation capabilities to match North Korea’s rapidly improving long-range missile capabilities, there is an urgent need to improve U.S. homeland defense. The GMD system has well-documented limitations, and the Trump administration should make prudent investments to fix the program, emphasizing the need for cost-effective, reliable capabilities. In addition, the United States and its allies should field a combination of intelligence, surveillance, and reconnaissance and strike capabilities that can threaten North Korea’s road-mobile transporter erector launchers and ballistic-missile submarines.

#### Satellites are key to overall cyber-vulnerability of critical infrastructure---attacks risk blackouts and collapse crisis response and deterrence relationships

Patricia Lewis 16, research director for international security at Chatham House; and David Livingstone, associate fellow for international security at Chatham House, 11/21/16, “The cyber threat in outer space,” https://thebulletin.org/2016/11/the-cyber-threat-in-outer-space/

Satellites that orbit the Earth form the exoskeleton of the world’s critical infrastructure. Global communications, air transport, maritime trade, financial services, weather and environmental monitoring, and defense systems all depend on an expansive network of satellites in space. As the September 2014 cyber attack on the US weather system starkly demonstrated, the strategic space-based assets of America and other nations have serious cyber vulnerabilities. In the maritime arena too, space-based monitoring systems are regularly being jammed or spoofed by vessel operators entering false information in order to disguise their illicit activities.

The vulnerability of satellites, their ground stations, and other space assets to cyber attack is often overlooked in wider discussions of cyber threats to critical national infrastructure. Yet just as with other digital networked systems, satellites are vulnerable to cyber attacks that include data theft, jamming, spoofing, and satellite hijacking. All of these present serious risks for societies and critical infrastructures, and analyzing the intersection between cyber security and space security is essential to understanding this evolving problem. So too is the need for an ogranized global effort to confront these threats. Despite some progress at the United Nations and elsewhere, there is currently no international body dedicated to the issue of cyber security in space. Establishing such a multi-stakeholder regime, with the aim of assessing risks and promoting best practices, would begin to close this critical gap.

The nature of the threat. Cyber risks for space-based systems take many forms. While one attack might involve the jamming, spoofing, or hacking of communications or navigational networks, another might target or hijack control systems or specific electronics for missions, shutting down satellites, altering their orbits, or “grilling” their solar cells through deliberate exposure to damaging radiation. Still another might strike at satellite control centers on the ground.

As in other areas of cyber conflict, players and motivations abound. States or non-state armed groups could use such attacks to create military advantages in space prior to or during a war. Government agencies or corporations with sufficient computing power to crack encryption codes could use cyber attacks on satellite systems to steal strategic quantities of intellectual property. Well-resourced criminal organizations could steal significant amounts of cash. Groups or even governments could initiate catastrophic levels of satellite run-ins with space debris, perhaps even causing a cascade of collisions—called the Kessler Effect—that could deny everyone the use of space for the foreseeable future. Even individual hackers who simply want to show off their skills could create inadvertent mayhem.

Perhaps the most worrying vulnerabilities involve satellite-enabled navigational systems. Many such systems have been developed, from Europe (notably the new Galileo system) to Asia, but the most ubiquitous is the US global-positioning system commonly known as GPS. Much of the world’s infrastructure relies on this system, yet it was not originally intended for civilian use, and therefore not designed with security in mind. A successful spoofing cyber attack could introduce erroneous timing signals, which are used for determining precise locations. Aimed at a power grid, this type of manipulation could potentially trigger catastrophic overloads, leading to cascading equipment failures and even major blackouts. Spoofers could also target banks and stock exchanges by manipulating automated time-stamps on transactions. Earlier this year, when 15 satellites accidentally broadcast signals that were inaccurate by 13 microseconds, telecom companies using Chronos GPS services were hit with 12 hours of thousands of system errors.

The threat to military technology looms large as well. Not enough attention has been paid, at least not in the open literature, to the increasing vulnerability of space-based assets, ground stations, and associated command-and-control systems. Cyber attacks on satellites have the potential to undermine the integrity of strategic-weapons systems and destabilize deterrence relationships. And in the event of a military crisis, the potential for cyber attacks could cast doubt on intelligence and increase the risk of misperception, not to mention threaten missile systems, both strategic and tactical, which rely on satellites and the space infrastructure for navigation and targeting, command and control, operational monitoring, and other functions. Because cyber technologies are within the grasp of most states and non-state actors, they level the strategic field and create hitherto unparalleled opportunities for small belligerent governments or terrorist groups to instigate high-impact attacks.

Your smart fridge isn’t helping. As satellites and satellite constellations continue to grow in number—a very good thing in terms of human connectedness, scientific research, and space exploration—so do entry points and communications pathways for cyber attacks, the so-called Internet of Things (or, as we now like to think of it, Gadgnet) that has sprung up due to our love of digital devices. Yet cyber defenses have failed to keep up with this growth, mostly due to the high cost of (optional) built-in security in a world of smaller and cheaper satellites, even though this is ultimately the most cost-effective and sustainable approach to cyber safety in space.

The international supply chain of satellite components, with the associated uncertainties about provenance and standards of production, along with back-door holes in encryption, is increasingly hard to regulate. The costs associated with cyber security, in both software and hardware, are rising, and in low-cost space missions where the commercial price of implementing security measures rivals the value of the mission, the temptation to neglect them and hope for the best is high. In the rush to get products to market, designers and manufacturers often skip or pay only passing attention to important security controls. This is already causing immense concern for machine designers, manufacturers, and insurance companies. Indeed, the October 2016 Dyn attack that resulted in denial-of-service strikes on major websites such as Twitter, Spotify, and Reddit appears to have harnessed botnets on personal computers through poorly secured home devices connected to each other and the outside world through wireless routers.

Reducing risks, building resilience. The 2011 US International Strategy for Cyberspace stressed that international approaches and cooperation are needed in order to address and mitigate the full range of cyber threats to military systems, and indeed international cooperation will be crucial in any response to space-based cyber threats, both military and civilian.

#### Grid collapse causes extinction.

Sherrell R. Greene 18, Nuclear Engineering M.S. degrees from the University of Tennessee, recognized subject matter expert in nuclear reactor safety, nuclear fuel cycle technologies, and advanced reactor concept development, worked at the Oak Ridge National Laboratory (ORNL) for over three decades, as Director of Research Reactor Development Programs and Director of Nuclear Technology Programs; Sept 07, 2018 “Enhancing Electric Grid, Critical Infrastructure, and Societal Resilience with Resilient Nuclear Power Plants (rNPPs),” Nuclear Technology 205(3), https://www.tandfonline.com/doi/full/10.1080/00295450.2018.1505357?cookieSet=1]

There are a variety of events that could deal crippling [devastating] blows to a nation’s Grid, Critical Infrastructure, and social fabric. The types of catastrophes under consideration here are “very bad day” scenarios that might result from severe GMDs induced by solar CMEs, HEMP attacks, cyber attacks, etc.5

As briefly discussed in Sec. III.C, the probability of a GMD of the magnitude of the 1859 Carrington Event is now believed to be on the order of 1%/year. The Earth narrowly missed (by only several days) intercepting a CME stream in July 2012 that would have created a GMD equal to or larger than the Carrington Event.41 Lloyd’s, in its 2013 report, “Solar Storm Risk to the North American Electric Grid,” 42 stated the following: “A Carrington-level, extreme geomagnetic storm is almost inevitable in the future…The total U.S. population at risk of extended power outage from a Carrington-level storm is between 20-40 million, with durations of 16 days to 1-2 years…The total economic cost for such a scenario is estimated at $0.6-2.6 trillion USD.” Analyses conducted subsequent to the Lloyd’s assessment indicated the geographical area impacted by the CME would be larger than that estimated in Lloyd’s analysis (extending farther northward along the New England coast of the United States and in the state of Minnesota),43 and that the actual consequences of such an event could actually be greater than estimated by Lloyd’s.

Based on “Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures” to Congress in 2008 (Ref. 39), a HEMP attack over the Central U.S. could impact virtually the entire North American continent. The consequences of such an event are difficult to quantify with confidence. Experts affiliated with the aforementioned Commission and others familiar with the details of the Commission’s work have stated in Congressional testimony that such an event could “kill up to 90 percent of the national population through starvation, disease, and societal collapse.” 44,45 Most of these consequences are either direct or indirect impacts of the predicted collapse of virtually the entire U.S. Critical Infrastructure system in the wake of the attack.

Last, recent analyses by both the U.S. Department of Energy46 and the U.S. National Academies of Sciences, Engineering, and Medicine47 have concluded that cyber threats to the U.S. Grid from both state-level and substatelevel entities are likely to grow in number and sophistication in the coming years, posing a growing threat to the U.S. Grid.

These three “very bad day” scenarios are not creations of overzealous science fiction writers. A variety of mitigating actions to reduce both the vulnerability and the consequences of these events has been identified, and some are being implemented. However, the fact remains that events such as those described here have the potential to change life as we know it in the United States and other developed nations in the 21st century, whether the events occur individually, or simultaneously, and with or without coordinated physical attacks on Critical Infrastructure assets.

#### A fractured governance framework for space that has been oriented around individual countries, not a collective defense, emboldens Chinese attacks that drive escalation – US-NATO military cooperation over space hardens civilian targets, improves dialogue around safeguards, and centralizes info networks.

Liselotte Odgaard 22, professor at the Norwegian Institute for Defense Studies, 2/24/2022, "NATO’s China Role: Defending Cyber and Outer Space," *Washington Quarterly,* 45(1), pp 175-180, https://doi.org/10.1080/0163660X.2022.2059145, sg

NATO in Cyber and Outer Space

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

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

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

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

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

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

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

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

### 1AC – Russia Advantage

#### NATO’s ambiguous threshold for what constitutes “armed attack” sufficient to activate Article 5 ensures Russian gray zone probing against allied space assets, risking cascading escalation

Tomas Jermalavičius and Alejandro Leal 20,Head of Studies and Research Fellow at the International Centre for Defence and Security; research assistant at ICDS, post-graduate degree candidate in technology governance and digital transformation at Tallinn University of Technology; Securing Democracy, December 2020, "Gravity of ‘Star NATO’: Can the Alliance Pull the Baltics Into Military Space Affairs?" <https://securingdemocracy.gmfus.org/wp-content/uploads/2020/12/towards-nato2030-the-regional-perspective-of-the-baltic-states-and-poland-read-in-english.pdf>

The geopolitical context, technological trends and new concepts of warfare raise the unpalatable prospect of the militarisation of space. The Outer Space Treaty does not prohibit that – it only bans the deployment of nuclear weapons in it.12 But while an attack against terrestrial objects on the Alliance’s territory from future space-based weapons would constitute a clear act of armed aggression, it remains to be seen if an attack on, for instance, satellites owned by an Allied government could eventually trigger requests to activate Article 5 of the Washington Treaty. Even if the current answer is “no” or “it depends,” it will be hard to avoid further discussions given the growing importance of the space domain.13 After all, the Alliance has already agreed that devastating cyberattacks could prompt an invocation of the collective defence clause, and some nations are very clear about their national responses to acts of aggression in outer space. For instance, the French Space Defence Strategy of 2019 explicitly states that “in the event of armed aggression in space, France may avail itself of its right of self defence.”14 It is hard to imagine its Allies, such as the Baltic States, standing aside should Paris decide to request the activation of Article 5 in response to an escalating conflict in outer space.

Aggression in outer space or from the surface of the Earth against space-based assets is not in the realm of technological fiction. Various countries are developing and deploying counter-space capabilities that are able to destroy, degrade, deny or compromise space-based assets. These include kinetic means, such as anti-satellite (ASAT) missiles, as well as non-kinetic capabilities. Countries ranging from China and India to Russia and the US have tested and demonstrated their ability to destroy satellites with missiles.15 Russia is also developing a new system that is able to deploy into outer space swarms of small “killer satellites” loaded with explosives that would be carried into orbit by missiles launched from a MiG-31BM fighter aircraft.16 This is a concept that will enable counter-space operations that are cheaper, faster, larger in scale and less demanding (e.g. in targeting accuracy) than employing ground-launched ASAT missiles.

The destruction of a satellite, however, inevitably produces thousands of pieces of debris that scatter across Earth’s orbit, potentially provoking a chain reaction. Such an event – known as Kessler syndrome – could severely threaten space activities and prevent the use of satellites in specific orbital ranges for decades if not longer. Given that Russia itself (and China, for that matter) is becoming increasingly dependent on space infrastructure as a result of its military modernisation, some analysis suggests that Moscow is interested in developing a diverse set of kinetic counter-space capabilities primarily as a deterrent for such space-dependent powers as the US, as well as being an escalation control instrument that expands the range of options available to decision-makers.17 In the event of a regional military crisis in the Baltic area, this would echo the logic of nuclear signalling in order to deter the US and other Allies from reinforcing the Baltic States.

At the same time, the application of more affordable and easily available electronic and cyber-warfare methods could be just as disruptive. Satellites are vulnerable to cyber and electronic attacks, which can have reversable or irreversible effects. This includes the use of radio-frequency energy to interfere with or jam the communications of a satellite, the use of directed energy weapons to dazzle their sensors, and the use of software and network techniques to influence or compromise computer systems linked to satellite operations or even to hijack the satellites themselves.18 Such non-kinetic counterspace capabilities, as well as some means of kinetic attack (e.g. using hijacked satellites to damage or destroy other satellites, or conducting Rendezvous Proximity Operations to approach and damage an opponent’s satellites), will become part of the repertoire in the so called “grey zone” conflicts that Russia and China excel at and so far tend prefer to direct military confrontation. For the decision-makers in the Baltic States, this raises the spectre of space services (such as imagery, communications, or global positioning and navigation) provided by Allies or commercial partners becoming restricted or unavailable at some critical points during a security crisis manufactured by Russia.

If a mechanical failure – due to a natural incident or hostile action – leading to a denial of service or complete loss of space assets occurs during a period of heightened geopolitical tensions, the possibility of escalation and broader conflict could arise. At this point, in the words of Joan Johnson-Freese, “the chances of maintaining a space war at a limited level appear similar to those of fighting a limited nuclear war: not good.”19 Scenarios like this may require that NATO not only coordinate the development of new capabilities and enhance its space threat awareness, but also incorporate diplomacy into the implementation of its space policy in order to advance international norms of responsible behaviour with regard to space-based systems and assets, build transparency and trust, and preserve the overall strategic stability, which could be threatened by escalating conflict in outer space.20 For the Baltic States – which have become sceptical towards arms control, CSBM and other frameworks and initiatives involving Russia – this might become a difficult proposition, prompting them to define some clear “red lines”, the crossing of which might weaken the Alliance’s deterrence and defence posture. However, doing so would entail understanding strategic issues related to outer space and defining their own perspective.

The Baltic perspective and challenges

The recognition of outer space as an operational domain has various implications for the Alliance and its individual members, even if NATO’s ambition is not (yet) to become an actor in it. As Kęstutis Paulauskas points out, the “implementation of space as an operational domain will allow NATO’s military commanders to properly and fully take into account space requirements in training and exercises as well as defence and operational planning.”21 The Alliance will now be busy defining and refining its requirements for space capabilities and then, through the defence planning process, will seek to ensure that the capabilities of all NATO nations are catalogued and coordinated, as well as that national plans take into account NATO’s needs and do not leave any significant gaps when put together. The Alliance’s planning of multidomain operations (MDOs), joint doctrine development, standardisation processes, and training and exercises will include space considerations as a composite part.22 By establishing a Space Centre, the Alliance has already started to make some visible structural adjustments, allowing it develop space domain awareness, share data, and coordinate activities within NATO’s overall command structure – and there is much more less-visible but equally important work being done across the Alliance in order to implement its overarching space policy.23

Where does this put the Baltic States? The space domain has always been a blind spot in the defence planning and capability development processes in the three capitals. Just a few years back, mentioning the need to consider the implications of developments in outer space drew blank faces at best and outright ridicule at worst. Interest in support from space-based assets was confined to small, specialised military communities of practice such as ISR, communications, naval and special forces, or air surveillance. It seldom, if at all, entered the considerations of the high command or defence planners, as the Baltic States retained their steady focus on developing land forces as their top priority – even though land operations rely, to a considerable extent, on the availability of various space-based services. Space ignorance also stands in stark contrast to all the attention paid to the cyber domain, which was declared a new operational domain by NATO in 2016, leading to such steps as the establishment of a dedicated Cyber Command in the Estonian Defence Forces (EDF).24

NATO’s London decision is now tentatively putting space on the mental map of the defence leadership in the Baltic States. In a recent media interview, for instance, the Commander of the EDF Major General Martin Herem said that this was potentially a new area for trilateral Baltic military cooperation, and he even suggested that the Baltic States draw upon the civilian sector’s work in order to develop their own space-based capability (in the form of nanosatellites).25 Although this may sound like a somewhat poorly thought-through idea – not least because trilateral Baltic military cooperation has been underperforming in many other areas that are less challenging or complex than venturing into outer space – it still marks a welcome turn of sentiment regarding opportunities related to space as an operational domain.26 At the same time, it is necessary to understand that any national or regional ambition that is linked to a broader NATO framework would take a long time to acquire shape, to develop all the ingredients necessary for its success, and then to reach maturity as an integral part of national defence.

In this process, however, there are some issues and aspects that could already be addressed by Baltic defence policymakers and military planners in the short- and medium-term:

* At the policy level, there is a need for national and regional (e.g. within the format of the Baltic Ministerial Committee) discussions on what would constitute acts of aggression in outer space that would warrant the invocation of Article 5 and where the “grey zones” of conflict lie with regard to adversarial kinetic and nonkinetic action against the space assets and infrastructure of the Allies. This is a necessary mental exercise that would help the Baltics appreciate how various scenarios may unfold and when a collective diplomatic and military action might be called upon (or when scenarios would just warrant security consultations under Article 4).

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

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

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

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

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

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

#### A U.S.-Russian space war spills over to ground-based nuclear miscalculation due to attacks on early-warning

James Acton and Ankit Panda 20, Co-Director of the Nuclear Policy Program at the Carnegie Endowment for International Peace; Stanton Senior Fellow with the Nuclear Policy Program at the Carnegie Endowment for International Peace; Defense News, December 2, “Why the Pentagon must think harder about inadvertent escalation,” <https://www.defensenews.com/opinion/commentary/2020/12/02/why-the-pentagon-must-think-harder-about-inadvertent-escalation/>

In a paradox worthy of the nuclear age, the conventional capabilities that have enabled the United States to reduce its reliance on nuclear weapons have also increased the risk of misperception that could spark a nuclear war.

The United States now bases its war plans around using its exquisite conventional forces to sever the connections between an adversary’s leadership and its military forces. But in an escalating conflict on the Korean Peninsula, such operations could look to North Korean leader Kim Jong Un like an attempt at regime change — even if the United States did not seek to depose him — and thus induce him to gamble on nuclear use to try to terrify the United States into backing off.

In a war against Russia, meanwhile, the United States might try to protect its satellites by attacking the radars that Russia uses to track space assets. Such radars, however, are also used to detect attacks on Russia’s nuclear forces, thus giving Moscow the ability to launch those forces before they are destroyed. As a result, Moscow might wrongly conclude that attacks on those early-warning radars were the opening salvo of a U.S. campaign to destroy its nuclear forces. Again, a nuclear war could be the result.

Concerns about so-called inadvertent escalation have now reached Congress. As part of the fiscal 2020 National Defense Authorization Act, Congress requested that the undersecretary of defense for policy prepare a report “detailing the Department’s efforts to develop and implement guidance to ensure that the risks of inadvertent escalation to a nuclear war are considered within the decision-making processes with regard to relevant Department activities.”

The Pentagon’s newly released response is titled “Managing Risks of Nuclear Escalation.” Note the (presumably deliberate) absence of the word “inadvertent” in the title. This document is deeply concerned with one particular escalation risk: that the United States’ nuclear-armed adversaries — Russia, China and North Korea — may underestimate U.S. resolve or capabilities. This danger is real, but it has a flipside: that an adversary may assess U.S. war aims to be more ambitious or expansive than they actually are.

#### ASAT attacks cause global nuclear war and collapse terrestrial deterrence---turns every conflict scenario

Laura Grego 18, senior scientist in the Global Security Program at the Union of Concerned Scientists, 3/19/18, “Space and Crisis Stability,” https://www.law.upenn.edu/live/files/7804-grego-space-and-crisis-stabilitypdf

For the foreseeable future, military tensions between the United States, China, and Russia are likely to remain high, as are those between China and India. Even absent intentional confrontation, regional problems, such as those in the Baltics and East and South Asia, have the potential to draw these actors into conflict. Thus, it is imperative to pay attention to any pathways that could lead an actor considering crossing the nuclear threshold, or approaching it very closely.

The United States and Russia continue to retain large nuclear arsenals on high alert1 . Each are developing new strategic weapons, including hypersonic conventional prompt global strike systems with a suggestion mission of holding ground-based anti-satellite weapons at risk.2 Russia has declared the existence of novel nuclear delivery systems as a response to US missile defense systems,3 weapons which complicate the management of crises. China is reportedly considering increasing the size, capacity and alert status of its nuclear weapons delivery systems4 and is also developing new kinds of strategic weapons. China is also developing hypersonic weapons,5 and the ingredients for an arms race around these technologies is in place. India continues to increase the sophistication of its strategic posture. And India, China, Russia and the United States have or are pursuing missile defense technologies that are important both in the nuclear realm but in space issues, since missile defenses present demonstrated or inherent antisatellite capabilities.

Thus it is critical to ensure that in times of tension, no actor escalates the crisis inadvertently or against their better judgment, and that misperception does not play an important role in the initiation or progress of the crisis. And that hostilities, if initiated, resolve as quickly as possible.

Thomas Schelling‘s encapsulated an aspect of this idea in his landmark work this way:

This is the problem of surprise attack. If surprise carries an advantage, it is worth while [sic] to avert it by striking first. Fear that the other may be about to strike in the mistaken belief that we are about to strike gives us a motive for striking, and so justifies the other‘s motive. But if the gains from even successful surprise are less desired than no war at all, there is no ―fundamental‖ basis for an attack by each side. Nevertheless, it look as though a modest temptation on each side to sneak in the first place — a temptation too small by itself to motivate an attack — might become compounded through a process of interacting expectations, with additional motive for attack being produced by successive cycles of ―He thinks we think he thinks we think … he think we think he‘ll attack; so he thinks we will; so he will; so we must.6

This suggests that it is important to make the advantage of surprise attack negligible and the disadvantages as great as possible, to make sure that all actors understand this, and to make sure that actors have as clear an understanding of each other‘s motivations as possible to avoid miscalculation.

In the last twenty years, space assets have become important not only for strategic missions but also increasingly underpin conventional military force for modern militaries, and especially those with expeditionary forces, such as the United States. They are essential not only for militaries, but are a critical provider of essential civilian, commercial, and scientific services. Not only do satellites perform many more missions than they have in the past, there are many more spacefaring nations. While most satellites belong to the United States, Russia, and China, more than sixty countries own satellites or a large stake in one.7

At the same time, the technologies that are useful for holding satellites at risk have grown significantly in sophistication and capacity even in the last decade, and have become more widely available. This is particularly problematic because attacks on satellites can create or escalate terrestrial crises in potentially difficult to predict ways. The world is drifting towards a space regime that faces an ever more prevalent and more sophisticated anti-satellite technology and greater numbers and types of targets in space, with very little mutual understanding about how actions in space are perceived.

#### Cyber-weapons are the only usable ASATs---U.S. dependence on satellite infrastructure incentivizes attacks that risk nuclear war

Abhijeet Singh Baghel 19, M.S. in Cybersecurity, Utica College, December 2019, “Cyber Warfare in Outer Space,” ProQuest Dissertations Publishing, document ID: 27670535

A future war in space includes the possibility of one or more anti-satellite (ASAT) attacks which could destroy one or several important satellites and quickly escalate to a nuclear conflict. In 2014, the Obama administration initiated the need to develop new ASAT defense strategies and technology to counter China after its second ASAT test the year before (Kulacki, 2016). Attacking any U.S. intelligence, surveillance, and reconnaissance (ISR) satellite, Global Positioning System (GPS) or communication satellites using missiles such as long-range missiles or Co-Orbital ASATS is expensive, time-consuming, and is hard to keep a secret (Hitchens, 2019d & Wright, 2012). It could be used to deter initial U.S. involvement in conflict but would have devastating impacts on its loss (Please see Appendix A & B for more information).

It is no secret that the U.S.’s major vulnerabilities lie with modernizing the National Airspace System (NAS) and using only one source for timing, navigation, and communication (aka GPS) whereas Russia, Europe, China, and others utilize additional forms of satellite navigation systems (Livingstone & Lewis, 2016). Therefore, only the U.S. would suffer losses with the disruption or destruction of the GPS constellation. To achieve enough damage to the GPS constellation and other space-based assets would require several satellites to be disabled to successfully disrupt the network and disable the U.S. This would have to be done in quick succession before the U.S. could retaliate which is also hard to do and the adversary would have to covertly launch its missiles from several locations or maneuver ASATs currently in orbit to attack its targets. On the other hand, hostile cyber operations are a much bigger threat to the operation of satellites such as GPS (Findler, 2019). As both cyberspace and space assets increasingly rely on each other it is imperative to implement flexible, proactive cybersecurity measures as new threat actors, companies, and technologies are always expanding and evolving space activities (Findler, 2019).

Space and cyberspace share several similarities. Both, along with international waters and airspace, are a global common[s] for the international competition which in turn determines the global distribution of power (Heftye, 2017). Both have applications that affect the everyday lives of many people and economies worldwide (Asbek, 2014). Although cyberspace is a man-made domain, it produces virtual results used for military operations and, along with space, provides adversaries a viable platform for exploitation.

In the last decade the integration of internet-based infrastructure into space systems, such as communications satellites has become an integral part of how satellites operate (Mather, 2018). Along with ASATS, other technologies are being developed to “deny, degrade, deceive, disrupt, or destroy space assets,” thus rendering space infrastructure useless (DOD & DNI, 2011). This includes lasers capable of blinding and knocking down space assets, jamming signals from space, and cyberattacks on satellites which are often considered electronic attacks that are reversable in comparison to orbital threats or nuclear explosions which are irreversible as shown in Figure 1 (Harrison, Johnson, & Roberts, 2019).

The major difference between physical weapons and cyber-attacks is the cost and time associated with an attack. Space assets are vulnerable to cyber threats and the growing dependence on them for commercial and military purposes alike could pose a serious national security threat. There was a time that critical infrastructure was supported by its proprietary technologies of which many have been replaced with internet-based technologies. As a result, nearly anything can be attacked through the internet, especially the interconnected space-assets which will inevitably be a primary target in the case of significant conflict.

#### Attacks on space assets and orbital weapons trigger rapid escalation to great power nuclear war

Michael P. Gleason 20, national security senior project engineer at The Aerospace Corporation’s Center for Space Policy and Strategy, previously senior strategic space analyst in the Office of the Secretary of Defense Office of Net Assessment; and Peter L. Hays, retired Air Force Lt Col who works as a defense contractor in the Pentagon supporting the assistant secretary of the Air Force for Space Acquisition and Integration, October 2020, “A ROADMAP FOR ASSESSING SPACE WEAPONS,” <https://aerospace.org/sites/default/files/2020-10/Gleason-Hays_SpaceWeapons_20201005_1.pdf>

In addition, some argue that space weapons present broader geopolitical risks due to their potential effects on deterrence and strategic stability. Space capabilities have a close relationship to nuclear stability and the potential for escalation between great powers. Space weapons could therefore alter how decisionmakers calculate nuclear deterrence. Many of the visions of space-to-Earth weapons imagine them having incredible speed and accuracy tied to the ability to target any point on Earth with minimal or even no warning. At enough scale and with sufficient destructive effects, such attributes would threaten a first-strike capability; i.e., the ability to wipe out a target country’s nuclear deterrent before it has a chance to launch a retaliatory strike. If so, nuclear deterrence may fail, a consideration that may outweigh all others. Similarly, some have comparable concerns about space-based ballistic missile defenses nullifying a country’s nuclear deterrent and providing a nuclear first-strike incentive for the country that possesses such capability.

Earth-to-space weapons create concerns because targeting early warning satellites, strategic surveillance satellites, and nuclear command and control communication satellites could also be perceived as the immediate prelude to a nuclear first strike by an adversary, triggering a response on the nuclear escalation ladder. Even if space weapons do not fatally undermine nuclear deterrence, they still offer another path to rapid nuclear escalation.

Space weapons might upset strategic stability in other ways as well. Space is considered an offensive dominant arena, meaning it is materially easier and less costly to attack a satellite—including space-based weapons—than to defend a satellite. Earth-to-space and space-to-space weapons provide an offensive capability for attacking targets in space. Political scientists contend that war is more likely when the offensive is dominant—especially if it is difficult to distinguish between offensive and defensive weapons—and argue that there are strong incentives for striking first should a conflict appear inevitable.13 Surprise attack is perceived as leading to large rewards. Space weapons provide a first-mover advantage for striking in space, but their speed could create crisis instability since decisionmakers—on all sides—will have very little time (perhaps only a handful of minutes) to decide what to do in the face of a sudden attack in space, creating a high risk of rapid escalation due to misunderstanding, miscommunication, and miscalculation.

Finally, the use of destructive, non-reversible kinetic Earth-to-space or space-to-space weapons would likely leave a persistent cloud of debris and pose a long-term (potentially decades or much longer) hazard to all satellites, including commercial and scientific satellites as well as satellites from non-adversary nations. Using weapons with non-kinetic, non-permanent affects would mitigate this risk.

The Previous Debate: Changes in Context, Assumptions, and Alternatives

A vigorous public discussion covering many of the factors discussed above flared during the last period in which the U.S. seriously considered the merits of space-based weapons, peaking around 2002 and waning a few years later.14 But a lot has changed since then.

The earlier debate centered around two key alternatives: the first was whether the United States should deploy space-based weapons first—well before China or Russia would be capable of doing so effectively—in order to take a significant strategic leap ahead or, second, whether the United States should practice restraint in order to preserve strategic stability and not provoke China or Russia to react in kind. Those core alternatives are no longer operative. Since that era, China has deployed operational ground-based, direct-ascent, kinetic-kill ASATs and demonstrated co-orbital ASAT capabilities.15 Russia has also tested ground-based, direct-ascent kinetic ASATs and appears to have tested in-orbit anti-satellite weaponry as well. The United States no longer gets to choose whether to leap ahead or to seek to inspire restraint among U.S. competitors. Indeed, today both China and Russia have the capability to station weapons in space and the June 2020 Defense Space Strategy states bluntly that China and Russia have already weaponized space.16 While a future administration could revise U.S. strategy in space or attempt to secure new international agreements restricting space weapons, the U.S. has rung a bell that cannot be unrung by declaring space as a warfighting domain and by revealing some of what is known about potential adversaries’ activities there. There will be implications on behavior by allies, adversaries, and third parties, as well as within the U.S. government.

#### The US would retaliate to an attack on a satellite – NC3 failure is sufficient for a nuclear response

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

In January 2018, details of the Trump administration’s Nuclear Posture Review (NPR) were posted online by the Huffington Post, provoking widespread alarm over what were viewed as dangerous shifts in U.S. nuclear policy. Arousing most concern was a call for the acquisition of several types of low-yield nuclear weapons, a proposal viewed by many analysts as increasing the risk of nuclear weapons use.

Another initiative incorporated in the strategy document also aroused concern: the claim that an enemy cyberattack on U.S. nuclear command, control, and communications (NC3) facilities would constitute a “non-nuclear strategic attack” of sufficient magnitude to justify the use of nuclear weapons in response.

Under the Obama administration’s NPR report, released in April 2010, the circumstances under which the United States would consider responding to non-nuclear attacks with nuclear weapons were said to be few. “The United States will continue to…reduce the role of nuclear weapons in deterring non-nuclear attacks,” the report stated. Although little was said about what sort of non-nuclear attacks might be deemed severe enough to justify a nuclear response, cyberstrikes were not identified as one of these. The 2018 NPR report, however, portrayed a very different environment, one in which nuclear combat is seen as increasingly possible and in which non-nuclear strategic threats, especially in cyberspace, were viewed as sufficiently menacing to justify a nuclear response. Speaking of Russian technological progress, for example, the draft version of the Trump administration’s NPR report stated, “To…correct any Russian misperceptions of advantage, the president will have an expanding range of limited and graduated [nuclear] options to credibly deter Russian nuclear or non-nuclear strategic attacks, which could now include attacks against U.S. NC3, in space and cyberspace.”1

The notion that a cyberattack on U.S. digital systems, even those used for nuclear weapons, would constitute sufficient grounds to launch a nuclear attack was seen by many observers as a dangerous shift in policy, greatly increasing the risk of accidental or inadvertent nuclear escalation in a crisis. “The entire broadening of the landscape for nuclear deterrence is a very fundamental step in the wrong direction,” said former Secretary of Energy Ernest Moniz. “I think the idea of nuclear deterrence of cyberattacks, broadly, certainly does not make any sense.”2

Despite such admonitions, the Pentagon reaffirmed its views on the links between cyberattacks and nuclear weapons use when it released the final version of the NPR report in February 2018. The official text now states that the president must possess a spectrum of nuclear weapons with which to respond to “attacks against U.S. NC3,” and it identifies cyberattacks as one form of non-nuclear strategic warfare that could trigger a nuclear response.

That cyberwarfare had risen to this level of threat, the 2018 NPR report indicated, was a product of the enhanced cybercapabilities of potential adversaries and of the creeping obsolescence of many existing U.S. NC3 systems. To overcome these vulnerabilities, it called for substantial investment in an upgraded NC3 infrastructure. Not mentioned, however, were extensive U.S. efforts to employ cybertools to infiltrate and potentially incapacitate the NC3 systems of likely adversaries, including Russia, China, and North Korea.

For the past several years, the U.S. Department of Defense has been exploring how it could employ its own very robust cyberattack capabilities to compromise or destroy enemy missiles from such states as North Korea before they can be fired, a strategy sometimes called “left of launch.”3 Russia and China can assume, on this basis, that their own launch facilities are being probed for such vulnerabilities, presumably leading them to adopt escalatory policies such as those espoused in the 2018 NPR report. Wherever one looks, therefore, the links between cyberwar and nuclear war are growing.

The Nuclear-Cyber Connection

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.6

Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.7 Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.8 Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.9

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to paralyze the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”10

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike.

“The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.11 Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

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

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

‘Defending Forward’

Under these circumstances, one would think the major powers would seek to place restrictions on the use of offensive cyberweapons, especially those aimed at critical NC3 systems. This approach, however, is not being pursued by the United States and the other major powers.

Under the Obama administration, the Department of Defense was empowered to conduct offensive cyberstrikes on foreign states and entities in response to like attacks on the United States, but any such moves required high-level review by the White House and were rarely approved. This approach was embedded in Presidential Policy Directive 20 (PPD-20), adopted in October 2012, which states that any cyberaction that might result in “significant consequences,” such as loss of life or adverse foreign policy impacts, required “specific presidential approval.”

Officials in the Trump administration found this requirement unduly restrictive and so persuaded the president to rescind PPD-20 and replace it with a more permissive measure. The resulting document, National Security Presidential Memorandum 13 (NSPM-13), was approved in September 2018 but has not been made public. From what is known of NSPM-13, senior military commanders, such as Nakasone, enjoy preapproval to undertake offensive strikes against foreign entities under certain specified conditions without further White House clearance. In accordance with the new policy, military planners can prepare for offensive cyberattacks by seeking vulnerabilities in adversarial computer networks and by implanting malware in these weak spots for potential utilization if a retaliatory strike is initiated.15

As translated into formal military doctrine, this approach is described as “defending forward,” or seeking out the originators of cyberattacks aimed at this country and neutralizing them through counterstrikes and the insertion of malware for future activation. “Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.”16

In embracing this strategy, Nakasone and other senior officials insist that their intention is defensive: to protect U.S. cyberspace against attack and deter future assaults by letting opponents know their own systems will be crippled if they persist in malicious behavior. “For any nation that’s taking cyber activity against the United States,” said National Security Advisor John Bolton when announcing the adoption of NSPM-13, “they should expect…we will respond offensively as well as defensively.”17 For any potential adversary following these developments, defending forward will certainly be interpreted as preparation for offensive strikes in the event of a crisis, inviting stepped up defensive and offensive moves on their part.

Much less is known about the strategic cyberwar policies of other powers, but they likely parallel those of the United States. China, for example, has long been known to employ cyberspace to spy on U.S. military technological capabilities and steal what they can for use in developing their own weapons systems. Russia has been even more aggressive in its use of cyberspace, employing cyberweapons to cripple Ukraine’s electrical grid in 2015 and to influence elections. That Moscow has also sought to infiltrate the U.S. electrical grid suggests that it too intends to defend forward, by preparing for possible cyberattacks on U.S. command, control, and communications capabilities, including NC3 facilities.

Although occurring largely in secret, what can aptly be called “an arms race in cyberspace” is underway. Where this might lead is difficult to foresee, but it is certain to involve the development of ever more potent cyberweapons. Each nuclear power will seek to enhance its defenses against future cyberattack. Yet, just as is the case in missile warfare, it is easier and cheaper to devise new offensive cybersystems than defensive ones. In the event of a crisis, then, there will be a strong temptation to employ the new technologies early in the encounter, when they might be used to maximum effect, setting in motion an escalatory process resulting in nuclear weapons use. As noted, the mere fact that disruptive malware is known to have been embedded in the vital command-and-control systems of a nuclear power could lead it to distrust its early-warning and intelligence systems and, in a panicky response to ambiguous signals, assume the worst and launch its nuclear weapons.

Arms Control in Cyberspace

Given the various ways in which conflict in cyberspace could result in nuclear weapons use, steps must be taken to minimize the risk of escalation from one domain to the other, but conceiving of agreements to curb malicious and escalatory behavior in cyberspace is no easy task. Computer software cannot readily be classified and counted the way planes and missiles can, and states do not agree on definitions of offensive and defensive cyberweapons, let alone on measures to control them. Nevertheless, some efforts have been made to develop rules and protocols to restrain the destabilizing use of cybertechnologies, and these provide a framework for further consideration.

Perhaps the most extensive effort to adopt rules for acceptable behavior in cyberspace has been undertaken by the United Nations, in accordance with a series of General Assembly resolutions on the topic. This process first gained momentum in December 2011, when that body, “expressing concern” that emerging cybertechnologies “can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security,” established a group of governmental experts to assess the dangers in cyberspace and consider “possible cooperative measures to address them, including norms, rules, or principles of responsible behavior of States.”18

In its initial report, released in June 2013, the experts group warned of increasing threats to the safety of what it described as the realm of information and communications technology (ICT). “States are concerned,” it noted, “that embedding harmful hidden functions in ICTs could be used in ways that affect secure and reliable ICT use…and damage national security.” With this in mind, it affirmed a basic principle: “International law, and in particular the Charter of the United Nations, is applicable” in the ICT domain. On this basis, it called on member states to work together in “the application of norms derived from existing international law relevant to the use of ICTs.” Furthermore, as part of this effort, it recommended the crafting of confidence-building measures, such as the creation of information-sharing mechanisms to investigate serious cybersecurity incidents, aimed at minimizing the risk of unintended consequences.19

As the evidence of dangerous developments in cyberspace multiplied, UN General Assembly Resolution 68/243, called for the formation of a new experts group to consider restraints on ICT malpractice. That body released its report in July 2015, providing the most comprehensive blueprint to date for the management of cyberspace. Building on the earlier experts group report, it articulated a set of norms that should govern behavior in this realm. Foremost among these was the precept that states “should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure” of another country. Other norms articulated in the report include the proviso that states should not allow their territory to be used for “internationally wrongful acts using ICTs” and should seek to “prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.”20

By articulating a set of fundamental norms, the 2015 experts group report provides a useful starting point for further consideration of arms control in cyberspace. Lacking any decision-making authority, however, the UN group in advocating for those norms called only for conversations among states on their implementation and the adoption of “voluntary, non-binding norms” for responsible behavior. The General Assembly, addressing the topic on several occasions since then, has only reiterated the principles of the 2015 report and called on member states to follow its guidance without achieving any obvious, genuine progress.

Several other initiatives have been undertaken by states and nonstate entities to promote restraint in cyberspace. In February 2017, Brad Smith, the president of Microsoft, called for the formulation of a “Digital Geneva Convention,” modeled on the existing, post-World War II Geneva Conventions, aimed at protecting civilians from the negative consequences of cyberattacks.21 Some academics, including scholars at the Notre Dame Institute for Advanced Study, have carried this notion further, calling for the worldwide embrace of "cyberpeace" based on the adoption of common norms and rules.22 “Just as the world’s governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war,” he declared, “we need a Digital Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace.”

President Emmanuel Macron of France has advocated for similar measures at the international level. In November 2018, he unveiled the “Paris Call for Trust and Security in Cyberspace” at a major gathering in the French capital. Essentially a rewording of past UN resolutions and the 2015 experts group report, it called for international cooperation in reducing malicious behavior, especially cybercrime and political warfare.23 Although signed by leaders of more than 50 countries, including France, Germany, Italy, Japan, and the United Kingdom, President Donald Trump refused to endorse the Paris call, presumably because it might infringe on U.S. plans to employ cyberweapons in an offensive mode (no reasons were provided for the U.S. refusal to sign).24

At this point, the likelihood that the United States, Russia, and China will adopt and respect international constraints on the use of cyberweapons aimed at the critical information and communications systems of their adversaries appears virtually nil. Nevertheless, it is vitally important that UN officials, industry figures, and prominent national leaders continue to articulate such norms and call for their adoption. Hopefully, these precepts will form the basis for binding international agreements, when enough key governments are prepared to embrace such measures. In the meantime, it is essential that policymakers and arms control advocates pursue other routes to arms control in cyberspace.

Perhaps the most promising approach in this regard is the adoption of formal or informal agreements to eschew certain behaviors that would increase the risk of unintended or accidental nuclear escalation. This would involve meetings between U.S. and Russian officials, possibly under the auspices of the currently suspended Strategic Stability Dialogue; between U.S. and Chinese officials; or possibly all three together aimed at identifying certain rules of the road to which all sides would agree to adhere, such as a ban on the implantation of malware in the NC3 systems of their adversaries.

A precedent for such high-level accords is provided by U.S. President Barack Obama’s September 2015 agreement with Chinese President Xi Jinping to bar the use of cyberspace for the theft of intellectual property. Although there is widespread debate over the extent to which China has abided by the 2015 accord, there is general agreement that it did result for a time in a diminished level of Chinese cyberespionage in the United States.25

Such an approach was advanced by Stoutland and Pitts-Kieter in their 2018 study of cyberweapons and nuclear stability. “As a priority first step,” they said, “the United States should seek to initiate a bilateral dialogue with Russia” intended to “develop mutual understanding on how cyber threats can affect deterrence and strategic stability.” Such talks, they wrote, “should be held with a view toward developing a shared understanding of our mutual interest in minimizing that risk and identifying practical ways to address it bilaterally and multilaterally.”26

At present, none of these approaches for the control of cyberspace appears to be making any headway. As a consequence, the arms race in cyberspace is rapidly gaining momentum, greatly increasing the likelihood that future confrontations among the major powers will entail the early use of sophisticated cyberweapons, magnifying the risk of rapid and uncontrolled nuclear escalation. Because this danger has received far less attention than other pathways to escalation, it is essential that policymakers and arms control advocates devote far more effort to controlling cyberspace than they have up until now.

#### Any direct conflict with Russia would quickly draw in other powers and cause extinction

CJ Atkins 22, Ph.D. in political science from York University in Toronto, March 17, 2022, “Why a Ukraine ‘no-fly zone’ would mean the end of the world…literally” https://www.peoplesworld.org/article/why-a-ukraine-no-fly-zone-would-mean-the-end-of-the-worldliterally/

The reality is that enforcing a no-fly zone would literally mean that NATO (which basically implies U.S.) warplanes and missiles would be shooting down Russian planes—American military personnel killing Russian military personnel.

That would mean war—immediate war between Russia and the 30 nations of the U.S.-dominated NATO alliance. And a war between Russia and the United States could very easily escalate to an all-out nuclear confrontation. Russia already put its nuclear forces on high alert before the invasion of Ukraine and warned others to stay out, and U.S. missiles are always ready to launch at a moment’s notice.

No one should underestimate the consequences at stake.

A nuclear war between Russia and the United States would mean hundreds of millions of people dead within hours, or even minutes. Washington, New York, Los Angeles, Chicago, Moscow, St. Petersburg, Kiev, London, Paris, Berlin, and so many more cities would be wiped off the map. In such a nuclear exchange, it would probably also be hard to keep other nuclear powers from being dragged in, so Beijing, Shanghai, Taipei, and various metropolises far removed from the war zone could also be vaporized.

Some voices in the media, well aware of what a no-fly zone would risk, are willing to gamble the future of humanity. Sam Bowman, editor of the publication Works in Progress and former executive director of the Adam Smith Institute, a capitalist think tank, wrote on Twitter on March 14:

“My view is basically that nuclear war is worth risking for some things, like keeping as much of Europe free and independent of Russia as we can. But I think that’s a hard position to hold if you think the extinction of humanity is so bad that avoiding it trumps everything else.”

God save the free market, everything else be damned—so goes the logic apparently.

Luckily, Biden, other NATO leaders, and most in the U.S. Congress recognize the reality that if there is a nuclear war, there won’t be any Europe, any free markets, any humanity, or anything else left—and so they continue to resist calls for a no-fly zone, so far.

#### Mounting Russian ASAT capabilities necessitate a clarification of non-kinetic response thresholds

Marcin Piotrowski ’19, Ph.D. in Political Science from the University of Warsaw, Analyst with the International Security Program at the Polish Institute of International Affairs; Polish Institute of International Affairs, November 14, "Russia’s Approach to Anti-satellite Weapons and Systems," <https://pism.pl/file/8abbf9bc-8742-4f18-a2e9-c09c73ac69d0>

Implications for the U.S. and NATO. Russia is concerned about the United States’ growing technological advantage and military domination in space and is proposing international laws aimed at limiting ASAT. At the same time, the Russian authorities are developing kinetic ASAT weapons, which are presented as a response to similar projects carried out by China, the U.S. and India. Russia is currently able to add ASAT functions to missile defence systems such as A-235 and S-400, which can intercept exo-atmospheric warheads. In the next few years, it will also be able to use kinetic ASAT weapons (Rudolf and S-500) against civilian and military satellites in low-earth orbit and to deploy robotic satellites capable of disrupting military and civilian satellites in higher orbits. Russia’s ASAT weapons are an element of its “asymmetric response” to the development of the United States’ missile defence, new ground-launched missiles and hypersonic weapons. The U.S. is also paying close attention to Russia’s visible and advanced non-kinetic ASAT capabilities in terms of electronic and cyber-attacks. These threats from Russia were among the factors justifying the recent creation of a new space force branch of the military in the United States.

The broadening spectrum of Russia’s ASAT capabilities also requires a response from NATO and EU states. The Alliance approved a space policy in June, and the next stage might take place at the December meeting of NATO heads of state and government in London, where space will be recognised as a fifth domain of military operations and the Allies will work on a specific space strategy. NATO’s doctrines current see air and space as one, so need to be updated to take account of new threats. Within NATO there is a need to address the implications of ASAT weapons on Article 4 of the Washington Treaty. It may be that non-kinetic disruption of a satellite belonging to any NATO member will be the subject of consultations under Article 4, and the Alliance could decide that the physical destruction of a member’s satellite may be deemed an act of aggression that would call for Article 5 to be invoked. Allied exercises should incorporate ASAT-attack and GPS-jamming scenarios in future, particularly when planning large-scale exercises such as the upcoming Defender 20. Poland’s armed forces technical modernisation programme for the period to 2035 assumes the acquisition of reconnaissance satellites, so additional protection from non-kinetic attacks might be necessary. The EU institutions and countries should use information campaigns to increase awareness among civilians who rely on satellites vulnerable to non-kinetic ASAT attacks during peacetime or in hybrid warfare.

### 1AC - Plan

#### The United States federal government should substantially increase its space cybersecurity resilience efforts with the North Atlantic Treaty Organization including at least clarifying response to cyber attacks in space

### 1AC - Solvency

#### International action is key – US cooperation with NATO secures satellite assets

David Fidler 18, the James Louis Calamaras Emeritus Professor of Law at Indiana University, Adjunct Senior Fellow for Cybersecurity and Global Health at the Council on Foreign Relations, 4/3/18, “Cybersecurity and the New Era of Space Activities,” https://www.cfr.org/report/cybersecurity-and-new-era-space-activities

The tasks of securing outer space and cyberspace are converging. The internet increasingly depends on space-enabled communication and information services. Likewise, the operation of satellites and other space assets relies on internet-based networks, which makes these assets, like cars and medical equipment, devices on the internet of things. New government actors, companies, goals, and technologies are expanding and transforming space activities. However, neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace, which could increase national security risks.

To meet these challenges, government, industry, and international action is needed. The Donald J. Trump administration’s National Space Council should develop cybersecurity recommendations for space activities, and federal agencies should prioritize these within the government and in cooperation with the private sector. In crafting needed legislation for commercial space activities, Congress should bolster industry efforts to strengthen cybersecurity. Private-sector actors should strengthen their adoption of cybersecurity best practices and collaborate with one another on improving implementation of cybersecurity strategies. Internationally, the United States should pursue collaboration on space cybersecurity through the North Atlantic Treaty Organization (NATO), plurilateral space cooperation mechanisms, and bilateral forums.

Outer space has been a national security priority for spacefaring nations since the 1950s. Governments started space programs for intelligence, military, political, and scientific purposes and developed countermeasures against space-based threats from rivals, such as anti-satellite capabilities. Countries managed security competition by banning weapons of mass destruction in space and cooperating on peaceful uses of space. Government programs catalyzed private-sector adaptation of dual-use technologies to provide satellite communication services.

Despite the importance of satellites, the U.S. General Accounting Office concluded [PDF] in 2002 that efforts on critical infrastructure protection did not include the satellite industry, but should do so. Similarly, cybersecurity has not been a priority in government and private-sector space endeavors. One leading analysis [PDF] asserted that cybersecurity discussions often overlook space activities’ vulnerability to cyberattack. For example, neither the UN governmental group of experts (GGE) on outer space nor the UN GGE on cyberspace addressed the convergence of their respective agendas.

Governments, critical infrastructure, and economies rely on space-dependent services—for example, the Global Positioning System (GPS)—that are vulnerable to hostile cyber operations. Geopolitical competition fuels the militarization of space, which heightens state incentives to devise cyber espionage, interference, and attack strategies against rivals’ space operations. The United States suspects that China has engaged in cyber operations against U.S. satellites. Chinese military writings emphasize [PDF] the need to target satellites to “blind and deafen the enemy.” The then commander of Air Force Space Command, General John E. Hyten, told Congress in 2016 that “adversaries are developing . . . cyber tools to deny, degrade, and destroy” [PDF] U.S. space capabilities that support war fighting, critical infrastructure, and economic activity. Other countries likely believe the United States is preparing to conduct cyber espionage, disruption, and attack operations against the space assets of rival states.

The commercialization of space heightens cybersecurity concerns for many reasons, including market incentives to lower costs and innovate quickly, often at the expense of software and hardware security. Entrepreneurial activities—dubbed the New Space sector—are underway in space transport, space tourism, asteroid mining, lunar operations, and missions to Mars. A small-satellite (“smallsat”) revolution involving spacecraft far smaller than traditional satellites is unfolding. Networks of linked smallsats can provide internet access, communications, data storage and transmission, imaging, and remote sensing. This next generation of satellites harnesses innovations in computing, electronics, miniaturization, imaging, sensors, big data, and artificial intelligence. Satellite services for Earth observations from space are growing. They support many policy and commercial purposes and contribute to agricultural productivity, transportation efficiency, and environmental monitoring. Commercial space activities use cutting-edge technologies and produce valuable data and are, thus, targets for cyber espionage, including economic cyber espionage, and cybercrime.

Challenges

Space agencies, the satellite industry, cybersecurity researchers, nongovernmental bodies, and intergovernmental satellite organizations show increasing awareness of the space cybersecurity challenge. Nevertheless, experts are worried. NASA’s then chief information security officer, Jeanette Hanna-Ruiz, warned that “it’s a matter of time before someone hacks into something in space.” Chatham House’s David Livingstone asserted that “people are just shuffling . . . paper around” and suggested that only “a disaster” might catalyze serious action. Josh Hartman, a former senior Pentagon official and Air Force officer, argued before the satellite industry’s first cybersecurity summit held in 2017 that, on cybersecurity, “most of the space community . . . has their heads in the sand.” The “attack surface” of space activities is expanding, but governments and industry are not taking adequate action.

Protecting space activities requires understanding the particular cyber vulnerabilities that arise in various space operations. For example, satellite cybersecurity encompasses the satellite itself, transmissions to and from Earth, and ground stations. U.S. military and intelligence satellite systems are vulnerable to kinetic and cyberattacks. Civilian smallsat systems might also prove insecure, given the lack of cybersecurity in their design, their use of commercial off-the-shelf components, and the vulnerabilities potentially created by connecting satellites to operate as complex, orbiting networks.

Neither international law nor diplomacy has grappled effectively with space cybersecurity. Multiple bodies of international law are relevant, but controversies about whether and how international law applies to cyberspace have adversely affected cyber diplomacy. Such travails have elevated the prominence of nongovernmental efforts to clarify international law’s application in cyberspace, such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. However, states continue to conduct cyber operations that violate international law. For example, the UN International Telecommunication Union prohibits interference with satellite transmissions, yet such interference frequently occurs.

The militarization of space potentially threatens the requirement in the Outer Space Treaty (OST) that space activities comply with international law to maintain international peace and security and promote international cooperation. The United States has declared that space is now a “war-fighting domain,” and China’s and Russia’s military ambitions in space are growing. The UN Committee on Disarmament’s work on a treaty to prevent an arms race in space failed. As happened with cyberspace, these difficulties in space diplomacy have increased nongovernmental interest in clarifying how international law applies to military operations in space.

The commercialization of space fuels concerns that the private sector will unduly influence how states interpret the OST’s duty to authorize and supervise nongovernmental space activities. The debate over whether U.S. support for commercial space activities violates this OST requirement might also create diplomatic problems.

New diplomatic initiatives on space cybersecurity would encounter headwinds. Putting “space” before “cybersecurity” does not alleviate the geopolitical tensions that already limit cooperation on cyberspace and space. The United States, China, and Russia have not agreed on how to approach cybersecurity or address military activities in space. Recent diplomatic activities on space and cybersecurity concluded without addressing space cybersecurity, including the UN GGEs on cyberspace and outer space and the European Union’s code of conduct for space activities [PDF]. Negotiations in the UN Committee on Peaceful Uses of Outer Space on guidelines for the long-term sustainability of space activities considered but did not adopt proposed guidelines [PDF] on information-security policies for the terrestrial and orbital parts of space systems. Controversies and disagreements during these efforts suggest that reopening them for space cybersecurity would not be effective. Further, the increased number of spacefaring nations, which now includes such countries as South Korea and the United Arab Emirates, complicates diplomacy by requiring more countries to reach consensus.

States might also believe more diplomatic activity is not necessary because they already have sufficient incentives to refrain from dangerous cyber operations in space. Disabling a satellite through cyber means could turn it into space debris—already a major problem—that threatens space activities for all countries. The importance of intelligence satellites in maintaining nuclear deterrence also encourages restraint in interfering with the satellites of rival nuclear powers. Following trends on Earth, countries might want to avoid diplomatic activity in order to engage in cyber operations in space that “subvert the integrity of political, social, and economic systems, rather than destroy physical infrastructure” by, for example, manipulating or hijacking an adversary’s space infrastructure to spread propaganda and misinformation.

Recommendations

Government

The United States can provide leadership on cybersecurity in outer space through a comprehensive strategy. The Trump administration is positioned to advance space cybersecurity because its priorities include improving critical infrastructure cybersecurity, addressing security threats to space operations [PDF], and promoting commercial space activities. The administration resurrected the National Space Council and should task it with developing recommendations on strengthening the cybersecurity of space infrastructure. To do so, the council should convene government officials and leaders from the commercial space sector to share insights on managing cybersecurity as space and cyberspace merge. These leaders should include people who have led both information technology and space enterprises, such as Paul Allen (Stratolaunch Systems), Jeff Bezos (Blue Origin), and Elon Musk (SpaceX). The Trump administration should instruct the Department of Commerce, Department of Homeland Security, Federal Aviation Administration, Federal Communications Commission, and NASA to make cybersecurity a priority in their space collaborations with the private sector.

With private-sector space activities expanding, Congress should adopt a comprehensive regulatory framework for the commercial space sector. Current law does not regulate the full range of space activities the private sector is planning, a problem recognized [PDF] but not addressed during the Barack Obama administration. A comprehensive framework would provide commercial space enterprises with regulatory certainty and help the United States comply with its OST obligation to authorize and supervise nongovernmental space activities. The legislation should emphasize the importance of existing federal law on cybersecurity information sharing, provide government assistance to industry-led efforts to strengthen space cybersecurity (especially concerning threats from state actors), and—as happened in other sectors, such as energy—facilitate public-private collaborations on cybersecurity.

Industry

Improving space cybersecurity requires extending good cybersecurity practices into the commercial space sector and addressing problems specific to space activities. Advice for this sector repeats familiar mantras, such as the need for intra-sector collaboration, information sharing, enterprise risk management, encryption, insider threat prevention, and supply chain protection. The federal government has, for example, rightly stressed [PDF] the utility of the Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity [PDF] for satellite companies.

Industry associations in space sectors should move from identifying general principles and recommendations, such as those in the Joint Statement on the Satellite Industry’s Commitment to Cybersecurity, to supporting implementation activities. The Satellite Industry Association could, for example, include in its annual State of the Satellite Industry Report [PDF] information on the industry’s cybersecurity activities, as is done in other industries.

International

The difficulty of reaching multilateral agreement on cybersecurity and space issues means the United States should address space cybersecurity in plurilateral and bilateral contexts. The United States should raise space cybersecurity within NATO, given the alliance’s plans to upgrade its satellite and cyber defense capabilities. U.S. bilateral cybersecurity cooperation with spacefaring countries, such as India and Japan, should include space cybersecurity. With their history of collaboration, NASA and the European Space Agency, which is increasingly aware of cybersecurity threats to its programs, should sign a memorandum of understanding to cooperate on space cybersecurity.

More ambitiously, the United States should use effective mechanisms of space diplomacy to improve space cybersecurity. For example, the International Space Station (ISS) has involved the United States, Canada, Japan, Russia, and the European Space Agency managing the “the most politically complex space exploration program ever undertaken.” The United States should discuss the need for more cooperation on space cybersecurity within the ISS framework. In addition, the United States could lead establishment of an intergovernmental coordination mechanism for developing guidance on space cybersecurity. The mechanism could be modeled on the Inter-Agency Space Debris Coordination Committee (IADC), composed of space agencies from leading spacefaring countries. The IADC’s nonbinding guidelines are credited with reducing space debris produced by new launches.

Conclusion

Actions at the national, industry, and international levels can harness growing awareness about space cybersecurity and strengthen policy and industry practices as the convergence of space and cyberspace accelerates. Outer space might not be the “final frontier for cybersecurity,” but achieving cybersecurity beyond Earth is one of the many responsibilities the new era of space activities creates for governments and societies.

#### NATO-US space cooperation over info sharing and cross-organization liaison communications solves Russian and Chinese attacks

Frank Rose 20, Analyst at Elcano Royal Institute working on the technology and digital agenda, former senior fellow and the co-director of the Center for Security, Strategy, and Technology in the Foreign Policy program at the Brookings Institution, 4/22/2020, "NATO and outer space: Now what?," https://www.brookings.edu/blog/order-from-chaos/2020/04/22/nato-and-outer-space-now-what/, sg

THE EMERGING ANTI-SATELLITE THREAT

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

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

IMPROVE INTELLIGENCE-SHARING

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

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

MAINSTREAM OUTER SPACE AT NATO

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

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

ENSURE COOPERATION AND COORDINATION WITH THE UNITED STATES

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

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

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

#### NATO unity is key – interoperability in space enables effective communication

Beyza Unal 19, PhD Old Dominion University, senior research fellow with the International Security Department at Chatham House, specializes in nuclear and cyber policies, worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, William J. Fulbright alumna, July 2019, “Cybersecurity of NATO’s Space-based Strategic Assets,” https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

Interoperability enables allies to operate their space systems without having to make adaptations so that their systems can function efficiently.

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

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

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

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

# 2AC Case

## 2AC – China Adv

### 2AC – Cyber Solves

#### Only revitalizing NATO cooperation can stop a Sinocentric world order---failure to mobilize various geographic focuses allows numerous cyberspace threats.

Liselotte Odgaard 22, professor at the Norwegian Institute for Defense Studies, 2/24/2022, "NATO’s China Role: Defending Cyber and Outer Space," *Washington Quarterly*, 45(1), pp 175-180, https://doi.org/10.1080/0163660X.2022.2059145, sg

Rather than highlighting the need for a division of labor within NATO, the 2022 invasion has highlighted that Russia’s appetite for threatening Europe with military action is closely entwined with its long-standing strategic cooperation with China. Intelligence reports that China told Russia in February 2022 not to invade Ukraine before the end of the Winter Olympics in Beijing testify to the closely orchestrated Chinese-Russian approach to the West.18 Moscow and Beijing are both strategic opponents of the US, a shared status that has spurred them to coordinate their separate geostrategic priorities in Europe and the Indo-Pacific, forging unison pushback against what they consider Western encroachments on their spheres of interest.19 The poorer than expected performance of the Russian armed forces in its 2022 war with Ukraine has pushed China to try to appear neutral. Nevertheless, China has joined Russia in opposing further enlargement of NATO, and in the Indo-Pacific, Russia has joined China in opposing Taiwanese independence.20 It would be wise for Europe and the US to plan for Sino-Russian geostrategic coordination to continue unless more clear evidence that China will abandon Russia is presented. One thing is certain: China will work with the partners that help it advance a Sinocentric international order based on authoritarian regimes. And to counter this development, Europe and the United States need to devise effective mechanisms for joint responses to Beijing as well as to Moscow.

A US-European division of labor is not likely to help NATO develop tools to defend itself against threats from China and Russia. The lack of electronic warfare in Russia’s war with Ukraine has revealed gaps between its concept of operations and the tactics of the Ukrainian military. As demonstrated in prior operations in Syria and the Donbas, Russia will adapt and learn in the short and long term. For example, Russia can be expected to improve its electromagnetic spectrum management in order to enhance its planning and management of forces on the battlefield. Meanwhile, China is watching the performance of the parties involved in the war with a view to update its cyber and space capabilities as well as strategic concepts. As a consequence, both Russian and Chinese threats will continue to increasingly emerge in the cyber and space domains. This calls for global and functional defenses rather than an exclusive geographical focus. It is more important than ever to design NATO for a future where threats toward transatlantic security are global and requires a unified response.

### 2AC – Deterrence Solves

#### There are growing cyber threats to the NATO’s satellites – Russia and China are rapidly advancing their cyber capabilities and have the potential to attack the NATO’s space based assets

Karl-Heinz Brunner 21, member NATO Parliamentary Assembly and the Bundestag Defence Committee and Subcommittee on Disarmament, Arms Control, and Non-Proliferation, October 2021, “Space and Security – NATO’s Role,” NATO Parliamentary Assembly, Science and Technology Committee, https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/025%20STC%2021%20E%20-%20SPACE%20AND%20SECURITY%20-%20BRUNNER\_2.pdf

42. Space denial capabilities of NATO (near-)peer competitors have significantly increased in recent years, and so have the number of tests of such technologies. Several countries possess weapon systems that have the potential to harm space assets at any time. According to CSIS’s 2020-Space Threat Assessment there are four types of systems that can be used to damage or destroy space-based assets (Harrison, Johnson, Roberts, Way, & Young, 2020): (1) kinetic physical counterspace weapons, built to directly strike satellites or the ground stations operating them; (2) non-kinetic weapons, including lasers, high powered microwave (HPM) weapons, and electromagnetic pulse (EMP) weapons, that can physically affect space assets without any direct contact; (3) electronic attacks targeting signal transmissions to and from satellites by interfering with radio-frequencies (RF) by creating noise in the same frequencies (jamming) or by falsifying a signal and tricking the receiver into it (spoofing), thus corrupting the data; (4) cyberattacks, that target data instead of transmission frequencies. 43. Kinetic physical counterspace weapons have attracted the most attention by far. Tests of direct-ascent anti-satellite (ASAT) weapons have increased as more countries develop capabilities in this domain (Harrison, Johnson, Roberts, Way, & Young, 2020). The most prominent of these tests has arguably been the destruction of a satellite by China in 2007 which increased space debris in LEO by roughly 10% and was followed by broad international condemnation (Ohlandt, McClintock, & Flanagan, 2021). A more recent ASAT test by China, conducted in 2018, was further evidence of Beijing’s growing prowess and ambition in space. Building on extensive experience from Soviet-era ASAT-programmes, Russia has also invested in numerous kinetic physical counterspace capabilities and allegedly has a range of ground-based and air-launched directascent ASAT missiles that could target satellites at its disposal (Harrison, Johnson, Roberts G., Way, & Young, 2020). 44. In addition to direct-ascent systems, co-orbital ASAT-weapons have also already been deployed in space. Their activity is more difficult to detect, however, as it is very similar to on-orbit maintenance or debris removal missions. As most space technologies, co-orbital weapons are a dual-use technology and can be used for both civilian and military purposes. Arguably, any asset in the orbits above earth can be qualified as a weapon just because of its high velocity. With speeds between 11,000 (GEO) and 28,000 (LEO) kilometres per hour, a satellite that changes orbit becomes a kinetic weapon by definition. 45. Some of the most advanced space denial assets have been developed and tested by the People’s Republic of China (PRC). The Pentagon’s annual China military power report notes that Beijing’s space capabilities include orbiting space robots (U.S. Department of Defense, 2020). Similarly, Russia has repeatedly launched inspection-satellites into LEO, which could potentially serve as co-orbital ASAT weapons. Although Moscow has not officially announced any plans to develop space based ASAT weapons, US Space Command accused the Kremlin of testing such weapons-systems under the guise of maintenance in 2020 (US Space Command, 2020). 46. Other than China and Russia, numerous other states are working on counter-space capabilities (Raju, 2020). The threat is also illustrated by the variety of modes of action against satellites: missiles, co-orbital, jamming, directed energy and cyber (Weeden & Samson, 2020). Research and development in these areas is significant, progress is rapid, and some capabilities such as jamming are already in use, in the Middle East (BBC, 2012) or to disrupt NATO exercises in the High North (Deutsche Welle, 2018). Even civilian systems, such as those intended for rendezvous and proximity operations to dock with a space station or perform maintenance, could be dual-use and pose a threat in the vicinity of military satellites or those providing services essential to our economies and lifestyles. 47. While receiving less public attention than their kinetic counterparts, non-kinetic weapon systems such as lasers and electronic technologies enabling jamming or spoofing have also been increasingly developed and tested. According to the Rand Corporation, China continues to develop space weapons and has developed jamming capabilities and tested them in exercises (Manson & Shepherd, 2020). 48. The development of China’s non-kinetic capabilities dates back to the purchase of Soviet-era equipment from Ukraine in the late 1990s (CSIS, 2018). Since then, Beijing’s indigenous space industry has made the ability to jam satellite communications one of its priorities (USCC, 2015) and has developed and tested several systems (DIA, 2019). China’s electronic warfare capacity includes an ionospheric radar located on the island of Hainan that is able to influence particles up to 2,000 kilometres. In 2020, officials announced an airborne laser which, although developed to target military aircraft or missiles, could potentially be used against satellites (Zhen, 2020). 49. Russia, too, has been consistently enhancing its space denial capabilities. The state armament programme for the period until 2027 lists the development of defensive space-based systems deployed to protect Russian satellites (Zak, 2018). Moreover, Russia is commonly believed to be testing electronic counterspace warfare, jamming and spoofing adversaries’ satellites in conflict zones as well as in nearby territories (Harrison, Johnson, Roberts, Way, & Young, 2020) and even on GPS-Satellites within its own state borders (BBC, 2018). 50. Finally, several actors in space have developed substantial knowledge in the cyber realm. As cyber-attacks are significantly cheaper and much harder to attribute than direct-ascent or co-orbital ASAT, they are a compelling alternative to these weapon systems. Russia has demonstrated its cyber capabilities as early as 1998, when it allegedly took control of a US-German satellite, pointed it at the Sun and thus destroyed its instruments (Tucker, 2019). The Chinese government appears to also have tested its cyber capabilities in several instances such as during the 2014 National Oceanographic and Atmospheric Administration (NOAA) hack (Al-Rodhan, 2020). The attack disrupted weather information and impacted end users around the globe (Al-Rodhan, 2020). More generally, research and development in space denial capabilities is significant, progress is rapid, and some capabilities, such as jamming, are already in use, for example in the Middle East (BBC, 2012) or to disrupt NATO exercises in the High North (Deutsche Welle, 2018).

### 2AC – Yes China Attack

#### China and Russia are already beginning to be aggressive – they are developing weapons that will be used to commit acts of war in space.

Rogin ’21 (Josh Rogin, columnist for the Global Opinions section of The Washington Post and political analyst for CNN. “A shadow war in space is heating up fast” 11/30/21, https://www.washingtonpost.com/opinions/2021/11/30/space-race-china-david-thompson/)

When Russia blows up a satellite in space with a missile ([as it did this month](https://www.bbc.com/news/science-environment-59299101)), or when China tests a new hypersonic missile ([as it did last month](https://www.armscontrol.org/act/2021-11/news/china-tested-hypersonic-capability-us-says)), the ongoing arms race in space leaps into the news. But in between these “[Sputnik](https://www.nytimes.com/2021/10/27/us/politics/china-hypersonic-missile.html)”-like moments, outside the public’s view, the United States and its adversaries are battling in space every day.

While Washington officials and experts [warn of the risks](https://www.rand.org/blog/2020/10/how-to-avoid-a-space-arms-race.html) of an arms race in space, the United States’ adversaries are constantly conducting operations against U.S. satellites that skirt the line between intelligence operations and acts of war. The pace of conflict is intensifying, according to a top Space Force general, who told me that China could overtake the United States to become the number one power in space by the end of the decade.

“The threats are really growing and expanding every single day. And it’s really an evolution of activity that’s been happening for a long time,” Gen. David Thompson, the Space Force’s first vice chief of space operations, told me in an interview on the sidelines of the recent [Halifax International Security Forum](https://halifaxtheforum.org/). “We’re really at a point now where there’s a whole host of ways that our space systems can be threatened.”

[John W. “Jay” Raymond: How the U.S. Space Force is trying to bring order to increasingly messy outer space](https://www.washingtonpost.com/opinions/2021/11/29/space-activity-its-debris-increases-us-works-establish-international-norms-rules/?itid=lk_interstitial_manual_6)

Right now, Space Force is dealing with what Thompson calls “reversible attacks” on U.S. government satellites (meaning attacks that don’t permanently damage the satellites) “every single day.” Both China and Russia are regularly attacking U.S. satellites with non-kinetic means, including lasers, radio frequency jammers and cyber attacks, he said.

Thompson repeatedly declined to comment on whether China or Russia has attacked a U.S. military satellite in a way that did permanent or significant damage, telling me that would be classified if it had happened. The Chinese military is quickly deploying ground-based systems for doing battle in space, [such as lasers](https://spacenews.com/op-ed-u-s-satellites-increasingly-vulnerable-to-chinas-ground-based-lasers/) that can [damage nosy U.S. intelligence community satellites](https://www.smh.com.au/world/asia/space-lasers-and-the-new-battlefield-emerging-under-china-s-anti-satellite-tactics-20210804-p58ft2.html), which could be considered an act of war.

“The Chinese are actually well ahead [of Russia],” Thompson said. “They're fielding operational systems at an incredible rate.”

Both the Russians and the Chinese are working on satellites that can attack other satellites, he said. For some time now there have been reports that China was developing a [satellite that could claw](https://medium.com/war-is-boring/chinas-mystery-satellite-could-be-a-dangerous-new-weapon-630a858923ec) another satellite or [grab one with a robotic arm](https://www.foxnews.com/world/china-satellite-launch-space-weapons) or a grappling hook. The Chinese government has several reasons to want to disable U.S. satellites, which have been useful in revealing concentration camps built to intern Uyghur Muslims and [new Chinese nuclear missile silo fields](https://fas.org/blogs/security/2021/07/china-is-building-a-second-nuclear-missile-silo-field/).

In 2019, Russia deployed a small satellite into an orbit so close to a U.S. “national security satellite” that the U.S. government didn’t know whether it was attacking or not, Thompson said. Then, the Russian satellite backed away and conducted a weapons test. It released a small target and then shot it with a projectile.

“It maneuvered close, it maneuvered dangerously, it maneuvered threateningly so that they were coming close enough that there was a concern of collision,” he said. “So clearly, the Russians were sending us a message.”

China is building its own version of satellite-based global positioning systems, said Thompson. That’s in addition to the “couple of hundred” intelligence, surveillance and reconnaissance satellites China has now deployed to watch over any part of the globe. China is also putting satellites into space at twice the rate of the United States, meaning that if nothing changes on our end, China will surpass the United States in capability in space in a few years, he estimated.

“We are still the best in the world, clearly in terms of capability. They're catching up quickly,” he said. “We should be concerned by the end of this decade if we don't adapt.”

While China is quickly [weaponizing space](https://thediplomat.com/2017/01/how-china-is-weaponizing-outer-space/), [its government points fingers](https://www.globaltimes.cn/page/202109/1235454.shtml) at United States, claiming that Washington is the diplomatic stumbling black. [There are reports](https://www.nytimes.com/2021/11/28/us/politics/china-nuclear-arms-race.html) that the Biden administration is reaching out to Beijing to establish new negotiations for a nuclear arms control, as well as international norms for cyberspace and space, but U.S. officials say that China won’t meaningfully engage.

## 2AC – Russia Adv

### 2AC – Grey Zones Bad

#### Grey zones increase the likelihood of cyber attacks – those could escalate

Pearson and Landay ’22 (James Pearson, European Cybersecurity Correspondent for Reuters, Jonathan Landay, U.S. National Security Correspondent for Reuters, Winner of the 2017 Arthur Ross Media Award. “Cyberattack on NATO could trigger collective defence clause – official” 02/28/22, <https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/>)

A cyberattack on a NATO member state could trigger Article 5, its collective defence clause, a NATO official said on Monday, amid concerns that chaos in cyberspace around Russia's invasion of Ukraine could spill over into other territories.

The military alliance has for years made clear that a serious cyberattack could trigger the clause, but such a scenario has so far been largely hypothetical.

"Allies also recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as an armed attack," the official told Reuters.

"We will not speculate on how serious a cyberattack would have to be in order to trigger a collective response. Any response could include diplomatic and economic sanctions, cyber measures, or even conventional forces, depending on the nature of the attack," the official said.

Whether or not a cyberattack met the threshold of an attack large enough to trigger Article 5 was a "political decision for NATO Allies to make," they added.

Britain and the United States have warned of potential cyberattacks on Ukraine which could have international consequences should, for example, malicious software designed to target networks in Ukraine start to spread elsewhere.

There has also been concern among cybersecurity experts that Russia could team up with some of the gangs and people who release malicious software, such as malware used to hold Colonial Pipeline to ransom in the United States last year.

U.S. Senate Intelligence Committee Chairman Mark Warner said there were no clear guidelines on how NATO (North Atlantic Treaty Organization) should respond, should such an attack take place.

"These are things that have been in hypothetical discussion for a decade, but because we've not come to any universal conclusion on what those standards should be, what level of attribution is needed, we're kind of in a very grey area," he told Reuters.

He posed the hypothetical case of a Russian cyberattack on Ukraine that impacts NATO member Poland, triggering power outages that result in hospital patients dying or knocking out traffic lights, causing fatal road accidents involving U.S. troops deployed there.

"The West may have wanted strategic ambiguity in this area, and that may still be the right choice," he added.

"But have we sufficiently made clear to the Russians the red lines on cyber or frankly to the NATO public, the American public, on red lines on cyber? I don't think we've done that."

Warner said he was "pleasantly surprised" a massive Russian cyberattack had not occurred. But he added that such an attack "becomes even more dangerous with Putin elevating the readiness of his nuclear weapons."

### 2AC – No Kinetic

#### Satellites most vulnerable to cyber attacks while kinetic dangers remain extremely rare

Adam Ali.Zare Hudaib 16; Network & Cyber Security Expert / Penetration Tester / Ethical Hackers Trainer / Ethical Hacker / IT Security Trainer., Published: 2016; "Satellite Network Hacking & Security Analysis"; Adam Ali.Zare HudaibInternational Journal of Computer Science and Security (IJCSS), Volume (10); Accessed: 6-22-2022; https://www.academia.edu/24899095/Satellite\_Network\_Hacking\_and\_Security\_Analysis)//Pen-SY

Satellite networks are also vulnerable to cyber terrorism or coordinated space-based and groundbased threats and attacks committed by unlawful and/or politically motivated terrorist groups who target critical communications systems such as satellite networks to cause data corruption, disruption of critical infrastructure services, economic damage, harm, and loss of life [22]. Satellite network attacks attributed to cyber terrorismcan result in disruptions in financial markets and disclosure of government, law enforcement, medical, and/or military classified data [22]. Intentional satellite system incursions motivated by cyber terrorismraise questions about the dependability, reliability, availability, and security of satellite network services and erode public confidence in the integrity of satellite-dependent, critical infrastructure applications [22]. Vulnerable Software While kinetic dangers (i.e., being hit and/or damaged by stray objects such as meteorites or other satellites) remain rare, satellite systems are remarkably vulnerable to a range of cybersecurity issues and hostile attacks because they are hugely complex and expensive, take months to deploy, and the primary emphasis is on getting a working system that meets specification and the contract deliverables. Most cyber exploit attacks take advantage of incomplete code that does not boundary check incoming data allowing for stack buffer overflow attacks. These are very prominent in embedded C and C++ systems and require an additional vulnerability assessment exercise, at great cost and time, in order to fully secure a system. In these cases an internal buffer may be overrun by an intentionally ‘malformed’ packet and code execution achieved by overwriting the area of memory where the return address resides. Once basic code execution is achieved, new threads and processes may be started and most, if not all, facilities within the system can be accessed [23].

#### No kinetic attacks – hacking is cheaper, harder to attribute, can be easily scaled across targets, and are reversible – infinitely more strategic.

Waterman ’21 (Shaun Waterman, award-winning journalist and communicator who has worked for the BBC, United Press International and POLITICO, and an expert on cybersecurity and counter-terrorism who has presented at leading conferences like Hacker Halted and the Aspen Security Forum. “Hacking the Space Force” 07/22/21 <https://www.airforcemag.com/article/hacking-the-space-force/>)

And that’s not a moment too soon: Unclassified threat assessments show that vital U.S. space assets are increasingly vulnerable to a range of emerging threats. However, hacking is a much lower-cost way of interfering with a satellite than kinetic or directed-energy attacks, and can more easily be scaled across multiple targets, according to the Aerospace Corp. And because many cyberattacks are reversible and can be hard to attribute, they offer an adversary a much greater opportunity to hide their hand—or at least preserve some plausible deniability—said Craig Miller, president of government systems at Viasat Inc., which provides satellite hardware and services to DOD.

“Someone can launch a cyber attack, and there’re ways to obscure it and obfuscate it, so that it’s difficult to find the source. … And they’re also often reversible, you can turn them off, or you can stop them, whereas other effects [like kinetic or directed-energy attacks] cause permanent damage, and it’s much clearer who did it,” he said.

The low cost character of these attacks makes it a matter of when—not if—they’ll be employed, Miller said. “The non­attributable, nondestructive nature of cyber makes it far more likely that it’ll actually be employed. And that’s the real danger of cyber attacks—you’re going to see them.”

Satellites are vulnerable, noted Miller, because they remain operational for decades. “Some of this hardware has been in space for 20 years. And it’s ’90s vintage hardware with ’90s vintage security and, in some cases, ’90s vintage operating systems that are very vulnerable.”

### 2AC – No Kinetic – Russia

#### Russia won’t risk a kinetic attack on NATO satellites – too worried about the response. Will only risk cyberattack.

Hitchens ’22 (Theresa Hitchens, Space and Air Force reporter at Breaking Defense, former Defense News editor, former senior research associate at the University of Maryland’s Center for International and Security Studies at Maryland (CISSM), former director of the United Nations Institute for Disarmament Research (UNIDIR). “[Russia could target American space firms to blind Ukraine](https://breakingdefense.com/2022/02/in-ukraine-conflict-russia-could-go-after-american-commercial-isr-providers/)” 02/15/22 <https://breakingdefense.com/2022/02/in-ukraine-conflict-russia-could-go-after-american-commercial-isr-providers/>)

There is little question that Russia will jam and/or spoof GPS receivers should it decide to invade Ukraine, as going after GPS has become almost ubiquitous as a first military move since the conflict in Kosovo.

But US government officials, former officials and outside experts are divided on how worried the US government ought to be about attacks aside from GPS jamming. Specifically, there is concern that Russia could directly target US [intelligence, surveillance and reconnaissance (ISR)](https://breakingdefense.com/tag/intelligence-surveillance-and-reconnaissance/) satellites, including [commercial remote sensing](https://breakingdefense.com/tag/commercial-remote-sensing/) birds.

A kinetic attack, such as the one [Russia tested](https://breakingdefense.com/2021/11/suspected-russian-ground-launched-asat-test-scatters-dangerous-debris-through-leo/) in November, seems unlikely, as it would risk drawing the US into a conflict the President Joe Biden has said he has no plans to join. But Russia has a whole host of non-kinetic options for targeting satellite systems that could still be disruptive or destructive for American industry and its government customer, and which raise the question about where the line is between an act of aggression and an act of war.

Attacks on ISR sats: will they or won’t they?

The Russian military has routinely jammed GPS in Eastern Ukraine since the Crimean conflict in 2014, according to experts inside and outside the US government, and often spoofs GPS simply to disguise President Vladimir Putin’s movements around Moscow.

“We’ve seen lots of evidence of non-destructive counterspace capabilities being used by Russia in both Eastern Ukraine and Syria since 2014 and there’s a lot of evidence that these capabilities are fully integrated into their units at the doctrinal and operational level,” said Brian Weeden of Secure World Foundation (SWF). “So, I definitely expect ubiquitous use of jamming, spoofing, and cyber attacks against services like the civil GPS signals and satellite communications if Russia opens a new front in Ukraine.”

That evidence — as well as a wealth of information about Russia’s effort to develop destructive anti-satellite technology — is publicly documented in SWF’s 2021 annual [Global Counterspace Capabilities](https://swfound.org/counterspace/) report, as well as the sister report by the Center for Strategic and International Studies (CSIS) called [Space Threat Assessment 2021](https://www.csis.org/analysis/space-threat-assessment-2021).

Russia’s calculus on other types of satellites, however, is an open question. In particular, the fact that Ukraine is reliant on outside sources, including the US, for imagery about Russian troop movements raises the possibility that Russian military commanders might see those satellites as targets.

“Even though [America is] not directly involved in the conflict in other domains, we will be in space, because we’re likely going to be providing real time tactical intelligence from our space based assets to the Ukrainian forces. And that makes our space assets a target for the Russians,” CSIS’s Todd Harrison said.

Such attacks will be more likely if Russian forces find themselves in trouble in Ukraine, he said, “because Ukrainians are acting on really good intelligence about where the Russians are.” Thus, “Russia might try to cut that off” using “laser dazzling” to blind satellite cameras “or even maybe even a kinetic ASAT weapon.”

However, several other experts said the odds on Moscow directly targeting US government spy or missile warning satellites are low because Putin does not want the US or its allies to become involved in Ukraine. An attack on those ISR satellites, especially using a destructive ASAT such as the one [Russia tested on Nov. 15](https://breakingdefense.com/2021/11/suspected-russian-ground-launched-asat-test-scatters-dangerous-debris-through-leo/), would almost certainly guarantee a US response.

“I doubt that the Russians would do anything in space. The US and their allies have made it clear they have no desire or intention to become embroiled in the actual conflict although they are certainly ready with sanctions and to respond if needed,” Doug Loverro, former head of Pentagon space policy, said in an email.

“It’s easier to stay out of conflict when you have no direct attack on US or NATO assets. And the Russians do not want the US involved, so they will likely avoid any direct physical attack on US assets.”

Weeden agreed, saying “It’s extremely unlikely that Russia would escalate that to destructive attacks against US or NATO satellites. We have never seen those kinds of counterspace attacks used in warfare to date and it would almost certainly draw the US and NATO into the conflict, something Russia desperately doesn’t want to happen.”

On the other hand, Loverro said that jamming and cyber attacks are not just possible but likely — noting that the Law of Armed Conflict (LOAC) clearly sets out that any satellites being used by Ukraine, no matter who owns those satellites, are fair game.

“The likelihood of jamming is quite high (as are cyber-attacks) because under anyone’s interpretation of the LOAC, any communication/information systems being used by the Ukrainians are legitimate targets, even if the other end belong to the US or NATO,” Loverro said.

### 2AC – NC3 Key

#### Cybersecurity in space is the largest threat to NC3 integrity --- US collaboration with NATO allies to develop new measures now is key.

Dr. Jared Dunnmon 17, postdoctoral fellow in the Computer Science Department at Stanford, 2017, “Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace”, https://www.jstor.org/stable/pdf/resrep23162.5.pdf \\SYang

While rapid advances in information technology, communications, and computation have yielded many improvements to NC3 systems, these improvements have come at the cost of NC3 surety and security. The two domains in which these costs are most apparent are the two newest arenas of conflict: outer space and cyberspace. In the words of Admiral Haney, “the space domain, along with cyberspace, is simultaneously more critical to all U.S. operations yet more vulnerable than ever to hostile actions.”14 The worrisome combination of international norms that have been far outpaced by the speed of technological advancement and democratization of key space and cyber technologies has led the United States to a point where it is difficult to be confident that the current NC3 structure is resilient in a cyber-physical sense. Outer Space The major threat to NC3 posed by vulnerabilities in space-based assets results from potential disruptions to both early warning and communications functions. As noted by Frank Rose, former deputy assistant secretary of state for defense policy and verification operations, The United States in particular is deeply reliant upon space. While such reliance enables the United States and our allies and partners to undertake a range of operations in support of peace and security, this reliance has increasingly been viewed by potential adversaries as a vulnerability to be exploited through the development of counterspace capabilities. This reality is particularly emergent in the context of NC3. At present, it is known that Russia and China are actively pursuing or already maintain such capabilities as laser weapons for satellite denial, electromagnetic (EM) jamming for communications degradation, and physical antisatellite (ASAT) systems. Given heavy reliance on satellites such as Advanced Extremely High Frequency (AEHF) and Air Force Satellite Communications (AFSATCOM) in the NC3 system, ensuring both reliability and resiliency to these types of threats will be critical to creating a flexible and efficient NC3 system. Cyberspace In the cyber domain, potential vulnerabilities exist in all three parts of the command, control, and communications triad. Specifically, due to cyberspace’s relatively low cost of entry, cyber threats range from state-sponsored offensive military operations and espionage activities, to [violent extremist organizations] intent on disrupting our way of life, to cyber criminals and recreational hackers seeking financial gain and notoriety. Additionally, the U.S. supply chain and critical infrastructure remains vulnerable to cyber attack, and even as we detect and defeat attacks, attribution remains a significant challenge. At present, assumptions are that NC3 is secured via a combination of air gaps, technological superiority in outer space and cyberspace, and human intervention in the control loop. Unfortunately, this is not always the case. In the intercontinental ballistic missile (ICBM) program, for instance, documented vulnerabilities include potential entry into the firewalled NC3 system, phony orders being conveyed via a backup antenna, distributed denial of service (DDoS) attacks on the nuclear infrastructure, and even a direct attack on thousands of feet of cable of the Hardened Intersite Cable System. For the strategic ballistic missile submarine (SSBN) component, it has been widely publicized that the United States has chosen to use Linux-based operating systems in its SSBNs, as opposed to Windows XP-based architectures currently used by the British Trident program. While neither of these operating systems is inherently problematic, the fact that their use in specific functional domains has been published so widely will enable hackers to focus on the correct class of exploits to use against these systems. This observation, furthermore, hints at a distressing reality: with the emergence of ubiquitous cyber threats, the U.S. acquisition process has already begun moving toward increased levels of security and classification across the Department of Defense (DoD) enterprise, which hinders efficiency at all levels of the acquisition process. Without firing a shot, the opponent may well have caused substantial cost to the United States already due to the inefficiency resultant from broadly increased data security and classification procedures. With the bomber airborne component of the command, control, and communications triad, the Air Force has experienced several NC3 breakdowns in the past several decades, the most recent of which involved the inadvertent placement of several nuclear warheads in a strategic bomber that flew over the United States. While this latter situation was not necessarily a cyber failure of commission, it is certainly one of omission in the sense that appropriate command and control safeguards were not in place to prevent such a mistake from occurring. Critical infrastructure that either directly or indirectly supports the nuclear enterprise, such as the domestic power grid is also vulnerable to cyber attack. Janet Napolitano, former secretary of homeland security, recently estimated that an adversary could disable one of the major U.S. power grids with 80 to 90 percent probability of success. The frequency of such cyber vulnerabilities generally correlates with the size of the codebase—one can usually assume one error per thousand lines of code. For perspective, a generic Linux operating system had 15 million lines of code as of 2011. Thus, while the National Nuclear Security Administration (NNSA) currently deploys a wide variety of cyber-defense techniques in defense of nuclear assets, including vulnerability scanning, firewalls, commercial antivirus systems, encryption, data loss prevention, data at rest security, network monitoring, enterprise forensics, and automated security control assessment, it is impractical to find every possible vulnerability in a large codebase and thus impossible to guarantee absolute security from zero-day exploits.2Further, post-detection attribution remains a challenge that usually takes weeks to sort out, meaning that attribution may be unachievable on timescales characteristic of a crisis. Many of the most daunting challenges for NC3 resilience lie at the intersection of cyberspace and outer space domains, where cyber attacks are directed at space-based NC3 assets. A recent study revealed substantial numbers of exploitable flaws in many widely used commercial satellite architectures, including the Iridium constellation, International Maritime Satellites (INMARSAT), and other satellites commonly used by both North Atlantic Treaty Organization (NATO) forces and critical infrastructure systems. Key vulnerability categories included hard-coded credentials (undocumented credentials that can authenticate in documented interfaces), undocumented protocols (protocols not intended for end users), insecure protocols (end-user protocols that pose a security risk), and backdoors (mechanisms used to access features not intended for end users). Outcomes from reported exploits included control over systems as varied as land-based communication and aircraft navigation, either of which could have a debilitating effect on MEECN integrity and ultimate NC3 efficacy. Understanding and mitigating the potential effects of these cyber threats to space-based assets will be imperative in ensuring the continued effectiveness of NC3.

### 2AC – Yes Russia Attack

#### Russia has capability to destroy NATO satellites and GPS – already hacked Ukraine.

Ayres ’22 (Thomas Ayres, retired U.S. Army major general, former general counsel of the Department of the Air Force. “Russia’s war could spread to space; the U.S. should be prepared” 04/26/22 https://spacenews.com/op-ed-russias-war-could-spread-to-space-the-u-s-should-be-prepared/)

As background, recall that in November 2021, while amassing forces on Ukraine’s borders, Russia launched an ASAT satellite missile that destroyed one of its own satellites in orbit. It caused hazardous orbital debris and at the time seemed senseless. Russian authorities blathered and quibbled.

In hindsight, Russia’s demonstration of offensive space capabilities was on their pre-invasion checklist. This preparatory step to invading Ukraine sent a dual warning. First, when Russia invades, don’t interfere with Russian space systems upon which the Russian military relies. Second, if you seek to come to Ukraine’s aid, U.S. and NATO satellites upon which you rely will be in jeopardy.

Even earlier, Russia has been saber rattling in space. In February 2020, Gen. John “Jay” Raymond, the chief of space operations of the U.S. Space Force, reported that a Russian inspector satellite had actively maneuvered near a U.S. national security satellite. The inspector satellite, as if from a Russian nesting doll, detached from another satellite to purposefully approach and threaten the U.S. satellite.

This precursor message was also exceptionally clear. The satellites on which the data for the blue dot on your phone, nearly every global financial transaction, and the effectiveness of military forces relies, are not beyond Russian reach.

Russia’s provocations in space continue even while we cooperate on the International Space Station (ISS). But the invasion has changed that calculus as well. Upon the announcement of U.S. sanctions on the aerospace industry, the director of Roscosmos, the Russian Space Agency, tweeted, “If you block cooperation with us, who will save the International Space Stations (ISS) from an uncontrolled de-orbit and fall into the United States or … Europe?”

With American astronauts on board, purposeful sabotage of the ISS would certainly be an act of war. Looking for other avenues to voice displeasure, Roscosmos looked at the commercial space industry. They demanded the United Kingdom guarantee OneWeb’s satellites, which were to be launched on Russian Soyuz rockets, not be used for military purposes. The United Kingdom demurred and SpaceX rockets have come to OneWeb’s rescue.

Rather than passively awaiting further signals of Russian power in space at a threshold below an act of war, the U.S. can and should take clear measures to deter Russian aggressive action in space, in addition to the recently announced self-imposed ASAT ban.  Failing to do so only invites Russian attempts to harass, degrade or even mistakenly destroy U.S. satellites.

First, the intelligence community should remain focused on attributing harmful or menacing Russian moves in space and reveal them. Just as the U.S. published Russia’s playbook on the ground prior to the invasion of Ukraine, the U.S. should reveal every dangerous or unprofessional movement of satellites near friendly satellites and thereby send our own signals to deter Russian malign activity in Space

Second, the Biden administration must forcefully pronounce a redline in space.  Even as SpaceX and Elon Musk helpfully delivered Starlink terminals, the U.S. must message that uninterrupted internet and satellite communications for U.S. and NATO forces and allies in eastern Europe is a national security asset. If our satellite network is attacked in any manner, it will be considered an act of war.

## 2AC – Solvency

### 2AC – Solvency – Post Strat Con

#### **Cooperating over space-based cybersecurity including at least clarifying Article 5 solves.**

Rose Gottemoeller 6-26; Department of Social Sciences, United States Military Academy; Defence Studies, June 26, 2022; “Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept,” https://doi.org/10.1080/14702436.2022.2082955

NATO’s ability to achieve its core tasks of Collective Defense, Crisis Management, and Cooperative Security requires strength and resilience of each member state. It is critical to build a common strategic culture among Allies that embraces the technological complexity of these new domains and seeks to address the challenges of the strategic environment. While member states will continue to have differential capabilities within each domain, the culture among Allies must reflect a desire to maintain a competitive edge by growing human capital and technological development. Political elites of member states must also understand how this technological complexity may shape their decision making and their understanding of escalatory pathways (Kubiak and Mishra 2022). NATO must foster a culture of adaptability and flexibility to handle the everchanging nature of cyber, space, and EDT. Consensus, communication, and cooperation, described below, serve as the foundational pillars upon which a resilient and adaptable Alliance grows.

Consensus

Consensus is at the heart of the Alliance. To properly integrate cyber and space domains into the Strategic Concept, Allies should seek internal consensus on three topics: 1) the threshold of cyberattack or space action upon which Allies can invoke Article 5 2) actions short-of-war that must addressed by steady-state defense operations or that require a collective Allied response 3) actions that NATO will proactively take in these domains to ensure adequate defense in cyberspace.

First, although the Comprehensive Cyber Defense Policy acknowledges that Allies may invoke Article 5 after experiencing a cyberattack, it is not clear what threshold of cyberattack constitutes a violation of Article 5. This must be explored further by the Allies to reduce delay in consensus in the event of a cyberattack. Second, Allies must also seek to understand what cyber operations place NATO’s core tasks of Collective Defense, Crisis Management, and Cooperative Security at risk. Cyber operations, such as espionage and cyber-enabled information operations, are often used to subvert and erode state power outside periods of conventional conflict. The 2010 NATO Strategic Concept narrowly scopes defense and deterrence to cyber attacks; however, it is precisely cyber operations short-of-force that require thoughtful consideration to integrate within the forthcoming NATO Strategic Concept. Cyber operations create and amplify crises, eroding the “territorial integrity, political independence and security of its members” (NATO 2010, 9). This is best illustrated with numerous attempts to sow division through election interference (Sarts 2017). Cyber operations undermine the collective nature of defense by exploiting democratic society and wedge driving among NATO states. The democratic nature and open information environment of most Allies makes the Alliance particularly vulnerable to cyber operations short-of-force. Member states must reach consensus that cyber operations below the threshold of war are still critical threats to the effectiveness of the Alliance. This also extends to actions in space that threaten the essential tasks of the Alliance but fall short of physical destruction (Smith 2022).

While consensus is required among members to identify these thresholds, the Allies must also reach consensus on whether to reveal or conceal these thresholds beyond the Alliance. NATO must ask if a clearly declared threshold in cyber and space domains bolsters deterrence or whether deterrence in these domains operates differently than conventional armed conflict. One consideration that may inform this discussion: Will adversaries test the limits to find a covert threshold or does the strategic ambiguity provide a greater deterrent? If Allies believe that a declared Article 5 threshold will be tested by adversaries to challenge the credibility of the threshold, it may be worth concealing. If Allies believe that concealing an Article 5 threshold would increase probing attacks that test the limit of the Alliance, it may be worth revealing. Regardless, an openly declared threshold upon which member states can invoke Article 5 must also overcome the limitations of the cyber domain that make deterrence difficult. Moreso than armed attack, cyber operations continue to generate significant uncertainty about intentions, and can be concealed from the public due to their often-clandestine nature (Lonergan and Lonergan 2022). Also, the timing associated with attribution could reduce the salience of a response (Baliga et al 2020). These features of the cyber domain may make deterrence by punishment less credible and may make Article 5 invocation slow to realize. Therefore, if NATO would like to publicly declare a threshold to invoke Article 5 in cyber and space, NATO must acknowledge these challenges to preserve the credibility of the threshold. NATO must also over-communicate that, across all domains, Article 5 must be invoked by an Ally and is not an automatic escalation pathway.

Finally, Allies must seek consensus on how NATO uses cyber operations short-offorce within the context of cyber defense. As offense-defense distinguishability is muddled in cyberspace, Allies must decide whether Defense and Deterrence is best advanced by in-network activity or whether NATO will operate outside their network as a form of defensive practice (Slayton 2017). There has been a large academic debate on the efficacy of deterrence by punishment in cyberspace (Gartzke and Lindsay 2019; Nye 2017; Brantly 2018). Recently, scholars have coalesced around deterrence by denial as the most effective deterrent in cyberspace. However, deterrence by denial is most successful when states are willing to conduct counter-cyber operations. Yet, these operations can be controversial for their offensive nature; for example, the United States cyber doctrine of “Persistent Engagement” and “Hunt Forward” utilize offensive means for defensive ends (Borghard and Lonergan 2021). The Allies should seek consensus as to what operational actions within the cyber domain best uphold Collective Defense.

Communication

Communication is central to properly integrating cyber and space into the NATO Strategic Concept and contributes to the resilience of and within the Alliance. Communication about cyber, space, and EDT should purposefully occur with two audiences in mind: intra-Alliance communication among member states and extraAlliance communication intended for NATO’s adversaries and partners.

Intra-Alliance communication must focus on three primary objectives: 1) reducing technical barriers for political decision makers to facilitate their response to rapidly evolving space and cyber development; 2) creating common understanding among member states at varying degrees of capabilities; 3) eliminating stove-piping of complex technologies. The technical nature of these domains can intimidate or create high barriers to entry for political decision makers. Decision makers must be able to understand crises to manage them. NATO must seek to integrate experts who can serve as the translators between decision makers and technicians in the field to facilitate consensus and development within cyber and space domains. Intra-alliance communication and knowledge sharing can also help overcome disparities among member states who have differential capabilities. Additionally, intra-Alliance communication between conventional domains and the cyber, space and EDT operational and policy cells will further integrate these new domains into the fabric of the Alliance.

Extra-Alliance communication must: 1) enhance credibility of deterrence through clear, credible guarantees of punishment and communication of NATO’s capabilities (Lonergan and Montgomery 2022) and 2) collectively attribute perpetrators and disclose discovered vulnerabilities to improve the resilience of these domains. Deterrence relies on a clear understanding of cost–benefit analysis (Lindsay and Gartzke 2018). NATO must clearly communicate their capabilities and the range of potential consequences so adversaries understand the costly nature of attempting to overcome NATO’s defensive capabilities and the high costs by way of punishment should they succeed. Communication strategies should emphasize the resolve of NATO in addressing cyber, space, and EDT threats and, most essentially, the political will to respond to a cyber or space attack. These external communication strategies harden the deterrent by bolstering credibility of a response without tying their hands to a specific response. Moreover, communication through public attribution, as was illustrated in the 2020 Microsoft Exchange Hack (Connolly 2021), demonstrates consensus about the identity of the perpetrator and increases costs for cyber adversaries (Egloff 2020; Egloff and Smeets 2021; Hedgecock 2021). Taken together, intra-Alliance communication improves the resilience of the Alliance and enhances Cooperative Security and Crisis Management. While extra-Alliance communication serves to bolster the Collective Defense.

Cooperation

The cyber and space domains have often been interpreted as public commons. As a result, these commons are difficult to govern and serve as the intersection of public and private actors. NATO must seek to lead cooperation within the Alliance, across partnership states, and with private actors to maintain a scientific edge (Rugolo and Monic 2022). NATO currently supports the Industry Cyber Partnership to improve Allies’ network security and increase resilience. This industry partnership must be replicated in a NATO Industry Emerging Technology Partnership, to facilitate a competitive edge in capabilities that are on the horizon or not fully realized in the operational security environment. The agreement to establish Defense Innovation Accelerator for the North Atlantic (DIANA) for civil-military cooperation at the 2021 Brussels Summit, is a step in the right direction. Once established, cooperation must also be facilitated across partnership hubs within NATO to prevent stove piping of innovation. Additionally, it is critical that these innovation centers encourage partnerships across the entire spectrum of private industry, from startups and garage innovators to large scale private corporations with extensive scale research and development (Kosal 2022). Finally, intra-Alliance cooperation requires intelligence sharing and capability development among member states to ensure that the Alliance continues to meet the challenges of the strategic environment. One example of intra-Alliance cooperation that compliments NATO’s efforts is the European Union’s initiatives to bolster cybersecurity. The European Union Agency for Cybersecurity’s efforts to improve capacity, cooperation, and a whole-of-society approach to cybersecurity ultimately bolster NATO’s deterrence by denial by hardening the attack surface of Europe.

Recommendations

In keeping with the current NATO essential core tasks- Collective Defense, Crisis Management, Cooperative Security- and the structure of the existing Strategic Concept, we submit several recommendations for consideration in 2022 NATO Strategic Concept: In discussions of the Security Environment within the forthcoming Strategic Concept, NATO must enhance the discussion of cyber, space, and EDT. We recommend that NATO change the language from “cyber attack” to “cyber operation” to capture the wide spectrum of activities that subvert and erode state power including cyber espionage and cyber-enable information operations In discussions of the Collective Defense, we recommend that NATO address how the space domain fits within the context of defense and deterrence, while also acknowledging the critical role that space plays in maintaining communications and interoperability among Allies. NATO must also incorporate public attribution of cyber operations as a political and strategic tool that can bolster the collective defense and cooperative security of member states. We recommend that NATO reach consensus on a threshold that constitutes an “attack against all” in the cyber and space domain. Allies must also decide whether to only communicate the existence of the threshold or to publicly reveal the threshold upon which a member may invoke Article 5.

### 2AC – AT: Alt Cause

#### The plan solves US exceptionalism in space and overcomes alt causes

James Clay Moltz 11, professor in the National Security Affairs Department at the Naval Postgraduate School, October 2011, “Coalition Building in Space: Where Networks are Power,” <https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf>

Despite the advantages of creating such an allied network for space, it must be admitted that a number of current obstacles exist to such efforts. Traditional U.S. thinking about U.S. exceptionalism in space would have to be revised and a more egalitarian view of alliance partners adopted. The U.S. State and Defense Departments would need to engage in ITAR reform and craft new military-to-military agreements (of the type the U.S. has with Australia) to allow the sharing of space information. In Congress, a new political willingness to fund space systems that would not be solely for national benefit or under purely national control would need to emerge. At the technical level, new integration with allied industry would likely be necessary to create common standards and interfaces, which would initially cost time and money. Still, given the emerging risks in space of and the possible benefits to be achieved by joint efforts, these problems do not seem insurmountable.

### 2AC – AT: Norms Fail

#### Norms are key to crisis stability – building them in advance is goldilocks for deterrence and signaling escalation thresholds

Audrey M. Schaffer 17 Director for Space Strategy and Plans in the Office of the Under Secretary of Defense for Policy. September 28, 2017; “The Role of Space Norms in Protection and Defense.” Joint Force Quarterly 87. <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-87_88-92_Schaffer.pdf?ver=2017-09-28-092555-747>]

Militaries stand to gain additional unique advantages from widespread adherence to operational space norms. Norms can serve to highlight abnormal behavior, enabling warning of and protection against space threats. Militaries, therefore, should support domestic and international initiatives to shape operational norms of behavior, and they should lend their expertise to norm development efforts. As international space norms take shape, militaries can then analyze abnormal behavior, characterizing those specific behaviors they would consider hostile or aggressive and determining how to respond appropriately in different situations. Militaries may also need to consider whether to evolve operational policies and practices to meet behavioral expectations.

Norms are not a panacea for constraining aggressive, hostile, provocative, or otherwise deliberately irresponsible behavior in outer space. Norms may be enough to dissuade a rational actor from routinely engaging in irresponsible acts, but they will not prevent a committed aggressor from deliberately disrupting or denying space services it deems detrimental to its interests. Norms, however, can play a critical role in detecting and responding to potential threats.

Norms enable early detection of potentially hostile actions or intentions in space. If a satellite exhibits behaviors contrary to operational norms, this is a clear flag to monitor its activities more closely. In times of peace, such activities are likely to be nothing more than an anomaly, which may deserve increased monitoring to preserve spaceflight safety or to mitigate harmful electromagnetic interference. In periods of heightened tensions, norms can form the basis of criteria for early indications and warning of potentially aggressive actions.

To have maximum value in identifying “abnormal” behavior, norms should be widely accepted, such as through voluntary guidelines or international standards. Short of explicit international acceptance, national or allied declaratory policies can communicate those behaviors considered to be a demonstration of hostile intent, shaping tacit understanding of acceptable and unacceptable behaviors. If these agreements and/or communications are clear, and norms are generally observed in times of peace, then we can assume in times of crisis that behavior contrary to norms is most likely a deliberate choice. These assumptions will be a critical input to crisis decisionmaking and, by extension, may have a significant effect on crisis stability. Both an under-reaction and over-reaction to anomalous behaviors could have serious and unintended consequences for international peace and security.

To the extent that the international community can observe what is happening in space, norms will shape world opinion about these behaviors, branding them as simply irresponsible or something more egregious such as potentially unlawful. This will require, at a minimum, compelling evidence based on space situational awareness information from a trusted source. Confirmation from multiple, independent, international, and/or commercial sources of space situational awareness will have a positive and reinforcing effect on detecting bad behavior in outer space. Nations may condemn those who choose to engage in behavior contrary to norms. Condemnation, however, is a double-edged sword; a nation cannot take others to task for violating international norms and simultaneously seek to operate with impunity. At first glance, military space operators may bristle at the implication that norms may constrain their freedom of action in space. Militaries, though, already accept legally binding constraints in all domains. For example, fundamental to the conduct of modern warfare is international humanitarian law (also known as the Law of War or the Law of Armed Conflict),2 which seeks to limit the effects of conflict, especially on noncombatants. Militaries around the world translate international humanitarian law into rules of engagement that guide servicemembers. A future space norms regime could be fashioned similarly to other regimes that govern activities in shared spaces and allow for differences in the application of rules to government or military actors and private actors. For example, Article 3 of the Convention on International Civil Aviation provides that the Convention does not apply to “state” aircraft, though such aircraft are required to exercise due regard for the safety of navigation of civil aviation.3 Article 48 of the Constitution of the International Telecommunication Union likewise provides freedom for military radio installations, but requires them, so far as possible, to observe provisions to prevent harmful interference.4 As in these other domains, safety and sustainability focused space norms, while remaining good and responsible practice no matter the situation, need not be strictly adhered to by militaries at all times. Even if militaries are not expressly required to follow norms, they nonetheless should be prepared to make more deliberate behavioral choices because of how actions inconsistent with norms will be interpreted. This not only requires a strategic and holistic perspective on national security space behaviors, especially in periods of crisis, but also creates opportunities for deliberate signaling. Just as increasing airborne reconnaissance or forward-deploying aircraft carriers can demonstrate interest and stake, so too can maneuvering satellites demonstrate readiness and resolve. Ensuring that the desired signals are received requires significant communication and/or agreement on norms of behavior well in advance of a crisis. Norms also provide clarity to acquirers, operators, and decisionmakers. Similar to how the Department of Defense (DOD) reviews all new weapons systems to ensure they can be operated in accordance with international law, acquirers and operators could look to space norms for guidance on what capabilities and actions would be permissible and under what circumstances. This ensures resources are not expended on systems that political leaders will not employ and provides guidance for operational planners on how to protect and defend space systems in a manner that will be deemed acceptable in different situations.

Norms—or rather the violation thereof—also enable the creation of thresholds, triggers, and rules of engagement that allow militaries to employ passive or active measures to protect threatened space systems. Norms, ironically, may enhance freedom of action when it is needed most. Because norms support the development of criteria for judging hostile acts or hostile intent in space, they enable actions to be taken in self-defense.

#### Clarifying escalation thresholds in advance is key to preventing miscalc in a crisis – lack of cold war experience in space makes preemptive norms essential

James P. Finch 14, Principal Director for Countering Weapons of Mass Destruction, Office of the Under Secretary of Defense for Policy, where he previously acted as the Principal Director for Space Policy. He has held space-related leadership positions in the Office of the Secretary of Defense and Headquarters U.S. Air Force. December 30, 2014, "Bringing Space Crisis Stability Down to Earth." https://ndupress.ndu.edu/Media/News/Article/577582/bringing-space-crisis-stability-down-to-earth/]

Simply put, the weapon, target, and context all contribute to the perceived intent and effects of a counterspace attack. Unlike in other domains, tremendous ambiguity exists regarding the use of counterspace weapons. This means that all of these variables would be open to interpretation in crises, and it should be remembered that an inherent characteristic of crises is a short timeframe for decisionmaking. When time is short and the potential cost of inaction is significant, or even catastrophic, decisionmakers tend to lean toward worst-case interpretations of an adversary’s actions. This is a clear recipe for inadvertent miscalculation.

Bringing Space Down to Earth

The Cold War adversaries had many years to develop mutual understandings about the nature and role of nuclear weapons, and these understandings contributed to strategic stability. These understandings were born out of realworld crises, such as the Berlin crises, Korean War, and Cuban missile crisis. They also emerged from dialogues, such as formal summits and long-running arms control negotiations. The former are certainly much more dangerous than the latter, and no one wants to see the space equivalent of a Cuban missile crisis.

There are signs of progress. The United Nations Group of Government Experts recently recommended bilateral and multilateral transparency and confidence-building measures. In addition, the European Union is leading open-ended consultations to develop an “International Code of Conduct for Outer Space Activities.” While these measures will help promote the responsible use of space, they do not squarely address the current lack of mutual understanding regarding how space attacks will be perceived in the midst of a crisis. This is of particular concern for the United States and China, which, as previously noted, increasingly rely on space systems to execute their political and military strategies.

At the government-to-government (so-called Track 1) level, there is not currently a productive venue for the United States and China to develop a mutual understanding of how space plays into crisis stability. While space security has been incorporated into existing diplomatic and defense dialogues, these steps in the right direction have been slow and tentative, and there is much work to be done.

Recently, some engagements led by think tanks (known as Track 1.5 dialogues due to mixed delegations of government and academics) have begun to explore the issue, and it is clear that both sides harbor a lot of mistrust and misperception. The United States continues to raise questions about China’s military modernization and its potential coercion of regional neighbors over contested territory. China continues to question the implications of expanding U.S. missile defenses and, to a lesser extent, the U.S. rebalance to the Asia-Pacific region.

Suspicions about space activities fit within this broader geopolitical mistrust. The United States continues to express concern about Chinese space activities and China’s lack of transparency when it comes to unique space launch profiles or robotics experiments. China, for its part, expresses concerns about U.S. activities, such as the reusable experimental test platform known as the X-37B. These misperceptions are hard to resolve, both because of the inherent dual-use nature of space systems and the difficulty in creating transparency for a regime so far removed from terra firma. Resolving such suspicions and building trust take time and require a common understanding of the nature of the space domain and space systems.

Returning to the formulation of Colby, recall that “in a stable situation . . . major war would only come about because one party truly sought it, not because of miscalculation.” Miscalculation is best avoided when each side understands the implications of its actions and understands how the other side will interpret and react to those actions. This situation does not exist in today’s environment regarding space systems and space weapons. We lack a common understanding of how space will contribute to, or come to define, potential crises between the United States and China. As both countries seek to define a “new type of great power relationship,” it would be wise to consider how new technologies and operational concepts are best managed during crises. Given both sides’ growing reliance on space systems to achieve their future military and political aims, a lack of understanding comes with great peril. We should strive to build a common framework now, using dialogues during peacetime, before provocative actions in space during a crisis imperil stability here on Earth.

#### Failure to establish coherent space policy ends credible deterrence, encourages first strikes, and deliberate risk-taking. Independently, a litany of thumpers outweigh the link.

Tim Swieijs and Frans Osinga 20; Director of Research at The Hague Centre for Strategic Studies, PhD in War Studies from King’s College London; Professor of War Studies at Leiden University, PhD from the Clingendael Institute of International Relations; 4/4/20; "VIII. Maintaining NATO’s Technological Edge," Whitehall Papers, Vol. 95, Issue 1, p. 104-118]

Space assets are increasingly central to the functioning of globally networked societies. Satellite launch capabilities are proliferating, while the cost of satellites is decreasing. Fourteen states can now launch their own satellites and more than 80 states possess space-based assets, while numerous commercial providers offer services from space to anyone who can afford them.14 Space-based assets are also increasingly critical enablers of current and future military operations, with most CS4IR functions depending on them. Major military powers without space-based assets are in essence deaf, blind and mute, and indeed paralysed. Intelligence, communication, precision weapons and logistics all depend on properly functioning space systems.

Not surprisingly, space is increasingly regarded as a military domain. Space is now starting to be weaponised, the terms of the 1967 Outer Space Treaty notwithstanding. In March 2019, India became the fourth country to demonstrate a direct-ascent anti-satellite (ASAT) capability in a live test, following the US, Russia and China, which first did so in 2007. These tests are emblematic of a more pervasive trend. The US, under President Donald Trump, re-established a Space Command in 2019 as a precursor to an eventual Space Force. In China, the Strategic Support Force, established in 2015, has an important role in further developing the PLA’s space warfare capabilities. Russia, building on the vast infrastructure established during Soviet times, remains an important space power.

In strictly military terms, Europe’s space powers lag behind China, Russia and the US, which are currently recalibrating their military space postures and are actively investing not only in greater numbers of satellites, but also in stronger protection of those systems, better encrypted download and upload datalinks, and further development of ASAT missile systems, satellite jammers and directed energy weapons.15 China has embarked on a manned programme seeking to establish a research station on the Moon in the mid-2020s and to post humans there for extended periods in the 2030s.16 The US also intends to return to the Moon; the first unmanned mission to transport cargo is planned for 2021, to be followed by a manned mission in 2024.17

Meanwhile, billionaires Elon Musk, Jeff Bezos and Richard Branson have each launched their own space corporations, based on grand visions of space exploration, exploitation and colonisation. At the same time, the US government is redrafting its rules and regulations, no longer designating space as a ‘global commons’ but clearly pursuing the objective to ‘unshackle business activity in space’.18 If history is any guide, attempts to establish control over economic resources will likely be accompanied by the deployment of military power to enforce and guarantee that control. Space, in sum, truly constitutes a new frontier for the conduct of terrestrial and, down the line, extra-terrestrial competition and conflict.

Implications for NATO

The literature on revolutions in military affairs (RMAs) suggests that those who manage to harness and exploit new technologies, combine them with novel operational and organisational concepts and evolve a new way of war stand to gain significantly – a sobering insight in this era of strategic competition. This is not lost on, for instance, Putin, who highlighted the impact of AI on the international order when he observed that ‘artificial intelligence is the future,…whoever becomes the leader in this sphere will become the ruler of the world’.19 Chinese leaders have expressed similar views.20

Whether the technological trends described above signal the advent of another RMA or merely represent incremental change remains subject to debate.21 Regardless, the implications of the technological progress summarised here are already being made manifest and are likely to progressively materialise during the 2020s. The first attacks with swarms of drones have already taken place in Syria, Libya and Saudi Arabia, executed not by a state but by various non-state actors.

NATO members already face an assortment of challenges, including the vicious conflict dynamics in Northern Africa, the Middle East and Southwest Asia, which are not likely to disappear soon. Further, Russia’s nuclear and conventional modernisation, in combination with its antiaccess/ area denial (A2/AD) capabilities, has cast doubt on the credibility of NATO’s conventional and nuclear deterrence posture.22 In this latter context, it has become painfully clear that the armed forces of European NATO members, in particular, have neglected the demands of joint highintensity warfare at their own peril. For NATO, these developments therefore suggest, at a minimum, a strong imperative to not only rebuild its capabilities, but also to keep pace with rapid technological advances.

NATO Initiatives

In recent years, NATO launched a series of initiatives to regain capabilities and expertise, with member states pledging to increase defence spending. Current capability improvement plans focus on enhancing readiness, regaining lost capabilities in artillery, tanks, transport and C2 assets; and introducing fifthgeneration jet fighters in greater numbers than those ordered prior to 2014. Cyber capabilities are also receiving a boost now that cyberspace has been designated a warfighting domain. The Alliance will enhance missile defence in the next decade by fielding state-of-the-art US radar systems in various Eastern European member states. Furthermore, NATO has formulated a roadmap for research on emerging technologies such as AI, quantum computing, autonomy and hypersonic missiles. Various organisations, such as NATO’s Science and Technology Organization (STO) and different centres of excellence, aim to support knowledge diffusion, create awareness and stimulate research and development. The STO conducts research on more than 250 projects across seven domains that canvass a wide spectrum of emerging technologies.23

European NATO member states that are also EU members have similarly agreed on a series of capability improvement initiatives. Following the 2016 EU Global Strategy, the EU launched the Coordinated Annual Review on Defence (CARD), the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). These initiatives focus on the range of capability targets identified in the 2018 update to the EU Capability Development Plan. The goals are to achieve a measure of strategic autonomy and to create a coherent full-spectrum force package. This force package aims to ensure air and information superiority and access to space-based systems; to support cyber response operations, naval manoeuvrability and air mobility; and finally, and more generically, to develop ‘innovative technologies for enhanced future military capabilities’.24 The US, meanwhile, has announced its determination to leverage the potential of emerging technologies in what has been labelled the ‘Third Offset’. In parallel with this initiative, the US is exploring a new operational concept – ‘Multi-Domain Operations’ – that harnesses and exploits these new capabilities and may play the same role as the AirLand Battle concept of the 1980s.25

Challenges

Despite these efforts, the developments sketched in this chapter present NATO members with an assortment of financial, ethical and military strategic challenges. For NATO’s European member states in particular, the Third Offset poses a considerable financial burden.26 Although European member states currently spend $264 billion collectively on defence, and despite a decade of improvement initiatives, the capability shortfalls that came to light in Operation Allied Force in Kosovo in 1999 persist.27 In 2012, one study concluded that without US contributions, Europe would struggle to conduct a so-called ‘Small Joint Operation, Air- Heavy’ – an operation comparable to Operation Allied Force or Unified Protector in Libya (2011).28 In 2020, European armed forces remain critically dependent on the US for C4ISR and suppression of enemy air defences (SEAD) capabilities, cruise missiles, ballistic missile defence, stealth aircraft and electronic warfare assets. The same applies to creating and manning effective operational headquarters that rely on state-of-theart C2 technology as well as expertise in operational-level planning and commanding joint operations. Estimates indicate that without the US, the defence of the Baltic states and Poland would require an additional investment by European states of about $288−357 billion.29

Adapting to the new geopolitical environment and implementing capability improvements for their armed forces has proven difficult for Europe’s defence organisations, however, not least because of budgetary realities.30 Defence cooperation initiatives also suffer because European defence industries remain fractured and compartmentalised along national lines, and have a diminishing ability to nationally develop and manufacture complex leading-edge military capabilities. Remedying several of the capability shortfalls – those pertaining to large and complex systems such as tanker aircraft or electronic warfare platforms – also exceeds the requirements of individual countries and calls for collective action. In addition, actually fielding the necessary new capabilities takes at least a decade.31 Finally, while high-end weapon systems and emerging technologies claim much of the Alliance’s attention, funds will also be needed for restoring more mundane capabilities such as ammunition stockpiles and transport capacity, which will enable rapid reinforcement and a sustained military campaign. Given the rather dismal European track record in actually achieving military transformation as envisioned by NATO, investments in Third Offset technologies may never actually materialise and might not produce the necessary improvements even if they did.32

Another challenge lies in the controversial nature of some of these technologies. While the technologies may yield many military benefits, the legality and ethics of, for instance, deploying unmanned and semiautonomous weapon systems are hotly debated throughout society, academia, parliaments and religious circles (including the Vatican). Expert groups discuss the ethical and legal issues associated with military AI, including in the context of the UN Convention on Certain Conventional Weapons. António Guterres, former UN Secretary-General, captured prevailing concerns when he warned in 2018 that ‘the prospect of machines with the discretion and power to take human life is morally repugnant’.33 Opponents of these weapon systems allege that they will result in the ‘dronification’ of foreign affairs and the dehumanisation of warfare: because the use of drones reduces the need to deploy soldiers, political leaders might be more inclined to resort to force or escalation during a crisis, with war as the result. If both contestants possess such an arsenal, what happens when one of them runs out of these systems?34 As a number of potential adversaries will certainly continue to field unmanned systems and develop military AI applications, NATO member states will need to recalibrate their capability portfolios to include defensive counter-drone capabilities and, given their increased vulnerability to drone attack, will need to reconsider which wars are worth fighting. The advent of military AI also raises military-strategic concerns, including how NATO should respond if Russia and China successfully integrate military AI and get inside Western OODA loops. NATO member states will therefore need to consider which military AI applications they want to develop and under which specific conditions they deem their use ethically acceptable.

A related concern pertains to the deployment of immature AI to the battlefield, which would increase fog and friction and fuel unwanted escalatory spirals. The potential destabilising effects of the combination of new and, in some cases, untested technologies and their impact on the strategic balance of power, escalation dynamics and war presents another challenge. Emerging military space capabilities will pose a serious risk to the dynamics underlying deterrence in a multipolar world which are already under pressure due to a new generation of multiple independently targeted re-entry vehicles (MIRVs), the emergence of hypersonic (> Mach 5) missile gliders and the advent of global conventional prompt strike systems. If military powers can shut down the eyes and ears of adversaries by taking out their satellite systems, these adversaries may be unable to (fully) retaliate. This undermines credible deterrence and creates escalatory tendencies by giving parties an incentive to strike first. Ubiquitous surveillance systems (including spacebased sensors) that are guided by AI and can reveal the location of nuclear missiles (even onboard submarines) increase this risk, as the accurate knowledge these systems provide might prompt pre-emptive strikes or deliberate escalation and risk-taking. Increasingly effective cyber attacks against nuclear C2 systems can likewise undermine deterrence. Hypersonic weapons (with conventional or nuclear pay loads), which can evade current state-of-the-art missile defence systems, may render C2 facilities, aircraft carriers and nuclear missile complexes vulnerable.35 The potential unintended strategic consequences of each of the new technologies, and in particular the unpredictable effects of their deployment in combination, will certainly be topics of considerable political and societal debate within NATO’s European populations that do not necessarily support increases in defence expenditures in general and increased spending on nuclear and unmanned capabilities in particular.

### 2AC – Clarifying Key

#### Article 5 is the most important barrier to cohesive NATO space policy

Stickings 20[Alexandra Stickings, RUSI Newsbrief, 15 October 2020, “Space as an Operational Domain: What Next for NATO?,” https://rusi.org/publication/rusi-newsbrief/space-operational-domain-what-next-nato]

Military Sciences, NATO

While it is encouraging that the Alliance is moving forward in its thinking on the space domain, questions remain. Will the Alliance continue to rely on the assets of a relatively small number of members, and how will collective priorities be balanced against those of individual states? Similarly, what does this mean for states with few or no sovereign space assets, and will investment in space become a requirement for all members in the future? Finally, and most importantly, how do activities in space fit into the context of an event that triggers Article 5? These are all issues NATO will need to grapple with to ensure it fully realises the benefits that space can bring and is able to withstand any activities that threaten its access. Recognising the importance of the domain is one thing, deciding how to act is another.

NATO AND SPACE: A BRIEF HISTORY

NATO was formed before the beginning of the first ‘space age’ and for most of its history, the US has provided the majority of available space assets, such as the US Air Force-managed GPS system, which is used for a range of activities including navigation and precision-guided munitions. Although a programme beginning in the early 1970s saw the deployment of NATO communications satellites, this policy was changed in the early 2000s to one giving NATO access to satellites operated by member states. Since that time, NATO has not operated its own space assets, instead relying on members to provide access and information.

National satellite programmes have played an increasingly important role in NATO operations, both during conflict and in its ongoing operations, training exercises and intelligence, surveillance and reconnaissance (ISR) activities. NATO’s 2019 declaration is a recognition of these longstanding activities and intention to respond to the increased security concerns regarding space rather than a completely new policy in itself. Space is now a priority, rather than an afterthought. It does, however, raise a question as to whether the current model is effective, relying as it does on the goodwill of states to share their assets and the difficulties that can be present in ensuring integration and interoperability. While this recognition is a step forward, further issues must be taken into consideration for the development of a truly workable NATO space policy and strategy.

#### That splits the alliance.

Schütz '19[Torben; July 2019; Associate Fellow in the Security, Defense, and Armaments program of the German Council on Foreign Relations; "Technology and Strategy: the Changing Security Environment in Space Demands New Diplomatic and Military Answers," https://www.ssoar.info/ssoar/bitstream/handle/document/63288/ssoar-2019-schutz-Technology\_and\_Strategy\_the\_Changing.pdf]

While Also Preparing for the Worst by Strengthening NATO’s Role in Space

Given the importance of space assets for Western military and civilian operations, and the risk of negotiation failures in arms control initiatives, Germany should, however, also support NATO considerations to designate space as a military-operational domain of its own, set apart from land, air, sea and cyberspace. A domain describes a “critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission”.7 Designating space as such a domain would prompt NATO more closely to analyze its vulnerabilities in space and its dependence on both civilian and military space-based assets. This would increase NATO’s understanding of the entanglement of space and non-space operations and facilitate considerations about deterrence and defense in space.

NATO member states will also have to answer two crucial questions for the alliance: Does an attack on the space asset of one ally constitutes an Article 5 incident? And will national space assets come under the command of NATO in case of an attack?

NATO’s position on cyberattacks might serve as an example for integrating space into the Article 5-framework, especially given the fact that cyber- and electronic attacks on space assets are the most likely ones. NATO has so far kept the threshold for triggering Article 5 consciously vague in cyberspace, ultimately leaving it to the North Atlantic Council to decide whether to count an attack as an Article 5 event. A similar approach could be taken to cover non-physical attacks on space assets, while physical attacks could be covered by Article 4 of the North Atlantic Treaty, which states that allies can “consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened“.8 In the case of cyberspace, the alliance designated cyberattacks as a possible trigger for Article 5, even before it designated cyberspace as its own military-operational domain.9 Given the close integration of most space and other military assets, it would further make sense for NATO members to subordinate their space assets to NATO supreme command in case of an attack on the alliance, just as with other military capabilities.

Declaring space as a domain would align NATO with some of its major members in this regard, since the USA10, the UK11, France12 and Germany13 all list space as an operational domain beside land, air, sea, and cyberspace. While NATO allies hold largely identical threat perceptions about the changing security environment in space, disagreements might arise over the importance of space and the re-allocation of resources (i.e. funds and personnel) toward developing NATO’s instruments, structures, and capabilities in a future space domain. Furthermore, the debate about subordinating national space assets will, most likely, see diverging opinions within the alliance, especially by states with a high interest in retaining their strategic autonomy. Moreover, allies might disagree over the central question of whether to weaponize space – that is, to station offensive weapons in orbit –, or whether to pursue other instruments to increase their resilience, such as arms control regimes or more passive reactions like the duplication of space assets. Consequently, Germany should facilitate the political debate within the alliance about these open questions and potential challenges. As the scheduled NATO summit in London on December 3-4, 2019 will address “current and emerging security challenges”,14 space might become an important topic. It also has the potential to further deepen NATO’s internal rifts if it is not properly addressed.

### 2AC – No Lasers

#### It’s propaganda–the technology needed to destroy satellites with lasers is years away and current ones only destroy drones

Theresa Hitchens 5/19, Space and Air Force reporter at Breaking Defense. The former Defense News editor was a senior research associate at the University of Maryland’s Center for International and Security Studies at Maryland (CISSM), 5/19/2022, “Don’t be dazzled by Russia’s laser weapons claims: Experts”, Breaking Defense, https://breakingdefense.com/2022/05/dont-be-dazzled-by-russias-laser-weapons-claims-experts/

The ability to dazzle a satellite at that range isn’t a particularly amazing capability, especially given that most modern optical imaging satellites carry cameras that included lenses that function like human eyelids, and simply close when they detect any potentially blinding light source (natural or otherwise).

“Laser systems that can damage tougher and more distant targets such as ICBMs or orbiting satellites are quite some years away. Satellite sensors definitely can be vulnerable to being dazzled or blinded if they are not protected, but certainly much less so if they are well-designed,” Grego said.

The 2022 Defense Intelligence Agency report on “Challenges to Security in Space,” which tends toward the forward-leaning in its threat assessments, found that Beijing “may” field lasers that could cause structural satellite damage by the mid- to late-2020s; and Russia maybe by 2030.

As for Zadira, Borisov’s comments appear to indicate that it is aimed at drones, not satellites. That makes sense, said one defense industry source, in that Ukraine is successfully deploying drones in the on-going war.

“This article seems to be lumping together counterdrone lasers with counterspace lasers. Those are two very different applications, and I have not yet seen anything to suggest that Russia has used counterspace laser,” the industry source said.

“Counterdrone lasers make perfect sense and that is not surprising at all — Russia is getting hammered by small, loitering drones right now. I’m not convinced their ‘prototype’ system will actually prove effective, but I have no doubt they are trying to get it to work,” the source added.

Grego agreed: “The Zadira looks to be a battlefield laser weapon designed to target nearby and relatively fragile systems such as drones. Countries like the United States already deploy laser systems for such targets. The Army has short-range laser defenses and the Navy is beginning to field a system that could target things like rubber dinghies, and the Pentagon is aiming to field more powerful systems that could destroy artillery or mortars.”

Just last month Breaking Defense reported Israel’s announcement that its laser system took out not only drones but mortars and rockets in mid-air.

Among those less than impressed with the Kremlin’s claim was Ukrainian President Volodymyr Zelenskyy, who mocked it as desperate propaganda.

### 2AC – Military key

#### Application of current advanced cybersecurity procedures to space-based assets solves

Laetitia Zarkan Cesari et al 21, Laetitia is a visiting scholar at the International Institute of Air and Space Law (IIASL) at Leiden University and an associate member at the Institute for Strategic and Defense Studies (IESD) at Lyon 3 Jean Moulin University. She holds a master's degree in space law and telecommunications from Luxembourg University, a master's degree in aeronautics law from the Toulouse 1 Capitole University, October 2021, “Space as NATO’s Operational Domain: The Case of the Cyber Threats against GNSS” International Astronautical Federation, https://spacegeneration.org/wp-content/uploads/2022/04/IAC-21E927x66298\_Space-as-NATOs-Operational-Domain-The-Case-of-the-Cyberthreats-against-GNSS\_Paper.pdf/BL

4.3 Cyber Threats Against GNSS

Ground stations - how can we prevent threats? Preventive method and time-based method. Previous attack on ISS. GNSS are specifically vulnerable to hostile cyber operations because of the very low power of their signals and services and constitute potential primary targets in future wars because of their importance not only for military operations, but also for critical national infrastructure and key economic sectors. Unlike physical attacks they are not likely to cause major damages to the satellite navigation system. Recent cyber operations against GNSS were jamming and spoofing [48] although other types of attacks such as hacking or eavesdropping of communications satellite systems, are also technically possible. In 2018, during NATO Trident Juncture, NATO's biggest military maneuverer since the end of the Cold War [49] took place in southern and central Norway, plus the North Atlantic and Baltic Sea between October 25 and November 7. NATO officials confirmed the disruption on November 11 [50]. Cybersecurity for satellite Ground Systems has been neglected. With the increasing number of small satellites and a global network of ground stations needed to provide low latency for data getting between low earth orbit and users, the threat surface for cyberattacks has grown significantly. We are in a phase in which we need to mitigate the risks by simplifying the necessary controls, using time-based methods for analysing controls and preventive cybersecurity mechanisms on new systems in order to provide data assurance. The targeting of space ground systems increased over the last years with highly sophisticated attacks occurring over the last couple of years. Many attacks took place for different reasons, like the non-update of certain vital software to the operating system and that was the case of the International Space Station computers. In 2008, hackers infiltrated the Johnson Space Center’s mission control computer network and were able to have the mission control network upload a malicious Trojan horse access program onto computers on the ISS disrupting on-board communications [51]. In March 2011, the theft of an unencrypted NASA laptop resulted in the loss of algorithms used to command and control the International Space Station [52]. Another cybersecurity issue concerns the vulnerabilities in GPS receivers’ software which rendered GPS’s precision timing invalid. Here instead of spoofing or jamming the GPS signal, the actors attack the inherent weaknesses of GPS’s design to disrupt the timing. Most of the existing cybersecurity risk management policies emphasize on identifying potential cybersecurity issues in the early phase of acquisition, in a way the security of these systems is built into the ground systems right before the deployment. The first step in a good cybersecurity strategy is having a risk management framework to determine what assets are most attractive to hackers and how they should be protected. This means considering all the existing assets (physical and virtual) and the cost associated with the access to these assets by the hacker. We need to consider the type of data that we have in transit like the commands and control communications, live monitoring information, satellite data that will be transferred and the data at rest like databases with satellite information, secured APIs etc. Among the existing effective frameworks, we mention the Cybersecurity Maturity Model Certification (CMMC) [53] that is a program initiated by the United States Department of Defense (DoD) in order to measure their defence contractors' capabilities, readiness, and sophistication in the area of cybersecurity. The CMMC have different stages of security maturity: 1. Scanning - This is the first step that a corporation thinking about cybersecurity will have; 2. Managed Assessment and Compliance; 3. Formalized Analysis and Prioritization; and 4. Attack Focused Management ending with Stage Optimization While existing frameworks provide current guidance on cybersecurity, it’s important to monitor for any recommended changes on a regular basis. Many security control models only address the presence of controls first and do not quantify what those controls provide. The assessment of risk in these models remains qualitative and the risk in these models becomes a subjective measurement. The Time-Based Security method develops the idea of the evaluation of every security measure a system puts in place using a simple mathematical formula for the: Protection Time > Detection Time + Response Time Protection Time is the time a security measure will provide before it becomes compromised or disrupted. Detection Time is the time it takes for the people controlling the system to find out that a compromise occurred. Response Time is the time it takes those people controlling the system to act accordingly. As a result, protection measures from every security process should allocate more protection time than it takes for the system managers to detect and respond to the potential attack. This model provides a method for evaluating successive multiple controls. If the satellite control console is the target, then each successive control preventing access to it is judged. A high-level example could test the time it takes attackers to: (1) access to the base network, (2) access to the satellite control network, and finally, (3) access to the console. Commanders then can make true risk-based decisions on whether they can afford additional protections. The major issue of a quantitative time-based model becomes the requirement for granular testing of every security control on an existing system. The time-based method is applied to new systems, but the selection of security controls becomes a difficult process if the system designers do not consider security at the outset of the design. The selection of security controls in the time-based model may overwhelm system designers. Without an idea of what to protect in a new or modernized ground system, the quantitative model only provides best guesses. Consequently, the quantitative models work best in existing systems. Another model for risk-based evaluation of space ground systems uses a preventative mission assurance model based on redefining cyberspace as anything processing a signal and then using the six steps of the data lifecycle: generation, processing, storage, communication, consumption, and destruction in evaluating the risk to the system. Unlike the other models that consider the detection and usually the threat vector, this preventive model focuses specifically on the vulnerability [51] Generally, if we can build a system without vulnerabilities of the operating system then we can assure security. This preventative model requires the reengineering of communication channels. It does not provide adaptive methods for dealing with existing cyber security channels as those found in existing space systems. In the future, this model will be extremely considered for the modernization and re-engineering of the Air Force Satellite Control Network (AFSCN) ground station network architecture coordinating communications to more than 100 satellites via nine ground stations positioned around the globe. Threat elements release new risks of attacks daily, so security operations should be adapted in a sustainable way. It is crucial to consider risk models to assess the strength of existing controls against the threats addressing most potential security vulnerabilities. Having an established framework that will react fast and effectively is mandatory at this stage. Quantum technologies bring potential new capabilities, to develop parameters of threats, solve the algorithms behind encryption keys that protect our data and the Internet's infrastructure and transform cybersecurity. capabilities and negate adversarial interference with space systems.

5.1 Strategies for building defences for the intersection of space & cyber domains, considering the provisions of the North Atlantic Treaty and other relevant instruments of the Organization

NATO relies on its Allied capabilities; therefore, it is essential to have a unique coordinate system to respond during a crisis. The already existing exercises, such as the Crisis Management Exercise (CMX) which focus on cyber, and resilience should be implemented with space assets. This internal and partner consultation and decision-making procedures at the strategic political military level would help to strengthen the alliance response and resilience. Therefore, NATO has to operate with a renewed focus on improving proficiency in Allied Cyberspace and Electromagnetic Spectrum Operations, by building awareness, developing policies and strategies, acquiring new capabilities, working with industry and academia, and training people to become experts. Building defence is possible by “raising awareness” throughout the NATO systems, and by creation of regulation through NATO security framework , in a standardized and collective way which require a proactive effort to prevent, detect and prepare forces to respond to incidents, by developing guidelines, resources, and working groups focusing on emerging technologies to protect the space assets, and test coherency of the rules and their application by raising preparedness, building blocks between law and policy requirements for collective defence. The traditional policy creation mechanisms are based on multilateralism. States and most of the traditional international organizations struggle to adapt themselves to evolving realities of the new technologies and their applications and implications in new domains, such as cyber and space. Another aspect is to keep the will and interests of member states alive for policy development. This requires NATO to revise and update/adapt its mechanisms, in a way to support a clear-eyed, inclusive policy development, to overcome siloed or single domain-based approaches, to manoeuvre and react in the extremely complex environments. As a military-security organization, and as to its foundational concerns, unlike UN, NATO cannot represent an open forum for the intellectual construction, however, can support and benefit from the effective participation of the commercial actors, which own operate and manage these new domains, and can assess and adapt these new policies created to remain at the speed of relevance, as highlighted in JAPCC 2021 meeting this year.

### 2AC – Say Yes – General

#### NATO will say yes–they’ve been experiencing widespread cyber attacks on satellites and need better security

David Jones 3/18, reporter for Cybersecurity Dive. He has been a reporter and editor for more than 25 years, 3/18/2022, Cybersecurity Dive, “Cyberthreats grow as US, NATO countries press Russia sanctions”, https://www.cybersecuritydive.com/news/cyberthreats-russia-war/620640/

The FBI and Cybersecurity and Infrastructure Security Agency on Thursday said they are aware of possible threats to satellite communications networks in the U.S. and abroad. The agencies are urging organizations to check for insecure remote access tools and urging companies report any suspicious network activity.

Dive Insight:

Cyberthreats against U.S. and allied companies will come from a variety of sources, ranging from state-sponsored actors and others sympathetic to Russia, according to Forrester.

Major energy companies like Shell, Exxon and BP have left billions of dollars on the table after withdrawing from business in Russia. Mastercard and Visa also pulled out and iconic brands like Coca-Cola and McDonald’s suspended new business amid mounting consumer pressure to cease operations.

Attacks may come from sympathetic ransomware groups like Conti, ransomware as a service operators or even insiders sympathetic to Russian interests, according to Forrester.

“There’s no such thing as neutral in something like this,” Jeff Pollard, VP, principal analyst at Forrester, said via email, adding that companies really don’t have a choice to stay on the sidelines.

“The stance your company takes does come with risks — and your cybersecurity team needs to be ready for the choices your company takes, because any stance marks you as a target for some set of threat actors,” he said.

Forrester is urging corporate CISOs to help prepare a communications plan to the board of directors and top executives. Businesses should update plans constantly to prevent being surprised by events.

Executives should even prepare a list of frequently asked questions, so senior executives can properly communicate any security risk questions to the public, the research firm said.

Multiple threats have already been identified directly targeting organizations in Ukraine as well as more widespread threats facing Europe and U.S. organizations. Earlier this week, ESET researchers released information about a third data wiping malware, called CaddyWiper, which destroyed user data and partition information.

Prior research uncovered HermeticWiper and IsaacWiper. Russian state-sponsored actors have also targeted organizations by exploiting the PrintNightmare vulnerability and misconfigured MFA settings.

Critical infrastructure providers have been on high alert regarding the potential for retaliatory threats against U.S. or other western organizations.

“CISA remains concerned about the threat to U.S. and allied satellite communications networks,” Eric Goldstein, executive assistant director for cybersecurity at CISA, said in a statement, while urging organizations to immediately implement the steps in the advisory.

### 2AC – Say Yes – Turkey

#### Turkey will say yes–they want a better cybersecurity framework to follow from NATO

Kieran Hatton 20, Design Research Intern Duo Security Leveraging User Insight Data to Improve Passwordless Experiences on 36 Million Devices, 4/27/2020, “Turkey’s New Cyber Security Center is Necessary, but is It Enough?”, Medium, https://medium.com/meddah-a-u-s-turkey-storytelling-project/turkeys-new-cyber-security-center-is-necessary-but-is-it-enough-89b7ef8cd347

However, USOM’s defenses are unlikely to dissuade stronger foreign state actors, like those involved in the United Arab Emirates remote hacking of former Turkish deputy prime minister Mehmet Şimşek, from seeking ways to disrupt Turkish cyber protections. States like Russia, Iran, and Saudi Arabia maintain competitive relations with Turkey. These nations are therefore incentivized to deploy malware to harm critical Turkish infrastructure.

Turkey should implement a cybersecurity framework. Attacks from foreign states as well as non-state actors are often effective given the Turkish government’s lack of familiarity with cybersecurity measures. Turkish government officials have been reported using unencrypted, traditional email or other unsecured accounts to transmit sensitive information. A cybersecurity framework streamlines digital defense measures and greatly reduces the risk of cyber threats by providing a blueprint for systems which meet rigorous cybersecurity standards. These can be in various forms: multinational, like the European Union’s Cybersecurity Certification Framework; organizational, like the International Organization for Standardization’s (ISO) 2700 and National Institute for Standards and Technology’s (NIST) framework; and, even indigenous, like the Saudi Arabia Monetary Authority Cybersecurity Framework.

For more robust systems to bolster USOM without an explicit cybersecurity framework, Turkish cybersecurity experts and government officials may seek help from National Atlantic Treaty Organization (NATO) allies. The Turkish government can access incredible resources through two central channels: The Cyber Security Collaboration Hub (CSCH) and the Cooperative Cyber Defence Centre of Excellence (CCDCE).

Within NATO, the Communications and Information Agency (NCI) oversees the CSCH. The CSCH is newer than the CCDCE. Established in February 2019, the CSCH is an NCI initiative to provide an information center to benefit NATO countries’ CERTs. The CSCH did not require member state buy-in, additional costs, or staff changes. Turkey’s USOM maintains a route of access to this resource as a member nation of NATO. Both the CSCH and USOM are newer additions to NATO’s cybersecurity force and may experience organizational growing pains throughout the next few years.

While accredited through — but not part of — NATO, the Cooperative Cyber Defence Centre of Excellence (CCDCE) aggregates cyber resources among Sponsoring Nations in NATO. In 2018, 21 members participated as Sponsoring Nations, including Turkey. As such, Turkish experts can access CCDCE archives and collected cybersecurity documentation.

The CCDCE’s Tallinn Manual 2.0, a collection of rigorous research regarding cyber operations and the applicability of international law to the cyber realm, may also inform Turkish military strategy through cyberwarfare.

Cyberwarfare remains a formidable force in the face of dwindling traditional warfighting. Turkish armed forces, observing health precautions following the novel coronavirus, abated their attacks in Iraq and Syria without halting them completely. Unintended consequences of this continued fighting could include increased Syrian refugees flooding into areas under Turkish control, creating a hotbed for the potential spread of COVID-19. Hundreds of infected residing in camps could quickly turn into thousands across northeastern Syria and southwestern Turkey. Cyber offensives present an option to pursue Turkish interests while minimizing casualties on and off the battlefield.

USOM needs to be the first step in a process of erecting cyber defenses across the country. A nascent program is not necessarily ineffective, but the center will have to combat many cyberattacks against Turkey’s still-vulnerable systems. The country must implement a cybersecurity framework, utilize NATO resources, and seek ways to expand USOM’s team and training to other SOCs amid the COVID-19 pandemic to truly provide robust cybersecurity protections against the majority of cyberattacks.

### 2AC – Say Yes – Europe

#### Europe will say yes–Russia’s been attacking their satellites and they’re deciding how to respond

Laurens Cerulus 5/10, leads POLITICO Europe's team of reporters covering cybersecurity, privacy and data protection issues as Cybersecurity Editor, 5/10/2022, “EU, UK blame Russia for Ukraine satellite hack”, https://www.politico.eu/article/eu-countries-blame-ukraine-satellite-hack-on-russia/

The EU and the U.K. on Tuesday slammed the Russian government for an "unacceptable" cyberattack on satellite communications provider Viasat in February that brought down Ukrainian networks.

The attack happened just an hour before Moscow started its invasion of Ukraine, the EU said in a statement, adding it was "yet another example of Russia’s continued pattern of irresponsible behaviour in cyberspace, which also formed an integral part of its illegal and unjustified invasion of Ukraine."

The bloc is "considering further steps to prevent, discourage, deter and respond to such malicious behaviour," it said. Countries can agree to slap sanctions on cyberattackers, and the EU has previously done so with the Russian intelligence services that were behind some of the most devastating cyberattacks in the past years.

### 2AC – Say Yes – Canada

#### Canada will say yes–they want increased satellite cybersecurity

CSA 19, Canadian Space Agency, 6/14/2019, “Cybersecurity from space: the Government of Canada invests in quantum technology”, Government of Canada, https://www.canada.ca/en/space-agency/news/2019/06/cybersecurity-from-space-the-government-of-canada-invests-in-quantum-technology.html

Our digital economy depends on keeping data safe from hackers. Cybersecurity is a priority for the Government of Canada. The Canadian Space Agency's Quantum EncrYption and Science Satellite (QEYSSat) mission will test quantum technology that protects communications in space.

The Canadian Space Agency (CSA) is awarding a contract worth $30 million to Honeywell for the design and implementation phases of the QEYSSat mission.

Current encryption methods are expected to be rendered obsolete within the next decade by the exceptional processing power of quantum computers. Slated for launch in 2022, QEYSSat will demonstrate quantum key distribution (QKD) technology in space. This emerging encryption technology will offer Canada a new, more effective method of securing the transfer of information.

Under this contract, Honeywell will build, test, deliver, provide training for and commission the QEYSSat satellite, which will create a link between ground and space to transmit encryption keys. The work is expected to extend until the end of 2022.

The QEYSSat mission is the culmination of a series of research and technology development activities undertaken by the Institute for Quantum Computing, with support from the Government of Canada. It will bring Canada a step closer to an operational quantum communications service from space, and will advance technology to help meet Canada's cybersecurity priorities.

The lessons learned from the QEYSSat mission will be applied to develop future operational systems for government and provide safer, more secure access to services for Canadians. Commercial applications will include enhanced security for internet-based activities, as well as daily financial transactions such as ATM banking.

In addition to the safety and security principle of Canada's Digital Charter, this initiative aligns with the Government of Canada's Innovation and Skills Plan and the new Space Strategy for Canada through enabling future secure communications, as well as enhancing security and sovereignty.

Quotes

"The QEYSSat mission is another step forward in our government's plan to foster a Canada where citizens have confidence that their data is safe and privacy is respected. In doing so, the development of these new technologies will also bring tremendous potential to transform markets and build a stronger economy that works for everyone."

- The Honourable Navdeep Bains, Minister of Innovation, Science and Economic Development

Quick facts

Quantum computers will be millions of times faster than any conventional computer, which means that they will be able to decipher passwords, personal identification numbers and other current safeguards quickly, putting confidential and personal information at risk.

Current quantum encryption technology (QKD), relies on ground fibre-optic cables and is currently limited to a 200-kilometre distance. QEYSSat will seek to demonstrate QKD between a satellite and a ground network as a way to overcome the distance limits.

Through testing and demonstration of the QKD in space, the CSA will provide a government-owned, space-based platform for federal stakeholders and Canada's scientific community.

Budget 2017 provided $80.9 million to the Canadian Space Agency to support new projects and utilize Canadian innovations in space including the Quantum Encryption and Science Satellite (QEYSSat) mission. This mission will support emerging Canadian capabilities in the area of quantum key distribution, which has the potential to support secure communications through unbreakable encryption codes.

### 2AC – Say Yes – Germany

#### Germany will say yes–thousands of their satellites recently got attacked by Russian cyberattacks, BUT doesn’t thump–they strictly affected wind farms

Reuters 2/28, international news agency owned by Thomson Reuters. It employs around 2,500 journalists and 600 photojournalists in about 200 locations worldwide, 2/28/2022, “UPDATE 2-Satellite outage knocks out thousands of Enercon's wind turbines”, https://www.reuters.com/article/ukraine-crisis-cyber-enercon-idCNL8N2V36NR

Remote control of 5,800 wind turbines knocked out

Enercon says disruption coincided with Russian invasion

Says working with providers to resolve problem

German watchdog BSI says aware of the indicent (Adds German cybersecurity watchdog BSI)

BERLIN/FRANKFURT, Feb 28 (Reuters) - Germany’s Enercon on Monday said a “massive disruption” of satellite connections in Europe was affecting the operations of 5,800 wind turbines in central Europe.

It said the satellite connections stopped working on Thursday, knocking out remote monitoring and control of the wind turbines, which have a total capacity of 11 gigawatt (GW).

“The exact cause of the disruption is not yet known. The communication services failed almost simultaneously with the start of the Russian invasion of Ukraine,” Enercon said in a statement.

The company said it had no further information on who or what may have caused the disruption.

Enercon has informed Germany’s cybersecurity watchdog BSI and is working with the relevant providers of the satellite communication networks to resolve the disruption, which it said affected around 30,000 satellite terminals used by companies and organisations from various sectors across Europe.

BSI said it was aware that a satellite-based communications operator has experienced a malfunction and that this had restricted the maintenance of some wind turbines, without providing details.

“However, no effects on power grid stability are currently expected due to redundant communication capabilities of the responsible grid operators. Further investigations into the cause are being carried out by the company concerned in close exchange with the responsible authorities,” BSI said.

U.S.-listed satellite communications firm Viasat Inc said earlier on Monday it was investigating a suspected cyberattack that caused a partial outage in its residential broadband services in Ukraine and other European countries.

Enercon is working with the operators of the affected wind farms to set up alternative ways to regain remote control of the turbines, it said, without naming the operators.

There was no risk to the turbines as they continued to operate on “auto mode,” the company said.

### 2AC – Solves ASATs

#### Utilizing active AND passive countermeasures perfects defense against ASAT attacks and promotes info sharing and trust.

Antonio Carlo 20, professor at the Sapienza University of Rome; Nikolaos Veazoglou, professor at the National and Kapodistrian University of Athens, 3/30/2020, "ASAT Weapons: Enhancing NATO’s Operational Capabilities in the Emerging Space Dependent Era," http://dx.doi.org/10.1007/978-3-030-43890-6\_34, sg

5 Actions that Can Be Taken to Contrast ASAT Weapons

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

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

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

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

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

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

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

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

### 2AC – Solves Generic

#### The plan solves through linking centers, info-sharing through integration, bilateral threat awareness, analysis of vulnerable commercial assets, security-by-design, and initiation of discussions towards standardization of defense posture.

Dr. Beyza Unal 19, Former Deputy Director of the International Security Program, July 1 2019, “Cybersecurity of NATO’s Space-based Strategic Assets”, https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets-0/2-cyber-risks-space-based-strategic \\SYang

Recommendations and Observations

Some of the recommendations and observations suggested below are activities that are currently in the planning stage – as part of the NATO Space Working Group Action Plan, or as part of ongoing discussions with allies. However, these activities have not yet been implemented and require continuous attention.

Encouraging allied member countries to be responsible for protecting their own space capabilities, and to consider space in national force structures rather than in the NATO command structure. In addition, NATO should consider how the configuration for space assets between the allies and NATO would look in time of conflict.

There is a need for a NATO Centre of Excellence (CoE) for space. In cyberspace, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) shares information between NATO, the allies and NATO partner countries. However, the alliance lacks an established CoE for space policy.

NATO is trying to link national space operational centres (to date, these include those of the UK and Canada) in order to establish routine contact and for regular information-sharing. It would be valuable to incorporate all allies that have space capabilities into this initiative; and to start discussions with allies that have space aspirations.

NATO lacks a 24/7 operational cell that can observe and monitor activities relating to space. It could create a space coordination cell, in order to coordinate knowledge and data in all of the six capability areas outlined in this paper.

Further planning needs to go into the integration of new technologies when securing satellites from cyberattack. Aspirations in this area may include the ability for satellites to configure and fix themselves.

A NATO Industrial Advisory Group (NIAG) study is required in order to examine ways of sharing information between NATO and the private sector. Through this study, NIAG could provide industry advice to the Conference of National Armaments Directors and to other NATO units. Such advice could shape NATO military capability requirements and be linked to the next cycle of the NDPP.

Current cybersecurity maturity standards and guidelines (such as those published by the US National Institute of Standards and Technology) help organizations to improve their cybersecurity measures and best practices. How effectively cybersecurity maturity standards can be applied to space-sector maturity should be analysed further. If the two areas are different in essence, then separate standards and guidelines for space could be developed.

Securing space assets against cyberattacks at the design stage is particularly important, and should be a fundamental component of satellite and ground station design from the initial concept – giving rise to a ‘security-by-design’ approach.

Information Sharing and Analysis Centers (ISACs) help improve collaboration and resilience in the cyber realm. Similar types of national centres in the space sector could provide insights and could improve engagement between allies.

The annual NATO Information Assurance Symposium (NIAS) Cyber Security Symposium could focus on space in upcoming years.

The potential establishment of a NATO science and technology committee, involving or led by the NATO Communications and Information Agency (NCI Agency), could be further explored. Such a committee could be relied upon to give advice on relevant cyberthreats and vulnerabilities, such as those related to the integrity or security of supply chains.

The NCI Agency is responsible for operating and defending NATO’s networks, and rapid sharing of information has proved to be one of the most effective defences in cyberspace. In the cyber domain, there are certain tools in place – such as the Malware Information Sharing Platform (MISP) – that promote cooperation and information-sharing among allies. Information-sharing could also be more closely examined in relation to the space sector. Through sharing information and explanations of operational impact, NATO could increase allies’ awareness with regards to space-based threats.

NATO should further increase its efforts to strengthen its cyberdefence posture through the NATO Industry Cyber Partnership: enhancing collaboration between the public and private sectors is one of the fastest and least expensive ways to increase cyber resilience, improve incident handling and mitigate vulnerability to attack. Moreover, this should foster timely information-sharing on cyberthreats, allowing stakeholders to enhance situational awareness and better protect their networks. In practice, for instance, it should facilitate rapid and early bilateral exchange of non-classified technical information related to cyberthreats and vulnerabilities. Improvements in the cyber domain would have a positive impact on the space realm.

Under a future NATO Space Policy, defence planners should define NATO’s space capability requirements and present them to all allies by means of the NDPP.73

NATO Space Policy could lead to recognizing space as the fifth domain. This would help NATO better plan for future operations that use space assets and technology and to incorporate space into the defence planning structure.

Increasing awareness at all levels require holistic exercises and tests in order to give end users experience in how these systems actually work. Therefore, space considerations should be incorporated into existing exercises and training.

The entanglement between commercial and military space assets may also cause vulnerabilities. In future, military systems will be increasingly connected to non-military systems. This has important implications for the laws of armed conflict, as the combination of civilian, commercial and military capabilities in the cyber domain and space raises the risk that civilian capabilities used for military purposes qualify as legitimate military targets.

NATO should ensure that contractors that rely on commercial standards follow minimum cybersecurity arrangements.

NATO may consider ensuring that commercial contracts meet military protection standards, in order to mitigate the risk posed by the military’s use of commercial space assets.

NATO should conduct a gap analysis that will identify the following: which countries NATO relies upon for space services; what type of capabilities these countries possess; what type of capabilities they should have for future warfare; and what actions NATO needs to take (the latter being subsequently enshrined in an action plan).

Although NATO does not lead development of the space sector and it is the allies that provide space capabilities, NATO can still initiate informal discussions with the allies on the establishment of targets for space resilience. In the cyber realm, for instance, cybersecurity targets have been incorporated into the NDPP.

Mapping out recurring threats to space systems and promoting standardization to address common weaknesses may increase resilience. If standardization is unwanted due to its risks, then a voluntary ‘best practice’ approach can be utilized. NATO’s military command may also enter into direct discussions with the allies to set up minimum requirements. In this regard, a commanders’ intent paper can also capture space infrastructure.

#### NATO is growing increasingly reliant on its cyber and space capabilities – space based assets provide services important to deterrence and security

Karl-Heinz Brunner 21, member NATO Parliamentary Assembly and the Bundestag Defence Committee and Subcommittee on Disarmament, Arms Control, and Non-Proliferation, October 2021, “Space and Security – NATO’s Role,” NATO Parliamentary Assembly, Science and Technology Committee, https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/025%20STC%2021%20E%20-%20SPACE%20AND%20SECURITY%20-%20BRUNNER\_2.pdf

Space is essential to the Alliance’s deterrence and defence (NATO, 2020). NATO Allies rely heavily on space for the protection of their homelands and for military operations around the globe. Space is an “enabling domain” as it is closely interconnected with the other security domains relevant for NATO: maritime, air, land, and cyber space. Together with cyber, space will therefore play a critical role for the security of Allied nations. 37. Satellites provide precise information on movements by friend and foe through imagery or via signal interceptions. They transfer huge amounts of data from and to the battlefield: operating a single Global Hawk, for instance, requires roughly 500 megabits of satellite bandwidth per second. This is five times the total amount of satellite communications that US forces used during operations in the First Gulf War (The Economist, 2019). 38. During the 1991 Gulf War, often referred to as “the first space war”, space systems evolved from strategic assets to tactical enablers. Satellites provided near real-time information down to the tactical level throughout operation Desert Storm for the first time. Space assets, originally developed to detect strategic missile launches, were transformed into tools that worked “down to do scope reporting” in 1991 (Strout, 2021). The use of satellite-based information contributed to the quick and decisive victory of the US-led forces. 39. Today, many of NATO’s most advanced systems depend heavily on space-based assets. Examples include the Alliance’s Ballistic Missile Defence (BMD) programme, the Airborne Warning and Control Systems (AWACs) and the Ground Surveillance System (AGS) (Moon, 2017). NATO’s Joint Air Power (JAP) is equally dependent on the national capabilities in the space domain of Allied states as they support operations in the air as well as on the ground and on the seas (Bockel, 2018). 40. The Alliance defines five core areas where it heavily depends on space-based assets (NATO, March 2020). These are (1) positioning and navigation: enabling precision strikes, force navigation or combat search and rescue (CSAR) missions; (2) integrated tactical warning and threat assessment: securing force protection, providing crucial information on missile launches and thus allowing attribution; (3) environmental monitoring: enabling meteorological forecasting and sound mission planning; (4) communications for command and control purposes and (5) intelligence, surveillance and reconnaissance (ISR) capabilities: providing intelligence on and off the battlefield and informing targeting decisions. A key benefit of space access is that it increases the ability of the Alliance to respond, thus making it is crucially important for deterrence. Deterrence is largely based upon the adversary knowing that NATO is prepared to act, and to act the Alliance must first Observe, Orientate and Decide, as described by the military strategist John Boyd. Information gained from space can accelerate the OODA loop (OODA loop – Observe, Orient, Decide, Act) and prevent the need for conflict through careful focused action. 41. Free access to space and resilient space infrastructures are essential for operational capability and defence. As a consequence, the dependence of modern armed forces on space has become one of their greatest vulnerabilities. In the early days of space infrastructure, only the U.S. and the Soviet Union were capable of launching satellites into orbit. Space-denial technologies were either non-existent or in their infancy. After the fall of the iron curtain, the threat to Western space assets and capabilities was significantly diminished. The recent evolution of space capabilities, especially on the commercial side, and the increased number of space-faring nations has changed this situation, however.

## 2AC – Add Ons

### 2AC – Ag

#### War in cyberspace opens vulnerabilities to seize control of satellites and shut them down

Abhijeet Singh Baghel 19, cybersecurity researcher, recipient of a Master of Science in Cybersecurity from Utica College, December 2019, “Cyber Warfare in Outer Space,” p. 12-13

The need for cybersecurity. Cyberspace is infused throughout each warfighting domain. Outer space is no different and space operations rely heavily on cyberspace to complete missions which means this field is no stranger to cyberspace threats. An adversary could use a cyberattack to simply monitor and collect signals intelligence to use against its target indirectly or could employ cyber espionage to gain critical technical expertise to bolster military research and development (Defense Intelligence Agency, 2019). In these examples, intelligence gathered in cyberspace is weaponized to ensure information superiority, which plays a vital role in military and political strategy in times of war and peace. In addition to space assets, it is important to protect classified space operations intelligence by ensuring its confidentiality, availability, and integrity to successfully maintain space dominance (Mather, 2018). When security measures are not adequate to ensure this, it opens possibilities for adversaries to hack into space combatant commands and operation centers and possibly corrupt important data or render space assets useless by seizing control (Harrison, Johnson, & Roberts, 2019). Cyberattacks are relatively cheap and do not require substantial 13 resources to complete, just an understanding of the sophisticated target. For example, China is prepared to employ cyber operations against U.S. satellite and ground stations to deescalate future conflicts by preventing the U.S.’s ability to operate during the early stages of a conflict. This is no surprise as China has already performed cyberattacks on satellites belonging to the U.S. Geological Survey, NASA, and NOAA and several others multiple times since 2007 (Gruss, 2014 and Harrison, Johnson, & Roberts, 2019).

**Satellites key for ag**

Steven Tompkins 19, Inmarsat’s director of sector development for agriculture, 3/18/2022, “Inmarsat's Steven Tompkins cuts through the jargon to explain why satellite connectivity is the key to a global, digitalized agriculture industry,” <https://www.inmarsat.com/en/insights/enterprise/2019/enabling-the-connected-farm-the-importance-of-satellite-communications.html>, Inmarsat

The Agri-Tech Revolution, Agriculture 4.0, the smart and connected farm. There is no shortage of buzzwords hinting at a digitalised future, or solutions being touted as game-changing for the global agricultural industry. Commonly claimed benefits include increasing crop yields, and a reduction in input costs and the reliance on manual labour.

Many of these solutions rely on reliable internet connectivity in the field to push data from one place to another, but there are still vast swathes of agricultural land that suffer from unreliable or non-existent connectivity, either lacking cellular or broadband connectivity. If we are to take advantage of the huge possibilities available to us, overcoming our connectivity challenges will be crucial.

**This is where satellite communications can help**. When I tell people that I am an agriculturalist working for a satellite company, almost always the response is related to an experience of using space imagery (known as Earth Observation) to help automate processes such as crop scouting. But there is another breed of satellites that don’t produce images but do provide fast and reliable internet and voice communications across the world in areas that cellular and fibre connectivity cannot reach.

Ubiquitous connectivity from satellites opens up huge possibilities for farmers in remote areas to take advantage of the Agri-Tech Revolution. In some cases, this is as simple as connecting frontline worker teams in large plantations to operations centres to prioritise workload and create efficiencies. Taking it one step further, satellite communications can be a bridge to enable farmers to connect data producing devices in the field (such as weather stations, sensors, data from farm machinery) to business applications.

Known by the tech world as the ‘Internet of Things’ or IoT, this approach collects data from the field and harnesses it to **support intelligent decision-making**. For instance: obtaining real-time data on nutrient status in the field from NPK (Nitrogen Phosphorous and Potassium) sensors, alongside crop monitoring data and hyper-local weather that would allow you to make completelyobjective risk-based decisions on when and where to apply fertiliser.

**Precision ag solves global food security---satellites are key.**

Robert Bell 18, businessman with over 30 years of experience as an association manager and business consultant for both nonprofit and profit-driven and organizations operating in the IT outsourcing, telecommunications, and financial services industries, 10/11/2018, “How Will Precision Agriculture Feed the World?”; <https://www.satellitetoday.com/imagery-and-sensing/2018/10/11/how-will-precision-agriculture-feed-the-world/>, Via Satellite

By the year 2050, the world’s population is expected to hit 10 billion. Feeding that population will mean **increasing global food production** by 70 percent — without poisoning the world’s water supply with nitrates in the process and meeting rising demands for high food quality.

That, in a nutshell, is the reason why **agriculture needs to go digital**, and in a hurry. The good news is that the adoption of new agriculture technology (agtech) over the past decade has been strong in many places. According to a 2016 study from the U.S. Department of Agriculture, tractors guided by Global Positioning System (GPS) are in use on 50 percent of corn and soybean acreage in the U.S. Yield mapping — which means developing precise data on what sections of a field produce the biggest yield — is used on 40 percent of that acreage. Variable-Rate Technology (VRT) covers about 30 percent with systems that apply fertilizer based on yield maps, substantially reducing waste and excess use.

The bad news comes in two flavors. First, big farms in excess of 2,900 acres are twice as likely to use agtech, because its scale makes it more affordable and profitable. Second, precision agriculture is largely restricted to rich nations. Their farmers have more money to spend, and large farms make up a much higher percentage of land in agricultural production.

A Better Glass of Wine As one example, take winegrowers. They are among the high-end producers who have made precision agriculture central to their business. They do yield mapping in great detail, down to 2-meter blocks, and adding data on everything from soil acidity clay and water retention to yield to every block. The data comes from close inspection and testing in the field, but the **mapping is made possible by GPS**, which also can be used to steer mechanized pruning, watering, and harvesting machines.

**Satellite imagery** is also **vital**. Infrared sensors in space produce data that can be analyzed to produce a Normalized Difference Vegetation Index (NDVI), which accurately measures the amount of leaf area in a block. Take repeated scans, and the winegrower can see how much leaf the vines are putting on — an important measure of health — and focus attention on the blocks where there is too much or too little.

Held Back by Bandwidth This kind of technology investment has led some to call today’s farmers the high-tech entrepreneurs of rural regions. But whether in rich or poor nations, those high-tech entrepreneurs face one big constraint: bandwidth. According to Microsoft, 23 million people in rural areas lack broadband internet access in the U.S. In Europe, 21 percent of rural populations had no access to the internet in 2017. Go to developing nations and the numbers accelerate: 69 million in Brazil, 378 million in China, and 725 million in India.

As we all know, there is broadband — and then there’s better broadband. The computer I am working on is connected to the web at 300 Mbps at a cost of about $80 per month. Precision agriculture is part of the Big Data revolution. To leverage its value, these rural high-tech entrepreneurs need significant bandwidth for download of **satellite imagery**, connectivity for drones, access to cloud computing platforms that aggregate huge data sets, and upload of their own big data sets. They need high-capacity connectivity not only at home, but in the field. The alternative is to drive all their automated equipment up to the barn and plug it in to their computers for upload and download of data.

Precision farmers in developing nations are finding ingenious and low-cost solutions that give them some capability over 3G and 4G mobile. But we all know the limits of that connectivity, particularly in areas where coverage is sparse.

If there were no other reason why Geostationary Orbit (GEO) High Throughput Satellite (HTS) and the coming generation of **high-capacity Low Earth Orbit** (LEO) **satellites** were needed, this requirement would be enough. The market for precision farming technology is estimated to be worth $5.09 billion in 2018 and headed for $9.53 billion in 2023, growing at 13.4 percent Compound Annual Growth Rate (CAGR).

Mother Earth will have **another 2.4 billion** mouths to feed in a few decades, and the connected, technology-rich farm is the **only way** she is going to do it.

### 2AC – Debris

#### Squo decentralized satellite planning endorses Chinese cyber-attacks that cause satellites to collide, creating tons of space debris---otherwise known as the Kessler Syndrome.

Jan Kallberg 12, scientist at the agency-sponsored Insider Threat Research Program and is an Assistant Professor at the United States Military Academy, 3/1/2012, "Designer Satellite Collisions from Covert Cyber War," *Strategic Studies Quarterly,* 1(1), pp 130-132, https://www.researchgate.net/publication/256031426\_Designer\_Satellite\_Collisions\_from\_Covert\_Cyber\_War, sg

Cyber Attacks in Space. The life span of a satellite is between five and 30 years, and even afterward it can still be orbiting with enough propellant to move through space and with functional communications which could be reactivated. Space contains thousands of satellites, both active and inactive, launched by numerous organizations and countries, hosting 5,000 space-borne transponders communicating with Earth. Every transmission is a potential inlet for a cyber attack. Older satellites share technological similarities, providing opportunities to cyber-exploit industrial systems for control and processing. Supervisory control and data acquisition (SCADA) systems within our municipalities, facilities, infrastructure, and factories are designed and built on older technology and hardware, sometimes designed decades ago, and the software is seldom updated. These SCADA systems are considered a strategic vulnerability and have drawn growing attention from the US cyber-defense community in recent years. Satellites may be based on hardware and technology from the 1980s for one very simple reason—they are unlikely to be upgraded after they have been launched into space.

Terrestrial cyber attacks are a single exploit on thousands, if not millions, of identical systems, and the exploit will be eliminated afterward by updates or upgrades. The difference between satellites and terrestrial cyber exploits is that a satellite is in many cases custom made, whereas the computing design is proprietary. Cyber attacks in space exploit a single system, or limited group of systems, within a larger group of satellites. These space-borne assets have a variety of operating systems, embedded software, and designs from disparate technological legacies. As more nations engage in launching satellites with a variety of technical sophistication, the risk for hijacking and manipulation through covert activity increases. A satellite’s onboard computer (OBC) can allow reconfiguration and software updates, which increase its vulnerability to cyber-attacks. A vulnerable satellite that will be orbiting for the next 10 years can be preset by a cyber perpetrator for unauthorized usage when needed.

Even with the most-advanced digital forensics tools, tracing a cyber attack is complicated on terrestrial computer systems, which are physically accessible. Space-borne systems do not allow physical access, thus, lack of access to the computer system nullifies several options for forensic evidence gathering. The only trace from the perpetrator is the actual transmissions and wireless attempts to penetrate the system. If these transmissions are not captured, the trace is lost.

If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Attribution can be graduated, and the level varies as to what would be accepted as an “attributed” attack. The national leadership can accept a lower level of tangible attribution, based on earlier intelligence reports and adversarial modus operandi, than the international community might demand, but it is restrained in taking action. China has had a growing interest in building cyber warfare capabilities21 and is one of several nations that would have a sincere interest in degrading US space assets. Currently, nationstates are restrained by the political and economic repercussions of an attributed attack, but covert cyber war targeting US space assets removes the restraint of attribution.

A cyber attack resulting in a space collision would lack attribution and thus would be attractive to our covert adversaries. A collision between a suddenly moving foreign satellite and a mission-critical US satellite is neither a coincidence nor an accident. But without attribution, it does not matter that this is so obvious. Other forms of direct and indirect attack would be traceable to an attacker, which could result in military, economic, and political repercussions. In criminology we know that the major consideration of a perpetrator for premeditated acts is the risk of getting caught. The size of any repercussions if caught is secondary. If a cyber attack can destroy or disable US satellites with no attribution or traceability, it is likely to be considered by those who are openly adversaries and certainly by those who are covert. From a cyber warfare perspective, this creates an opportunity for a third party to hack and hijack a satellite with the express purpose of colliding with a mission-critical US satellite. The attack could be either a direct collision or an indirect attack using the debris cloud from another collision. The ramming satellite can come from any country or international organization. The easiest way to perpetuate this attack would be to hijack satellites from countries less technically advanced or from less-protected or outdated systems.

The Hypervelocity Eight Ball. The term hypervelocity eight ball refers to the hitting of targeted satellites, directly or indirectly, with the intent to destroy the target by collision with hypervelocity objects. As previously discussed, the adversary can create a direct attack by ramming targeted US satellites with space vehicles through unauthorized cyber commands. The target for the initial step in an indirect attack may well be another satellite, part of a delivery vehicle, or space junk that will create significant debris upon impact. The collision creates hundreds or thousands of debris pieces that continue in space at high velocity. The debris cloud will affect other satellites in the collision orbit and may even initiate the Kessler Syndrome, causing proliferating damages if the threshold is reached.

#### Debris blocks space colonization AND creates a cascade of satellite destruction.

Dov Greenbaum 20, PhD in genetics and bioinformatics with a focus on emerging technologies and IP, 11/20/2020, "Space debris puts exploration at risk,” *Science,* 370(6519), pp 922, https://www.science.org/doi/10.1126/science.abf2682, sg

Space debris puts exploration at risk

Humans have now lived aboard the International Space Station (ISS) for 20 years (1). As we look toward the next 20 years, we must address the dangers that space debris poses to both manned missions and crucial satellites. National policy-makers and international organizations must develop actionable rules and regulations that preserve our ability to explore space.

With tens of millions of pieces of space junk rocketing around our planet at thousands of kilometers an hour, debris is a substantial threat to our expanding networks of satellites and even the ISS itself (2–4). The European Space Agency (ESA) puts much of the blame on the failure to properly dispose of expiring satellites (2). The recently signed Artemis Accords similarly point to the value of “end-of-mission planning and implementation [and…] post-mission disposal” in reducing debris (5). With the rapid expansion of the satellite orbital population—many of which are relatively cheaply produced with comparatively high failure rates (6)—this problem will likely get much worse before it gets better.

Unfortunately, Cold War cooperation led to rules designed primarily for nation states, not for the corporations that are now launching literally thousands of new satellites. Meanwhile, the nation states have mostly neglected to implement the necessary local space regulations that would promote the long-term sustainability of equitable space exploration. This tragedy of the commons will damage the space environment and eventually impair commercial space endeavors. Space debris threatens efforts ranging from the emerging mini-satellite mega-constellations that aim to democratize internet access to space tourism. In a worst case scenario, orbital debris could start a self-sustaining cascade of destruction that would litter the Low Earth Orbit with enough debris to make it effectively unusable (7).

### 2AC – Laundry List

#### Russian and Chinese cyber operations against space-based capabilities can decimate NATO’s ability to [everything].

Dr. Beyza Unal 19, Former Deputy Director of the International Security Program, July 1 2019, “Cybersecurity of NATO’s Space-based Strategic Assets”, https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets-0/2-cyber-risks-space-based-strategic \*\*Altered for ableist language. We do not endorse any ableist language.

Considering that digital technologies are fundamental to all six of the space-dependent capabilities described above, none of them is immune to cyberattacks. Moreover, any digital system that relies upon near real-time information is vulnerable to cyberattacks. The loss of one or more of these capabilities because of human or system error or through offensive cyber operations conducted by an adversary, could have severe strategic, operational and tactical consequences. In order to understand the value of each space-dependent capability, it is important to analyse the consequences of cyberattacks on each.

Cyberattacks on military weapons systems may have operational and strategic consequences that change the way the military operates in conflict. Although electronic warfare has been in use for more than a century, sophisticated cyberattacks on the systems of NATO or its key member countries have a new and distinct impact on decision-making and on how NATO conducts its operations. Cyberattacks on military systems could also have a paralysing effect on strategic military and political decision-making and could render NATO countries vulnerable to Russian or Chinese information and deception operations.

Timing is a crucial element of PNT capability. Most of the electronics used in military, civilian and commercial spheres depend on timing signals. By intercepting securely transmitted data through cyber means, an adversary may jeopardize the alliance’s missions and services. A compromised system would also diminish reliance on data received, as data confidentiality would be brought into question through possible acts of spoofing and deception.

The involvement of Russia and the US in the Syrian conflict, and the use of electronic techniques, such as signal jamming, and cyber means, such as hacking and spoofing, demonstrates the potential operational uses of cyberattacks. Russia’s electronic warfare capability involves not only an air defence capability but also integrates cyber operations.58

What type of consequences would result from cyberattacks within space-based systems? What would be the operational and strategic impact? The table below outlines some of the potential consequences for each capability:

Table 2: NATO space-dependent capabilities and potential consequences from their absence NATO space-dependent capabilities Potential impact from the loss of capabilities Position, navigation and timing (PNT) • Impacts on the civilian airspace, such as airliners losing on-board navigation systems (which is not directly within NATO’s purview, but which would affect the scale of the conflict or crisis in general. Moreover, an attack on civil systems could result in military consequences). • Losing contact with the alliance’s forces and assets during their deployment. • Loss of the time signal and its impact on the functioning of warships and guided missiles. • Losing connection with ships, aircraft, carriers etc. in conflict due to interference to their navigation systems. • Loss of precise time to create financial transaction timestamps as financial sector’s internal clocks rely on GPS. • Cyberattacks on the guidance mechanism of a weapon (such as a missile) that would result in failure of weapons delivery accuracy. • Impact on the security of mission-critical assets and mission assurance.59 Intelligence, surveillance and reconnaissance (ISR) • Interference to the ISR capability that leads to faulty assessment and response to threats. • NATO could lose the possibility to transmit ISR information over potential adversaries’ territory. • Loss of situational awareness in peacetime and at times of conflict, resulting in faulty decision-making. • Loss of battlefield awareness for the commander, thus putting the desired operational objective in danger. • Manipulation of ISR data through spoofing attacks, which could cripple defensive systems by sending falsified or excess information to decision-makers. Missile defence • The loss of missile defence capabilities in peacetime due to cyberattacks would diminish situational awareness on ballistic missile launches in the world – reducing intelligence on when and where a missile is launched, and by whom. In times of conflict and warfare, losing this capability may result in unintentional escalation. • In times of conflict, such a loss will have strategic, operational and tactical consequences for NATO missions and operations. • Cyberattacks on missile defence could occur in the form of spoofing, thus deceiving the ballistic missile command system. • The inadequate interception of the upcoming ballistic missile may result with civilian casualties. Communications • Losing communication systems or receiving spoofed data, thus compromising the integrity of information received. • Decision-makers (including presidents, prime ministers and senior military cadres) may not be able to send the necessary orders down the chain of command. • Decisions based on faulty information may lead to escalation and decrease the threshold for conflict. Space situational awareness • Loss of control or destruction of satellite control systems through the targeting of those systems or of mission packages by cyberattacks. • Altering the orbit of the satellite or ‘grilling’ its solar cells by exposing it to high levels of ionizing radiation.60 • Inability to detect, predict or assess space debris or its re-entry, which could impact on life. • Disruption of missions and all other space services, thus impacting on military operations and on human life. Environmental monitoring • Cyberattacks on weather systems or on environmental monitoring systems may cause problems in defence planning for an attack as the military rely on daily weather information to conduct its operations. • Weather information is fundamental for land, air, and maritime domains. Cyberattacks on weather forecasting systems could impact on operational capacity.

### 2AC – NATO Strength

#### Space capabilities are critical for all NATO-based operations.

Antonio Carlo 20, professor at the Sapienza University of Rome; Nikolaos Veazoglou, professor at the National and Kapodistrian University of Athens, 3/30/2020, "ASAT Weapons: Enhancing NATO’s Operational Capabilities in the Emerging Space Dependent Era," http://dx.doi.org/10.1007/978-3-030-43890-6\_34, sg

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

* Satellite Communications (SATCOM): One of the most widespread functions of satellites, either civilian or military, is telecommunications. SATCOM provides support to C2 through its multiple applications, such as the establishment of communications in regions with minimal or even non existent infrastructure; transmission of intelligence; relay of messages and control of UVs.
* Position, Navigation and Timing (PNT): The PNT data provided by space-based assets are essential for the prosecution of NATO operations, since they are used for precision targeting; tracking of friendly and enemy forces; provision of precise timing which is also vital for the function of networks and accurate navigation of troops.
* Environmental Monitoring: Meteorological and oceanographic data collected by satellites are crucial to NATO forces since they play an important role in the planning of missions and the selection of the optimal weapons system to be deployed based on weather conditions. Also the knowledge of the conditions on the theater of operations allows forces to take advantage of them, for example the prediction of flooding based on maps developed in Afghanistan was used enhancing military operations and provide humanitarian support [7].
* Space Situational Awareness (SSA): Space situational awareness is the knowledge regarding the outer space environment, natural and operational, and its effects on NATO operations. SSA applications includes knowledge regarding the operational capabilities and limitations of both allied and adversary space platforms; tracking of space debris; observation of space weather; tracking of adversary activities in outer space and detecting attacks against space based assets. SSA is essential for the function of satellites and the conducting of their missions.
* Intelligence, Surveillance and Reconnaissance (ISR): Space based assets equipped with sophisticated sensors provide a host of services, such as intelligence gathering, including Signal Intelligence (SIGNIT); target information and damage assessment; warning of attacks and situational awareness.
* NATO Shared Early Warning (SEW): Dedicated sensors onboard satellites can detect the launch of ballistic missiles and track their trajectory. Satellites also provide NATO with the capacity to detect nuclear explosions (Nuclear Detonation Detection System) which is essential for identifying any violations of international treaties banning nuclear detonations (e.g. the Partial Test Ban Treaty).

### 2AC – SSA

#### Plan spills over---a shift in cyber policy in space to integration of component assessment, interoperability, official guidance, and a security framework allows NATO to fully leverage space.

Berenike Vollmer 21, President and Co-Founder at The Sciences Po Cybersecurity Association, Non-Resident Visiting Scholar affiliated to NATO CCDCOE Tallinn, Cyber Threat Analyst and ISAO Manager for Cyber Intelligence, February 2021, “NATO'S MISSION-CRITICAL SPACE CAPABILITIES UNDER THREAT: Cybersecurity Gaps in the Military Space Asset Supply Chain”, https://www.researchgate.net/publication/349519572\_NATO'S\_MISSION-CRITICAL\_SPACE\_CAPABILITIES\_UNDER\_THREAT\_Cybersecurity\_Gaps\_in\_the\_Military\_Space\_Asset\_Supply\_Chain \\SYang

POLICY RECOMMENDATIONS AWARENESS Initiate Intersectoral Collaboration: • Aligning differing security and ethical standards between countries; • Organizing at least one annual space asset CSCRM symposium by executives from both sides to exchange on current challenges and estimated organizational impact; • Establishing further PPPs along the SASC, for example with: o CCSDS and ISO; o Space ISAC; o US AIA; o CERTs, CSIRTs and ENISA; and/or o OSA; • Utilizing the upcoming CCDCOE Tallinn Manual 3.0 multi-stakeholder project, as well as the 2020 EU Cybersecurity Strategy for the Digital Decade to address gaps. Increase NATO Strategic Level Engagement: • Creating mission-specific guidance, agreements, and security considerations; • Establishing recurrent executive-level SC leadership councils; • Timely increase of resources and staffing. Spur Exchange of Academic Expertise: • Strategically investing in space asset Research and Development (R&D) and the development of viable alternatives, such as through NATO STO’s Information Systems Technology Panel; • Realizing the establishment of a NATO Space Technology Centre under guidance of NCIA; • Considering attack vectors originating from new and upcoming technology, such as AI being increasingly implemented in space assets; • Inviting outside organisations and cybersecurity experts to provide expertise and differing perspectives on the topic, such as through cooperation between NCIA and Europol EPE. Conduct Mission-Specific Cyber SASC Risk Assessments: • Ensuring knowledge on specific procurement and SC environment around each mission, thus sourcing the materials to the level of integrity required; • Moving from detective to preventive third-party cybersecurity management capabilities; • Establishing a formal programme through manifesting policies, governance, procedures, tools, and processes on data sent to and received by any supplier; • Assessing NATO-procured ICT components, such as hardware, software, and services; • Analysing suppliers, suppliers’ sources, and the larger SC ecosystem; • Dedicating specified NATO personnel to effectively assessing and communicating supplier risks to NATO’s executive leadership. Chapter 7: Conclusion 71 Train Cyber SASC Risk Management throughout NATO Exercises: • Including cyber SASC risk management at least in every midsize to large NATO exercise to support a forward-leaning, collective defence approach; • Facilitating space asset CSCRM training for relevant stakeholder organization-wide as well as for key suppliers; • Facilitating individual end user training for each redeployment; • Engaging white hat hackers to penetration test for possible vulnerabilities throughout trainings; • Continuous phishing simulation exercises, mapping upcoming cyber SC threats and priorities, or tabletop exercises to determine key stakeholders and their responsibilities; • Sharing training and test reports to both the military and intelligence community and the commercial sector. REGULATION Streamline Security and Classification Levels: • Implementing formatting standardization for eased data integration and processing, e.g., agreeing on specific SATCOM frequencies, software, timing formatting; • Streamlining classification levels; • Streamlining strict clearances of staff and a good operational understanding of interacting with commercial representatives and users. Enhance Procurement Contract Requirements: • Creating a standardized public-private security framework for NATO-specific SASC cybersecurity: o Streamlining working language, external and internal assessments, incident reporting and communications across all partners and entities, thus creating a single-entry point for suppliers; o Adopting a standards-oriented, streamlined supplier risk approach to CSCRM processes; o Incorporating strengthened insurances, such as for data privacy, into negotiations with suppliers; o Better monitoring progress and operations via customer and supplier assessments to determine CSCRM maturity; o Ensuring that contractors comply with military protection standards. • Including mandatory reports of all space asset cyber breaches, and guidance on prioritization and determination of critical components and responsibilities; • Substituting Security by Obscurity by Security by Design and Default; • Integrating or partially adopting industry standards and procedures into supplier contracts: o NAS9933; o DOD CMMC; o ISO 27001; o NIST SP 800-37; o NIST SP 800-53; o NIST SP 800-171; o NIST 800-172; and o US SPD-5. Chapter 7: Conclusion 72 By completely or partly adopting these policy recommendations, NATO would strive to fully leverage the potential of its 2019 Space Policy and its Declaration of Space as an Operational Domain. Additionally, this would allow NATO to function as a formal and informal MS consultation forum on SASC cybersecurity. This way, it would make full use of its broad collective MS portfolio, best practices and lessons learned, as suggested by NATO SG Stoltenberg. These findings are in line with the assumptions of neoliberal institutionalist theory. As has been shown, NATO and national actors seek to maximize their gain from space assets to maintain relative power and the ability to deter. This behaviour is enforced by commercial competition and innovation. Throughout this thesis, this was proven by findings which align with neoliberal institutionalist theory, thus highlighting that a) Lacking cooperation between NATO as an international organization and its MS, as well as commercial SC partners, hinders to find problem solutions and create internationally binding regulations; b) Commercial competitiveness spurred by the search for economic efficiency, competitive advantage, and cheaper labour trades off security concerns. Following neoliberal institutionalism, and aligned with above presented policy recommendations, NATO’s role should be to guide and advise MS in resolving global political and economic issues, to reduce individual cost and uncertainty. Therefore, NATO should consider a shift from regarding cyber SASC risk management from being ‘nice-to-have’ to being mandated and critical. Doing so will ease safeguarding of delivery and integrity of NATO mission-critical data, better integrate suppliers and manufacturers along the cyber SASC, and increase transparency, responsibility, and liability. Furthermore, this will ease NATO to stay competitive, deterring and up to date with innovative technology, enhancing outcomes of NATO missions and operations to the best possible extent.

#### NATO’s eager to create a unified allied space network and doctrine---key to norms and deterring hostile Russian and Chinese counterspace

-Allies nervous about Chinese and Russian capabilities

-NATO declared space an operational domain, eager for norm building and monitoring

Aaron Bateman 20, Ph.D. candidate in the history of science and technology at Johns Hopkins University, previously U.S. Air Force intelligence officer, 4/29/20, “AMERICA NEEDS A COALITION TO WIN A SPACE WAR,” https://warontherocks.com/2020/04/america-needs-a-coalition-to-win-a-space-war/

In February, Gen. Jay Raymond, the new chief of space operations and the head of U.S. Space Command, publicly stated that two Russian spacecraft were tailing a U.S. satellite. He said that Russia’s behavior was “highly unusual and disturbing.” On April 15, U.S. Space Command announced that Russia tested an anti-satellite weapon. Russia and China both recognize that American high-precision warfighting is dependent on space systems. According to the U.S. director of national intelligence, both Russia and China are developing capabilities to destroy U.S. satellites in all orbital regimes — at all altitudes. But, unlike in the past, the United States is not on its own. It has allies and partners to turn to.

During the Cold War, the United States and Soviet Union were the two dominant space powers and both worked diligently to develop space weapons. European allies, France in particular, decried efforts to create anti-satellite systems. Since the collapse of the Soviet Union, the number of spacefaring nations has markedly increased. And, as the world has become more dependent on space systems, attitudes about space security have changed. The United States has demonstrated its commitment to space security through the revival of U.S. Space Command and the establishment of the U.S. Space Force. Other countries have, too. France and Japan, for example, have announced the creation of their own military space commands. NATO has declared that space is an operational domain. Now, the United States has allies who are eager to create a more robust network for monitoring adversary activity on orbit and to establish a unified space doctrine to achieve a resilient space security framework. Washington can build a coalition with its spacefaring allies to effectively prepare for and win a war that extends into outer space. Indeed, the United States should leverage its allies to build a more robust network to monitor and track activities in space. While doing so, Washington should lead its allies and the world to develop norms and practices that prevent destabilizing military activities in space.

#### US cooperation with NATO shapes projects towards interoperability in Europe---key to missile warning, navigation, SSA, and space deterrence

Christopher M. Martinez 20, Col., U.S. Army, senior planner for the Army G-2, 8/27/20, “It Is Time to Embrace the European Union’s Strategic Autonomy in Space,” [https://www.960cyber.afrc.af.mil/News/Article-Display/Article/2325432/it-is-time-to-embrace-the-european-unions-strategic-autonomy-in-space/](https://www.960cyber.afrc.af.mil/News/Article-Display/Article/2325432/it-is-time-to-embrace-the-european-unions-strategic-autonomy-in-space/#sdendnote26sym)

This article discusses why and how the United States should pivot from holding a long-standing skeptical view toward the European Union’s (EU) strategic autonomy (SA) initiatives in the space domain to embracing them. The article first highlights how the EU has advanced its research and development in space. It then discusses how the strategic environment has changed, specifically with NATO declaring space an operational domain, the US supporting greater interoperability with European allies and partners within its National Defense Strategy, Russia’s growing threat to the Baltics, and Europe’s increased appetite to leverage space for defense purposes. The article then recommends how the United States could embrace and further the EU’s space initiatives by leveraging Washington’s power within NATO—all while remaining cognizant of Europe’s waning views of the US defense industrial base. Finally, the article demonstrates how the United States, European Union, and NATO could all benefit from America’s pivot in this burgeoning domain.

Introduction and Background

Over the past two decades, the European Union has taken significant steps to assume greater responsibility in strengthening its security and building its defense industrial base. In 2016, the bloc codified this effort in its “Global Strategy.” Within this strategic document, the European Union introduced the concept of strategic autonomy (SA) as it relates to European security and defense. Although the strategy recognized that NATO exists to defend its members—most of which are European—from external attack, it stressed that Europeans must be better equipped, trained, and organized to contribute decisively to such collective efforts, as well as to act autonomously if and when necessary.1 Since the European Union announced its SA plan, its member states have aggressively collaborated on 47 new defense projects within the EU’s Permanent Structured Cooperation (PESCO) framework and process. 2 These projects are largely focused in the areas of space; air; land; maritime; cyber; training; logistics; and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). 3

Specifically within the space domain, the PESCO projects aim to enhance space-based ballistic missile early warning systems, military use of the Galileo Global Navigation Satellite System (GNSS), and space situational awareness (SSA).4 For example, France is leading the Timely Warning and Interception with Space-based Theater Surveillance (TWISTER) project with support from Spain, Finland, Italy, and the Netherlands. This project will enable Europeans to better detect, track, and counter missile threats through a combination of enhanced capabilities for space-based early warning and endoatmospheric interceptors.5 France is also leading the EU Radio Navigation Solution (EURAS) project. Belgium, Germany, Spain, Italy, and Poland have a supporting role in this initiative, which will promote the development of EU military positioning, navigation, and timing capabilities and leverage the GNSS public-regulated service.6 Additionally, Italy and France co-lead the European Military Space Surveillance Awareness Network (EU-SSA-N) project, which calls for developing an autonomous, sovereign EU military SSA capability that is interoperable, integrated, and harmonized with the EU Space Surveillance and Tracking (SST) support framework.7 Together, the EU-SSA-N and SST will detect, catalogue, and predict movements of space objects and debris orbiting earth and alert spacecraft operators in an effort to mitigate the risk of collision.8 In another initiative, Germany is leading Austria, Greece, France, Portugal, and Romania in the Geo-Meteorological and Oceanographic (GEOMETOC) Support Coordination Element (GMSE) project that will leverage data derived from member states’ meteorological, environmental monitoring, and oceanographic satellites to support military operations.9 Finally, Spain is leading Germany, France, Italy, Portugal, and the Netherlands in the Strategic Command and Control (C2) System for Common Security and Defense Policy (CSDP) Missions and Operations project, which will leverage satellite communications and remote sensing to execute missions and operations where the European Union takes a leading role in conflict prevention, peacekeeping operations, and crisis management.10

These initiatives are clearly indicative of the EU’s desire to assume greater responsibility in the collective defense of Europe. One may think the United States would welcome or even encourage EU member state collaboration to enhance the security of Europe; however, for the better part of 20 years, US administrations have largely met such initiatives with reservations and mixed views. Pres. Bill Clinton took a firm stance that EU defense initiatives must not decouple the United States from Europe, duplicate NATO structures and capabilities, nor discriminate against NATO members that do not belong to the EU.11 The George W. Bush administration was also critical of such initiatives, while the Obama administration was somewhat more supportive.12 In recent years, the Trump administration has raised concerns that the initiatives may limit US influence in Europe, harm alliance interoperability, and steal market share from American defense contractors in the European market.13

Why Washington Should Support the EU’s Strategic Autonomy

If the Unites States were to reassess the strategic environment, as it pertains to the transatlantic alliance, the analysis may lead America to reconsider its long-standing unenthusiastic position on the EU’s SA defense initiatives, particularly those in the space domain. Below, are several reasons why it is an opportune time to embrace such initiatives:

NATO’s Newest Operational Domain: Space

In December 2019, 29 heads of state and government from each NATO member state met in London. One of the key deliverables of the meeting was NATO declaring space a new military operational domain—joining air, land, sea, and cyberspace.14 With the declaration, NATO will begin strengthening capabilities in the space domain. According to NATO’s recently published military strategy, NATO has no intention to put weapons in space and does not seek to become an autonomous space actor.15 Instead, NATO will serve as a forum for allies to share relevant information to increase interoperability and to ensure the alliance’s operations receive necessary support from national space capabilities.16

Although some argue NATO is slow to respond to changes in the operational environment, such critics should consider NATO’s aggressive response to the burgeoning cyberspace domain before passing judgment. In 2014, the allies made cyberdefense a core part of collective defense, declaring that a cyberattack could lead to the invocation of the collective defense clause, commonly referred to as Article 5, of NATO’s founding treaty.17 Moreover, in 2016, the allies recognized cyberspace as a new military operational domain and further pledged to enhance the cyber defenses of their national networks and infrastructure as a matter of priority.18 Since then, NATO has created cyber rapid reaction teams to respond to cyberattacks, established a Cyberspace Operations Center to adapt and respond to the evolving threat landscape, and integrated sovereign cyber capabilities into alliance operations and missions.19

NATO, specifically the EU member states within the alliance, both collectively and individually, have unquestionably built capacity in a short period within the cyberspace domain. These efforts have enhanced the collective defense of Europe. Arguably, if NATO were to build capacity and leverage its member states’ capabilities in the space domain as quickly as it did in the cyberspace domain, the United States could indirectly further enhance the collective defense of Europe by welcoming, shaping, and informing such initiatives in a manner that complements NATO’s deterrence efforts.

#### Effective, integrated allied space operations deter attacks on space capabilities that risk nuclear war

Kestutis Paulauskas 20, Senior Strategy Officer at NATO’s Allied Command Transformation in Norfolk, US, 3/13/20, “Space: NATO’s latest frontier,” https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html

A major surprise attack by an adversary on Allied space capabilities could significantly undermine the credibility of nuclear deterrence (for example, by compromising the Alliance’s ability to detect launches of Intercontinental Ballistic Missiles). It could indeed be a precursor to major global conflict.

How to deter such attacks? Deterrence theory stipulates two ways: deterrence by denial (deny adversary the benefits it is seeking) and deterrence by punishment (ensure that the cost for its action will be prohibitive for the adversary).

The credibility of deterrence – in either of its iterations – rests on a combination of 1) political resolve, 2) capability to inflict pain and 3) clear communication of said resolve and capability. It is admittedly difficult to use space capabilities for messaging – unlike aircraft or ships. Showing off a tiny cube sat soundlessly orbiting in empty space is not a very threatening message. It is also extremely difficult to deny an anti-satellite attack. Moreover, some countries like North Korea and Iran do not have similar space capabilities that could be held at risk, so a deterrence through a threat of symmetric and proportionate punishment (“you take down our satellites, we will take down your satellites”) is not a viable option.

In light of this conundrum, the United States has publicly adopted cross-domain deterrence (in its National Security Strategy), which is based on the idea of punishment: “any harmful interference with or an attack on critical components of our space architecture that directly affects this vital US interest will be met with a deliberate response at a time, place, manner, and domain of our choosing.”

Should deterrence fail, the best defence against an anti-satellite weapons threat would be to go after – through cyber or kinetic means – the enemy’s launch capabilities and ground control stations.

Kinetic action produces debris, the ultimate deterrence to actual war in space. Chinese and Russian investment in space capabilities should make them also increasingly dependent on space. Because of space debris, space can be considered a realm of ‘MAD’ – mutually assured destruction. A war in space is effectively unwinnable. Unless an irrational actor with anti-space capabilities would feel very disadvantaged and desperate, and would consider making space inoperable a victory.

In light of the Alliance’s space-related vulnerability, an ever bigger focus needs to be placed on resilience and survivability of space capabilities. This can be achieved by placing more satellites in orbit, developing more multi-purpose satellites, involving more Allies and doing so in cooperation with commercial actors. Maintaining a robust infrastructure to service or quickly replace disabled satellites will be critical. These are all ingredients of an effectively deterrence by denial: no matter how many Allied satellites an adversary would be able to target and take out of action, it would not affect the Alliance’s ability to rely on space support to its operations.

### 2AC – ! Russia/China Alliance

#### Existential war with China or Russia is a real threat – especially if China can conduct cyberattacks on US satellites.

Dean, ’19 (Eric Dean, Future Readiness Officer at the Office of the Chief of Chaplains, US Army. “Can the United States Wage Existential Warfare Without Foundational Principles or Truths?” 03/25/19 https://www.cgscfoundation.org/wp-content/uploads/2022/02/5-Dean-Existential-Warfare.pdf)

For many Americans, the idea of waging existential warfare is the stuff of dystopian films. In the years following the Second World War, the United States emerged as one of two global superpowers whose ability to exercise its influence and will was challenged only by the Soviet Union. Since the fall of the Soviet Union, however, the U.S. has maintained global superiority—or dominance—in every domain of warfare, enjoying a unique status as the world’s only superpower. Over the past three decades, the military prowess of the United States has been largely without peer, thus the notion of existential warfare is inconceivable for many Americans. Further adding to this collective American naiveté is the fact that the last time the United States fought foreign forces on American soil was during the War of 1812, a time so far removed from the American conscience that it is difficult to imagine. Though the United States has suffered isolated attacks since then at Pearl Harbor and again on 9/11, the U.S. always has taken the fight to its enemies in their homelands, sparing our own the destruction and suffering war inevitably brings. Consequently, the possibility of waging a truly existential war is difficult at best for the average American to consider. The reality however is that if war were to break out tonight between the United States and an alliance of SinoRussian forces, the U.S. likely would lose. In simulated wargames conducted by the RAND Corporation, the U.S. continues to lose catastrophically against Russia and China as its bases, warships, and aircraft are decimated.1 RAND analyst, David Ochmanek, confirms that there is no situation under current conditions in which the United States emerges victorious in a war with Russia and China.2 With Russia touting hypersonic, precision-guided intercontinental ballistic missiles, the repercussions of consolidating personnel and equipment under Base Realignment and Closure, as well as staging large numbers of personnel and aircraft on a few large airbases and aircraft carriers translates to catastrophic loss of life and strategic assets within minutes for United States forces.3 China poses an equally devastating threat to communication networks, effectively employing a superior cyber and electronic warfare campaign against U.S. satellites, network, and communication systems.4 According to Robert Work, a former deputy secretary of defense and wargaming expert, the U.S has wargamed cyber and electronic warfare in field exercises, but “the simulated enemy forces tend to shut down United States networks so effectively that nothing works and nobody else gets any training done.”5 Assuming U.S forces somehow were able to organize and wage land warfare after these initial devastating assaults, United States ground forces would not fare much better. According to another recent RAND study, both Russian and Chinese rocket systems match or outrange current U.S. capabilities.6 Similarly, Russian field artillery outranges anything currently within the U.S. arsenal.7 Thus the reality is that should the U.S. to go to war today against a Sino-Russian force, our current forward-deployed and expeditionary-focused military forces would be destroyed or severely damaged, resulting in the Nation suddenly finding itself in it what would be an existential war conducted under large-scale combat operation conditions.8 In addition to the strategic and tactical disadvantages facing the U.S., the very nature of large-scale combat operations in a multi-domain environment where battles will be brutally fought in mega-cities creates a significant moral dilemma for American political and military leaders. The expected catastrophic loss of civilian and military lives undoubtedly will result in enormous public pressure to develop weapons and tactics to quickly end such a conflict, positing that the achieved victory will justify the means.9

# 2AC – CP

## AT: DOS CP

### 2AC – DoD Key

#### Faster communications, info sharing, human capital, knowledge base all make DoD key for alliance cyber cooperation---better relationships helps promotes norms better.

NIST ’11, “DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE”, National Institute of Standards and Technology, [https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf //](https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf%20//) Ali

DoD’s Strengths and Opportunities in Cyberspace

As does the nation as a whole, DoD relies on a secure and reliable cyberspace that protects fundamental freedoms, privacy, and the free flow of information. In support of both U.S. core commitments and national security, DoD has significant strengths and opportunities in cyberspace. The U.S. military’s ability to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler of DoD missions. More broadly, DoD’s depth of knowledge in the global information and communications technology sector, including its cybersecurity expertise, provides the Department with strategic advantages in cyberspace. The quality of the United States’ human capital and knowledge base in both the public and private sectors provides DoD with a strong foundation on which to build current and future cyber capabilities. DoD has played a crucial role in building and leveraging the technological prowess of the U.S. private sector through investments in people, research, and technology. DoD will continue to embrace this spirit of entrepreneurship and work in partnership with these communities and institutions to succeed in its future cyberspace activities. Given the dynamism of cyberspace, nations must work together to defend their common interests and promote security. DoD’s relationship with U.S. allies and international partners provides a strong foundation upon which to further U.S. international cyberspace cooperation. Continued international engagement, collective self-defense, and the establishment of international cyberspace norms will also serve to strengthen cyberspace for the benefit of all.

## AT: OCO CP

### 2AC – No Solvency

#### Shifting NATO’s space strategy from deterrence by punishment to denial is key to space deterrence.

John J. Klein and Nickolas J. Boensch 20, John @ George Washington University’s Space Policy Institute, Nickolas is @ Bryce Space and Technology, October 2020, “Role of Space in Deterrence,” Handbook of Space Security, p. 111-126/BL

Because states derive strategic advantages from satellites and potential rivals may seek to deny a state this advantage, the concept of “space deterrence” is a relevant concept for space powers. Deterrence by punishment, compellence, deterrence by denial, and dissuasion are important ideas in the formulation of a sound space strategy. Taking the commonly accepted definition mentioned previously, space deterrence refers to persuading a potential enemy that it is in its own interests to avoid certain courses of activity in, through, or from space. Regardless of the chosen terminology or definition, what is ultimately important is that there are actions that can be taken relative to space that affect the decision-making of others.

One of the most essential distinctions in deterrence theory is between deterrence by punishment and by denial (Snyder 1961). Deterrence by punishment concerns the threat of credible and potentially overwhelming force or other retaliatory action against any would-be adversary to discourage potential aggressors from conducting hostile actions. Deterrence by denial refers to the capability to deny the other party any gains from the behavior that is to be deterred (Snyder 1961). This concept refers similarly to deterring an adversary by presenting a credible capability to prevent it from achieving the potential gains adequate to motivate the action (Krepinevich and Martinage 2008).

A related but distinct concept is compellence, which involves convincing an adversary to cease some current undesired action. Compellence is often described as a direct action that persuades an opponent to give up something that is desired (Schelling 1966). While deterrence has a negative object – it discourages unwanted actions – the object of compellence is positive. Effort is expended to force or convince an actor to conform to one’s will.

Both military and nonmilitary means are applicable when seeking to affect the thinking of others to enable deterrence by punishment, deterrence by denial, and compellence. Nonmilitary means equate to the soft power, or the diplomatic, informational, and economic instruments of national power (Nye 2005). Nonmilitary means can be used to affect another state leader’s thought processes – whether reinforcing a currently held view that is beneficial to the deterring state or changing the view of another state’s leadership or polities. Consequently, a practical implementation of space deterrence may entail political and diplomatic efforts, such as new international treaties or agreements; multimedia stories presenting news in a favorable perspective; and commerce and trade activities that increase one’s own economic influence or affect negatively a potential adversary or opposing alliance (Klein 2019)

Deterrence by Punishment

A deterrence by punishment approach in space is underpinned in the belief that the threat of credible and potentially overwhelming force or other retaliatory action against any would-be adversary is sufficient to deter most potential aggressors from conducting hostile actions in space. Such a strategy should clearly convey the capability and credibility behind the threat and communicate the specific behavior sought to be discouraged (Morgan 1977). As part of its broader space strategy, the United States seeks to deter attacks against its satellites. The 2017 US National Security Strategy conveys that harmful interference or attacks targeting US satellites will be met with a deliberate response in the “time, place, manner, and domain” of its choosing (The White House 2017). A US joint doctrine describes that, consistent with the right to self-defense, the United States may utilize its space assets to target the space capabilities of an adversary to deter potential threats (Joint Chiefs of Staff 2018). Some security experts view that the punishment portion of the US space deterrence strategy has been pursued and emphasized extensively, perhaps to the detriment of other approaches to secure US interests in space (JohnsonFreese 2017).

Many analysts have identified challenges associated with implementing a deterrence by punishment approach in the space domain. These include establishing appropriate thresholds for retaliation for both non-kinetic and reversible attacks on satellites, differences in severity due to no loss of life when compared to terrestrial action, and having the requisite attribution capabilities and processes. The absence of explicit threshold that a state would retaliate against complicates efforts to deter adversaries. Some policy makers question whether non-kinetic and reversible actions are hostile acts or armed attacks that warrant a military response (Harrison et al. 2017). Reversible and non-kinetic actions on satellites supporting tactical operations may be treated differently from large-scale kinetic attacks on satellites supporting nuclear command or control or early warning missions. However, between these extremes, there is still a highly uncertain boundary that complicates deterrence efforts (MacDonald et al. 2016). Ultimately, what is considered an armed attack or hostile act in space necessitating a retaliatory response will depend on the broader geopolitical context.

Another challenge for a space deterrence strategy is that attacks on satellites typically are unlikely to result in loss of human life. Consequently, hostile actions in space may be considered by some polities to be less escalatory or grave as conflict on Earth. The frequently used adage that captures this thinking is “satellites don’t have mothers.” This view may cause decision-makers to view aggression in space as never rising to levels that would warrant a military response, whether terrestrially or in space. Moreover, because military actions in space are unlikely to produce direct casualties, there may be an appeal to turn to these activities as tensions between competing states escalate (MacDonald et al. 2016). Perceptions that hostilities in space are less severe than terrestrial conflict can be discouraging to those hoping to deter attacks against one’s satellites.

Regardless, the thought that the non-casualty-generating effects of space actions preclude a deterrent threat is unfounded. Article 2(4) of the United Nations Charter describes the need to refrain from the threat or use of force against a state’s territorial integrity – which may be interpreted as a state’s physical property. Self-defense and retaliatory threats to deter a potential armed attack against a state’s satellites are then appropriate and justified. Upon further examination, one may dispel a historical challenge surrounding space deterrence by punishment: a hostile action against a state’s space systems may still be deterred by threat of retaliation, even if there is no loss of life.

Yet another challenge to effective deterrence in space lies in the difficulty of attributing who or what caused a satellite to cease to function normally. Military actions in space can produce various effects, may be non-kinetic and reversible, and in some cases these effects may be difficult to identify and attribute. An effective deterrent requires timely assessment of the event to orient and respond appropriately. Operating at hundreds to more than 30,000 km above the Earth’s surface makes it difficult to physically inspect and track satellites, thereby making determining and assessing damage an onerous endeavor. The hostile space environment – where satellites face solar activity, scorching and frigid temperatures, radiation, electromagnetic activity, and an increasing amount of debris – further complicates efforts (Wright et al. 2005). Operators must distinguish between intentional interference from adversaries and interference arising from normal operation in a hostile environment.

Some authors argue that the difficulties associated with attribution may be less worrisome than originally thought (Harrison et al. 2009). An attack on a state’s satellites unconnected to a terrestrial strategic event is thought to be highly unlikely. Attacks on satellites will occur following the terrestrial breakdown of general deterrence between states. The source of an attack may be less nebulous than space deterrence literature has declared, particularly if the attacking state launches a coordinated attack on many satellites to try to gain command of space early in the conflict. Drawing from this example, intelligence gleaned prior to the attack may be a more meaningful method of attribution than enabled by postattack space situational awareness (SSA) assessment.

Regardless of this assessment, in the current context of the global proliferation of counterspace capabilities, there will likely be ample room for misperception and miscalculation in a state’s leadership. This necessitates robust SSA capability to address issues of identifying, assessing, and attributing activities that occur in orbit. Greater SSA capabilities allow a state to differentiate between intentional attacks and malfunctions due to the satellite itself or the hostile environment it inhabits, thereby reducing the potential for misinterpretations and miscalculations (Sheldon 2008). Effective SSA capabilities will necessitate knowing what on-orbit systems are present, along with their location, capabilities, historical anomalies, operating patterns, and intended use. Such information will facilitate those preparatory measures needed to pit one’s strengths against a potential adversary’s weakness. Because SSA is a global endeavor, information sharing architectures must be designed to include ethe international community and commercial industry. This means that much of the data and resulting information provided through SSA systems should be releasable and disseminated to many of those participating in the global effort.

Today’s security challenges can complicate the implementation of a deterrence by punishment strategy. While some security analysts assess that thresholds for retaliation, differences in severity for space actions, and ensuring a sufficient attribution capability may be less problematic than many think, it remains to be seen whether this is confirmed in practice.

Deterrence by Denial

Among many security professionals, deterrence by denial is often associated with the concept of dissuasion – activities that seek to influence the decision calculus of potential adversaries to discourage the initiation of military competition. A strategy incorporating dissuasion seeks to convey the futility of conducting a hostile act, affecting the confidence of a potential adversary’s leadership and causing decisionmakers to not pursue a military confrontation in the first place. To be most effective, dissuasion activities occur before a threat manifests itself. Some national security professionals note that dissuasion works outside the potential threat of military action as a kind of “pre-deterrence,” because those states dissuaded will not require to be deterred by punishment (Krepinevich and Martinage 2008). While a deterrent that seeks to punish an adversary is tailored to distinct actions by specific actors at definite times, deterrence by denial commonly lacks this specificity and exists as a general deterrent, one that shapes the security environment through a broad, latent deterrent effect originating from one’s reputation and capabilities (Morgan 1977).

A deterrence by denial strategy for space seeks to frustrate or complicate the adversary’s plans by introducing greater costs and reducing associated benefit. Over the past several years, there has been a greater emphasis on the role of deterrence by denial in the broader US space deterrence strategy. Rather than threatening retaliation against the aggressor’s satellites or terrestrial targets of value, a US space deterrence by denial strategy emphasizes reducing an adversary’s incentive to attack US satellites (Vedda and Hays 2018). A potential adversary may be deterred if it concludes that an attack in space will be ineffectual in achieving the desired effect. Much of deterrence by denial and dissuasion necessitates preparing for potential conflict during peacetime. Because dissuasion involves discouraging the initiation of military competition, for the space domain the requisite peacetime preparedness is included within the contexts of space mission assurance and resilience.

According the US joint literature, mission assurance entails a process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of the Department of Defense mission essential functions in any operating environment or condition (Office of the Assistant Secretary of Defense for Homeland Defense 2015). Similar to mission assurance but with a different focus, resilience is an architecture’s ability 116 J. J. Klein and N. J. Boensch to support mission success with higher probability; shorter periods of reduced capability; and across a wider range of scenarios, conditions, and threats, despite hostile action or adverse conditions (Joint Chiefs of Staff 2018). Resilience may leverage cross domain solutions, along with commercial and international capabilities. By definition, space mission assurance and resilience efforts can prevent a potential adversary from achieving its objectives or realizing any benefit from aggressive action. Space mission assurance and resiliency help convey the futility of conducting a hostile act and, consequently, enhance deterrence by denial and dissuasion efforts.

Space mission assurance efforts consist of defensive operations, which include off-board protection elements; reconstitution, which includes launching replacement satellites or activating new ground stations; and resilience, which includes on-board protection elements (Joint Chiefs of Staff 2018). Resilience in capabilities includes disaggregation, distribution, diversification, deception, protection, and proliferation. Disaggregation is the separation of dissimilar capabilities into separate platforms or payloads. Distribution utilizes a number of nodes, working together, to perform the same mission or functions as a single node. Diversification is contributing to the same mission in multiple ways, using different platforms, different orbits, or systems and capabilities of commercial, civil, or international partners. Deception is hiding one’s strengths and weaknesses from one’s adversaries. Protection is utilizing active and passive measures to ensure space systems provide mission support in any operating environment or condition. Proliferation is deploying larger numbers of the same platform, payloads, or systems of the same type to perform the same mission.

Space mission assurance may be supported by a number of preparations preceding a potential conflict. These preparations may include hardening against cyber threats and signal jamming, incorporating shutters for remote sensing satellites to minimize the effects of dazzling by lasers, or increasing the mobility of satellites through novel propulsion technologies (Kueter and Sheldon 2013). Preparations taken in peacetime may include employment of proliferated constellations of small satellites to complicate an adversary’s space ambitions. Furthermore, the conduct and training of one’s space and terrestrial forces may grant an ample deterrent effect, even if no ancillary preparations have been made. One method of frustrating an adversary’s plans may be to train forces to fight under degraded conditions where military forces lose access to space-enabled capabilities, thereby depriving potential aggressors some of the appeal of attacking satellites (Harrison et al. 2009). Consequently, a potential aggressor may be convinced that the prospects for success are too costly, with little benefit.

Another method of frustrating an adversary’s space control plans is to reduce one’s vulnerability by transitioning traditional space-derived services to terrestrial alternatives, a concept termed space avoidance. Its advocates seek to increase space deterrence by minimizing one’s presence in space, thereby diminishing an adversary’s perceived benefits of attacking one’s satellites (Coletta 2009). For example, some space avoidance advocates suggest this may be achieved by using unmanned aerial systems (UAS) for tactical reconnaissance systems instead of remote sensing satellites. Creating redundancy through terrestrial alternatives is prudent, but one should not be misled when judging whether reliance on space can be abated entirely. UAS are a valuable supplementary resource to space-derived intelligence, surveillance, and reconnaissance (ISR); however, most UAS still require space-derived positioning information and communications to operate. Many forms of military power – sea power and airpower, for example – cannot easily reduce reliance on space-derived services. While states should seek to increase terrestrial redundancy to complicate an adversary’s plans, a strategy of space avoidance intending to greatly reduce reliance on space is not feasible in modern warfare.

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

Some security experts consider the North Atlantic Treaty Organization (NATO) as being uniquely positioned to bolster deterrence in space through its cooperative alliance. The alliance is increasingly reliant on space for its collective defense and economic prosperity, and an attack on the space assets of any one ally impacts the security of all allies (Schulte 2012). Security experts assert that while NATO is dependent on space-enabled capabilities, its space doctrine and planning have not kept up. Presently, NATO officials are considering how the alliance should address the growing military capabilities of Russia and China, to include issuing NATO’s first strategy for space. The strategy is expected to make space an official domain of operation, giving structure to discourse on military developments in space and NATO’s response. The alliance may also decide that attacks in space would trigger the organization’s Article 5 provisions on collective defense, although internal differences on the subject remain. Analysts have long held that NATO should continue to build the expertise and capacity to conduct operations enabled by space; ensure that doctrine, requirements, and planning account for the operational advantages provided by space; and adapt exercises and training to ensure forces can effectively exploit space-based capabilities (Schulte 2012). It is still uncertain whether NATO’s space strategy will implement these recommendations. A deterrence by denial strategy presents its own challenges. The cost of fielding and launching the most robust, defendable space systems can become a financial burden (Coletta 2009). Hardened, dispersed, disaggregated, or diversified capabilities may cost more to develop, launch, integrate, and operate. Also, resilient architectures may not be able to match the performance of those exquisite space systems. In most cases, smaller, proliferated constellations of satellites will augment, rather than replace these exquisite systems. The space strategist then must consider the benefits of defensive approaches, along with associated time and fiscal procurement costs, when finally deciding upon the best approach. Another challenge of deterrence by denial is that one’s space mission assurance and resilience efforts must be widely publicized to be effective in dissuading others.

## AT: Process CP

### 2AC – Certainty Deficit

#### Clear cooperation is key to space deterrence.

John J. Klein and Nickolas J. Boensch 20, John @ George Washington University’s Space Policy Institute, Nickolas is @ Bryce Space and Technology, October 2020, “Role of Space in Deterrence,” Handbook of Space Security, p. 111-126/BL

Effective Communication Is Required

Any effort to affect an adversary’s decision-making is best served by clearly communicating one’s desire, intent, capability, credibility, and rationale for military response. This requisite communication may be achieved through official statements or policy documents or more importantly through a demonstrated history of consistent actions (Klein 2019). If the deterring state is not clear in identifying the specific behaviors that it is trying to deter and conveying the threat of what will transpire if an aggressor chooses not to be deterred – along with the defensive capabilities mobilized to discourage them – then the prospects for successful deterrence are diminished. If one’s deterrent message is not received or comprehended, then it will be difficult for deterrence to succeed (Schelling 1966).

In addition to the impediments in communicating deterrence in general, deterrence in space presents its own unique challenges that further complicate it potential success. The remoteness of space, highly classified nature of many of these systems, and perpetual concerns regarding dual-use technology all contribute to an environment where both sides of the deterrence relationship have limited awareness of or insight on the others behavior and conduct (Todd Harrison et al. 2017). Indeed, the dual-use nature of space systems can be particularly troublesome when attempting to clearly comprehend or communicate intent, because motive and intent are made more ambiguous when a state fields dual-use capabilities that can be used for civil, commercial, or military purposes.

Often in analysis of high-technology systems, capability is considered equal to intent (Gray 1993). While China is often at the center of debates over capability and intent, some security experts note the United States fields many of the same dual-use systems that elicit concern among its rivals (Johnson-Freese 2017). Intent is a frequently subjective matter and dependent upon one’s worldview. For example, the Soviet Union viewed the US Space Shuttle program as a potential ASAT weapon because Soviet military leadership thought the Shuttle was capable of retrieving satellites and de-orbiting them (Wright et al. 2005). Assuming a worst case of intent based solely on an enemy’s capabilities can raise the possibility of miscalculation and increase tensions among states when potentially none may be warranted.

### 2AC – Delay Deficit

#### Delay emboldens adversarial hacking that jeopardizes NATO capability.

Beyza Unal 19, Former Deputy Director of International Security Programme at the Chatham House, 7/1/2019, " Cybersecurity of NATO’s Space-based Strategic Assets,” https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf, sg

Timing is a crucial element of PNT capability. Most of the electronics used in military, civilian and commercial spheres depend on timing signals. By intercepting securely transmitted data through cyber means, an adversary may jeopardize the alliance’s missions and services. A compromised system would also diminish reliance on data received, as data confidentiality would be brought into question through possible acts of spoofing and deception.

The involvement of Russia and the US in the Syrian conflict, and the use of electronic techniques, such as signal jamming,57 and cyber means, such as hacking and spoofing, demonstrates the potential operational uses of cyberattacks. Russia’s electronic warfare capability involves not only an air defence capability but also integrates cyber operations.58

## AT: Turkey PIC

### 2AC – No Solvency

#### Full NATO participation is key – solves two front conflict in the Pacific and with Russia.

Stickings, ’20 (Alexandra Stickings, Associate Fellow at the Royal United Services Institute with a focus in military space, space warfare, counterspace capabilities and international space programmes, holds an MSc in International Security and Global Governance from Birkbeck College, University of London, a BA(Hons) in International Studies from the Open University, and a BSc(Hons) in Physics with Astronomy from the University of Nottingham. “Space as an Operational Domain: What Next for NATO?” https://rusi.org/explore-our-research/publications/rusi-newsbrief/space-operational-domain-what-next-nato)

This is not to say that all NATO members will, or should, develop extensive military space programmes. Not only is this not practical or financially feasible for many but it also does not take into account the other ways that states can contribute to a secure and resilient collective space architecture. Space situational awareness (SSA), also often referred to as space domain awareness (SDA), [involves](https://spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/) monitoring the orbital environment, tracking satellites and pieces of debris, assessing the threat of space weather and the actions and intent of space actors – in short, acquiring as full a picture as possible about what is happening in orbit. It is an essential activity for protecting space assets, but is still an activity carried out by relatively few NATO members. States without space capabilities can be involved in this through developing their own SSA programmes or hosting ground stations as part of existing programmes, as well as participating in intelligence activities. These options would be particularly important should there be a future requirement for all member states to contribute to the NATO space enterprise.

The Alliance must also take into account potential future conflicting priorities. One such possible scenario relates to the increased attention of the US on its interests in the Pacific, while significant NATO focus remains on the threat posed by Russia, particularly in Northern and Eastern Europe. Ensuring that assets are available to monitor Russian activity in the High North or on its borders is essential. Reliance on one or a few states for these assets may not be sustainable, particularly if there is a hesitation to make them available, and it may be the case that NATO will need to acquire dedicated capabilities to carry out priority operations, either through a national programme that is managed by NATO, or one similar to that of NATO communications satellites.

It is clear that more work is required to ensure NATO space policy is effective, both now and as new developments in space emerge. This is an activity not just for NATO as a whole but for each member state individually. For those with larger sovereign programmes, they must assess the balance between their own and NATO’s future priorities and what effect this may have on their space assets, as well as their willingness to allow others access to what may be sensitive programmes. For smaller states, including those without any space programme, thought must be given to how comfortable they are with reliance on others as well as the ways in which they can contribute to the Alliance’s space policy, whether through deploying space assets or involvement in space surveillance and intelligence. Simply being a user of space, rather than an actor, does not negate the need for participation in space defence and resilience. Every member state has a role to play. Both NATO and space security are collective activities, and neither can work without the participation of all concerned. The next step for NATO is to develop a space strategy that does just this.

## AT: Unilat CP

### 2AC – NATO Key

#### NATO led cooperation is key for deescalating space conflicts AND successful incorporation of the private sector.

Nicholas Nelson 22, Senior Fellow for Emerging Tech and Policy at the Center for European Policy Analysis, 1/27/2022, "Space — NATO’s Fuddled Frontier," https://cepa.org/space-natos-fuddled-frontier/, sg

First and foremost, whether or not NATO should pursue its own indigenous capabilities within the space domain is an ongoing dialogue. This is not without precedent, as NATO still operates its own airborne early warning (AWACS) and RQ-4D Global Hawk drones. That said, it seems those arguing for a minimalist approach are winning the strategy discussions. This is unfortunate for an alliance that continues to evolve: without its own space capabilities, NATO could be relegated to observer status in a future conflict.

This leads to the critical issue of Article 5. The policy statement says: “A decision as to when such attacks would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.” This leaves much to the imagination.

Before the abortive “red lines” in Syria, such guardrails were key in preventing the Cold War from turning hot. NATO would do well to define these for space sooner rather than later. Would an attack on a national technical means verification (NTM) satellite trigger Article 5? What about on a dual-use (those with both a defense and commercial use) communications satellite, or even a purely commercial satellite internet asset? The alliance needs to clearly outline these to prevent miscalculations by potential adversaries.

Thirdly and finally, is industry engagement. Within the space sector, the majority of new capabilities and significant innovation over the last decade have been driven by venture-backed space startups, across the entire value chain including launch services, satellite manufacturing, and satellite imagery. Despite this, the policy only highlights the NATO Industrial Advisory Group and the NATO-Industry Forum, which have seen only limited engagement with the leading venture-backed companies in the space sector and defense more generally These groups still disproportionately rely on legacy aerospace and defense companies. If NATO is not proactive in soliciting and providing incentivization to venture-backed companies, it will be left even further behind technologically.

#### NATO is uniquely key in an era of evolving cyber threats---major gaps in cyber security require a comprehensive policy solution but US opposition to standards means NATO coordination is necessary.

Gil Baram & Omree Weschler 20, head of research at the Yuval Ne’eman workshop for science, technology and security, and a research fellow at the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University; senior researcher for cybersecurity policies and strategy at the Yuval Ne’eman Workshop for Science, Technology and Security in Tel Aviv University, June 2020, “Cyber Threats to Space Systems: Current Risks and the Role of NATO”, https://www.japcc.org/essays/cyber-threats-to-space-systems/ \\SYang

The Weaponization of Space: a Worrisome Trend

Recent years have seen a growing arms-race in space, with nations striving to develop and test offensive space capabilities, and space force-building processes taking place within their militaries:1 In December 2018, the US Air Force’s National Air and Space Intelligence Center published a report, arguing that both China and Russia are developing space weapons.2 During 2019 the US and France have established dedicated space commands.3 In March 2019, India conducted its first test of an anti-satellite weapon. The case of India, a country without a history of offensive space activities, illustrates the magnitude of the space arms-race. With space becoming increasingly weaponized, the vulnerabilities of space systems, initially built without basic or sufficient security mechanisms, are becoming both apparent and dangerous, rendering them exposed to cyber threats.

In December 2019, NATO foreign ministers formally declared space as an ‘operational domain,’ extending the alliance’s range from land, sea, air and cyberspace to operations in space. Cyber threats to space systems run the wide range from vulnerabilities in the physical ground and space segments to the satellites’ data links and supply chains. As cyber warfare and hybrid threats become the ‘weapon of choice’ for state and non-state actors, and global economy and daily life grow increasingly dependent on space, space systems may well become the next front in cyber conflict.

This paper suggests a comprehensive approach to this threat landscape, and offers integrated strategic solutions for the cyber defence of space systems.

Existing Cyber Threats to Space Assets

Space systems are usually divided into three technological and operational segments, which are responsible for different functions and are therefore exposed to different cyber threats: the ground segment, the space segment, and the link segment.

The ground segment consists of all the ground elements of space systems and allows command, control and management of the satellite itself and the data arriving from the payload and delivered to the users.4

Due to their role in collecting data, the ground stations and terminals are exposed to the threat of cyber espionage from states and non-state actors. Moreover, the military aspect of satellites and their importance to national security render them prime targets for hostile takeover, disruption and shutdown. Most cyberattacks on the ground segment exploit web vulnerabilities and allow the attacker to lure ground station personnel to download malwares and Trojans to ground stations’ computers.5

Infiltrating the ground station’s network can allow the attackers to access the satellite itself. Hostile access could enable the attacker to execute a Denial of Service (DoS) attack6 and may involve taking over Industrial Control Systems (ICS) in order to control the satellite and damage it.7

The space segment consists of the satellites themselves. Major security gaps within satellites’ architecture exist in both old and new satellites. Old satellites with life spans of decades were built with no awareness for cyber security; today, small satellites manufacturers tend to prioritize fast and cheap production, in which the investment in cyber security is perceived as a hurdle.

Cyber threats to space segments usually derive from vulnerabilities in ground stations, in network components, and in the receivers which receive the data from the satellite, thus allowing the attacker to infiltrate to the network and remain undetected. Another threat may involve the introduction of a malware into the satellite’s hardware in the supply chain, in order to compromise ground units at a later stage.8

Consequences of cyberattacks on satellites could also be aggravated due to the rising connection and use of Internet of Things (IoT) devices. An attack on a communication satellite could cause wide disruptions to communication channels across countries, cause panic, and endanger national security.9

The link segment consists of the signal transmission between the satellite and the ground station, as well as between satellites.

The most common threat is GPS jamming. As GPS systems rely on radio signals sent from the satellite in order to determine the location of the users, GPS jammers send signals over the same frequency as the GPS device, in order to override or distort the GPS satellite signals. GPS jammers are widely accessible and cheap to purchase, rendering them available also to poorer state-actors. In November 2018, Russia was suspected of disrupting GPS signals in northern Norway and Finland as the two nations participated in NATO’s Trident Juncture exercise.10 Another type of attack is ‘spoofing’ – faking signals by broadcasting incorrect GPS signals, structured to resemble genuine ones. Spoofing is harder to carry out than jamming, but if executed effectively, can be much more dangerous, mainly because the victims do not necessarily know that they are being spoofed. According to a 2017 US Maritime Administration report, the GPS systems of at least 20 ships were spoofed, leading the ships 32 kilometres inland to the Gelendzhik Airport in the Black Sea, away from the original destination. The incident raised assumptions among experts that Russia had been experimenting new GPS spoofing techniques as part of its electronic warfare capabilities.11

While some experts define jamming and spoofing as physical threats as they involve disrupting or tampering with frequency signalling, an attacker could also intercept unencrypted satellite traffic.

As cyber threats are becoming more substantial, the lack of procedures and policies is hampering efforts to mitigate the threats. However, several solutions have been suggested in recent years.

Threat Response and Mitigation

Mitigating cyber threats to space systems can be divided into technological solutions, which consist of introducing new technologies as well as upgrading existing ones, and policy solutions, which consist of actions and protocols of conduct.

Technological Solutions

In response to the rising cyber threats to space systems, many state agencies, contractors and commercial companies have started developing new technologies, or upgrading existing ones which were not secured by design. In December 2018, Lockheed Martin was awarded a US Air Force contract to modernize GPS ground control systems to support an anti-jamming GPS signal named M-Code, which will allow the Air Force to continue operating the GPS3 constellation with existing ground systems until 2025.12 In January 2019, NASA announced that it would start testing an open-source Blockchain platform in order to address potential issues of privacy and to prevent spoofing, DoS and other attacks.13

In March 2019, Lockheed Martin announced it had developed a new software-defined satellite architecture called SmartSat as a space segment solution, which will enable more capabilities and greater control of in-orbit satellites for ground operators. This architecture is expected to gain operators greater precision in diagnosing problems such as cyber incidents, as well as to allow satellites to back each other up. Operators will also be able to update on-board cyber defences to address new threats.14

While the technological solutions being developed will mitigate cyber threats, these tend to address very particular threats. In addition, being provided by a host of different entities, these are difficult to bring together within a unified, coordinated framework. A comprehensive problem requires a comprehensive, unified and systematic policy solution to guide the efforts to protect space assets and services.

Policy Solutions

As the military space sector increasingly relies on commercial technologies, a comprehensive policy solution should focus on commercial space companies and government acquisition contracts. A possible solution which could include both civilian and military space assets and activities would be introducing strict cybersecurity requirements for all components of space systems and their supply chains. A recent example of such requirements is the Cybersecurity Maturity Model Certification (CMMC) which was introduced by the US Department of Defense for all defence contractors, including small vendors.15 A smart model system which defines different levels of requirements for different products and technologies would demand a high-security level for inherently vulnerable products, without imposing a disproportionate burden on smaller companies. Such a model of cybersecurity standards should be a threshold condition for bidding for government contracts. Additionally, employing strict standards in government contracts is likely to usher in changes across the whole industry, and will therefore help promote the security of commercial and off-the-shelf technologies.

The Role of NATO

NATO as an Alliance was founded for providing a collective defence and cooperative security for its member states. So far, research has suggested that the EU may prove a more suitable entity for promoting new industrial approaches, due to its economic and regulatory authorities.16 However, NATO has an important role to play in any inclusive comprehensive solution due to the importance of the US. Any industry standards mechanism should include the US space industry, as Europe’s production relies heavily on US-produced components and technologies which should endeavour to design for trans-Atlantic interoperability17. NATO’s leading role as a coordinator and mediator is crucial, as the US is likely to resist any standards mechanism that would push American vendors out of the European space market. NATO’s role would therefore derive from its position as a transatlantic alliance with connections to both Europe and the US, and its ability to require common standards and compliance across the alliance. As a unified standards mechanism should be agreed by all member states, NATO could act as a forum for negotiations between its member states and the industry, as well as between Europe and the US. Discussions and consultations as well as further research can take place in conjunction with NATO’s Industry Advisory Group (NIAG) and NATO’s Industry Cyber Partnership (NCIP), as final results would be incorporated into the NATO Defence Planning Process (NDPP).

#### NATO is uniquely susceptible to and unprepared for space-based cyberattacks because it relies on individual member states---urgent action is key.

Liina Lumiste 19, Legal researcher on international law and advisor on domestic public law, xx/xx/2019, “Space – NATO cyber security’s weak spot”, https://ccdcoe.org/library/publications/chatham-house-report-space-nato-cyber-securitys-weak-spot/ \\SYang

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

#### Cyberthreats can decimate NATO’s functioning in all areas of operation---overreliance and lack of protection.

Dr. Beyza Unal 19, Former Deputy Director of the International Security Program, July 1 2019, “Cybersecurity of NATO’s Space-based Strategic Assets”, https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets-0/2-cyber-risks-space-based-strategic \\SYang

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

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

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

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

This dependency on space-based technology has major implications for the way NATO conducts warfare today, and how it will do so in the future. For instance, in order to conduct precision strikes or earth observation through the use of unmanned aerial vehicles (UAVs – such as military drones), systems rely on so-called ‘beyond-line-of-sight’ (BLOS) communication via satellites – especially in times of crisis and conflict, since ground-based line-of-sight communications are vulnerable to physical attacks. Yet, cyberattacks on space technology or on the UAVs may lead them to misinterpret commands, or to lose contact with the command centre and fail in operation.

NATO currently uses six space-dependent capabilities for its alliance operations and missions:

* Position, navigation and timing (PNT)
* Intelligence, surveillance and reconnaissance (ISR)
* Missile defence
* Communications
* Space situational awareness (SSA)
* Environmental monitoring (weather forecasting)

The core functioning of these six capabilities for NATO operations includes:

* Providing communication in military operations and missions, for instance between a commander and their troops;
* Providing early warning, through detecting the hot plumes of a ballistic missile launch – thus, increasing the time available to respond to an upcoming threat;
* Providing a precise location for targeted strikes;34
* Providing imagery of targets, in order to observe, detect and analyse their status (situational awareness);
* Providing GPS for weapon guidance;
* Providing timing for secure communications; and
* Providing space surveillance and tracking.

The table below outlines the key roles for each capability:

**<<<TABLE 1 OMITTED>>>**

Identification is another important capability that is used in the NATO maritime domain for coastal tracking, and for identifying and locating ships and vessels. Using automatic identification systems (AIS), data is electronically transmitted between ships and the coastal stations. By providing similar functions, AIS supplements and provides resilience to maritime radar and is fundamental for avoiding collisions.36

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

#### Allied governance is uniquely effective in space---the counterplan forces a purely national model that forfeits integration, cost-sharing, and legitimacy

-National action can’t solve questions of international legitimacy, protecting the environment, and joint operations. CP key to beat out Russia and China

James Clay Moltz 11, professor in the National Security Affairs Department at the Naval Postgraduate School, October 2011, “Coalition Building in Space: Where Networks are Power,” <https://apps.dtic.mil/dtic/tr/fulltext/u2/a555238.pdf>

The issue of spacecraft vulnerability relates to certain basic facts of orbital physics combined with the relative transparency of space to radar, optical, and infrared observation. 6 These conditions make spacecraft liable to tracking by even amateur astronomers with only moderately sophisticated equipment, which is easily obtainable by any entry-level space power. While more complex guidance technology is required for actual attacks on space assets and a global network of radars is needed for conducting post-attack assessments of damage done, the ability of even moderately advanced space powers to conduct significant counterspace activities is not in question. Thus far, only Russia, the United States, and China have tested kinetic capabilities, but a number of other countries (including Iran) have carried out lesser forms of electronic interference. As a major space assessment conducted by NATO's Joint Air Power Competence Centre in 2009 reported on some of the current vulnerabilities faced by the alliance in space:

There are real and credible threats to Space systems. The ground systems are vulnerable to attack. There has been demonstrated use of GPS and SATCOM jammers. Anti-satellite (ASAT) weapons have been demonstrated by the Soviet Union ... and in January of 2007, China demonstrated its capability [ ... ]. The potential exists for ground-based laser weapons, electro-magnetic pulse, and co-orbital ASAT weapons. Additionally, there are risks of collision from Space debris and impacts from solar events. There have been many instances of satellite telecommunications interference and piracy.7

Space assets are also threatened by a field of orbital space debris that is steadily growing due to the increase in human space activity and the inability of space to "clean" itself quickly. Depending on the altitude of the orbit, it can take years, decades, or centuries for pieces of space debris to deorbit. In the meantime, these particles (even as small as 1 centimeter) represent 18,000 miles-per-hour speeding bullets, which can destroy solar cells and cause often fatal damage to any spacecraft that are unfortunate enough to cross their paths.8 Today's space environment is also characterized by an expansion in the number of civil, commercial, and military space actors, making international agreements more difficult than in the past.

In the face of these risks and evidence of both expanding military space programs and weapons test programs in several countries, the response by many U.S. military leaders, elected officials, and even experts is still a traditional call for exclusively national action to "defend" U.S. assets in space. To take just one U.S. example, Senator Jon Kyl (Rep., Arizona) stated after the 2007 Chinese ASAT test that the United States must deploy a fleet of space-based weapons to defend itself in space.9 He made no mention of the threat China posed to other allied nations or their possible contributions to the U.S. response.

Historical conditions of anarchy in the international system have contributed to a tendency among leaders to conceive mainly of national responses to international threats. States are already organized for national defense, countries are jealous of spending scarce resources in potentially risky ventures with foreigners (even allies), and there are relatively low levels of trust regarding the reliability of international organizations. But three factors have altered global dynamics in the last few decades, each of which has an important space component that supports the creation of an allied approach to space.

First, the scale of multinational interactions to deal with shared problems is increasing due to the growing "finiteness" of the globe, as the world's population continues to expand and as communications technologies become more intrusive and more widespread. Indeed, the very nature of the problems countries are facing is changing as the Earth becomes "smaller": almost all free land and airspace (up to 100 kilometers) have been claimed by nations (or otherwise allotted by international law), the sheer scale of industrial pollutants is beginning to have global effects, and such resources as clean air and water are becoming increasingly scarce. Other problems, such as climate change, are becoming recognized as requiring an international response. Despite its comparative vastness, near-Earth space faces some of the same risks of growing human activity, particularly due to the finiteness of its main, usable resources (geo-stationary orbital slots, radio frequencies available for broadcasting, and safe access to low-Earth orbit). All of these resources are becoming stressed by increasing human space activity.

Second, and related, economic globalization is an increasing fact of life. Unlike during the Cold War, when the world was dominated by two, nearly self-sufficient blocs, changes in the international economic system (due to both political and technological factors) has made commercial exchange possible across almost all political boundaries, vastly increasing global trade. Interdependent economic relationships are the rule in U.S. ties with our NATO and Asian allies and even, in some areas, with commercial partners like Russia and China. Similar to many industries, the commercial space industry has become truly international and now generates $161-billion in sales, 10 making it a valuable resource for both national governments and the global economy more generally. Technologies built in one country are frequently owned and marketed by another and are sold to clients in yet another. Strong corporate alliances have already been formed in the space industry, for example, linking Russian rocket motors with U.S. launch vehicles (International Launch Services) and U.S. sub-orbital flight technology with British funding and marketing (Virgin Galactic). With some offshore corporations like Intelsat, it is often diflicult to tell which individual country a space enterprise actually "belongs" to. National militaries are also purchasing bandwidth on a large number of commercial satellites, causing the breadth of a country's "critical assets" to expand. Some of these assets are already shared with other nations, although not in a joint operational sense. Yet devoted military space cooperation between countries remains highly restricted and out of step with these integrationist tends.

Third, in military affairs, questions of international legitimacy are placing a growing emphasis on the need to conduct operations via coalitions. Put simply, the unilateral use of force is seen as increasingly unacceptable within the international community. Largely for this reason, the United States fought under a U.N. mandate in 1991 in the Gulf War against Iraq's intervention into Kuwait and in Libya in 2011; it fought under a NATO mandate in the Balkans and now in Afghanistan; and it fought (less "legitimately" from the perspective of the rest of the world) with an ad hoc coalition of friends and allies in 2003 in Iraq. Indeed, there is a growing literature on the need for some international approval even for humanitarian interventions by military forces in the modern era.11 Ironically, given these pressures to cooperate in military activity, space remains an outlier. Unfortunately, the U.S. military has found by experience in Afghanistan that national barriers have impeded its effective use of space-derived data. As a one recent analysis of the problem of information-sharing in Afghanistan observes: "secrecy often keeps coalition team members from speaking about space-related topics with each other."12

But these points raise a critical "process" question: How do countries come to realize that their security needs in an area of activity have crossed the line from national to international? Realist political theory argues that security, by its very nature, is something that falls to states, as the essential building blocks of the international system and the repositories of sovereignty within it. Yet space is an area specifically delineated as beyond national sovereignty by international law in the 1967 Outer Space Treaty. The failure of states to expand collective governance mechanisms more in regard to space may be a factor of habit, perspective, and inertia, plus normal bureaucratic opposition to negotiations aimed at creating new, specialized institutions beyond national control.

Recent threats to U.S. space assets have been viewed as national security threats because there is a long U.S. tradition of self-reliance in international relations and a perspective that successful collective action is rarely achieved. But, in space, all countries have an interest in protecting the environment from military threats and, in fact, from any obstacles to either free access or free passage. These conditions create fundamental incentives for collective action that do not exist in other areas of international relations. Ironically, one of the primary obstacles to enhanced collective action to protect space security may be the thinking of the actors themselves, which still remains largely rooted in the unilateral traditions of security provision from past security frameworks. But, as Robert Keohane argues, "To pursue self-interest does not require maximizing freedom of action. On the contrary, intelligent and farsighted leaders understand that attainment of their objectives may depend on their commitment to institutions that make cooperation possible."13 Working with allies, therefore, may represent the best security solution available at this point in space history, and perhaps may serve as a bridge to broader forms of international cooperation in the future. Alliance-based efforts could mitigate a variety of emerging space-related security concerns. The prior existence of allied military institutions- particularly established patterns of cost-sharing, integration, joint operations, and joint training- both in the case of NATO and in various bilateral arrangements with Asian countries (such as Australia, Japan, and South Korea) should reduce typical collective action problems in forming such new mechanisms for space.

# 2AC – DA

## AT: Ambiguity DA

### 2AC – Ambiguity Bad

#### Ambiguity fails – escalates probing to find red lines and undermines NATO deterrence

Whitney L. Cissell 20; MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

The stability–instability paradox applies to the nuclear and conventional level, and indeed, Russia’s effort to avoid conventional-level warfare with the United States strengthens stability between the states at the conventional level similar to the strategic nuclear level. While U.S.–Russian nuclear stability is based on parity, conventional stability in this relationship is more complex. As shown in Chapter II, Russia has a strong aversion to conflict with the United States and NATO at the conventional level. Russia would be outmatched in military superiority after two to three weeks of conflict and beyond its near abroad and, thus, prefers to operate at the sub-conventional level below the threshold of armed conflict.227 In effect, Russia’s strategy of avoiding any actions that might trigger conventional conflict aims to bolster a sort of “firewall” between conventional warfare and gray zone conflict. NATO, up to now, has effectively obliged this Russian strategy by not brandishing threats of conventional escalation in response to Russian gray zone aggression, let alone undertaking conventional responses. As much as Russia seeks to avoid escalation to conventional warfare it could not win, it is also learning how averse NATO is to threaten such escalation. This aversion is ironic insofar as Cold War–era extended deterrence relied on NATO’s threat of escalatory nuclear responses to conventional attacks.

These respective Russian and NATO postures enhance conventional stability, but at the cost of fueling instability at the gray zone level, reflecting a form of the stability– instability paradox familiar in nuclear strategies. This tailored application of the stability– instability paradox to the specific Russian context yields a tiered relationship of stability between the United States and Russia at each level of warfare, as depicted in Figure 1, and helps explain why the United States and Russia are the most unstable at the subconventional level, on which this research focuses.

Cumulative deterrence may be an option to address the issues created when adapting conventional deterrence to the sub-conventional level including the credibility and communication of the threat. Cumulative deterrence has not been a standard element of U.S. deterrence strategy in the past, and there is limited academic literature and strategic thought about its use in areas outside of cyber and terrorism. However, this new security environment characterized by great power competition at levels below open conflict requires a new way of looking at the deterrence landscape at the sub-conventional level. Subject matter experts for this research confirm that a zero-tolerance deterrence mindset will not work at the sub-conventional level and that the United States might have to choose what portions of the gray zone it wants to deter because it may be difficult to deter everything.229

There is a precedent for applying a cumulative model and mindset of deterrence to limit and shape the sub-conventional level of conflict, and this suggests it may also be applied to the current U.S. need to deter Russia’s gray zone conflict. According to Thomas Rid, cumulative deterrence “consists of a series of acts of force to create—and maintain— general norms of behavior for many political actors over an extended period. Using force, consequently, does not represent a principal failure of deterrence but its maintenance through swift, certain, but measured responses.”230 Cumulative deterrence has been a key part of Israel’s strategy for decades and was developed in the conventional and subconventional level focusing on limiting and shaping ongoing conflicts against both state and non-state actors at the conventional and sub-conventional level.231 In addition, cumulative deterrence has recently been considered for use in deterring terrorism and cyberattacks, as it is designed for long-term sustained conflict, such as competition in the gray zone.232

Doron Almong describes cumulative deterrence as functioning on two levels: the macro, which creates an image of overwhelming military superiority, and the micro, which relies on responses to adversarial actions.233 Almong also explains that cumulative deterrence has three key features.

First, its effectiveness is measured in terms of the number of victories accumulated over the duration of the conflict, which might be envisioned as “assets in a victory bank.” Second, over time, these victories produce increasingly moderate behavior on the part of the adversary and a shift in its strategic, operational, and tactical goals until there is a near-absence of direct conflict. Third, this moderation may eventually result in political negotiations and perhaps even a peace agreement.234 Almong is describing cumulative deterrence as applied to the conventional level of warfare; however, in the context of Russia, the construct can be transposed to the subconventional level. At the sub-conventional level, U.S. responses over time to Russian gray zone aggression could moderate Russian behavior, causing a shift in Russia’s decision calculus and strategic goals, thereby diminishing the conflict.

The advantage of layering a strong conventional deterrence strategy with cumulative deterrence is that it allows the restoration of deterrence over time if conventional threats fail to deter at the sub-conventional level. Over time, cumulative deterrence responses to gray zone actions bolster the credibility of the United States and alter Russia’s decision calculus at the sub-conventional level, therefore strengthening deterrence overall. Successful deterrence at the sub-conventional level requires a reorientation in how the U.S. views deterrence, moving from a zero-tolerance strategy to the long-term attrition of gray zone conflict. This renewed mindset allows for tailored punitive strategies that over time limit the bounds of the gray zone through the reiteration of unacceptable behavior through punishment. Regardless of the level at which a state wishes to conduct warfare, all deterrence strategies rely on three aspects that must work in concert: sufficient capabilities, solid credibility, and strong communication of a threat.235 As Rid explains, confrontations should be “seen as necessary evils that should be kept on as low a level as possible, but that could not be pushed down to zero.”236 This argument assumes escalation control, which is to say that the United States can control escalation at the sub-conventional level on its own terms.

Many authors challenge the notion of escalation control, claiming that it is risky and nearly impossible. Scholars claim that avoiding escalation requires deterring the action and that a policy to deter one action could in fact risk escalation to another. Additionally, scholars claim, “Escalation control or management is an inherently imperfect business. It can be done well or poorly, but it is extremely rare for any set of policies to eliminate the risk of significant escalation altogether.”237 These same scholars agree that the risk of inadvertent escalation can be reduced, but they are concerned that policy makers are incorrectly assuming it can be eliminated altogether.238 The concerns over escalation control are valid; however, it is possible to control escalation and use the threat of escalation to bolster deterrence. Mazarr explains that the gray zone puts the defender in the position to escalate, which is part of the challenge of deterrence.239 Both escalation control and deterrence fundamentally rely on communication and a thorough understanding of the adversary. Proper communication of the capability and the resolve to use the capability to deny or punish an action are just as crucial to escalation control as they are to deterrence. The same scholars who express concerns over escalation control also admit there is a way to control the risk: “Escalation depends heavily on an astute understanding of how the adversary will perceive and interpret events that have not yet occurred—not only in a general sense, but also under the specific and often difficult-to-predict conditions that will shape the opponent’s perceptions and responses when a particular event occurs.”240 The United States can both mitigate escalation and contribute to deterrence by adding an element of ambiguity to its deterrence threats that leave something to chance but also allow a response that limits or controls the escalatory response of the adversary.

When the United States responds with an instrument of state power in any DIME category, such as the expulsion of 60 Russian diplomats in response to the Russian nerve agent attack on a British citizen in 2018, it can strengthen cumulative deterrence credibility. Some of the literature on cumulative deterrence suggests that deterrence works by banking “wins” by responding to events with military power. However, when adapted to the gray zone, it seems critical that all elements of state power must be utilized, not just the military. The military is sometimes—not always—an appropriate response to an action in the gray zone, so threatening military retaliation for every tactic in the gray zone is not credible; however, a state must still have the ability to impose costs on an adversary for an action to make cumulative deterrence successful.

### 2AC – Article IV Solves

#### Shift to Article IV solves---creates space for discussion and reserves Article V for large-scale attacks

John R Deni 19; Research Professor of Joint, Interagency, Intergovernmental, and Multinational Security Studies at the US Army War College’s Strategic Studies Institute; November 1st, 2019 “The Paradox at the Heart of NATO’s Return to Article 5”. <https://rusi.org/explore-our-research/publications/rusi-newsbrief/paradox-heart-natos-return-article-5>

However, in several important aspects, the Alliance response remains handicapped. Although NATO declared in 2016 and again in 2018 that it could consider a hybrid attack as grounds to invoke Article 5, the bar seems high – perhaps impossibly so. Achieving consensus – and quickly – in the face of an ambiguous attack or in response to ostensibly unrelated low-level provocations will not be an easy task. Perhaps more importantly, NATO remains in a defensive crouch when it comes to grey-zone challenges – Alliance rhetoric, exercises and actions emphasise response and reaction. It is precisely for this reason that grey-zone challenges against NATO are likely to be effective – actors such as Russia and China are evidently undeterred by the Alliance’s defensive posture, and attacks on Western institutions continue to this day. To be clear, defence is important, but in the current international security environment, offense and the competitive actions in between the two are equally important.

Given the arguably inadequate Alliance response to date, some guideposts may be helpful to illuminate the path ahead as NATO attempts to ensure collective defence remains robust into its eighth decade. First, Article 5 is an imperfect tool for determining when and where the West must spend blood and treasure in defence of its interests and way of life. Despite Alliance rhetoric regarding hybrid warfare as a potential Article 5 trigger, the threshold for Alliance-wide action is too high, and adversaries like Russia and China know it – this is why they pursue grey-zone tactics in the first place. To facilitate the speedy response that will be necessary to meet the needs of Allied defence against grey-zone challenges, greater, routine use can be made of Article 4 and Alliance-wide consultations and coordination on issues and topics that go beyond conventional military operations that are NATO’s bread and butter. For instance, the Alliance can and should conduct more vigorous, regular consultations and intensified coordination on topics such as keeping Chinese investment out of sensitive information-technology and logistics sectors, limiting and rolling back Russian broadcast and print media penetration of Western markets, undermining the Kremlin’s and Putin’s trustworthiness within Russia, and exposing Russian and Chinese official corruption at home and abroad, all as mechanisms to compete and thereby strengthen collective defence.

## AT: DoD Tradeoff

### 2AC – Thumper

#### The US just did security cooperation with Australia over space cybersecurity. Thumps the link.

Demetri Sevastopulo ’22, US-China Correspondent, “US and Australia boost space and cyber co-operation to counter China”, Financial Times, [https://www.ft.com/content/a6efecd9-8f7f-4072-ba86-f405c03bc005 //](https://www.ft.com/content/a6efecd9-8f7f-4072-ba86-f405c03bc005%20//) Ali

The US and Australia are boosting security co-operation in space and the cyber domain as the Indo-Pacific allies strengthen efforts to counter China, which is investing heavily in space and weapons such as hypersonic missiles. Admiral John “Lung” Aquilino, head of US Indo-Pacific Command, said the nations wanted to accelerate what the Pentagon calls “integrated deterrence”, combining all the elements of the military power of the US and its allies. “We’ve come a long way in a short time to be able to integrate the space and cyber domains,” said Aquilino, adding that Australia had capabilities that made it an “extremely high-end partner”. “We’re going to continue to work that and move the ball even further to synchronise those domains with our allies and partners,” the former Navy “**Top Gun**” fighter pilot told the Financial Times in an interview. Aquilino was joined by General James Dickinson, head of US Space Command, and Lieutenant General Charles “Tuna” Moore, an Air Force fighter pilot who serves as deputy head of US Cyber Command. The three flag officers were speaking ahead of meetings with Australian military and intelligence officials at Pine Gap, a top-secret joint US-Australia intelligence facility near Alice Springs that is instrumental in operating American reconnaissance satellites. Dickinson said Australia, which has just launched its own Space Command, was a critical partner in efforts to improve “space domain awareness” and monitor Chinese space operations. He said Australia helped allies overcome what the military calls the “tyranny of distance”.

## AT: Politics

### 2AC – Cyber Popular/Thumper

#### Cyber Workforce Program Act and State and Local Government Cybersecurity Act both thump and prove cybersecurity is bipartisan

Stephen Silver 6/23, technology writer for the National Interest, 6/23/2022, “Cyber in Focus: Biden Signs Pair of Bipartisan Cybersecurity Bills”, National Interest, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/cyber-focus-biden-signs-pair

This week, President Biden signed a pair of new bipartisan cybersecurity bills into law. According to The Hill, the bills are the Federal Rotational Cyber Workforce Program Act and the State and Local Government Cybersecurity Act. The two bills were generally noncontroversial and passed without much vocal opposition from members of either party.

In May, Biden issued an executive order on cybersecurity, titled Improving the Nation’s Cybersecurity. The president also thanked the bipartisan sponsors of the legislation.

The first bill, the Federal Rotational Cyber Workforce Program Act, took something of a circuitous route to the president’s desk. It passed the House back in 2019, during the previous Congress, and was reintroduced in April of 2021, before passing via unanimous consent in December. After passing the House via a voice vote in May, the bill was signed by the president this week.

According to The Hill, the rotational bill “establishes a program to allow cybersecurity professionals to rotate through multiple federal agencies and enhance their expertise,” while also requiring the Office of Personnel Management (OPM) to “distribute lists of open positions in the program to government employees annually.”

The second bill, the State and Local Government Cybersecurity Act, is meant to improve communications between the Department of Homeland Security and state and local governments on the issue of cybersecurity. It also requires the National Cybersecurity and Communications Integration Center (NCCIC) to “share security tools and protocols” with local governments.

“State and local governments with limited resources and cybersecurity expertise can struggle to secure their systems against malicious hackers that could expose their constituents’ personal data,” bill co-sponsor Senator Gary Peters (D-MI) said after the first Senate passage of the bill in 2019. “I’m pleased the Senate passed my bipartisan bill that will help ensure all levels of government can bolster their defenses and protect themselves from sophisticated cyber-attacks,” Peters continued.

#### Cybersecurity is bipartisan–medical devices and veterans affairs cybersecurity bills prove

Jacky Rosen 6/3, American politician serving as the junior United States senator from Nevada since 2019, “Rosen, Young Introduce Bipartisan Legislation to Strengthen Cybersecurity for Medical Devices”, Jacky Rosen, https://www.rosen.senate.gov/rosen-young-introduce-bipartisan-legislation-strengthen-cybersecurity-medical-devices

WASHINGTON, DC – U.S. Senator Jacky Rosen (D-NV), a member of the Senate Health, Education, Labor and Pensions Committee, recently introduced her bipartisan Strengthening Cybersecurity for Medical Devices Act with Senator Todd Young (R-IN), which would require the U.S. Food and Drug Administration (FDA) to review and update medical device cybersecurity guidelines and suggestions to ensure devices are protected from possible hacking and cyber attacks.

“In light of increased cyber threats, we must strengthen the security of our health care system’s cyber infrastructure,” said Senator Rosen. “This bipartisan bill I introduced with Senator Young will ensure that medical devices and technologies are up to date with the latest cybersecurity, protecting patients and health care systems.”

“Medical devices are increasingly connected to the Internet or other health care facility networks to provide features that improve the ability of health care providers to treat patients,” said Senator Young. “Our bill helps ensure medical devices are protected from cyberattacks and used safely and securely in order to reduce risks and vulnerabilities for patients.”

The bipartisan Strengthening Cybersecurity for Medical Devices Act would require the FDA, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA), to review guidance for industry and FDA staff regarding medical device cybersecurity and make updates as appropriate at least every two years. This provision would ensure a more timely review to keep the guidance current. The bill also requires FDA to share information publicly regarding federal resources for health care professionals, medical device manufacturers, and health systems to identify and address cyber vulnerabilities, and access support. Additionally, the bill requires a GAO report examining medical device cybersecurity vulnerabilities and recommendations for improving federal coordination to support cybersecurity for medical devices.

Senator Rosen has been a leader in strengthening America’s cybersecurity infrastructure. In March, she and Senator Bill Cassidy (R-LA) introduced their bipartisan Healthcare Cybersecurity Act, which would direct CISA to collaborate with the Department of Health and Human Services on improving cybersecurity in the Health Care and Public Health Sector, one of the United States’ sixteen critical infrastructure sectors. Senator Rosen has also introduced a bipartisan bill to bolster the cybersecurity of the Department of Veterans Affairs and protect veterans’ personal information.

### 2AC – Cyber Popular

#### Cybersecurity is bipartisan

Daniel Kroese 1/25, Associate Director of CISA's National Risk Management Center focusing on strategic engagement, 1/25/2022, “Bipartisan Cybersecurity Legislation — Continuing the Progress in 2022”, Paloalto Networks, https://www.paloaltonetworks.com/blog/2022/01/bipartisan-cybersecurity-policy/

Whether it’s government networks storing sensitive information or critical infrastructure systems, no entity is immune to cyber adversaries. Fortunately, the strong bipartisan consensus on cybersecurity threats has led to bipartisan interest in cybersecurity legislation.

At Palo Alto Networks, we appreciate the collaborative spirit on Capitol Hill, working with a wide range of stakeholders to get policy right. With the 2022 legislative calendar now in full swing, we see cybersecurity policy activity coalescing around several worthwhile pillars of activity.

Investing in Proactive Cyber Resilience

The American people understand the value of filling potholes on the streets and have recognized that our “digital potholes” demand equal attention. While there’s no silver bullet, we can’t ignore the economics. Better cybersecurity outcomes demand more dedicated cybersecurity investment.

History has taught us that investing in cyber resilience before something bad happens will almost always be cheaper in the long run. That’s why Palo Alto Networks was encouraged to see a State and Local Cybersecurity Grant Program included as a key provision in the Infrastructure Investment and Jobs Act.

The funds provided from this grant program will be cybersecurity game changers for jurisdictions all across the country. Similarly, the cybersecurity plans required to unlock those funds will promote a broad culture of cybersecurity vigilance that benefits us all. The multi-entity grant eligibility will promote innovative investments, such as security operations centers that span state lines.

Properly resourcing the Cybersecurity and Infrastructure Security Agency (CISA) will act as a force multiplier to ensure that investment in cybersecurity resilience is met with technical assistance and services to help organizations with capacity building. Both the House and Senate continue showing eagerness to fund CISA’s necessary maturation.

Investing in cybersecurity resilience will be foundational in gaining the upper hand on the ransomware epidemic. The White House has demonstrated strong leadership both domestically and internationally on this issue. That focus, coupled with dedicated funding, can meaningfully move the needle.