# Neg

# AT: Case

## AT: Squo

### 1NC – Squo solves

#### The aff became non inherent on June 29th whent NATO announced its Strategic Concept

NATO 22, 6-29-2022, “NATO 2022 STRATEGIC CONCEPT” https://www.nato.int/nato\_static\_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf/billy

24. We will expedite our digital transformation, adapt the NATO Command Structure for the information age and enhance our cyber defences, networks and infrastructure. We will promote innovation and increase our investments in emerging and disruptive technologies to retain our interoperability and military edge. We will work together to adopt and integrate new technologies, cooperate with the private sector, protect our innovation ecosystems, shape standards and commit to principles of responsible use that reflect our democratic values and human rights.

25. Maintaining secure use of and unfettered access to space and cyberspace are key to effective deterrence and defence. We will enhance our ability to operate effectively in space and cyberspace to prevent, detect, counter and respond to the full spectrum of threats, using all available tools. A single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty. We recognise the applicability of international law and will promote responsible behaviour in cyberspace and space. We will also boost the resilience of the space and cyber capabilities upon which we depend for our collective defence and security.

26. We will pursue a more robust, integrated and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security, as a national responsibility and a collective commitment rooted in Article 3 of the North Atlantic Treaty. We will work towards identifying and mitigating strategic vulnerabilities and dependencies, including with respect to our critical infrastructure, supply chains and health systems. We will enhance our energy security and invest in a stable and reliable energy supply, suppliers and sources. We will ensure civil preparedness to provide for continuity of government, the delivery of essential services to our populations and civil support to our armed forces. We will boost our capacity to prepare for, resist, respond to, and quickly recover from strategic shocks and disruptions, and ensure the continuity of the Alliance’s activities.

## AT: China Adv

### 1NC – Article 5 Key

#### Aff fails---only terrestrial retaliation can deter---otherwise China calculates mutual destruction to be net beneficial even if they’re rational, which they aren’t.

James Lewis 13, Senior vice president and program director at the Center for Strategic and International Studies (CSIS), “Reconsidering Deterrence for Space and Cyberspace”, https://www.stimson.org/wp-content/files/file-attachments/Anti-satellite%20Weapons%20-The%20Stimson%20Center.pdf \\SYang

In order to deter China from using ASAT weapons, China’s leaders would have to calculate that an ASAT attack would lead to an escalation of conflict or to damaging retaliation. In peacetime, Beijing would probably calculate that an ASAT attack might risk being seen as a casus belli. If so, it is unlikely that China’s kinetic or directed energy weapons would be used outside of conflict. If, however, Washington and Beijing are already engaged in an armed clash, the threat of the use of force in space is somewhat moot. Washington could, for example, threaten to escalate the conflict by warning that an attack on a satellite will result in the destruction of China’s space launch complex. Beijing may nonetheless calculate that at this stage of its military modernization, interfering with US satellites is worth any retaliatory interference with their own satellites, and that the risk of escalation in other domains is either low or acceptable. There is some evidence that Chinese military leaders may underestimate risk and overestimate the utility of asymmetric attacks. China has little experience with the arms control negotiations that underpinned nuclear deterrence, has a different conceptual framework for conflict and international relations, and lacks the experience of the Cold War for interpreting American actions and signals. Chinese military concepts on “deterrence” differ significantly from US concepts, meshing Schelling’s ideas of deterrence and compellence in ways that encourage use and increase the risk of miscalculation.7 Deterring Chinese ASAT attacks during armed conflict would require threatening something other than China’s own satellites, since the People’s Liberation Army (PLA) is not yet so dependent on space assets that the satellites’ loss would constrain their operations as much as the loss of American satellites would hurt US forces. In this situation, Chinese leaders may see an exchange of satellite attacks as working to their benefit. Only a credible threat to retaliate against a terrestrial target would change China’s calculus, but such threats bring the risk of escalation of conflict that would need to be weighed carefully. Responding to an attack on a military target in space or a military cyber network with an attack on the Chinese homeland would likely be seen by China as escalatory. Additionally, nationalist sentiment among the citizens of potential opponents like China or Iran suggests the most likely effect of US escalation unless it was sustained and broadly destructive, would be to reinforce support for the regime and for a continuation of the conflict. Belief shapes perception. The Kremlin believed that the United States was inherently aggressive and sought the destruction of the Soviet Union. Soviet political and military leaders debated whether the US investment in weapons was to retain a credible deterrent or to attain first strike capabilities. Paranoia also colors how authoritarian Chinese military leaders may underestimate risk and overestimate the utility of asymmetric attacks. regimes that lack domestic legitimacy view the United States. Cultural and linguistic differences also contribute to misinterpretation of deterrent messages.

### 1NC – Lasers Alt Cause

#### Chinese laser attacks are an alt cause

\*Brian Chow and \*\*Henry Sokolski 20, \*Senior Physical Scientist and Professor at RAND Corporation and \*\*Executive Director of the Nonproliferation Policy Education Center, 7/10/2020, “Op-ed | U.S. satellites increasingly vulnerable to China’s ground-based lasers”, Space News, https://spacenews.com/op-ed-u-s-satellites-increasingly-vulnerable-to-chinas-ground-based-lasers/

The Defense Intelligence Agency warned in January 2019 that China likely will field in 2020 a ground-based laser weapon that can counter low-orbit space-based sensors. By the mid-to-late 2020s it may field higher power systems that could damage the structures of non-optical satellites.

How real is the threat? Analysts have already identified five Chinese laser bases. One in Xinjiang has four main buildings. One of these building is thought to be for tracking satellites, while equipment in the other three could be used to dazzle or disable satellite sensors. If the Xinjiang facility is representative of the other four, all five bases can be located and are vulnerable to aerial attacks.

In addition to these bases, China operates several satellite laser ranging stations. These have been used to determine the orbits of satellites and space debris but could be used to damage U.S. and allied satellite sensors.

Of the world’s 50 satellite laser ranging stations, five fixed stations are in Shanghai, Changchun, Beijing, Wuhan and Kuming. Two Chinese satellite laser ranging stations are mobile.

The ranging system at the Shanghai station uses a laser with a relatively low average power of 2.8 watts. The wattage at other stations are most likely the same or lower. Another laser of 60 watts at the Shanghai station has been used routinely to measure space debris. Calculations show that a 1-watt laser has 1 in 1,000 chance to cause permanent damage to a sensor, while a 40-watt laser would double the chance. These odds are low but likely to increase.

In the near term China’s top priority is to deny America and its allies imagery with high resolution of 10 centimeters or better. Fortunately, to damage a satellite’s optical elements such as pixels and filters, an offensive anti-satellite laser would have to be located within roughly 10 kilometers of what one wants to take a picture of.

What should Washington do to counter sensor-damaging lasers? First, it should determine how many of the Chinese targets it wants to take pictures of that have a laser base or fixed satellite laser ranging station within roughly 10 kilometers. There are probably only a few such laser-protected targets.

Second, our military and intelligence analysts need to estimate the risks and costs of snapping pictures from space of these laser-protected targets (i.e., the chance of our satellites’ sensors being damaged and what their repair or replacement costs might be) and the benefits of getting such imagery. Such an analysis would likely recommend that the United States and its allies:

Take pictures whenever possible during peacetime, as the chance of damage is far higher during crisis.

Update imagery less frequently, because fewer trips mean less chance of being hit.

Use as low a resolution for imagery as much as possible, as low-resolution sensors and their satellites are cheap and numerous compared to dedicated military imagery satellites

Third, the United States should secure imagery of all needed resolutions, including 10 centimeters or better, any way it can using commercial and dedicated military systems during peacetime, crisis and wartime. Once it has a diversified group of imagery providers, laser damage to a few of our sensors would become far less valuable to our adversaries, leading them not to initiate such attacks in the first place.

Finally, the United States should extend the 2010 New Strategic Arms Reduction Treaty, which expires in February 2021, to keep its formal prohibitions on interference with national technical means of verification (including sensor-carrying satellites) in force. To the extent that Washington can bring China into arms negotiations with the Russians, it should focus on getting Beijing formally to agree to this prohibition.

The U.S. government will need to do more in the years ahead. Today, Chinese lasers must be located within roughly 10 kilometers of whatever Washington wants to snap pictures of to have any hope of beaming into American satellites’ telescope openings and damaging their sensors inside. Mid-decade, though, when Beijing acquires higher powered lasers, at least one of China’s lasers will be in range to damage several of our low earth orbiting satellites every day. As a result, Washington will not only have to make our satellite constellations resilient and harden some satellites’ exteriors and sensors, it must be prepared to disable China’s laser systems if they attack our satellites.

During this same period, the United States will also have to pay attention to Chinese satellite laser ranging stations and high power lasers that will have gone mobile. Because these mobile systems are likely to be dual-use, they cannot be banned. Instead, the United States and its allies should disadvantage any hostile use with diplomatic measures that would afford warning of such.

This could best be achieved by pushing for an international agreement to register all mobile dual-use lasers (including their locations), require their operators to announce their planned movement a month in advance, and demand their movements be broadcast in real time.

### 2NC – Lasers Alt Cause

#### China developed laser technology and are inclined to use them – satellite attacks inevitable

Chris Zappone 21; Digital Foreign Editor at The Age and Sydney Morning Herald, Published: 8-9-2021; "Space lasers and the new battlefield emerging under China’s anti-satellite tactics"; Sydney Morning Herald; Accessed: 6-30-2022; https://www.smh.com.au/world/asia/space-lasers-and-the-new-battlefield-emerging-under-china-s-anti-satellite-tactics-20210804-p58ft2.html)//Pen-SY

Space lasers are a real thing, even if they’re not generally made to blow up passing satellites. Designed to damage or disable sensor equipment on orbiting satellites, ground-based lasers can help hide a nation’s activities. Photography from satellites, for example, has been key in helping reveal the extent of Beijing’s detention of Muslim Uighurs in western China. Weeks before the Federation of American Scientists produced analysis showing missile silos being built in western China, US-based analysts – drawing attention to anti-satellite lasers in Xinjiang – warned that US satellites, the kind that could keep an eye on China’s military, were “increasingly vulnerable to China’s ground-based lasers”. Sydney-based space analyst Chris Flaherty said that when it came to lasers, “dazzling”, or interfering with a satellite’s camera, and “blinding”, permanently damaging a satellite, “are the prime technologies that are deployable right now”. The technology gives a country the power “to deny a satellite’s ability to operate, to shut it down or to damage it – without creating space debris”. Michael Duitsman of the California-based James Martin Centre for Nonproliferation Studies said the laser facility in Xinjiang was thought to have been started as far back as 2009. It “significantly predates both the Uighur cultural genocide and the current missile silo construction,” he said. Inspecting images from earlier this year, Duitsman said there had been some construction in the support area for the laser, as well as modification at one of the buildings. Concerns about the use of lasers used this way in a future space conflict are spreading. The prospect of a contest for space dominance between China, the US and Russia prompted the US to create the Space Force in 2019. Last month, Defence Minister Peter Dutton announced Australia would begin exploring options for Space Electronic Warfare, because it’s a capability that doesn’t “create debris or damage the space environment”. Flaherty said to better understand China’s intentions with lasers aimed at satellites, one need only look at the example Russia provides. In 2018, Russia unveiled its Peresvet laser system and positioned it near mobile units of intercontinental ballistic missiles. In doing so, it can temporarily blind passing satellites overhead from taking pictures. Flaherty said “any superpower that has important strategic assets ... will deploy a laser”. US-based China space analyst Dean Cheng believes Beijing would likely have installed them to frustrate the satellite photography of its military bases and equipment. “It would not be surprising if the Chinese wanted to limit Indian ability to see into Tibet,” said Cheng. He said lasers could be used to protect one of China’s missile silo fields, as well as naval and air bases that could be used in an invasion of Taiwan. But the ability to use lasers against satellites is well known by space-faring powers. “What is more problematic is that the West relies more on space for the conduct of military operations, so effective anti-satellite systems work much more to the benefit of” Russia or China, which focus their military closer to their own regions, Cheng says. Economically, the West has more to lose in such a scenario because widely adopted Western technologies such as GPS have evolved to rely on peaceful access to space. Simply raising questions about China’s capabilities to disrupt a rival nation’s satellites is part of the new game, one that differs from the Cold War rivalry. The physical distance of orbit makes it hard to know with certainty whether an outage of a satellite happened as a cause of an accident, or if something was the result of hard-to-detect aggression. For example, in 2006, China used a laser that temporarily blinded a US military reconnaissance satellite. “The action temporarily blinded the satellite but caused no permanent damage, leading to speculation that China may not have been intentionally trying to interfere with the satellite,” said US congressional testimony in 2019. Like the ambiguity of attributing the origin of a cyber attack, the cause of a problem in orbit is hard to determine as the satellite passes 200 kilometres overhead at a speed of 25,000 km/h. Messing with a rival’s satellites in orbit in ways that can easily be misinterpreted, using lasers, or some other directed energy, is a change from the Cold War. Back then Russian or American interference with each other’s satellites could easily be interpreted as a prelude to a nuclear launch, and so was something to generally avoid. Today, while the nuclear risk hasn’t gone away – as China’s missile silo building proves – technology has evolved, orbits have grown much more crowded, and so has the willingness of some space powers to court risk. China, among others, has been on a mission to build space power since it – and the world – witnessed volleys of US satellite-guided bombs raining down on Iraqi troops during the Persian Gulf War of 1991. “The Gulf War set off the next technology trend for countries to catch up,” Flaherty said. Since then, many more satellites and nations have entered orbit, producing data and services we rely on daily: GPS, space-based timing for transactions, Google maps, precise weather data for agriculture. If China or another power used lasers aggressively against orbiting satellites, it’s no longer about two superpowers facing off like during the Cold War space race, said Flaherty.

### 1NC – No Attack

#### Chinese cyber threats are overblown – the U.S. is far more advanced in its cyber and military capabilities and the lack of coordination in the Chinese military decks its ability to launch a major satellite cyber attack

Jon R. Lindsay 15, an Associate Professor at the School of Cybersecurity and Privacy at the Georgia Institute of Technology with a joint appointment in the Sam Nunn School of International Affairs and the School of Public Policy, “Exaggerating the Chinese Cyber Threat,” May 2015, Policy Brief, Quarterly Journal: International Security, <https://www.belfercenter.org/publication/exaggerating-chinese-cyber-threat>

The secrecy regarding the cyber capabilities and activities of the United States and China creates difficulty in estimating the relative balance of cyber power across the Pacific. Nevertheless, the United States appears to be gaining an increasing advantage. For every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and growing Western strengths.

Much of the international cyber insecurity that China generates reflects internal security concerns. China exploits foreign media and digital infrastructure to target political dissidents and minority populations. The use of national censorship architecture (the Great Firewall of China) to redirect inbound internet traffic to attack sites such as GreatFire.org and GitHub in March 2015 is just the latest example of this worrisome trend. Yet prioritizing political information control over technical cyber defense also damages China's own cybersecurity. Lax law enforcement and poor cyber defenses leave the country vulnerable to both cybercriminals and foreign spies. The fragmented and notoriously competitive nature of the Communist Party state further complicates coordination across military, police, and regulatory entities.

There is strong evidence that China continues to engage in aggressive cyber espionage campaigns against Western interests. Yet it struggles to convert even legitimately obtained foreign data into competitive advantage, let alone make sense of petabytes of stolen data. Absorption is especially challenging at the most sophisticated end of the value chain (e.g., advanced fighter aircraft), which is dominated by the United States. At the same time, the United States conducts its own cyber espionage against China , as the Edward Snowden leaks dramatized, which can indirectly aid U.S. firms (e.g., in government trade negotiations). China's uneven industrial development, fragmented cyber defenses, erratic cyber tradecraft, and the market dominance of U.S. technology firms provide considerable advantages to the United States.

Despite high levels of Chinese political harassment and espionage, there is little evidence of skill or subtlety in China's military cyber operations. Although Chinese strategists describe cyberspace as a highly asymmetric and decisive domain of warfare, China's military cyber capacity does not live up to its doctrinal aspirations. A disruptive attack on physical infrastructure requires careful testing, painstaking planning, and sophisticated intelligence. Even experienced U.S. cyber operators struggle with these challenges. By contrast, the Chinese military is rigidly hierarchical and has no wartime experience with complex information systems. Further, China's pursuit of military "informatization" (i.e., emulation of the U.S. network-centric style of operations) increases its dependence on vulnerable networks and exposure to foreign cyberattack.

To be sure, China engages in aggressive cyber campaigns, especially against nongovernmental organizations and firms less equipped to defend themselves than government entities. These activities, however, do not constitute major military threats against the United States, and they do nothing to defend China from the considerable intelligence and military advantages of the United States.

### 2NC – No Escalation – Empirics

#### All empirics go neg

Erica D. Borghard 19, assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University; and Shawn W. Lonergan, research affiliate of the Army Cyber Institute at the United States Military Academy at West Point, Ph.D. in Political Science from Columbia University, Fall 2019, “Cyber Operations as Imperfect Tools of Escalation,” Strategic Studies Quarterly, Vol. 13, No. 3, p. 122-145

There is a widespread view among practitioners and scholars that cyberspace is defined by an inherent potential for dangerous escalation dynamics between rivals.1 On the practitioner side, for example, senior US intelligence and military leaders expressed concerns about first-strike incentives leading to escalation in a 2017 joint statement to Congress, testifying that “adversaries equipped with [offensive cyber capabilities] could be prone to preemptive attack and rapid escalation in a future crisis, because both sides would have an incentive to strike first.”2 On the academic side, there is a palpable fear that cyberspace is an environment in which offense has advantages over defense and that this—coupled with factors such as problems of attribution, poor command and control, and the absence of meaningful thresholds or red lines—generates real risks of inadvertent escalation.3 Concerns about escalation grew even more passionate in the wake of the US Department of Defense’s release of its 2018 Cyber Strategy document, which articulates an operational concept of “defending forward” in which the DOD “disrupt[s] or halt[s] malicious cyber activity at its source.”4

However, there are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. Specifically, if cyberspace is in fact an environment that (perhaps even more so than others) generates severe escalation risks, why has cyber escalation not yet occurred? Most interactions between cyber rivals have been characterized by limited volleys that have not escalated beyond nuisance levels and have been largely contained below the use-of-force threshold.5 For example, in a survey of cyber incidents and responses between 2000 and 2014, Brandon Valeriano et al. find that “rivals tend to respond only to lower-level [cyber] incidents and the response tends to check the intrusion as opposed to seek escalation dominance. The majority of cyber escalation episodes are at a low severity threshold and are non-escalatory. These incidents are usually ‘tit-for-tat’ type responses within one step of the original incident.”6 Even in the two rare examples in which states employed kinetic force in response to adversary cyber operations—the US counter-ISIL drone campaign in 2015 and Israel’s airstrike against Hamas cyber operatives in 2019—the use of force was circumscribed and did not escalate the overall conflict (not to mention that force was used against nonstate adversaries with limited potential to meaningfully escalate in response to US or Israeli force).7

### 1NC – No Escalation

#### Cyber attacks don’t cause escalation – resources, reversibility, and lesser impact

Sarah Kreps, 19 — (Sarah Kreps; Political Science Department, Cornell University, Published: 9-29-2019; "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics"; OUP Academic; Accessed: 6-26-2022; https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971)//Pen-SY

The perseverance of the firebreak has come to define nuclear strategy, especially for the United States.1 It is also increasingly central to debates around US cyber strategy. Therefore, as critics of the persistent engagement strategy argue, understanding the logics of cyber escalation is vitally important to the strategy’s success [49–51]. Despite the importance of escalation for current US cyber strategy success, there is very little scholarly consensus about cyber escalation.2 As Joseph Nye asserts, “escalation ladders and thresholds are poorly understood” in the cyber realm [66]. A number of scholars and policymakers argue that cyber operations do not change the fundamental nature of escalation. For these scholars, it is the effects created by weapons that matter for escalation and not necessarily the means or the domain in which the effects are created. Cyberspace operations may have unique qualities, but the fundamental logics of escalation are tied to weapons’ effects and rather than how these effects are delivered. As long as cyberspace operations can create similar effects as operations in other domains, they create the same escalation ladders. The debate within this literature is about the technical ability of cyberspace operations to create the same effects as the other domains [56, 59, 60, 62, 67, 68]. Kostyuk et al., e.g., equate permanent damage to civilian infrastructure as the cyber equivalent of a nuclear war and existential attack, all of which should warrant a comparable escalatory response. They caveat that “at present, we do not believe a single mode of cyber attack alone would pose an existential threat to the US, however, this may change in the near future” [69]. Scholars within this line of reasoning devote significant attention to understanding the difficulty cyberspace operations have achieving access, the resources required for creating complex effects, and the highly-reversible nature of most cyberspace operations. Glaser and Farrell provide an effects-based typology and point to five characteristics of effects that may decrease escalation of cyberattacks: physical versus nonphysical damage (first- or second-order physical effects), no visible damage, military versus civilian, attacks that kill versus those that do not, and attacks in war versus peace [13]. According to this understanding of cyberspace and escalation, responses to a cyberattack should not be qualitatively different from any other attack as long as cyberattacks can advance to the level of nuclear or large-scale conventional capabilities [57, 59]. Until cyberspace attacks can provide the decisive edge toward taking territory or create the lethal effects comparable to large-scale or nuclear war, they will not be treated the same as attacks in other domains. The perspective is largely consistent with Valeriano and Maness’s quantitative analysis of cyberspace operations, who find cyber operations to be largely low intensity and find no evidence of higher intensity retaliation to cyber attacks [69].

### 2NC – No Escalation

#### Cyberattacks will not escalate – cyberattacks repeatedly evoke minor responses that don’t lead to escalation

Martin C. Libicki 20, Professor at the Center for Cyber Security Studies at the U.S. Naval Academy, “Correlations Between Cyberspace Attacks and Kinetic Attacks,” May 2020, 2020 12th International Conference on Cyber Conflict, http://195.222.11.251/uploads/2020/05/CyCon\_2020\_11\_Libicki.pdf

Overall, there is little public evidence that hostile events in cyberspace echo strongly outside it. Indeed, rarely do events in cyberspace – much less escalation in cyberspace – lead to serious responses at all. Some research suggests that even severe cyberattacks would generally be less likely than kinetic attacks to induce a response. Although opening cyberattacks can precede kinetic attacks, there are also cases when war comes as a surprise and cyberattacks are not used until the proper accesses to target systems have been gained. Cyberattacks have the potential to put hitherto sacrosanct targets – notably space systems, and other NC3 elements – in play, but cyberattacks have reportedly taken place against satellites while kinetic attacks (weapons tests aside) have not, so far. The failure to respond to cyberattacks may have played a role in enabling missile attacks on Saudi Aramco facilities, but the link is distant (seven years earlier) and tenuous. There is no analog (yet) in the Russo-Ukrainian conflict. Several reasons could be adduced to explain the lack of correlation. One is that while there could be cyberattacks consequential enough to induce echoes in the physical world, none have reached that threshold and it may well be that none could reach that threshold. Even as the attack surface for cyberspace operations keeps growing, hackers grow more talented, and their leaders more aware of the gains available from such operations – defense is not sleeping. Those who own networks are taking cybersecurity seriously (at long last), cloud computing may have helped put defenses in the hands of those for whom protection is a profit center, and the cybersecurity industry itself is robust. Succeeding generations of software – e.g., versions of Windows operation systems – are also more impervious to intrusions. Two is that, in common with many widely-feared phenomena, cyberattacks have evolved from an acute problem (one both rare and fearsome) to a chronic problem (more common, but something that one can adjust to). Three, the oft-expressed belief that cyberwar is war has yet to take hold. Because cyberspace operations are ambiguous (and not easily grasped even when clear) and their effects almost always temporary and not (yet) lethal, they may be considered something separate and apart. Time will tell whether this distinction will continue to be observed.

#### Cyberattacks aren’t perceived as an “armed attack” – they are non-lethal and elicit weaker responses than kinetic attacks

Martin C. Libicki 20, Professor at the Center for Cyber Security Studies at the U.S. Naval Academy, “Correlations Between Cyberspace Attacks and Kinetic Attacks,” May 2020, 2020 12th International Conference on Cyber Conflict, http://195.222.11.251/uploads/2020/05/CyCon\_2020\_11\_Libicki.pdf

4. PROPOSITION: CYBERATTACKS WILL BE TAKEN AS SERIOUSLY AS EQUALLY DAMAGING KINETIC ATTACKS If countries react to cyberattacks as they would to equivalent kinetic attacks, then an escalation in cyberspace (defined as above) could well result in a comparable escalation in physical space – again with the expected effects on international stability. But would they? Much of the answer depends on what constitutes “comparable.” Kinetic military effects tend to include death and destruction. No cyberattack has killed anyone directly, and few have actually broken physical things; wiping a hard drive – as many cyberattacks have done – still leaves the hard drive physically intact. But cyberattacks have been quite costly to their victims, even if measured solely in disruption and remediation costs. The NotPetya attacks were said to have cost their (mostly corporate) victims up to $8 billion (Greenberg 2018). Putatively, a kinetic attack that destroys $8 billion worth of military equipment but harms no one would be comparable and should, one would imagine, bring about a comparable reaction. Imagining a kinetic attack that breaks things but hurts no one used to be an exercise in fantasy. But the Iranian take-down of a $150 million U.S. Global Hawk in the summer of 2019 was such an attack. The U.S. response, a cyberattack, was also non-lethal. Lest this choice of avoiding lethality be ascribed to the individual characteristics of the U.S. President, note that the Pentagon was also thinking along similar lines. One of its favored options was to sink an Iranian craft, but only after giving its sailors time to get away (Baker, Schmitt, and Crowley 2019). Earlier, a Turkish shootdown of a Russian jet near the Syrian border had drawn a cyber response (e.g., DDOS attacks), but nothing violent (Murgia 2015). Returning to NotPetya, the U.S. reaction to this costly event was a limited set of sanctions. If Russia had deliberately disabled commercial satellites whose total replacement value summed to that much, would the United States have also limited its response to sanctions? One might counter that many of the affected corporations were not U.S.-headquartered: for example, Maersk, a Danish shipping company. If that matters, then replace United States by NATO and re-ask the question. So, while the non-lethality of cyberattacks means that a plausible response would be non-lethal, the failure to respond to NotPetya suggests that the broad scope of the cyberattack may have also played a role. Perhaps a cyberattack that damages software and thereby levies costs on victims is different in kind from a comparably costly kinetic attack that damages hardware. Research by Professor Jacqueline Schneider casts further doubt that a cyberattack would be treated as tantamount to a comparable kinetic attack (see Kreps and Schneider 2019). The results of two exercises – one conducted at the U.S. Naval War College and the other on-line – suggest that cyberattacks introduced into a simulated crisis were more often ignored or, at most, motivated a weak response in comparison to comparable kinetic attacks. In fairness, the United States has been used as the exemplar of how countries may respond to cyberattacks and other countries may react differently. But the United States deserves attention because it has responded most overtly, whether through public statements, levied sanctions, or news reports (Israel is also active, but it is a far smaller country and unique in many relevant respects). It is unclear whether the difference is that the United States suffers more cyberattacks than other countries (or seems to in part because of uncensored media coverage) or whether other countries have covert ways of responding that are not widely known. That noted, Jensen and Valeriano (2019) indicate that when citizens of the United States, Russia, and Israel were given a scenario with a major cyberattack, only a small percentage chose to escalate as a result. Roughly half of the respondents wanted something less than a titfor-tat response. They concluded that, “to date, cyber operations have tended to offer great powers escalatory offramps”. Conclusion: cyberattacks would be deemed less likely to garner a kinetic response than would kinetic attacks that levy comparable costs, because they are generally nonlethal and somehow considered less serious and more easily recovered from.

### 2NC – No Escalation – Grid

#### Critical infrastructure attacks don’t generate anywhere near the impact required to trigger escalation

Erica D. Borghard 19, assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University; and Shawn W. Lonergan, research affiliate of the Army Cyber Institute at the United States Military Academy at West Point, Ph.D. in Political Science from Columbia University, Fall 2019, “Cyber Operations as Imperfect Tools of Escalation,” Strategic Studies Quarterly, Vol. 13, No. 3, p. 122-145

Even under circumstances in which a state may possess the right cyber response capabilities at the desired time, its response may not generate sufficient costs against the target to be perceived as escalatory.41 Fundamental limits on the cost-generation potential of offensive cyber operations stem from the fact that cyber capabilities lack the physical violence of conventional and nuclear ones. Cyber weapons target data; they disrupt, manipulate, degrade, or destroy data resident on networks and systems or in transit.42 Moreover, aside from those cyber capabilities that permanently destroy data and for which there are no backups to which a target can revert, cyber effects are temporary and often reversible.

The utility of military instruments of power for the purposes of coercion or brute force inheres in their abilities to inflict—or credibly threaten to inflict—significant damage and harm against a target state (its civilian population or its military forces) to achieve a political objective.43 Cyber weapons could be (and have been) used to disrupt an adversary’s networks and systems—overwhelming them such that they temporarily lose the ability to function or the target loses confidence in their reliability—or even to produce destructive effects by destroying data resident on these systems or, in rarer circumstances, producing effects in the physical realm.44 While conducting multiple cyberattacks against a targeted state’s critical national infrastructure, for example, could in theory generate significant economic and national security consequences, the temporal aspects of offensive cyber operations as described above limit the ability of even the most capable states to sustain persistent, high-cost effects against multiple strategic targets over time. There is simply no guarantee that a state can generate significant costs against a target in the context of an unfolding crisis. This reality starkly contrasts with the relative predictability and reliability of conventional effects. Indeed, the empirical record has largely validated this claim; “the vast majority of malicious cyber activity has taken place far below the threshold of armed conflict between states, and has not risen to the level that would trigger such a conflict.”45 This is why, in Lin’s parlance, “going cyber is pre-escalatory” and countervalue cyberattacks (those that target civilian, rather than military, assets) occur “all the time now and are at the BOTTOM of the escalation ladder” [emphasis in original].46 Rather than their ability to wreak permanent, destructive effects, cyber operations are often prized for their temporary and reversible nature.47

One metric to assess the cost-generation potential of offensive cyber is in terms of loss of life. By this measure, cyber operations are unlikely to inflict significant harm. While theoretically possible that cyber operations could lead directly to a loss of life, no one has reportedly died to date as a direct result of a cyberattack despite over 30 years of recorded cyber operations.48 Even in hypothetical catastrophic scenarios, the cost in terms of human casualties is minimal. For instance, common worst-case scenarios of cyberattacks revolve around the loss of power stemming from a cyberattack on an electric grid.49 However, even in this instance, the conceivable damage from the loss of power over an extended period is far less than that which could be wreaked using basic, limited conventional capabilities. To draw a comparison, when Hurricane Sandy hit the United States’ eastern seaboard in late October 2012, over 8.5 million people were left without power—with many going weeks and even months before it was brought back online.50 Yet a US National Hurricane Center postmortem of Hurricane Sandy reported that of the 159 people in the United States killed either directly or indirectly, only “about 50 of these deaths were the result of extended power outages during cold weather, which led to deaths from hypothermia, falls in the dark by senior citizens, or carbon monoxide poisoning from improperly placed generators or cooking devices.”51 If a cyberattack took out power of a similar magnitude and duration of Hurricane Sandy, it is conceivable that an equivalent number of casualties would result. The 2015 synchronized cyberattacks against Ukrainian power companies, attributed to Russia, was the first known example of an offensive cyber operation targeting a state’s power grid. Its cost was ultimately low—service was temporarily disrupted to 225,000 customers for several hours, and energy providers operated at a limited capacity for some time after service was restored.52 There were no reported casualties from this power outage. While any casualty resulting from a cyberattack would certainly be lamentable, even worst-case scenario figures are minor in comparison to the cost in human lives stemming from other, even limited, kinetic military operations.

## AT: Russia Adv

### 1NC – Lasers Alt Cause

#### Russian laser attacks are an alt cause

Matthew Humphries 5/18, has a Bachelor's degree in Computer Science and a Master's degree in Games Development, “Russia Claims Its Peresvet Laser Weapon Can Blind Satellites, Burn Drones”, 5/18/2022, PCMag, https://www.pcmag.com/news/russia-claims-its-peresvet-laser-weapon-can-blind-satellites-burn-drones

Russia claims to have a laser weapon that can blind satellites in orbit around Earth as well as "inflict thermal destruction" on a drone in mid-air from miles away.

As Reuters reports(Opens in a new window), the mobile laser weapon is called Peresvet and was first announced back in 2018 by Vladimir Putin. At a conference in Moscow yesterday, deputy prime minister Yury Borisov stated that a recent test had seen the laser burn up a drone 5km (3 miles) away in just five seconds.

Borisov went on to claim that, "it can blind all satellite reconnaissance systems of a likely enemy in orbits of up to 1,500 km, disabling them during flight due to the use of laser radiation." Perhaps this is how Russia intends to take down Starlink if hacking continues to fail?

Peresvet is apparently being mass produced within Russia and supplied to its troops. If true, it suggests Russian forces may be using the mobile laser system in its war with Ukraine, although there's been no evidence of that presented thus far.

Borisov goes on to claim that "unannounced successors" to the existing Peresvet system are in development and that, "This is primarily a laser weapon, an electromagnetic wideband weapon that will replace (conventional weapons) in the next decade - this is not some sort of exotic idea; it is the reality."

### 1NC – No Attacks

#### Russia won’t attack satellites out of fear of nuke war

Nancy Gallagher 20, Director at the Center for International and Security Studies at Maryland, published 05-2020, “Space Governance and International Cooperation”, CISSM /billy

When applying the Strategic Stability logic to space, most U.S. defense analysts are missing the biggest reason why the United States should be willing to go beyond dialogue, transparency, and voluntary norms to stronger, more reliable forms of security cooperation—the connection to nuclear weapons and terrestrial strategic stability. DOD officials engaged in the space policy reviews have said that the main reason why the Soviets never attacked U.S. satellites was because they believed that would lead to a nuclear war. These officials assume that adversaries will be less inhibited now because the United States would probably respond to most kinds of space interference with non-military or conventional means. In other words, increased nuclear strategic stability has decreased space strategic stability.

### 1NC – No Escalation

#### Russian cyberattacks happening now – cyberattacks against Ukraine prove no escalation

Josephine Wolff 22, an associate professor of cybersecurity at The Fletcher School at Tufts University, March 2022, “Why Russia Hasn’t Launched Major Cyber Attacks Since the Invasion of Ukraine,” Time Magazine, Technology, <https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/>

In the relatively short and rapidly evolving history of cyber conflict, perhaps nothing has been established with greater certainty and more widely accepted than the idea that Russia has significant cyber capabilities and isn’t afraid to use them—especially on Ukraine. In 2015, Russian government hackers [breached the Ukrainian power grid](https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/), leading to widespread outages. In 2017, Russia deployed the [notorious NotPetya malware](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/) via Ukrainian accounting software and the virus quickly spread across the globe costing businesses billions of dollars in damage and disruption. In the months that followed the NotPetya attacks, many people [speculated](https://www.npr.org/2017/06/22/533951389/experts-suspect-russia-is-using-ukraine-as-a-cyberwar-testing-ground) that Ukraine served as a sort of “testing ground” for Russia’s cyberwar capabilities and that those capabilities were only growing in their sophistication and reach.

As tensions escalated between Russia and Ukraine, many people were expecting the conflict to have significant cyber components—the United States Department of Homeland Security even issued a [warning](https://thehill.com/policy/international/russia/595945-cyber-officials-urge-federal-agencies-to-armor-up-for-potential) to businesses to be on high alert for Russian cyberattacks, [as did](https://www.bbc.com/news/uk-60158874) the U.K.’s National Cyber Security Centre. What is surprising is that—so far, at least—the devastating Russian cyberattacks everyone has been expecting have yet to materialize. There’s no guarantee, of course, that a large-scale cyberattack on [Ukraine’s electrical grid](https://time.com/6153039/ukraines-electricity-grid-escape-russia/) or global banks or anything else isn’t just around the corner. Russia has proven time and again that it has few compunctions about targeting critical infrastructure and causing considerable collateral damage through acts of cyber aggression.

But as the invasion continues with few signs of any sophisticated cyber conflict, it seems less and less likely that Russia has significant cyber capabilities in reserve, ready to deploy if needed. Instead, it begins to look like Russia’s much vaunted cyber capabilities have been neglected in recent years, in favor of developing less expensive, less effective cyber weapons that cause less widespread damage and are considerably easier to contain and defend against. For instance, many of the [cyberattacks directed at Ukraine in the past month have been relatively basic distributed denial-of-service attacks](https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces/), in which hackers bombard Ukrainian government websites and servers with so much online traffic that those servers cannot respond to legitimate users and are forced offline for some period of time. Denial-of-service attacks can be effective for short-term disruptions but they’re hardly a new or impressive cyber capability—in fact, they’re what Russia used to target Estonia more than a decade ago in 2007. Moreover, launching these types of attacks requires no sophisticated technical capabilities or discovery of new vulnerabilities, and they typically have fairly contained impacts on the specific, targeted computers. Similarly, recent reports that Belarusian hackers are [trying to phish European officials](https://www.cyberscoop.com/ghostwriter-phishing-refugees-nato-russia-ukraine/) using compromised accounts belonging to Ukrainian armed services members suggests that not only are these efforts relying on fairly basic tactics like phishing emails, they are not even being carried out by Russian military hackers directly.

### 2NC – No Escalation – Generic

#### No cyber escalation

Erica D. Borghard 19, assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University; and Shawn W. Lonergan, research affiliate of the Army Cyber Institute at the United States Military Academy at West Point, Ph.D. in Political Science from Columbia University, Fall 2019, “Cyber Operations as Imperfect Tools of Escalation,” Strategic Studies Quarterly, Vol. 13, No. 3, p. 122-145

There are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. If cyberspace is in fact an environment that generates severe escalation risks, why has cyber escalation not yet occurred? We posit that cyber escalation has not occurred because cyber operations are poor tools of escalation. In particular, we argue that this stems from key characteristics of offensive cyber capabilities that limit escalation through four mechanisms. First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important tradeoffs for decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation—responding to a cyber incident with noncyber, kinetic instruments—is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential of offensive cyber operations.

#### Quick timeframes are a neg warrant---defenders can patch vulnerabilities within minutes, but escalation requires attackers to have sustained access---those defensive pauses prevent cyber-space escalation and allow decisionmakers to defuse crises

Erica D. Borghard 19, assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University; and Shawn W. Lonergan, research affiliate of the Army Cyber Institute at the United States Military Academy at West Point, Ph.D. in Political Science from Columbia University, Fall 2019, “Cyber Operations as Imperfect Tools of Escalation,” Strategic Studies Quarterly, Vol. 13, No. 3, p. 122-145

Third, these limitations become even more salient when we consider how strategic interactions are likely to play out over time during repeated crisis interactions. Because the virtual domain is changeable in a way that the physical world is not, actions taken by defenders in the context of a crisis can radically and unpredictably alter an attacker’s ability to deliver and sustain effects against a target over time.30 Access and capabilities are neither guaranteed nor indefinite—they have a shelf life.31 Footholds into a target’s network that were time intensive to develop can unexpectedly disappear as vulnerabilities in a network are patched. Exploits may have a short shelf life as revealing information about them enables targets to identify indicators of compromise (IOCs) and use these to prevent further damage from specific malware strains or quarantine malicious traffic using known malware signatures. An example of the latter is the US Cyber Command initiative, beginning in 2018, to share information about adversary malware by uploading samples to VirusTotal.32 Therefore, a target can “transition from vulnerability (to a particular attack) to invulnerability in, literally, minutes.”33 Third-party disclosure about software vulnerabilities by governments or private actors can also unintentionally precipitate the loss of access as exposure about vulnerability information enables network defenders to take measures to remedy them.34 For instance, the disclosures that began in 2016 by the group Shadow Brokers of purportedly pilfered US National Security Agency exploits and zero days ostensibly put US government accesses at risk.35 Put simply, a vulnerability upon which an access relies may in theory be only one update or disclosure away from being patched.

Thus, in the context of an ongoing crisis interaction between an attacker and defender, the former’s operational tempo is likely to be interrupted by the latter’s behavior, forcing the attacker to devote additional time to find or acquire new vulnerabilities and exploits in the midst of an offensive operation or campaign. As Inglis notes, to succeed in an offensive cyber campaign that unfolds over time, attackers must be able to sustain “the efficacy of tools under varying conditions caused by the defender’s response and the natural variability and dynamism of cyberspace.”36 The ability to build or acquire new accesses and capabilities “in real time” during a crisis is highly limited.37 Indeed, General Paul Nakasone remarked in a January 2019 interview on the radical difference in shelf life between conventional and cyber capabilities:

Compare the air and cyberspace domains. Weapons like JDAMs [ Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict.38

Therefore, as a 2013 Defense Science Board report notes, “offensive cyber will always be a fragile capability” when pitted against network defenders who are “continuously improving network defensive tools and techniques.”39

Each side can take defensive measures to blunt the impact and effectiveness of the other’s access and capabilities—particularly as information about them is revealed. Consequently, strategic accesses and capabilities are likely to become more vulnerable and less reliable over time, shrinking the set of cyber escalatory response options for all parties. This cycle is likely to generate temporal breaks in the pace of adversarial engagements in cyberspace, where states must regroup and develop or rebuild accesses and capabilities during an ongoing interaction. These pauses are likely to diffuse the pressure that typically accompanies—even defines—crisis situations, creating breathing space and, by extension, room for decisionmakers to deliberate alternative courses of action, for domestic political tensions to cool down, for intent to be communicated to adversaries, and for de-escalation pathways to be determined.

A potential counter to this argument is that most states likely already appreciate the time and resources required to develop accesses and tools, as well as their fragility. Therefore, those with sufficient resources are incentivized to alleviate these concerns through investing heavily in developing the ability to gain pre-positioned accesses and a range of capabilities and platforms to be prepared for the onset of a potential future crisis. Evidence of this kind of behavior could be, for example, the discovery of Russian malware in US critical infrastructure reported in 2018.40 While dormant access is almost certainly the case, states are likely to remain stymied by inadvertent or deliberate discovery of these efforts prior to a crisis. More importantly, even if pre-positioned accesses and capabilities are available in the opening moments of a crisis, the difficulties of maintaining them during iterated volleys between adversaries are likely to persist and blunt the ability of a given party to continue escalation of cyber capabilities.

### 2NC – No Escalation – Tech Barrier

#### Cyber weapons have to be uniquely tailored to each target---escalation can’t happen because the time pressure of a crisis doesn’t allow adversaries to gain access and deploy cyber capabilities

Erica D. Borghard 19, assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University; and Shawn W. Lonergan, research affiliate of the Army Cyber Institute at the United States Military Academy at West Point, Ph.D. in Political Science from Columbia University, Fall 2019, “Cyber Operations as Imperfect Tools of Escalation,” Strategic Studies Quarterly, Vol. 13, No. 3, p. 122-145

Second, in addition to being dependent on access, offensive cyber capabilities lack universal effectiveness. While nuclear or conventional munitions are target agnostic—in most cases, the same munition can be used to target an aircraft hangar, a massed enemy formation, a munitions factory, or a hospital—some cyber weapons must be tailored to a specific target set or type.23 As Martin Libicki notes, “A piece of malware that brings one system down may have absolutely no effect on another. The difference between the two may be as simple as which patch version of a piece of software each system runs.”24 The 2017 WannaCry ransomware attack that wreaked billions of dollars in damage and was attributed to North Korea’s Lazarus Group, for instance, targeted hundreds of thousands of computers around the world across a range of industries that were running an older version of Windows.25 The widespread damage belies the highly specific and targeted nature of the malware—almost all of the affected systems were running a version of Windows 7; the same strain of malware had no effect on computers running more up-to-date operating systems. Moreover, asset owners of targets of strategic significance—such as critical infrastructure—typically employ highly customized software and specific hardware with tailored configurations that are unique to those systems and usually only intimately understood by the original developers and manufacturers. It has been reported, for example, that the malware employed in the Stuxnet cyberattacks against the Iranian nuclear program was tailored to target the specific model of Siemens programmable logic controllers (PLC) used at the Natanz enrichment facility.26 Indeed, while Stuxnet was discovered in computers around the world, it delivered destructive effects only against the centrifuges in Natanz.27 The non-substitutability of entire classes of offensive capabilities by definition increases the cost of developing an arsenal of offensive cyber capabilities.28

Therefore, the time and resource requirements to gain access and develop specific offensive capabilities may render important escalatory response options infeasible or impractical at the desired time. Operational planning and execution must consider that a given capability may not be usable or even exist at a chosen time of employment.29 As the above discussion illustrates, many of the target sets that would represent strategic (and therefore escalatory) targets, such as a state’s critical infrastructure or nuclear command and control, demand extensive planning, pre-positioning, and capability development in advance of employing offensive capabilities. Therefore, the timing of a crisis plays a crucial role in decisions about cyber escalation responses. Specifically, the time required to develop access to hold strategic targets at risk means that, even if a state seeks to escalate against an adversary using cyber means, it may find itself limited by the accesses and capabilities it possesses at the moment a crisis occurs. Cyber response options may be limited to less decisive or more vulnerable target sets, rather than those that are more strategically significant.

### 2NC – No Escalation – Attribution

#### Lack of attribution is a neg warrant---nobody will escalate randomly before they’ve attributed an attack, and that time delay builds in opportunities for de-escalation

Erica D. Borghard 19, assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a research fellow at the Saltzman Institute of War and Peace Studies at Columbia University; and Shawn W. Lonergan, research affiliate of the Army Cyber Institute at the United States Military Academy at West Point, Ph.D. in Political Science from Columbia University, Fall 2019, “Cyber Operations as Imperfect Tools of Escalation,” Strategic Studies Quarterly, Vol. 13, No. 3, p. 122-145

Second, beyond operational requirements for secrecy, states make political decisions to eschew attribution for offensive cyber operations.64 States employ technical methods to avoid attribution (e.g., obfuscating points of departure of attacks by using spoofing, proxy servers, third-party infrastructure, compromised certificates, and other anonymizing capabilities) as well as make deliberate efforts to obscure command and control for cyberattacks (e.g., using cyber proxies with varying degrees of plausible deniability).65 The time requirements for a targeted state to achieve attribution at a reasonable confidence threshold, as well as its willingness to share potentially sensitive intelligence information with allies or domestic publics to justify any escalatory responses, create additional temporal breaks for the pressure of a crisis situation to diffuse and for decision-makers to evaluate alternative courses of action.

## AT: Solvency

### 1NC – Article 5 Not Key

#### No internal link – no card is reverse causal and says the plan stops the US from overreacting – the US could respond on its own without activating Article 5.

Ken Jones 15; MS in Cyber Systems and Operations from the Naval Postgraduate School; March 2015; "Cyber War: The Next Frontier for NATO," https://calhoun.nps.edu/bitstream/handle/10945/45201/15Mar\_Jones\_Ken.pdf?sequence=1&isAllowed=y

In light of the recent developments of NATO, it would seem to be in NATO’s best interest to remain ambiguous and allow the organization to approach its response to a cyber-attack on a case-by-case basis. For instance, the attacks on Estonia might require intervention on behalf of the Estonian people due to the fact they are a smaller, lesser defensible state. Estonia would not be successful standing up against Russia, and as Russia becomes more aggressive in the former-Soviet bloc region, small states like Estonia are at risk. If another attack were to occur against Estonia, the attacks would have to be more severe to invoke an Article 5 response. Such a response would enable NATO states to act as if they too have been attacked as per the mutual defense announcement against cyber-attacks at the Wales Summit. Yet, if the United States is attacked in a similar manner, there likely does not need to be the same scale of defense taken, because the United States has more resources and capabilities to respond on its own. Remaining ambiguous allows NATO to choose the best opportunities for supporting and defending member states.

### 1NC – Commercial Alt Cause

#### Cyber-vulnerabilities can be inserted at any point in the satellite supply chain and remain latent indefinitely---no way the aff can solve it

David Livingstone 16, associate fellow at Chatham House, was policy lead on Military Aid to the Civil Powers at the UK Ministry of Defence between 1994 and 1999; and Patricia M. Lewis is the research director of the International Security Department at Chatham House, September 2016, “Space, the Final Frontier for Cybersecurity?” <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf>

For a successful cyberattack to occur, the threat vector needs to be inserted within the system. This could take place during the manufacture, distribution or operation of the products and services that characterize the system. During the manufacturing and distribution phases, conventional physical security controls need to be applied to minimize the risk of cyberattacks. However, during operation, the conjunction of electromagnetic and cyber vulnerabilities becomes critical. As telecommunication systems integrate complex technology to improve performance, flexibility and efficiency, they are increasingly dependent on software that can be modified during operation rather than hardware or firmware that remains relatively unchanged once it has been designed and deployed. One example is the C-RAN (Cloud-Radio-Access-Network) concept being developed as part of the evolution of terrestrial mobile networks, and this type of software will be integrated into future satellite systems. Commercial tools such as SIM-toolkits are increasingly used to perform over-the-air provisioning and denial of service. Over-the-air software (both operating system and application) upgrades will be familiar to everyone using smart devices.

The ability to emulate a network, and to access, configure and control communications devices via wireless interfaces during normal operations also offers opportunities to an attacker to launch a large-scale cyberattack that remains latent within a system indefinitely, until activated at a time of the adversary’s choosing.

There exists, therefore, a need to create infrastructure and procedures that allow full system vulnerability assessment to be undertaken and mitigation strategies to be developed, taking into account both electromagnetic and cyber techniques. Such facilities need to be available during the design, development and operational phases. As the internet has become near-ubiquitous, as devices become ever more interconnected and as critical infrastructure becomes more complex, vulnerability to cyberattacks is increasingly becoming the focus of network security, risk management, mitigation and resilience techniques. A multidisciplinary approach to vulnerability assessments and the design and implementation of mitigation strategies is required, while cybersecurity and wireless professionals alike require both greater awareness and sophisticated tools. Assuring the space-based capability must be the principal driver of the agenda. The industry needs to take stock of the GNSS vulnerabilities and develop pragmatic approaches to countering them,41exploring and adapting new technologies, and building in redundancies.42 This will include ascertaining the prevalence of unintentional jamming and interference, and how jamming and spoofing play out in the realm of offensive state-initiated cyberattacks or may be used by terrorist groups.

### 1NC – Cyber Norms Fail

#### Cyber governance fails to stop risks to satellites---tech changes too fast and offensive capabilities are too diffused

David Livingstone 16, associate fellow at Chatham House, was policy lead on Military Aid to the Civil Powers at the UK Ministry of Defence between 1994 and 1999; and Patricia M. Lewis is the research director of the International Security Department at Chatham House, September 2016, “Space, the Final Frontier for Cybersecurity?” <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf>

• Cyberattacks on satellites can include jamming, spoofing and hacking attacks on communication networks; targeting control systems or mission packages; and attacks on the ground infrastructure such as satellite control centres. Possible cyberthreats against space-based systems include state-to-state and military actions; well-resourced organized criminal elements seeking financial gain; terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions; and individual hackers who want to fanfare their skills.

• Space is changing from a selective preserve of wealthy states or well-resourced academia, into one in which market forces dominate. Current technologies bring space capability into the reach of states, international organizations, corporations and individuals that a decade ago had no realistic ambition in this regard; and capabilities possessed a few years ago only by government security agencies are now in the commercial domain.

• The pace at which technology evolves makes it hard, or even impossible, to devise a timely response to space cyberthreats. Humans too are affected by ‘digital ageing’ and legacy issues, and younger people use space-based and cyber communications in ways that make it difficult for older generations – and thus by implication some senior decision-makers – to fully understand the range of technologies and threats.

• Technology alone cannot provide the basis for policymaking on cybersecurity. Entirely or largely technological approaches do not have the breadth or depth to allow comprehensive participation, and would exclude many stakeholders who could otherwise contribute usefully to responses to the variety of threats propagated through the internet.

• Development of a flexible, multilateral space and cybersecurity regime is urgently required. International cooperation will be crucial, but highly regulated action led by government or similar institutions is likely to be too slow to enable an effective response to space-based cyberthreats. Instead, a lightly regulated approach developing industry-led standards, particularly on collaboration, risk assessment, knowledge exchange and innovation, will better promote agility and effective threat responses.

• An international ‘community of the willing’ – made up of able states and other critical stakeholders within the international space supply chain and insurance industry – is likely to provide the best opportunity to develop a space cybersecurity regime competent to match the range of threats.

### 2NC – Cyber Norms Fail

#### Attribution’s impossible---means the plan’s norm can’t be enforced

Kenneth Lieberthal 12, director of the John L. Thornton China Center and senior fellow in Foreign Policy and Global Economy and Development at Brookings; and Peter W. Singer, director of the 21st Century Defense Initiative and a senior fellow in Foreign Policy at Brookings, February 2012, “Cybersecurity and U.S.-China Relations,” https://www.brookings.edu/wp-content/uploads/2016/06/0223\_cybersecurity\_china\_us\_lieberthal\_singer\_pdf\_english.pdf

Beyond just the issue of terminology, however, there are also other dimensions in the cyber arena that are especially consequential to U.S.-China relations and must inform any process aimed at engagement. Put simply, in this dynamic arena, it is necessary to be realistic about what types of activities can potentially be brought under control through agreed-upon actions and what things are effectively beyond the capacity of institutions to control. It is important to appreciate why this is so and, in that context, to focus on those areas that are still potentially subject to meaningful controls. Perhaps the most difficult is the problem of attribution.41

The ability to capture the operations of another computer and use it to launch activities that its owner does not intend and might even be unaware of (described inside the field as to “pwn,” a computer hacker term meaning to “own”) is very well developed and widely used. This often takes the form of creating botnets that link unrelated computers and enable the controller to leverage their combined computing and communications capabilities for a particular purpose. The resulting network of secretly linked devices can easily grow to extraordinary dimensions. For example, three not terribly sophisticated Spaniards allegedly created a global botnet that included over twelve million computers.42 In other cases, a controller may seek to capture and leverage only one or a small number of computers. In this case, the major purpose is more likely to be to conceal the controller’s identity.

Three key features of this capability to capture and utilize other computers are particularly important. First, there are no geographical limits. For example, a pernicious actor in Brazil can compromise computers in Russia and South Africa to launch attacks on systems in China (one can substitute almost any countries for the ones named here). Second, the owner of a captured computer typically has no idea that the computer is being used by a remote actor for pernicious purposes. And third, when some pernicious activity is perpetrated, sophisticated analysis can typically, at best, identify the computer being used to launch the attack. It is far more difficult to determine whether that computer is, in turn, being remotely controlled and, if so, by whom. Equally, even if it is not being remotely accessed, in many situations (such as a computer being used at a university or an internet café), it will be difficult to determine who the individual behind the computer is, or even what his nationality is or what organization he actually represents. Such information would be crucial in a crisis but is rarely available in a timely manner. In short, it is typically not feasible to identify the underlying command structure behind an attack with complete certainty. Instead, painstaking forensics may be a key driver to understanding the full chain of events.

It does not take much imagination to see how pernicious the resulting problems can be. Since many are inclined to assume that the Chinese government is behind most insidious activities that are launched by computers located in China, for example, bad actors elsewhere may be inclined to capture Chinese computers to use in their activities, and vice versa for the U.S. This same logic, though, also enables Chinese bad actors to deny responsibility, arguing that activities launched from China almost certainly are being perpetrated by others who want to take advantage of the widespread suspicions of China. And the same type of misdirection can be argued regarding computers physically located inside the U.S.

The issue of attribution is further complicated by the difficulty of establishing complicity. An effort might be attributed to an actor emanating from a certain geographic locale, but it is even more difficult to establish a formal role of a government as perpetrator or sanctioner of the operation. That is, the situation often parallels that of maritime security in centuries past, where the lines between what was criminal piracy and what was state-sanctioned privateering often proved fuzzy.43 There have been frequent reports of “patriotic hacker” communities and other non-state groups, including student and even cyber criminal groups that have been mobilized by their governments for such purposes of deniable, but directed, attack.44 Thus, in certain cases where the local state government may be needed to investigate and then prosecute those behind questionable cyber activity, the victims perceive that some elements of the state are actually a willing accomplice or planner of the attack, and thus unlikely to assist. An example would be the DDoS attacks on Estonia. Many believed Russian security services actually instigated them and thus that Russia was certainly not interested in finding and stopping the perpetrators.45

Attribution is further complicated by the fact it is quite difficult initially to determine even whether a packet is intended to be “hostile” or not (as one expert put it, “Packets are not like ICBMs”). A DNS query, for instance, may be a legitimate look up attempt or it may be an attempted penetration. And, even in the latter case, it may be a legitimate DNS lookup or it may be part of a large scale DDoS attack. On top of this, once malware enters into a system, it does not necessarily bear a telltale sign of where it was designed and sometimes even what its actual intent may be. Unlike fissionable materials, for example, where each nuclear reactor has a distinctive “signature” that typically permits tracking the origins of the material, even when malware is uncovered it usually does not point a finger at a particular culprit.

The long-running effort to figure out the origin and intent of the Conficker worm illustrates this problem. The worm was one of the most effective in recent history, assembling a global botnet of some 7 million compromised computers in networks that ranged from the British Parliament to Southwest Airlines to the French and German military to scores of computers in China (one security expert called it “the Holy Grail of a botnet”). Yet, even as the worm spread, investigators could only sift through the data for clues to its origin, which still left them uncertain. In one breakthrough, they found certain programming linked to a Ukrainian language keyboard. But, even then, they could not conclude whether this meant the malware was designed in Ukraine or whether the clue was a clever attempt at misdirection.46

### 1NC – Kinetic Alt Cause

#### Kinetic attacks more likely in space

Martin BLAŠŤÁK 22; Graduated in Bachelor's degree in International Relations and Diplomacy from the University of Derby. Currently a master's degree in Security Studies at Charles University., Published: 2/15/2022; "The Current Rise of Anti-Satellite Weaponry"; Security Outlines - česko-slovenský portál o bezpečnosti; Accessed: 6-26-2022; https://www.securityoutlines.cz/the-current-rise-of-anti-satellite-weaponry/)//Pen-SY

Though we might still believe that outer space is somewhat out of our reach, the fact is that we are dependent on space technologies in many ways. Their expensive and vulnerable nature makes them a perfect target for those who want to severely disrupt opponents’ communication, coordination, or intelligence activities. As such, several nations are currently equipped with or at least developing means of satellite disposal that range from ballistic missiles to communication jammers. The United States, China, Russia, India, and even Japan and France are looking forward to enhancing their counterspace arsenal to protect their ever more important space assets. Even though the development of ASAT weapons is still in the process, the number of nations capable of in-space operations has increased since the Cold War. The current geopolitical tension provides a catalyst for further incentives for the development of new weapons. Types of ASAT weapons When we talk about anti-satellite weaponry, what usually comes to mind are kinetic physical weapons. The technology behind kinetic weapons is accessible to a greater number of states (as it is based on ballistic weapons already in use) and their use has rather horrifying results, as illustrated clearly by the aftermath of the Fengyun-1C case, which was easily attributed to the Chinese and harmed the environment disastrously for the next few decades or even centuries [1]. In addition to direct ascent missiles, kinetic weapons can also take the form of a co-orbital device – a satellite equipped with a payload (usually explosive) sent to an intercepting orbit with another satellite [2]. The US, China, and India all have some degree of developed, tested, and somewhat operational ASAT kinetic capabilities. For example, the Indian missile test of 2019 (Mission Shakti) or the Chinese 2007 test (Fengyun-1C), which managed to destroy targeted satellites successfully. The US did not declare any official direct-ascent weapons, but it is agreed that their anti-ballistic missile interceptors could be used against enemy satellites. Furthermore, the US would be able to quickly develop dedicated ASAT systems [3].

### 2NC – Kinetic Inevitable

#### Litany of kinetic weapons with natural phenomenon make continuous disruption inevitable

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

2.4 Satellite Network Vulnerabilities Satellites’ transmissions are subject to lengthy delays, low bandwidth, and high bit-error rates that adversely impact real-time, interactive applications such as videoconferences and lead to data corruption, performance degradation, and cyber incursions. Atmospheric and interstellar noise; cosmic radiation; interference from electronic devices; and precipitation and rain absorption in the spectral frequencies employed by satellites impede network performance and information throughput and negatively affect provision of quality of service (QoS) guarantees [22]. Satellite network applications and services are also adversely impacted by geophysical events. In 1998, for example, tremendous explosions on the sun disrupted operations onboard PanAmSat’s Galaxy IV Satellite. As a consequence of these solar flares, digital paging services, bank transactions, and cable television programs across the U.S. were disabled [22]. According to the U.S. GAO (2002), satellite network functions can be compromised by groundbased antisatellite weapons, high-altitude nuclear explosions, stealth micro satellites, space mines, space-to-space missiles, and directed energy space weapons. For instance, as a consequence of intentional jamming resulting from cyber attacks on a Telestar-12 commercial satellite in 2003, U.S. governmentsupported broadcasts promoting regime changes in Iran were blocked by the Iranian Ministry of Post, Telegraph, and Telephone [22]. Satellite-based telephony services in Tehran were also disabled.

### 2NC – Kinetic – Iran

#### Alt causes – Iran’s ballistic missiles are modifications away from ASATs – makes satellite strikes inevitable

Caleb Larson 22 — (Caleb Larson; multimedia journalist and defense writer with the National Interest Published: 1-29-2022; "Does Iran Have Anti-Satellite Missiles?"; National Interest; Accessed: 6-30-2022; https://nationalinterest.org/blog/reboot/does-iran-have-anti-satellite-missiles-199900)//Pen-SY

Here's What You Need to Remember: Iran’s capabilities in space are most effective in denying the space sphere to adversaries, rather than actually controlling it themselves. In 2011, Iran was able to capture an American drone by jamming the drone’s GPS signal and spoofing another GPS signal. After the targeted killing of Iranian General Qassem Soleimani, Iran flexed a bit of its ballistic missile muscle in retaliation, striking several bases in Iraq that housed U.S. troops. Striking a target just across a national border is relatively easy. What is much harder, however, is striking an adversary’s satellites. Could Iran do it? Bombs Away A report from CSIS stated that Iran’s “missile forces [are] a potent tool for Iranian power projection and a credible threat to U.S. and partner military forces in the region.” While referencing Iran’s conventional ballistic missile capabilities, the report fails to mention that Iran’s missile arsenal is fully adequate for reaching satellites of varying orbits. Converting a missile from ground attack to space attack is not necessarily difficult. And space is a ripe target. Satellites are virtually defenseless from strikes by kill vehicles. The United States, and virtually the entire world is dependent on satellites for peaceful reasons like communications, for navigating by GPS—and for violent reasons, like guiding precision-guided munition, or snapping photos from nuclear test sites. One expert on the danger posed by anti-satellite capabilities wrote, “the military applications of ASAT missiles appear fairly obvious. China would seek to use the ASAT missiles to knock out U.S. satellites in order to degrade its C5ISR [Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance and Reconnaissance] capabilities, rendering distributed U.S. military and allied assets unable to communicate or share information.” If enough satellites were knocked out in a conflict scenario, troops would have to dust of the ole map and compass. Still, striking a satellite is no walk in the park—and more complicated that just launching a missile into space. Satellites are small, and some travel along their orbits quite fast. Striking satellites has been compared to hitting a bullet with another bullet. No Mental Limitations Challenges aside, could Iran knock out the United State’s satellites? A Defense Intelligence Agency report acknowledged Iran’s desire to shape the space battlefield. "Iran recognizes the strategic value of space and counterspace capabilities and will attempt to deny an adversary use of space during a conflict.” Iran does also have some capabilities, due to the aforementioned ballistic missile arsenal it maintains: “Because of the inherent overlap in technology between ICBMs and SLVs, Iran’s development of larger, more capable SLV boosters remains a concern for a future ICBM capability. Also, these advancements could be applied to developing a basic ground-based ASAT missile, should Iran choose to do so in the future.” Desire aside, Iran has some practical limitations to deal with: “Tehran states it has developed sophisticated capabilities, including SLVs and communications and remote sensing satellites, but its SLVs are only able to launch microsatellites into LEO [Low Earth Orbit} and have proven unreliable.”

### 1NC – Say No – General

#### NATO will say no–unease over different policies and internal disagreements

Benjamin Silverstein 20, research analyst for the Space Project at the Carnegie Endowment for International Peace, 8/3/2020, “NATO’S RETURN TO SPACE”, War On The Rocks, https://warontherocks.com/2020/08/natos-return-to-space/

The new NATO policy arrives at an unsettled time in space competition, as internationally accepted behavioral norms regarding the use of non-nuclear force in space have not crystalized. Progress in multinational organizations like the Conference on Disarmament has been stymied by profound disagreements, and there is no indication that non-binding measures developed outside multilateral forums would enhance security in space. Absent concrete norms or legal regulations on the use of force in space, some NATO members are pursuing active defenses to protect satellites, and others have demonstrated exoatmospheric capabilities that brew unease about the potential for overt conflict in space. NATO’s adversaries are also seeking advanced counterspace capabilities. For instance, Russia has conducted on-orbit maneuvers that some perceive as hostile, and in April conducted a missile test with anti-satellite applications, which the United States condemned.

### 2NC – Say No – Turkey

#### Turkey will say no–they’ve been undermining NATO’s cybersecurity with troll groups, the last thing they’ll want to do is strengthen it

Nordic Monitor 19, The Nordic Research Monitoring Network (Nordic Monitor) is a non-profit organization that aims to raise awareness of radical and violent extremist trends in Europe and beyond, with a specific focus on patterns that disrupt peace and harmony among community groups, with an emphasis on Turkey, 9/30/2019, “Turkey undermines NATO cyber-army initiative”, https://nordicmonitor.com/2019/09/turkey-undermines-nato-cyber-army-initiative/

As NATO has been working on a counter strategy to neutralize the non-conventional cyber threat that originates from Russia, Iran, China and others, NATO member Turkey has secretly been running a project to undermine the alliance structure from within.

The social media and Internet campaigns run by associates of Turkish President Recep Tayyip Erdoğan harbor anti-NATO and anti-Western sentiments and portray NATO and allies as enemies that are bent on harming Turkey. The most vicious group among various entities that were coordinated by Erdoğan and his office is identified as the Pelican group.

President Erdoğan paid a visit to the headquarters of his troll group Pelican, which is linked to his son-in-law, Treasury and Finance Minister Berat Albayrak. The visit on August 3, 2019 came just after announcements by the US and UK revealing that Turkey’s NATO allies had decided to create cyber-armies to fight against foreign adversaries.

The latest developments, in July, 2019, marked a turning point for Western military strategic planning. Officials from the US and the UK revealed that they had launched new military/intelligence divisions to counter malign Russian activity and threats from technologically sophisticated terror groups such as the Islamic State in Iraq and the Levant (ISIL). According to official releases, the new units will have an offensive and defensive propaganda mandate, taking the social media fight to Russia as well as to various state-sponsored terrorist groups using social media platforms to stir unrest and interfere in the workings of the West.

The US’s National Security Agency (NSA) chief, Gen. Paul Nakasone, announced the new US cybersecurity directorate on July 23 at the International Conference on Cyber Security. In parallel, Lt. Gen. Ivan Jones, the commander of the UK Field Army, said a new army formation of the UK, named 6 Division (6 Div), would widen its net, looking for a new generation of social media skills. To cybersecurity expert Zak Doffman, these structures are as close as we have seen in the West outside the intelligence and private contractor domain to the government-run hacking groups seen in Russia and China as well as in Iran and North Korea.

It is obvious that Erdoğan’s Ak trolls (a speculative term referring to the regime’s social media network) will also be under the surveillance of these divisions because of the alleged links to some terrorist groups. Furthermore, Ak troll strategies are similar to the hybrid threat posed by Russia with its own unique propaganda war and psychological warfare operations targeting the US and its allies.

President Erdoğan’s presence at Bosporus Global, the public face of the Pelican group, was a sign of his support for the hard-core Ak troll group, which benefited regularly from anti-American, anti-Israeli and anti-NATO rhetoric for their propaganda. During the meeting he was informed about the international activities of the Internet trolls as well as their projects, in which social media serves certain regime functions with the goal of protecting Erdoğan’s Islamist authoritarian rule, disseminating false information, promoting anti-Western propaganda and mitigating dissidence.

### 2NC – Say No – Europe

#### The EU will say no–they can’t afford to put China on the backburner

Federica Russo 20, researcher at the university of Amsterdam, 7/15/2020, “Assessing the EU-China relationship in Cyberspace”, EIAS, https://eias.org/publications/op-ed/assessing-the-eu-china-relationship-in-cyberspace/

The global system which is to emerge in the post-pandemic era – ever more connected and digitalised – will lead to the need of reinforced cyber security mechanisms and diplomacy. For example, the Internet of Things (IoT) will significantly expand the frontiers of cyberspace, connecting sensors and actuators within a cyber-physical ecosystem, reaching 100 billion of objects networked by 2025. According to data reported by the independent cybersecurity company McAfee, cybercrimes related to criminals gaining illicit access to personal network costed the world USD 600 billion in 2017, which is up to 0.8% of the global gross domestic product (GDP). However, with the advent of IoT, the economic impact is destined to be even greater because of the extraordinary flow of data which brings challenges in boosting cyberattack capabilities and increasing the scale of the disruption across several sectors with a potential domino effect.

Besides the above-mentioned obstacles, internal coordination can no longer be dissociated from international cooperation and key players such as China and the EU will have to navigate this complex reality and act accordingly. The EU should deepen its ties with China in the framework of a pragmatic cyber partnership to strengthen the dialogue, build mutual trust, improve the sharing of key information to mitigate threats, prompt action in response, enhance law enforcement and shared understanding of domestic cyber policies, as well as identify lessons to learn from. For example, the EU’s General Data Protection Regulation (GDPR) has been object of research in China following the aim of improving the country’s Cyber Security Law on data protection.

Evidently, the world will not benefit from cyber chaos, generated by the spread of disinformation, intellectual property and data theft, or cyberattacks on critical infrastructures. Building a heterogeneous network of partnerships and a constructive dialogue in the cyberspace with China, could also support the European Union in positioning itself as a reliable and stable interlocutor even in the physical domain, where the veil of mistrust among countries – along with societal and economic fractures created by the virus emergency – is altering the equilibrium of the global system. International collaboration and dialogue at the bilateral and multilateral stage will therefore be indispensable.

### 2NC – Say No – Canada

#### Canada will say no–they’re working closely with China over cybersecurity, but the plan puts them on the backburner

Dan Bousfield 17, researcher at the university of western Ontario, 8/2017, “Revisiting Cyber-Diplomacy: Canada-China Relations Online”, ResearchGate, https://www.researchgate.net/publication/319142200\_Revisiting\_Cyber-Diplomacy\_Canada-China\_Relations\_Online

New avenues of Cyber-Diplomacy between Canada and China emerged during US House Intelligence Committee hearings over the Chinese manufacturers Huawei and ZTE Inc. (U.S. Panel, 2012). American concerns about close links between these companies and the Chinese government have led to bans on their products in the American national broadband network (China’s Huawei, 2012). The US government drew upon national security concerns to politicize the Chinese regulation of network effects, forcing Huawei to abandon its expansion into the American market and to look instead toward Europe (Pfanner, 2012). Protectionism through national security is not new, and cyber threats can be used to undermine the liberal commitments to trade (seen most recently in the tensions following the US election). However, as a middle power in the postwar era, Canada has long been able to leverage its autonomy to facilitate greater coordination and cooperation between states. In the past this was linked to the cultivation of a strong Pearsonian peacekeeping mythos. However, increasingly, Canada has characterized its geopolitical image in terms of commerce and finance (Bousfield, 2013). The Cyber-Diplomacy of Canada’s support for the Chinese ICT industry presents new avenues for expanded engagement. In particular, despite Canadian involvement in North American security arrangements, the Canadian government has been much more willing to work with Chinese ICT firms to foster the image of being a ‘Silicon Valley North’ and it has worked closely with Chinese ICT providers. In addition, Huawei recently sponsored a report from the Economist Intelligence Unit on the extent to which countries were ICT globalized, ranking Canada in the top 10 (The ICT Globalisation Index, 2014). It is important to note that the report highlighted how cyber-security was not a primary concern in the relationship between developing and developed countries, and that ICT globalization also required support for ICT R&D, for which Canada was ranked first (The ICT Globalisation Index, 2014). Thus, there are opportunities for network efforts to facilitate ICT globalization despite geopolitical security concerns, and ways for middle-power countries such as Canada to mobilize their ICT strengths.

The impact of network effects and ICT development in Canada establish a foundation for parallels with China while establishing the importance of the academy in facilitating non-state 1054 D. Bousfield diplomacies. This stems from what Marshall Beier has characterized as the struggles of Canadian autonomy—namely, the tension between adopting independent policy positions while also being overshadowed and influenced by closeness to the American hegemon (Beier, 2005). Specifically, Canada’s longstanding cooperation in the ‘Five Eyes Intelligence Community’ and the 1946 UK/USA intelligence agreement has meant that Communications Security Establishment Canada has remained heavily classified and thus largely unable to engage in public debates about cyber issues (Cox, 2012). As Barry and Bratt have described, Canada’s security strategies are a ‘defense against help’, that is, doing enough to prevent the United States from acting unilaterally on Canada’s behalf (Barry & Bratt, 2008). This situation also explains Canada’s limited funding to securitize cyberspace, its delay in formulating a cyberpolicy framework, and its relative lack of transparency about its cyber policy options (Levin, Goodrick, & Ilkina, 2013; Van der Meulen, 2013). Secrecy, combined with Canada’s desire to preserve market autonomy in the face of American ICT network effects, has produced an oligopolistic ISP market with close ties to government interests. Because the government’s goals have been determined by the national interest in responding to global market forces, discussions in Canada about user actions and social preferences have fallen to non-state forums.

Cyber-Diplomacy in China remains defined by strong state centralization and efforts to pursue regulation through traditional diplomatic forums. Whereas Canada’s middlepowerdom has been characterized by a reliance on American security mechanisms, China is increasingly using traditional sites of diplomacy, such as the UN, to pursue its right to manage internet access. Proposals from China, Russia and Tajikistan have utilized intergovernmental forums to push for acceptance of circumscribed internet rights and efforts to push private governance of the internet web addresses (through the Internet Corporation for Assigned Names and Numbers) into systems of governance more directly controlled by nation states (General Assembly, 2011). The legitimacy of the UN system, combined with the justifications for sovereign control of the amorphous security threats online gives China wide latitude to institute Cyber-Diplomacy as it chooses. One common impact is China’s ability to enforce the removal of references to the GFC from UN publications and literature, exposing the susceptibility of Other Diplomacies to hierarchical governance (Deibert, 2012b). Yet, as Montsion argues, China’s ability to access non-traditional economic actors such as Canadian indigenous groups over the internet also speaks to challenge Other Diplomacies can pose to states (Montsion, 2016). Given that Canada and China have several regions defined by graduated sovereignty, the significance of Other Diplomacies is likely to continue. As the Hong Kong protests demonstrated, the ability to constrain the horizontal capabilities of the internet is a complex relationship between nationalism, regulatory capacity and local resistance.

### 2NC – Say No – Germany

#### Germany will say no–they want to cooperate with China over cybersecurity to improve their economy, but the plan puts them on the backburner

Wendy Wu 15, writer for South China Morning Post , 11/9/2015, “Handshake to end the hacking: China and Germany pledge for peace in cyberspace by 2016”, South China Morning Post, https://www.scmp.com/news/china/diplomacy-defence/article/1877288/china-and-germany-aim-reach-commercial-cyberspying-deal

China and Germany aim to wrap up a deal over commercial cyberespionage as early as next year, according to German ambassador to China Michael Clauss.

The two countries had agreed to start negotiating an agreement to abstain from such activity when Chancellor Angela Merkel visited China at the end of last month, Clauss said.

The aim was to sign the deal at the next Sino-German intergovernmental consultations in Beijing in the first half of 2016, he said, adding that the agreement would cover not only the cybertheft of intellectual property, but also data security.

"Such an agreement would also help to promote bilateral innovation cooperation, such as on Industry 4.0 and Made in China 2025," said Clauss, referring to the two countries' development strategies for their manufacturing sectors.

He said private companies and in particular small and medium-sized firms were important drivers for Germany's Industry 4.0 strategy, and that China was hoping to involve more German technology companies in its market.

"Improving data security and removing obstacles to moving data internationally would be important steps to enhance Sino-German cooperation on innovation," Clauss said.

The talks are the latest efforts by China to end a years-long turf war with Western countries, particularly the United States, over cyberattacks on the business and governmental sectors.

Read more: 'I indicated it has to stop': Obama gets tough on cyberspying as new China-US pact agreed against threat of sanctions

In September, US President Barack Obama hinted he was considering sanctions against Chinese institutions and individuals suspected of perpetrating cyberattacks against commercial targets.

At the time, Chinese officials said China was itself a victim of such attacks and denied the country had any cyberattack forces.

Shortly afterwards, during President Xi Jinping's state visit to the US in late September, Obama said the two countries had reached "a common understanding" against cyberespionage and agreed to "promote international rules of the road for appropriate conduct in cyberspace".

During Xi's trip to Britain a month later, the two countries agreed to establish a "high-level security dialogue" on issues such as cybercrime.

They also agreed "not to conduct or support cyber-enabled theft of intellectual property or trade secrets of confidential business information with the intent of providing competitive advantage".

Business executives are concerned that a lack of progress on protection of property rights, market access and data security as well as slow internet speeds will dissuade foreign investors from entering China and may hurt the business of those already established.

Clauss said internet speeds in China were a frequent gripe of German entrepreneurs and needed to be addressed.

Wang Yiwei, the director of the Centre for European Studies at Renmin University, said that the internet was "key for reindustrialisation" efforts.

"Cooperation and innovation requires a consensus on cybersecurity", he said.

"Cybersecurity is becoming a prominent issue. Internet hackers and infringement have hurt mutual trust between countries and hindered trade and investment," said Wang.

### 1NC – Shift

#### Countries shift to other ASATs – aff doesn’t change motive.

Kelsey Atherton 18; defense technology journalist for C4ISRNET, Fifth Domain, Defense News, and Military Times; 4/17/18; "Understanding the players, tactics for a possible war in space," https://www.c4isrnet.com/c2-comms/satellites/2018/04/17/understanding-the-players-tactics-for-a-possible-war-in-space/

Not With Sticks And Stones

A war in orbit could be fought from the ground, between satellites, or even in cyberspace. Weapons are categorized first by their relation to space. “Direct ascent” weapons are launched from sea, air, or the ground below orbit into orbit to destroy targets. “Co-orbital” capabilities are objects designed to be already placed in orbit, which might someday attack other objects in orbit. As for means of attack, those range from direct energy (lasers) to electronic warfare (jammers) to cyber means (the fifth domain in the fourth domain).

The distribution of these means is not even across space powers. China, Russia, and the United States are all identified as having both some possible co-orbital capability as well as direct ascent weapons, with both Russian and the United States also featuring known electronic warfare capabilities. Russia alone has a long-running program of directed energy weapons for counter-space, giving it the most diversified counter-space arsenal.

### 2NC – Shift

#### They could even strike ground stations.

Harrison '17 [Todd; October 2017; director of the Aerospace Security Project and the director of Defense Budget Analysis at CSIS, et al; "Escalation & Deterrence in the Second Space Age," https://www.csis.org/analysis/escalation-and-deterrence-second-space-age]

Rather than attacking the satellites on-orbit, an adversary could achieve similar effects by attacking the ground stations that support them. Ground stations are perhaps more vulnerable to attack, because they are often highly visible, located in foreign countries, and relatively soft targets. For military communications satellites, the data transmitted to and from forward-deployed users is often sent via satellite to a teleport ground station, where it is relayed through another satellite or terrestrial networks to users around the world. To reduce the dependence on ground stations, some military space systems use inter-satellite links to transmit data directly between satellites without passing through an intermediary ground station.

Ground stations are vulnerable to kinetic physical attack by several means. Guided missiles and rockets can be used to attack ground stations from range, while rocket-propelled grenades and small arms fire can be used to disable ground station antennas at close range. Ground stations can also be disrupted by attacking the electrical power grid, water lines, and the high-capacity communications lines that support them. While attacks against ground stations could have large implications, the effects would not be permanent. Unlike satellites, which require years to build and often cannot be repaired once they are launched, ground stations can be repaired in a matter of days or weeks, depending on the level of damage incurred.

#### Satellites are primarily attacked by targeting ground infra, AND targeting individual ones can’t cause their impacts

Sandra Erwin 5/19, covered the military, the Pentagon, Congress and the defense industry for nearly two decades as editor of NDIA’s National Defense Magazine and Pentagon correspondent for Real Clear Defense, 5/19/2022, “U.S. Space Force to step up protection of satellite ground systems in the wake of Russia’s cyber attacks”, Space News, https://spacenews.com/u-s-space-force-to-step-up-protection-of-satellite-ground-systems-in-the-wake-of-russias-cyber-attacks/

Almost three months into the war in Ukraine, it’s still too early to draw conclusions about Russia’s capabilities to disrupt satellite-based communications but one clear takeaway is the importance of protecting the ground systems and network user equipment that provide many entry points for cyber attackers, a senior U.S. Space Force official said May 19.

Space Force Lt. Gen. B. Chance Saltzman, deputy chief of space operations for nuclear and cyber, said he has been briefed on the details of Russian cyber attacks aimed at Ukrainian users of satellite internet services. “One of the observations that I would offer on that is that, if you think the only way to dismantle space capabilities is by shooting down satellites, you’re missing the bigger picture … as these cyber attacks are on ground networks,” Saltzman told reporters at a Defense Writers Group breakfast meeting.

The U.S. State Department last week formally blamed Russia for a late February cyberattack on Viasat’s KA-SAT satellite internet network. The attack disabled user terminals in Ukraine and across Europe that provide internet services to private citizens. Viasat said the satellite itself was not targeted and the attack affected 40,000 user terminals, a small fraction of the hundreds of thousands of customers of the network. Viasat said services have since been restored.

Separately, Elon Musk tweeted this month that Russian hackers have been trying to take down SpaceX’s Starlink broadband service the company is providing in Ukraine.

If the ground infrastructure that supports satellites becomes the main target, it will be important to have “assured networks that are defended by cyber professionals, or we’re not going to be effective in accomplishing our missions,” Saltzman said. “I think that’s a critical point that we’ve learned from this environment.”

Lt. Gen. Stephen Whiting, commander of the U.S. Space Force’s Space Operations Command, told SpaceNews last month that the most likely form of attack facing satellite networks today does not happen in space but on the ground. “Cyberspace is the soft underbelly of our global space networks,” said Whiting.

In response, the Space Operations Command is retraining cybersecurity specialists who protect desktop systems at Space Force bases to more demanding roles defending military satellite networks.

Saltzman said more time will be needed to evaluate the events in Ukraine as the conflict grinds on. “As a history major from Boston University, I will say some of these things take time and perspective to really draw the lessons. However, there’s clear observations that you can’t ignore.”

He said one of those observations is that satellite services today are nearly impossible to disrupt completely because of the large numbers of satellites that are now operating in orbit, Saltzman said, echoing comments made last week by the Space Force’s vice chief of space operations Gen. David Thompson.

“The commercial capabilities that have been given to the Ukrainians, those are in proliferated constellations like Starlink, and we’re seeing the value,” said Saltzman. Proliferated constellations are “very hard to deny, because it’s such a widespread set of targets. You can’t just jam one satellite and achieve that effect.”

### 1NC – Solar Flare Alt Cause

#### Various extreme space weather conditions makes satellite disruption inevitable

Dan Swinhoe 21 — (Dan Swinhoe; News Editor at Datacenter Dynamics, Published: 5-7-2021; "Just how resilient are satellites?"; No Publication; Accessed: 6-26-2022; https://www.datacenterdynamics.com/en/analysis/just-how-resilient-are-satellites/)//Pen-SY

Assuming a satellite survives the launch and calls home without any troubles, it faces a consstant battle for survival out in the harshness of space. Even Earth satellites in low orbits can see temperature swings of minus 50°C (-58°F) to plus 50°C (122°F) every 90 minutes, which can have a big effect on the equipment onboard, as can the lack of air. “Materials that you thought were quite solid can actually have some liquid or gaseous components which can leave into the vacuum of space, changing the properties of the material and causing it to shrink or become brittle,” says Andy Vick, head of disruptive technology at RAL Space. Space weather is another major contributor to satellite failures. Many of these bus-sized, multi-ton satellites are out in GEO, thousands of miles from Earth where there is little atmospheric protection from extreme conditions and large amounts of radiation. And the void can be surprisingly active and unpredictable when it comes to weather. X-rays, ultraviolet rays, radiation, and geomagnetic storms can all wreak havoc on-board; components can be damaged by the high current that discharges into the satellite or damaged by high-energy particles that penetrate the satellite. Space dust – literally tiny particles of rock dust – can hit the sats and become plasma and damage equipment. Sun Outages, where the satellite passes in front of the Sun, don't harm the satellite. However, the sun's interference swamps the signal from the satellite, causing a loss of data. These outages affect the signals from geostationary satellites, and can last for around ten minutes a day during the Equinox - but they are predictable. The University of Reading recently recorded the first ‘space hurricane’ which it described as a ‘1,000km-wide swirling mass of plasma raining electrons several hundred kilometers above the North Pole.’ The most notorious space weather event was the Carrington Event, a solar flare in 1859 that caused auroras as far south as the Caribbean, woke people in the night thinking it was morning, and caused telegraph lines to fail. Smaller events in 1989 caused blackouts and communication failures. A Carrington-level event today would cause worldwide electronics failures, and could wipe out all the satellite networks of the world if action wasn’t taken ahead of time. In a disaster report, space insurance consortium Atrium warned a single anomalously large proton flare or a number of flares in quick succession from our sun could result in a loss of power to all satellites in geosynchronous orbit and cost billions of dollars to fix. Dr. Holger Krag, head of the Space Safety Programme Office for the European Space Agency, tells DCD there is little that can be done to protect satellites from the impact of a solar flare beyond turning off key electrical systems ahead of time. But the unpredictable nature of the sun can make this a difficult task. To better predict coronal ejections from the sun and provide more notice about potential space weather events, the ESA has planned a mission called Lagrange, where spacecraft will be positioned at "Lagrange points", where the gravity of the Earth and Sun balance providing stable locations to observe the sun’s activity a few days ahead of the Earth’s position. “From [the L5] position, it can see the surface of the sun that would turn towards Earth three days later. We can see an advanced view of the activity area on the sun as it’s rotating around its axis towards the Earth,” says Dr. Krag. “At the same time, you can have a side view on the line between Earth and Sun so it can see coronal mass ejection traveling from the Sun to the Earth and it can measure the velocity of the ejections."

### 1NC – Terror Alt Cause

#### Too many groups can cyber-attack satellites---terrorists certainly have the capability to inflict catastrophic damage

David Livingstone 16, associate fellow at Chatham House, was policy lead on Military Aid to the Civil Powers at the UK Ministry of Defence between 1994 and 1999; and Patricia M. Lewis is the research director of the International Security Department at Chatham House, September 2016, “Space, the Final Frontier for Cybersecurity?” <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf>

Cyberthreats against space-based systems may be classified as follows:

• States setting out to create military advantages in space, or seeking to steal strategic quantities of intellectual property and having sufficient computing power to crack encryption codes, for example;

• Often well-resourced organized criminal elements seeking financial gain;

• Terrorist groups wishing to promote their causes, even up to the catastrophic level of satellite collisions with space debris including a cascade of collisions – called the Kessler Effect,23 denying the use of space for all actors;

• Individual hackers who simply want to prove and fanfare their skills;

• Any combinations of the organizations and individuals above.

And their methods would be:24

• Jamming, spoofing and hacking attacks on, for example, communication networks, by using space infrastructure;

• Attacks on satellites, by targeting their control systems or mission packages, perhaps taking control of the satellite to exploit its inherent capabilities, shut it down, alter its orbit (perhaps thereby ‘weaponizing’ it), or ‘cook’ or ‘grill’ its solar cells through deliberate exposure to damaging levels of highly ionizing radiation;

• Attacks on the ground infrastructure, such as satellite control centres, the associated networks and data centres, leading to potential global impacts (for example on weather forecasting systems, which use large quantities of space-derived data).

International cooperation will be crucial in any response to space-based cyberthreats, and is at the heart of current debates, for the following reasons:

• Large numbers of satellites orbit the Earth, traversing all territories, and their uplinks and downlinks are transmitted via ground stations from all around the world;

• These satellites are used worldwide, whether for communications, Earth observation or precise navigation and timing capabilities;

• Satellites are built with components from an internationalized supply chain.

Space is thus no longer a technological playground for the privileged few countries involved in sending humans to the moon, spying on others or putting communications leviathans into geostationary orbit.

For some states, there is still the simple allure of national prestige to be gained by entering the space race, with the successful launch of a sovereign vehicle being seen as a demonstration of technological achievement. More importantly, however, an ever increasing number of countries and private enterprises are commissioning satellites or buying timeshares in satellites for an equivalent number of reasons; and market forces and technological advances are leading to lower-cost launches, smaller and more reliable satellites, and satellite constellations that can provide aggregated capability. As service providers become more aware of how space can be used, they are looking to satellites to deliver reliable, cheap and persistent capabilities that support commercial enterprises.

### 2NC – Terror Alt Cause

#### Space privatization inevitable – lowers costs

Ashna Mehmood 21 — (Ashna Mehmood; Student of International Relations at National Defence University, Islamabad, Published: 8-9-2021; "Terrorism in Space: A Possibility"; Vol. 9 No. 1 (2021): A Journal of Strategic Studies; Accessed: 6-20-2022; http://journal.ciss.org.pk/index.php/ciss-insight/article/view/204)//Pen-SY

The Emergence of New Actors in Space The sixty-year-old paradigm of state-led agencies dominating the space is slowly experiencing a shift. The space sector faces a swarm of privately owned companies that wish to invest in the billion-dollar industry. From providing services and equipment for space missions to space launchers, human spaceflight, space tourism, and asteroid mining. These companies are working to develop easier, cheaper, and faster ways to access the space.16A few examples of these companies are SpaceX, Scaled Composites, Blue Origin, Virgin Galactic, Bigelow Aerospace, and the Sierra Nevada Corporation.The increase in investment in space programs has led to what one might call the commercialization or privatization of space. The emergence of new actors in space brings with it the emergence of new challenges. Unlike before, when a small group of states and big aerospace industries dominated the space, these new actors are likely to transform the oldstable system. As mentioned, the privatization of space will result in a decrease in the cost of space activities. While this does promise a sizeable increase in space development, it does have its fair share of drawbacks. Reduction in cost means increased participation. Furthermore if privatization continues at the same pace, soon it would not remain easy to regulate or control the actors in space. Hence, making it easier for terrorist groups to participate in space activities without attracting too much attention. In addition, reduced costs will allow them to develop their capacity to participate in sophiscated space activities.

#### Enables space terrorism – building capabilities now and the plan can’t solve private satellites

Ashna Mehmood 21 — (Ashna Mehmood; Student of International Relations at National Defence University, Islamabad, Published: 8-9-2021; "Terrorism in Space: A Possibility"; Vol. 9 No. 1 (2021): A Journal of Strategic Studies; Accessed: 6-20-2022; http://journal.ciss.org.pk/index.php/ciss-insight/article/view/204)//Pen-SY

Threat of Terrorism in space: Possibilities and Capabilities The threat of terrorism in space was highlighted by the US Under secretary of State, Robert Joseph, who warned the public at the George C. Marshall Institute about the potential terrorist attacks on US space assets in 2006.5His view was in conformity with the US 2006 Space policy, which argues about the capabilities and possible role played by transnational actors in interfering with space assets. There are three widely identified categories of ‘potential terrorist acts in space’: measures against satellites, attacks on launch facilities and ground stations, and user/service equipment attacks. An attack against satellites or an attempt to hijack them can cripple any state in today’s digital world since they relay on signals around the world and are used to operate our televisions, telephones, help in navigations through Global Positioning System (GPS), weather and climate prediction and monitoring systems, detecting underwater minerals, and for rapid and efficient communication.6 The ideal way to make affairs of a state on stand-hold would be through eliminating a satellite communication in its uses. However, that can be a difficult task. Other ways to achieve the same objective can be through disruption, denial, degradation, and deception of the space system. Different satellites have different purposes; military satellites are better shielded than a commercial satellite. Therefore a commercial satellite can be a suitable target for terrorists looking for new methods to achieve their objective of mass casualties and psychological effects. In advanced and developed states such as the US, traffic signals are controlled through cyber and satellite signals. A single disruption can cause accidents that can have a domino effect. Eventually it was observed that the first step to attack a satellite is to track it. To do so it only requires minimal technology such as stopwatches, sky maps, personal computers, and binoculars to observe a satellite’s orbital element. That’s why the US Undersecretary of State Robert Joseph showed concern overnon-governmental satellite observers tracking and posting satellite orbits on the internet, which the terrorist organizations can use for achieving their agendas. The simplest way to disrupt the satellite is through electronic interference, i.e. jamming or spoofing the satellite’s signals. Jamming means blocking or disturbing the communication signals travelling to and from the satellite by producing noise of the same radio frequency within the field of view of the satellite's antennas.7In contrast, spoofing is to mimic the characteristics of accurate signal so that the users receive a fake signal.Occurrences of hijacking and jamming are becoming increasingly common. In 2006, Thuraya Satellite Telecommunications of Abu Dhabi pinpointed that months-long intentional jamming of mobile satellite was detected to be originating from three different places in Libya .This major jamming event recorded in commercial satellite sectors were executed by some Libyan nationals. They were smuggling Marlboro cigarettes from Chad or Nigerinto Libya and they were usingThuraya satellite phones8to communicate with each other. They aimed to disrupt the communication signals to prevent the Libyan officials from overhearing their conversation. However, they jammed the signals on a large scale and ended up disrupting the signals beyond Libyan borders as well. As a result, Thuraya suffered huge losses as it tried to expand its network by launching a third satellite. If a gang of cigerrete smugglers in Libya in 2006 can have the capability to jam the signals outside Libyan borders, it is alarming to imagine what terrorists can do now, 14 years later.9Sri Lankan Tamil Tigers (LTTE) are declared terrorists by the US government.10 They hijacked Intelsat Ltd and used satellite transponder to broadcast their propaganda across the Indian subcontinent. Intelsat tried to shutdown LTTE’s pirating, but LTTE continued its satellite piracy for two years. Similarly in China, China’s Falun Gong hijacked the broadcasting signals of nine China Central Television stations, and ten provincial stations and broadcasted their agenda of religious spiritualism in 2002. Later in 2004, they again disrupted AsiaSat signals for 4 hours.Another way to attack satellites is by targeting their sensors with lasers. The laser beam can either interfere with or damage the satellite sensor. Also, it can melt fragile electronic connections as it induces thermo-mechanical stresses and structural damages. Moreover, satellites could be targeted as a whole through energy beams. However, it is a highly technical operation and requires several elements: reliable booster system with payload capacity, type of target that affects the delivery, up-to-date maintenance, and efficient crew, extensive space surveillance and tracking system, a medium to place the target in the range of the weapon, ability to kill the target, and ability to determine if the attack was successful or not. This is dangerous as an attack targeting a satellite may lead to secondary damages in the space orbitand may also hit the astronauts.

### 2NC – Terror Likely

#### Space terror likely and easy to succeed

Pawel Bernat 19 — (Pawel Bernat; Paweł Bernat Military University of Aviation · Department of Security Studies Doctor of Philosophy, Published: 12/23/2019; " Pawel Bernat & Elżbieta Posłuszna, The Threat of Space Terrorism in the Context of Irregular Warfare Strategies"; Philarchive; Accessed: 6-20-2022; https://philarchive.org/rec/BERTTO-30)//Pen-SY

Now, the question arises why the space sector would be an attractive target for weak actors like terrorist groups or individuals. A good way to answer it is to draw an analogy between the space sector and civil aviation because the latter for decades has been subject to various terrorist attacks. J. Laskowski names four main reasons why it has been so, i.e., (1) extensive media coverage, (2) symbolic meaning – by attacking the industry, the terrorist attacks the state the agency or company is registered in, (3) relative easiness to carry out such an attack, and (4) severe economic consequences (Laskowski, 2013:159-162). We can extend this list by the ones recognized by J. Harrison, namely that (5) such attacks are international events, (6) they can generate a sense of shame among the politicians of the attacked state, (7) they are effective (Harrison, 2012: 49-52). It seems that the abovementioned reason could also apply to the space industry and because of the unique and special character of it, like the amount of money involved, its symbolic significance, and worldwide media coverage, any act of space terrorism would release the goals the terrorists had in mind and hoped for. This is also why traditionally weak actors and adversaries of the states like the USA, Russia, or China would be potentially interested in targeting the space industry of those countries. For, a successful attack, i.e. such that would result in death and/or bring a lot of destruction to the infrastructure, would be a real blow to the country‘s internal and external perception, its finances, and would definitely slow down the development of space exploration As we can see in figure 1, all the odds are against strong actors and in favor of the weak ones, like more or less organized terrorist groups. Graphics excluded

#### Weak adversaries particularly likely to pursue space strikes

Pawel Bernat 19 — (Pawel Bernat; Paweł Bernat Military University of Aviation · Department of Security Studies Doctor of Philosophy, Published: 12/23/2019; " Pawel Bernat & Elżbieta Posłuszna, The Threat of Space Terrorism in the Context of Irregular Warfare Strategies"; Philarchive; Accessed: 6-20-2022; https://philarchive.org/rec/BERTTO-30)//Pen-SY

What is more significant from the safety and security perspective is the fact that the space industry has been gaining more and more strategic importance. Nowadays, we witness an unprecedented process of democratization of space technologies, including weapons, that could become a serious threat for orbital objects in the future. Obviously, weak actors are not in possession of ASAT weapon systems able to destroy satellites in the orbit (as for today, there are just five nation-states that have that capability, i.e., USA, Russia, China, Israel, and India); they do have though significant potential to disrupt / jam signals from and to satellites that may turn out to be lethal. The cases of the latter have already happened. For example, Sri Lankan terrorist group the Liberation Tigers of Tamil Eelam, otherwise known as the Tamil Tigers, hacked an Intelsat satellite and used a vacant Ku-band transponder to broadcast its message in Sri Lanka and the surrounding region without Intelsat‘s knowledge for over a year (de Selding, 2007) until Intelsat decided to shut down the satellite transponder in late April 2007 (McCoy, 2007). There might have also been cases of sabotage. In early 2015, a twenty-year-old U.S. Air Force Defence Meteorological Satellite Program Flight 13(DMSP-F13) craft blew up. The U.S., according to S.M. Pekkanen, attributed the event to a power failure and minimized its importance. However, the delay in admitting the event to the public caused speculations, whether it was an actual act of sabotage (Pekkanen, 2015). Of course, for obvious reasons, it is difficult to determine what truly happened. Another case worth mentioning is the launch of four rogue satellites on Indian PSLV launch vehicle on 12 January 2018. The satellites belonged to the Swarm Technologies – a space start-up based in California that had been denied placing them onto the orbit due to the small size of the devices (the concern was that they were too small to be tracked in space) (Christensen, 2018). While, as it seems, this case did not pose any danger for global security, it raises many questions regarding our current control system what is sent to the outer space. If it was possible for an American company to place in the orbit unlicensed satellites, it seems, that any other agent, including weak actors adversaries discussed in this paper, could do the same.

# CP

## China Adv CP

### 1NC---Adv CP---China War

#### The United States federal government should increase its cooperation with the People’s Republic of China over

#### Strengthening maritime consultation mechanisms,

#### Observing rules of conduct for air and maritime encounters,

#### Notifying each other of major military activities,

#### Resuming defense consultations tasked with improving crisis communication mechanisms and establishing CBMs,

#### Assigning a crisis management function to defense hotlines,

#### Assigning the role of emergency communication to embassies, special envoys, and a joint working group, and

#### Strengthening the role of Track 2 dialogues.

#### That solves.

Zhang Tuosheng ‘21 ,academic committee member at the Center for International Security and Strategy, Tsinghua University, and also Chairman of the Academic Committee, Grandview Institution. "Strengthening crisis management, the most urgent task in current China–US and China–Japan security relations." China International Strategy Review 3, no. 1 (2021): 34-55. // Ali

First, at present and in the foreseeable future, the focus of China–US crisis management should be placed on issues concerning the Taiwan Strait, the South China Sea, the Korean Peninsula, and cyberspace. Among these issues, security frictions in the South China Sea and on cybersecurity have emerged as the newest challenges for China and the US over the past 10 years. When strengthening crisis management measures, it is necessary to clarify each party’s bottom line as soon as possible. With regard to the Taiwan Strait and the Korean Peninsula, after long-term consultation, both China and the US have a clearer idea of the other’s bottom line. The key to crisis avoidance lies in never crossing one another’s bottom line. In the long run, the East China Sea and outer space will also become important areas that require strengthened crisis management.

Second, for the time being, China and the US should redouble their efforts to prevent contingencies in the sea or air due to the potential for misunderstanding, miscalculation, or accidental discharge of fire. The two sides must earnestly strengthen the military maritime consultation mechanism; strictly observe the rules of conduct for air and maritime encounters in order to ensure safety, as well as the mechanism of notification of major military activities plus the two annexes; and constantly enrich and improve these rules and mechanisms in practice. To this end, in addition to holding annual meetings to analyze the overall situation and evaluate various risks, relevant departments must strengthen regular and ad hoc consultations to eliminate hidden dangers in a timely manner and minimize security risks.

Third, while trying to resume and strengthen security and defense dialogues, the two sides should make crisis management an important item on their agendas. To this end, they must strive to create conditions to first resume the diplomatic and security dialogue (or the defense consultation), the joint staffs dialogue, the annual meeting of the military maritime consultation, and the law enforcement and cyber-security dialogue. These dialogues should cover setting up and improving bilateral crisis communication mechanisms, establishing various confidence- and security-building measures (including codes of conduct in the sea, air, space, and cyber-space), and ways to avoid the militarization of the South China Sea. In addition, the two sides should work hard to launch, as soon as possible, a strategic stability dialogue53 that focuses on nuclear strategy, nuclear development strategy, and related cybersecurity issues, as well as outer space security, missile defense deployment, and new conventional strategic weapons, and touches upon crisis stability and confidence-building measures in the nuclear field.

Fourth, China and the US should explicitly assign a crisis management function to the head-of-state and defense hotlines and strengthen the function to ensure the hotlines’ role in crisis prevention and control. To this end, the two sides should try to set up more frequent phone conversations and allow them to happen on short notice, thus giving full play to the hotlines’ role in exchanging information promptly, clarifying intentions, and sending clear signals. To establish crisis communication more quickly, the two sides should also seriously consider establishing a military hotline at the theater level. The various hotlines may, of course, be used in peacetime, but their function during a crisis is critical. The head-of-state hotline did not serve such a function during the 1999 embassy bombing incident and the 2001 aircraft collision incident. This history must not repeat itself.

Fifth, in addition to the various hotlines, the two sides should also give full play to the role of emergency communication through Chinese and American embassies and special envoys. The two should also set up a joint working group to respond to emergencies and task it with collecting and sharing risk information; discussing crisis prevention, control, and response plans; engaging in crisis communication as soon as possible and making recommendations to decision makers; and carrying out post-crisis review and evaluation. The joint working group may be placed under the diplomatic and security dialogue and led directly by the foreign and defense departments.

Sixth, the top leaders of the two countries and militaries should reach a common understanding on the basic principles of crisis management. In the Track 2 dialogue on security crisis management, experts from the two sides jointly proposed several basic principles of crisis management, such as “maintaining direct channels of communication and sending clear and specific signals”, “escalating slowly and responding in a tit-for-tat manner”, “acting on interests instead of ideology”, “exercising restraint in using extreme pressure and avoiding commitment traps”, and “dividing hard-to-resolve disputes into smaller, more manageable issues and aiming at gradual resolution”(Zhang and Swaine 2007, 7–10). If agreed upon and adopted, these basic principles will serve crisis management between China and the US well.

Seventh, China and the US should continue supporting and strengthening the role of Track 2 dialogues. Over the years, as a supplement to intergovernmental interactions, dialogues hosted by think tanks have played a positive role in helping the two sides conduct security cooperation, manage differences and crises, reduce mis-understanding and miscalculations, and increase mutual trust. Now that security and defense dialogues between the two governments are bogged down in difficulties, the various Track 2 security dialogues, such as the China–US Security Dialogue, China–US Strategic Nuclear Dynamics Dialogue, China–US Security Crisis Management Dialogue, and China–US Cybersecurity Dialogue, should be further boosted instead of being suspended.

### 2NC---XT: Solvency

#### Limiting Chinese capabilities is the wrong approach. Implicit understandings should establish that destructive capabilities are only there for deterrence---clarifies thresholds.

Andrew S. Erickson ’19, Professor of strategy and the research director in the U.S. Naval War College's China Maritime Studies Institute and a visiting professor in full-time residence in Harvard University's Department of Government. “U.S.-China Military-to-Military Relations: Policy Considerations in a Changing Environment”, Asia Policy, Vol. 14, No. 3 (JULY 2019), pp. 123-144 // Ali

Fifth, even absent related agreements, it is possible to pursue some measure of mutual restraint in the most dangerous and volatile areas. On the positive side of the ledger, some degree of cooperation is possible even when both parties face a security dilemma, although factors such as offense vs. defense, technology, and geography must be considered with particular care.43 Yet negotiating durable agreements under a great-power security dilemma can be extremely difficult, as both sides have incentives to cheat, and no outside party can adjudicate effectively.44 Each side’s belief that the other will simply pocket any concessions without reciprocal actions or benefits strongly disincentivizes unilateral restraint or accommodation. Fortunately, effective arms control and deterrence relations need not be limited to formal treaties; they simply require arranging forces in such a way that neither side has the incentive to act adversely toward the other. Thomas Schelling and Morton Halperin’s explication of this issue is worth considering in depth.45 A broader, more flexible form of engagement that applies Schelling and Halperin’s conceptual approach to focus on reducing the incentives to use capabilities rather than reducing the capabilities themselves can thus address U.S. and Chinese concerns that would render aspects of formal agreements deal-breakers. China appears absolutely unwilling to accept technical inferiority, and any agreement that attempts to keep the PLA in such a position will fail; nor will the United States voluntarily relinquish capabilities that it has labored and invested to develop, particularly in the face of a security dilemma. Informal understandings may evolve over time through informal communication, and may even lead to more explicit agreements.46 The overall strategic positions of the United States and China are relatively clear; it may be difficult to justify extensive dialogues that fail to go beyond policy platitudes. What could be useful to discuss are operational and perhaps even tactical specifics, which remain far less clear. The most realistic possibility to pursue over time is therefore some form of implicit, non-treaty-based understanding between the United States and China that even if the use of certain lower-end capabilities may be impossible to rule out, other types of capabilities are primarily for deterrence rather than actual operational use. This would help clarify thresholds, an important aspect of risk management.47 As explained previously, however, this approach will only be effective to the extent that both sides restrain themselves. It will fail if Beijing expects preemptive or unilateral concessions from Washington.

## EU CP

### 1NC – CP

#### The United States federal government should substantially increase its cyber resiliency efforts on space-based assets with the European Union

#### US-EU cooperation solves and spills over to NATO capabilities.

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

### 2NC – Solvency

#### EU space action solves---financial, commercial, and security initiatives guarantee success.

Raquel Jorge Ricart 22, Analyst at Elcano Royal Institute working on the technology and digital agenda and Masters in Security with a concentration in tech and cybersecurity, 2/23/2022, "Outer space: the new horizon on EU’s strategic autonomy," https://www.realinstitutoelcano.org/en/outer-space-the-new-horizon-on-eus-strategic-autonomy/, sg

Where is the EU’s strategic autonomy in outer space?

Space policy is nothing new to the EU, but it is only now that it has been given the outlook of strategic autonomy, both in markets and in security and defence. There are two reasons for this. The first is that the European space industry recorded a €1 billion drop in sales in 2020 (a 13% decrease year on year), an unprecedented figure in the past 30 years, according to the leading European association ASD Eurospace. This explains why Commissioner Breton recently announced the creation of a comprehensive package of measures:

* The launch of the CASSINI space investment fund with an investment capacity of at least €1 billion to support new space start-ups;
* The use of public procurement in a strategic way to reduce the commercial risk of new trials (test and de-risk), provide security to start-ups and build confidence with private investors in space projects;
* The development of a technology roadmap with long-term plans and investments coordination in space innovation through a Space Partnership;
* Greater communication between all industrial sectors working on space capabilities through the Space Launcher Industry Alliance and the Space Traffic Management Strategy. This is not only about space companies, but also about dependences on the supply chains from other industries, such as semiconductors, or industries which may impinge on European leadership over space, such as quantum technology.

The second pillar of measures touches on security and defence. The launch announcement of a Strategy on Defence and Space in 2023 and the integration of more space issues into the expected Strategic Compass are positive news due to the urgency of this topic, but also because they represent a major evolution with respect to previous strategies. The 2000 strategy addressed how to improve scientific knowledge, foster its benefits to society and how to strengthen the space market. Next strategies from 2011 and 2016 made reference to security issues, but mainly for civilian affairs. As of 2022, Borrell has committed to developing new mechanisms to respond to a space which is likely to become a battlefield. The idea is to focus on space domain awareness, the reinforcement of dual-use space infrastructures, a Galileo Threat Response Mechanism, and a first joint exercise by March 2022, among others. Additionally, space was included for the first time as a critical infrastructure in the latest proposal for the Directive on the Resilience of Critical Entities.

There is no doubt that the EU has positioned outer space as a new asset on its strategic autonomy’s horizon. There are still many issues to be discussed, resolved and even opened up. Some are: how to tackle the use of space data markets to increase the economic competitiveness of European companies and greater collaboration with each other; the need to carry out a mapping on existing assets, dependences and shortcomings in several project scenarios which are significant, critical or vital to assess and ensure the resilience of supply chains for space capabilities; which cooperation instruments should exist between member states, the EU and the European Space Agency to make sure funding for innovation is impactful; how to cooperate for a joint response to security and defence threats (e.g. following the cyber-diplomacy model on coordinated attribution at the EU level, or giving more competences); or how to interweave space policy with other plans in semiconductors, quantum technology and cyberspace, among others.

### 2NC – AT: NATO Key

#### NATO doesn’t own any space-based assets, it completely relies on allied nations.

Alessio Di Mare 21, Captain of NATO Space Operations Support, 5/1/2021, "The Role of Space Domain Awareness," https://www.japcc.org/essays/the-role-of-space-domain-awareness/, sg

The Present and Future Role of NATO

NATO neither has its own Space assets nor operates any. It relies on Space capabilities that Alliance nations provide on a voluntary basis. NATO operations strongly depend on Space services, so SDA also becomes a key resource for NATO and it needs more than just a ‘donation’ from Member States.

## Hotlines CP

### 1NC – Hotlines solve

#### Hotlines for cyber solve misperceptions and miscalcualtions

Ariel (Eli) Levite 19, nonresident senior fellow in the Nuclear Policy Program at the Carnegie Endowment; and Lyu Jinghua, visiting scholar with Carnegie’s Cyber Policy Initiative, 1/24/19, “Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?,” <https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213>

Third, enhance mechanisms and channels for routine as well as emergency bilateral information sharing and coordination on cyber events and notification of major military activities. This proposal builds on preexisting bilateral arrangements for sharing information, such as in the cooperation between the respective national CERTs from the two countries. However, what arrangements are now in place do not suffice to dispel misperceptions and prevent miscalculations, and avert explosive incidents especially in the political and military spheres. Blocking communications and blinding or, even worse, spoofing time and navigation systems of civilian and military assets in peacetime are especially prone to lead to escalation. While it is highly necessary to adopt mutually understood rules of the road in this sphere, a first step would be to establish or complement bilateral hotlines and other crises communications and consultation channels among both military commanders as well as high level decisionmakers with corresponding political/policy guidance to endow them with real substance.

It is also worth considering in this context how to apply the MOU on Notification of Major Military Activities in cyberspace. In this memorandum, signed by the U.S. Defense Department and Chinese Ministry of National Defense in November 2014, both sides “affirm their aspiration to establish a voluntary foundation for notifications of major military activities, such as exchange information voluntarily about their respective country’s security policy, strategy, and legal information, including the adjustment of respective national defense policies and strategy, by providing briefings and information about speeches, major government publications such as White Papers, strategy publications, and other official announcements related to policy and strategy,” and allow for “observation of military exercises and activities that should be voluntary and occur within the existing framework of bilateral U.S.-China military relations.”33 Similar voluntary exchange of information, interpretation of cyber strategy and publication, and invitation from either side to observe cyber exercises hosted or co-hosted by the other side could be one part of confidence-building efforts in cyberspace.

## Terrestrial CP

### 1NC – CP

#### Overreliance on Satellite-based GPS makes NATO vulnerable to Russian attack. Only terrestrial systems as backups solve.

Goward ’22 (Dana A. Goward,  president of Resilient Navigation & Timing Foundation. “Get the Bullseye Off GPS” 04/19/22, <https://spacenews.com/op-ed-get-the-bullseye-off-gps/>)

On Nov.15, 2021, a missile streaked into space from Russia. Once above the atmosphere, it released a kinetic kill vehicle that destroyed a retired Russian satellite. The resulting debris endangered other satellites and the International Space Station, including the Russian members of its crew.

A week later Russian troops massed along the border with Ukraine. A Russian news commentator recognized as Putin’s mouthpiece[bragged that Russia could destroy all 32 US Global Positioning System (GPS)](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220404_Harrison_SpaceThreatAssessment2022.pdf?K4A9o_D9NmYG2Gv98PxNigLxS4oYpHRa) satellites and blind NATO forces.

This was a particularly ominous warning.

U.S. critical infrastructure relies on precise timing and navigation signals from GPS satellites. At a December public meeting, a member of the National Security Council summed this up by[saying “GPS is still a single point of failure”](https://www.gpsworld.com/nsc-director-gps-still-a-single-point-of-failure/#:~:text=The%252520Global%252520Positioning%252520System%252520(GPS,director%252520for%252520Response%252520and%252520Resilience.) for America.

If GPS signals suddenly disappeared, transportation systems would immediately suffer. Everything would slow down, carry less capacity, and be more dangerous. Air travel would be less efficient and safe. Delivery services would be hamstrung. Uber and Lyft would be out of business.

Other critical systems would follow over subsequent days. Cellphone towers and internet switches would lose synchronization. Banks could not timestamp transactions. Control systems for electrical grids, sewer and water systems, and many industrial applications would fail or revert to inefficient manual operations.

And, of course, Putin would not even need not go through the trouble of shooting down satellites and risking all-out war. He could do it with the flip of a switch.

Russia excels at cyber and electronic warfare. State media has boasted of Russia’s ability to[make aircraft carriers useless](https://www.spacedaily.com/reports/Russian_E_Warriors_Render_Aircraft_Carriers_Useless_999.html). Russian forces regularly jam GPS and other satellite signals in various parts of the world. They also have perfected “spoofing,” sending false signals to make GPS users think they are someplace they are not.

Russian capabilities also reportedly extend into space with[nuclear-powered electronic warfare satellites](https://www.thespacereview.com/article/3809/1). These could jam GPS signals across the face of the planet.

A cyber or jamming attack would have clear advantages over destroying satellites. Cyber-attacks are often difficult to attribute and would be less likely to prompt a shooting war. Putin also would have the flexibility to undo things if they started to get out of hand, or once he got what he wanted.

Protecting GPS satellites and signals is essential to U.S. national and economic security. And to keep our national policy and global leadership from being held hostage by threats.

Some have recently opined in SpaceNews and other publications that the solution is more and better GPS. It is true that a modernized and capable GPS is essential.

Yet more of the same is unlikely to fix the problem. The most effective and least expensive solution is to make GPS a much less attractive target.

America’s over-dependence on GPS for essential positioning, navigation, and timing (PNT) services has long been recognized. To help manage the problem, in 2004 President Bush mandated the establishment of an alternative and backup system for GPS. Administrations promised in[2008](https://rntfnd.org/wp-content/uploads/DHS-Press-Release-GPS-Backup-2008.pdf) and[2015](https://rntfnd.org/wp-content/uploads/DSD-and-Dep-DOT-reply-to-Mr.-Garamendi.pdf) to do so. In 2018 a[law was enacted requiring a terrestrial backup for GPS](https://www.gpsworld.com/gps-to-get-terrestrial-backup-system/) by the end of 2020. Each time, though, a lack of perceived real threat and bureaucratic inertia resulted in no action being taken.

Russia has a terrestrial PNT system its civilians and military can use when signals from space are not available. So do[China](https://www.gpsworld.com/china-leads-world-with-plan-for-comprehensive-pnt/),[South Korea](https://www.gpsworld.com/south-korea-partners-with-broadcaster-on-eloran-and-10-cm-gps/), Iran, and Saudi Arabia.

We shut ours down in 2010.

And so, our GPS, and our way of life, remain hostage to those better prepared to survive severe solar storms, accidents, and malicious attacks of all kinds.

In a[January 2021 report to Congress](https://www.gpsworld.com/dot-report-l-band-uhf-lf-and-fiber-pnt-needed-to-protect-us/), the Department of Transportation identified the technologies and services needed to make GPS, and thus America, more secure. It offered a user-focused systems engineering approach that included signals from space, terrestrial transmitters, and fiber.

All these are readily available as mature commercial services. And the projected annual price tag to contract for them is a small fraction of the $1.5B spent on GPS each year.

PNT is critical tech infrastructure. Expanding and securing our national PNT capability could easily be included and funded as a project in the recently enacted Bipartisan Infrastructure Framework.

While GPS satellites and services are at risk from threats like severe solar weather and human error, the greatest risk is undoubtedly from malicious acts by other nations, terrorists, criminal organizations, and hackers.

Providing GPS alternatives will help protect satellites and signals by making them much less attractive targets. Why attack a system if it’s not a single point of failure? Or if users have alternatives operating in parallel or they can switch to in an instant?

GPS and the American people must be protected. We have the legal mandates and funding mechanisms in place. All we need is for the administration to follow the[2018 law](https://www.gpsworld.com/gps-to-get-terrestrial-backup-system/) and get the bullseye off GPS as soon as possible.

### 2NC – satellites bad

#### Satellites suck – their ever-increasing presence leads to collisions, which would take out the grid, GPS systems, and the internet.

Demiyanov, ’22 (Andrey Demiyanov, Jordan News Reporter. “Kessler Syndrome: An existential wave of doom across the horizon?” 09/01/22 https://www.jordannews.jo/Section-129/Technology/Kessler-Syndrome-An-existential-wave-of-doom-across-the-horizon-11705)

Knowing just how dangerous space debris can be and its century-long orbital decay, let’s now dive into the deep rabbit hole that is modern-day’s tech giant’s aspirations to launch more satellites into space.  
  
We have launched over 12,170 satellites into space; 7,630 are currently in orbit at varying orbits. Of those 7,630 there are over 3,000 inactive satellites, essentially space junk, hovering around the earth’s atmosphere cruising around at speeds of 27,500km per hour or more.   
  
Elon Musk, the modern-day layman’s hero of space exploration, has set forth a plan to put over 1,300 satellites into space to establish a satellite internet network that would enable even the most distanced individuals across the earth to gain access to the internet.   
  
Jeff Bezos has also set his sights on launching satellites into space to gain access to the developing industry of satellite internet, and there are currently over a dozen companies that are seeking to do the same.   
  
While the notion of internet access for all at an affordable rate throughout the world with a satellite dish sounds appealing — how far are can we push the envelope before Kessler’s model starts ringing the alarms?   
  
While many would argue it is essential to do so, the measure of sending out hundreds, if not thousands of satellites into orbit by these companies to simply provide a need that in theory can be provided through other means seems highly irrational when considering the long-term effects that this innovation may develop.   
  
Access to the internet, however, is just one side of the coin — countless telecommunication companies, government entities, and other stakeholders vested in the use of orbital bodies are continuously pushing Kessler’s model further and further into the red, wherein in the coming future, we may begin to genuinely have to worry about the aforementioned domino effect.   
  
The real problem   
  
Hypothetically, if the Kessler Syndrome becomes a reality and a chain of collisions to commence, the earth won’t exactly be bombarded with debris like in a sci-fi movie where the entire planet has fiery fail raining down on its residents.   
  
However, it will mean that hundreds of services that rely on satellite technologies will come to a complete standstill.   
  
Life without internet, telecommunications, or even basic GPS will become a reality. Launching further satellites into space will become extremely challenging, and space exploration may, in fact, be reasonably impacted as a result of the debris that will be left hovering thousands of kilometers over the earth.   
  
Kessler admitted that the chance of the collision is currently sitting at almost null percent back in 2009. The harsh reality is that ever since then, satellite launches have increased significantly, therefore increasing the total number of cosmic bodies making their rounds around the earth.   
  
And it appears that unless genuine exploration into the topic is performed and regulation is put into place, Kessler’s Syndrome won’t just be a hypothetical reality — but an inevitable time bomb that will eventually set humanity back into the dark ages.   
  
While the obvious solution at first glance may be to clean out space of such debris, not only is it highly costly but there is no rational way to determine what debris is potentially on its way to set off a collision chain and what debris can be left alone. Therefore, the only method to the madness is developing powerful enough systems that can measure trajectories of most, if not all, known space debris around the earth — and then mapping out their trajectories years ahead to predict what objects may pose a threat in the forthcoming future.   
  
But even that, in essence, is impossible. As mentioned, the earth’s gravitational pull extends hundreds of light-years, albeit at a significantly reduced strength.   
  
Considering that we have several planets in our solar system, all of which have their own gravitation fields that indirectly affect the trajectories of these objects, it becomes nearly impossible to accurately predict any kind of potential future.   
  
Perhaps, in the end, the only real way to prevent Kessler’s model from ever being realized is to simply limit the number of total space objects themselves. Perhaps tech enterprises must stop chasing the great and instead strive to do good.

## Unilat CP

### 1NC – Generic Unilat CP

#### Counterplan: The United States federal government should increase cybersecurity of space-based assets manufactured in the United States

#### Solves better---unilateral action key to defend against cyber-attacks on satellites---development and documentation of best standards, guidance, clarification of liability, *creation of an ISAC*, and *collaboration with the industry* solely in the US. Also avoids the link to the DOD tradeoff DA --- DHS is the government facilitator.

Gregory Falco 18, Research Fellow with the Belfer Center’s Cyber Security Project at Harvard Kennedy School, July 2018, “Job One for Space Force: Space Asset Cybersecurity”, http://osa-public.s3.amazonaws.com/papers/csp\_falco\_space\_asset-final.pdf, Cyber Security Project \\SYang

What can space asset organizations do? Organizations developing space assets are largely unregulated for cybersecurity purposes. The lack of specific space asset cybersecurity requirements necessitates a considerable degree of self-policing. Without mandatory standards, space asset organizations can improve their security either individually or collectively. What follows are some options to consider: • Employ existing cybersecurity standards and develop new standards for space systems where needed. There is no lack of cybersecurity standards and best practices available for developers to follow when attempting to design and develop secure systems. Many of these standards, like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, are well-documented and widely adopted in some form.28 Most space systems’ security can benefit from using these standards. In some cases, these standards may not apply for the specific technologies used in space systems. For these systems, space asset organizations should create new space asset-specific standards and best practices so that security can be applied consistently across the organization. Vendors of space asset organizations should also be held to these standards. This should involve the explicit testing and demonstration that vendors to these organizations conform to the security standard in place for the space asset organization. • Establish cybersecurity capabilities for mission systems and internal network/server systems. Similarly to what was done at NASA JPL, it is important to establish separate cybersecurity specialists for mission systems and internal networks/server systems. The distinction between the two systems are operational technology versus information technology—each one has very different operating and security requirements and need to be addressed accordingly. 28 Nicole Cieslak. “NIST Cybersecurity Framework Adoption on the Rise.” Tenable. 2016. https://www. tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise. To date, congress has provided little guidance in terms of enabling cybersecurity across sectors. One of the few examples includes the Cybersecurity Information Sharing Act (CISA) which was signed into law in late 2015 by President Obama. CISA is meant to help facilitate information sharing between the government and the private sector by limiting the liability of the private sector for certain attack disclosure.29 Congress should develop more laws that could be specifically relevant to space assets. Recommendations concerning these laws follows. • This is Urgent. Act quickly. Be proactive, not reactive. Do not wait to pass a law on space cybersecurity until there is a WannaCry (major ransomware attack that compromised healthcare systems around the world) or Mirai (IoT attack that took down a major DNS provider on the East Coast resulting in downtime for websites such as Facebook, Twitter and Reddit) equivalent for Space. It seems that action only occurs when a disaster strikes. A space cyberattack can have serious consequences as detailed previously and we cannot wait until something happens to pass legislation protecting these critical systems. • Clarify critical infrastructure security requirements to include underlying systems. Currently, policy concerning critical infrastructure security does not require third-party, enabling infrastructure to also comply with the same requirements. Space systems should be held to the same standards of the critical infrastructure on which they rely. • Assign responsibility and liability for cyber. Cybersecurity responsibility and associated liability for a breach should be clarified and assigned for space asset organizations. An important component of cybersecurity legislation currently under review concerns the liability of technology developers, owners and operators. In January 2017, the FTC sued D-Link for the vulnerability in their routers leading to the widespread Mirai botnet attack in October 2016.30 This was the first time a manufacturer was sued for the cybersecurity failures of their devices. Legal guidance concerning where liability falls will encourage the responsible party to take the necessary measures to secure their systems. Today’s lack of clarity around liability for the space asset ecosystem results in poor accountability and inaction to secure these important systems. • Make space asset organizations accountable for cybersecurity. All government contracts with space asset organizations should require the contractor to comply with key performance parameters (KPPs) pertaining to cybersecurity. Today, cybersecurity KPPs are a subcomponent of system survivability KPPs. Cybersecurity KPPs should be firmly enforced for all government contracts. • Expand 32 CFR 236 to include space asset organizations. Currently, the defense industrial base is required to report all cyber incidents that have affected or could affect national security under the Department of Defense-Defense Industrial Base Cybersecurity Activities Regulation31. Considering the critical posture of space systems and the U.S. reliance on these assets for both national security and critical infrastructure, space asset organizations should be included under this ruling. This would improve cybersecurity transparency between the government and space asset organizations. • Establish a Space System Information Sharing and Analysis Center (ISAC). Government agencies such as the Department of Homeland Security (DHS) could play a crucial role as a convener for public and private sector entities that work with space systems. The DHS could become an important facilitator for this sector’s efforts to improve cybersecurity by creating a Space System Information Sharing and Analysis Center. The DHS should require participation of government agencies that work with space systems ranging from the Department of Defense (DoD) to NASA to participate in the Space System ISAC. This would provide an incentive for private sector space asset organizations to also join. If 32 CFR 236 were expanded to include space asset organizations, the Space System ISAC could be made compulsory through this requirement. Sharing threat information across space system agencies and space asset organizations would be a logical step to improve the security posture of the sector. Some agencies or private organizations may be much further ahead in securing systems than others and sharing insights will help all ISAC members involved. What can a Space System ISAC do? Sharing threat information across space system agencies and space asset organizations would be a logical step to improve the security posture of the sector. Some agencies or private organizations may be much further ahead in securing systems than others and sharing insights will help all ISAC members involved. The recommendations for what a Space System ISAC should are as follows. • Encourage collaboration among space-relevant organizations. The DHS should require participation of government agencies that work with space systems ranging from the Department of Defense (DoD) to NASA to participate in the Space System ISAC. This would provide an incentive for private sector space asset organizations to also join. If 32 CFR 236 were expanded to include space asset organizations, the Space System ISAC could be made compulsory through this requirement. Sharing threat information across space system agencies and space asset organizations would be a logical step to improve the security posture of the sector. Some agencies or private organizations may be much farther ahead in securing systems than others and sharing insights will help all ISAC members. • Establish information sharing requirements. The Space System ISAC should require member entities to disclose vulnerability and attack information to one another within a predefined period. This would be in the spirit of the UK’s General Data Protection Regulation (GDPR) that requires an organization to disclose when personally identifiable information is breached within 72 hours of discovery. • Document and maintain space system cybersecurity best practices and standards. Member organizations should share internal or contractor standards for cybersecurity in a manner that does not release sensitive information. A master list of best practices should be shared across the Space System ISAC and curated. Member organizations can comment on the merits of the best practices and cater existing cybersecurity standards to be highly relevant to the idiosyncrasies of space systems. • Cooperate with ISACs for other critical infrastructure sectors that rely on space systems. Because space systems underpin other sectors, certain threat information for space systems should be shared with the relevant sectors that might be affected if an attack occurs. The Space System ISAC should work with the oil/gas, electricity and emergency services ISAC to communicate threats that are relevant to these critical infrastructure and services. The potentially affected critical infrastructure organizations could then work with the space asset organizations to remediate the vulnerability where appropriate.

### 1NC – Cyber Sanctions

#### Counterplan: The United States federal government should adopt a policy of unilateral cyber sanctions.

#### Unilateral cyber sanctions solves all of their internal links---best mode of deterrence.

Iryna Bogdanova and María Vásquez Callo-Müller 21, research fellow at the World Trade Institute (WTI), University of Berne, post-doctoral researcher at the University of Lucerne, December 7, 2021, “Unilateral Economic Sanctions to Deter and Punish Cyber-Attacks: Are They Here to Stay?”, https://www.ejiltalk.org/unilateral-economic-sanctions-to-deter-and-punish-cyber-attacks-are-they-here-to-stay/#:~:text=Unilateral%20cyber%20sanctions%20are%20restrictive,in%20other%20malicious%20cyber%20activities. \\SYang

When international cooperation fails to take root, unilateralism blossoms – as we see in the field of cybersecurity. Unilateral cyber sanctions are restrictive economic measures of a temporary nature imposed against individuals, legal entities, government bodies and officials that conduct or facilitate cyber-attacks or engage in other malicious cyber activities. They are imposed without any prior authorization of a regional or an international organization, i.e., according to states’ domestic laws.

The 2014 cyber-attack on Sony Pictures Entertainment, as a result of which private data, including unreleased movies, was stolen and emails were hacked as well as thousands of confidential documents were leaked, paved the way for the US cyber sanctions targeting North Korea, thus adding pressure to one of the most sanctioned countries in the world. In the following years, the United States expanded its cyber sanctions framework and used it to sanction malicious actors as well as states sponsoring them.

The European Union introduced a new framework for cyber sanctions in 2019 and the first cyber sanctions were announced in July 2020. Several non-EU member states expressed their desire to align with the EU cyber sanctions. The United Kingdom closely follows the EU cyber sanctions and enacted the Cyber Sanctions Regulations, which came into force on the exit day.

Leaving aside the politically salient debate on the legality of unilateral economic sanctions, the next paragraphs are devoted to the analysis of international law obligations that unilateral cyber sanctions may breach. A more in-depth analysis can be found here.

The existing cyber sanctions target government bodies as well as senior government officials and thus may entail freezing of government bodies’ assets along with travel bans on senior government officials. Freezing of government bodies’ assets may in theory violate the customary international law of state immunity, yet it is debatable. In particular, whether state property benefits from the enforcement immunity irrespective of the existence of a court proceeding is unsettled. Travel bans preventing senior government officials from fulfilling their functions encroach on the immunities guaranteed to such officials under international law, but this immunity entitlement is only guaranteed to the officials who represent the government and hence travel to other states for that purpose.

The consistency of unilateral cyber sanctions with the minimum due process rights may be questioned. For example, persons targeted under the EU cyber sanctions regime are guaranteed the right to good administration, the right to an effective remedy and to a fair trial, which are enshrined in the Charter of Fundamental Rights of the European Union. These guarantees are frequently invoked in disputes questioning the EU economic sanctions. Besides due process rights, other possible grounds to question the legality of unilateral cyber sanctions are the right to property, the right for family and private life and a prohibition of attacks on honour and reputation that are guaranteed under various international human rights treaties as well as domestic laws.

Against this backdrop, states may advance an argument that cyber sanctions are justified as countermeasures. Indeed, states are allowed to impose countermeasures if certain preconditions are met. First and foremost, there should be a previous violation of international law, which is remedied by countermeasures. Second, such violation should be attributed to a state. Third, countermeasures should not affect obligations for the protection of fundamental human rights. Furthermore, countermeasures should be proportional, temporary and adopted only after the procedural prerequisites were fulfilled. Even a shallow analysis demonstrates that the possibility to justify cyber sanctions as countermeasures is hindered by two main hurdles: the lack of internationally agreed obligations regulating malicious behaviour in cyberspace and the attribution of cyberattacks to a state under the rules of state responsibility.

Unilateral cyber sanctions may also violate bilateral agreements of economic nature and WTO commitments. By imposing unilateral cyber sanctions that either entail a complete economic boycott of sanctioned persons, as it is the case with the US cyber sanctions, or prohibit the provision of funds and economic resources to sanctioned individuals and entities as the EU regulations prescribe, states are blatantly acting in contradiction to their professed WTO commitments. Whether such actions can be justified either under national security exceptions embedded in bilateral agreements or under the WTO national security clause is debatable. Moreover, cyber sanctions, such as freezing of assets, property and interests in property can result in legal claims of indirect expropriation, violation of the Fair and Equitable Treatment and other standards of treatment incorporated in international investment agreements.

On a normative value of cyber sanctions, they may signal “red lines” of unacceptable behaviour in cyberspace and in such a way contribute towards the formulation of rules on responsible behaviour in cyberspace.

Given the ever-growing digitalization of all aspects of life and a steadily increasing number of cyber-attacks, it is expected that states would increasingly rely upon unilateral cyber sanctions to deter and punish cyber-attacks as well as their perpetrators. In this context, one may ponder what role is left for multilateralism when society is faced with imminent threats and there is a lack of effective international cooperation and whether in such circumstances unilateralism should be discussed and explored more openly?

### 2NC – Solves Allies

#### Solves their internal links about attacks on allied countries---US unilateral action enables it to act as a cyber framework nation for allies and causes follow-on.

Franklin D. Kramer 17, Robert J. Butler, Catherine Lotrionte, distinguished fellow and board director of the Atlantic Council; retired U.S. Air Force colonel and a former member of the Defense Department’s Senior Executive Service, the first Deputy Assistant Secretary of Defense for Cyber and Space Policy; Senior Associate at CSIS and a Senior Fellow at the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University and former Brent Scowcroft scholar at the Atlantic Council, “Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict”, https://www.jstor.org/stable/pdf/resrep03691.8.pdf \\SYang

In a conflict, cyber security will be as or more important in forward theaters as it will be in the United States. Most US allies and partners do not have the same cyber capabilities as DoD, yet it will be their infrastructures and national capabilities that US forces will be relying upon for numerous tasks. Accordingly, the concept of “extended cyber deterrence” will be an important role for the DoD in connection with each of the theaters noted above. The concepts are set forth in the issue brief “Cyber, Extended Deterrence, and ATO,”90 but their application goes beyond NATO to all arenas where US critical interests are intertwined with allies and partners. Most obviously, the United States will continue to develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of US war-fighting capabilities. As noted above, cyber tools potentially could disrupt an adversary’s communications, logistics, sensors, and military supporting infrastructure. The secretary of defense has stated that cyber is currently being used in the conflict with ISIS,91 and NATO has recently designated cyber an operational domain.92 Cyber will continue to be integrated into combat planning. Cyber security will be important not only for US forward forces, but also for the militaries and the critical infrastructures of host nations. It is notable that in each of the theaters that the United States plans for, the potential adversary has been identified as the source of significant cyber intrusions. Russia is responsible for the hacking of the Democratic National Committee, among many other cyber incidents.93 China is responsible for the attack on the Office of Personnel Management and Chinese officers have been indicted for continued cyber espionage.94 Iran is behind the tack on Saudi Arabia’s oil company and Iranian hackers have been indicted for attacks on American banks.95 North Korea is behind the attack on Sony and has regularly attacked South Korean networks.96 What these attacks demonstrate is the vulnerability of host nations to cyberattack, a vulnerability that could significantly undercut deterrence or the capacity of the United States and its allies and partners to prevail in a conflict. To mitigate such vulnerability, three key elements should be used: First, the United States needs to act as a “cyber framework nation” to support host nation capabilities. This would involve the establishment, transfer, training, and support of cyber capabilities to enhance protection, resilience, and restoration. For example, the United States could help a less cyber-capable ally establish an effective intrusion protection system, provide forensic support, and develop resilience capabilities to be utilized in the event of an attack by an adversary. There are several ways to undertake such efforts but one of the most useful would be to utilize the National Guard’s State Partnership Program. The program pairs state National Guard units with seventy-six countries.97 As noted above, the National Guard is substantially increasing its cyber capabilities, including its focus on critical infrastructures. That expertise can be utilized in working with allies and partners in conjunction with the relevant combatant command. The National Guard’s partnership efforts can build on what the NMTs and the National Guard are doing in the United States, adapted, of course, to the particulars of the host nation. The National Guard could also be part of an initiative to provide “fly away” cyber-warfare teams to provide host nation states’ “blue team” assistance to “operate in degraded environments,” including providing malware forensics and recovery/restoration support. In addition to the National Guard, the DoD Cyber Crime Center (DC3) could have a valuable international role. DC3’s current mission revolves around five focus areas: digital forensics, cyber training, technical solutions, Defense Industrial Base (DIB) cybersecurity, and analytics.98 Like the Guard, DC3 provides tremendous depth and breadth of support; applied to international requirements it could enhance a greater USG role through a modest budget. DC3’s mission could be expanded to support extended cyber deterrence, especially in the areas of building greater allied cyber resilience. Key elements could include growing international training and information-sharing programs for allies (similar to ongoing programs with DIB companies in the United States). Second, associated with US assistance, it will be important for the host nation to establish operational partnerships with key private entities, including ISPs and power grid operators. As discussed in the context of the United States, military, telecommunications, and electrical grid operators should help create, in advance, capabilities that would mitigate a high-end attack. The United States, as a cyber framework nation, would help the host nation organize for this effort. Depending on the theater, it may be important to undertake such efforts on a regional, as opposed to a national, basis. Again, the United States will be well positioned to help create the necessary regional activities. Third, host nations will need to undertake steps comparable to those identified for the United States. These include • identifying highest-priority national military cyber assets and supporting telecom and power grid networks that would need to be protected; • extending/enhancing automated intrusion protection and developing resilience efforts, starting with data classification and segmentation, to participating host nations’ militaries, telecommunication companies, and electrical grids. It will be important to utilize high-end protection capabilities, such as multi-factor authentication, end-to-end data encryption, and diverse and redundant networks to ensure best information ssurance practices in data confidentiality, integrity, and availability; • increasing detection capabilities by provisioning shared cyber threat intelligence capabilities. A cyber threat intelligence capability would develop and share cyber indications and warnings regarding the movement of high-end state cyberthreat activity towards host nation networks and information assets; and • developing cyber defense “playbooks” and training exercises for cyber-attack response, with techniques, tactics, and procedures (TTPs) developed to maximize the value of the defense and resilience capabilities noted above. National grid and telecommunications partners in the private sector would be included as part of the playbook TTPs and training exercises. As previously discussed by the authors: “Initially, the cyber framework nation can help to establish or enhance an existing national framework. Over time, simulations, exercises, and information sharing will help direct and prioritize other efforts by exposing gaps and opportunities. Joint exercises, when effective, usually result in some degree of information sharing. Explicit and incidental information sharing, especially between private and public sector partners, will be a critical requirement if operational protection and/or resilience is to be achieved. Each country should pick a model it finds compatible, but the keys are a combination of speed and full interchange. In the US, one of the most effective models is the ‘Information Sharing and Analysis Center (ISAC), a nonprofit organization that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.’ ISACs are typically developed around a critical infrastructure sector, such as the electrical grid or telecommunications sectors. The Financial Services ISAC is often considered the greater among equals, as it has a highly automated system for rapid cyber threat information exchange.”99 As the foregoing indicates, cyber will be a critical element of high-end conflict. Enhancing deterrence and defense will require extensive actions by allied and host nation militaries along with civil authorities and the ISPs and grid operators in the host nation. VI. CONCLUSION High-end conflict will create challenging requirements for cyber, far beyond those that are already faced on an ongoing basis. The DoD needs to work with civil authorities and the ISPs and grid operators in the United States and forward theaters to create the prospects for deterrence and, if necessary, to defend and prevail in conflict.

### 2NC – Solves Commercial

#### Integration of cybersecurity into private sector supply chains is uniquely key.

Katie Arcieri 21, e-commerce reporter for S&P Global Market Intelligence, July 12, 2021, “Securing private, public US space assets”, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/securing-private-public-us-space-assets-65316329 \\SYang

The Biden administration has recently focused its efforts on quelling cybersecurity threats here on Earth. But security threats also exist in outer space as the U.S. increasingly relies on government and commercial satellites and other space assets needed for telecommunications, 5G networks and defense systems technology.

The Wilson Center's Science and Technology Innovation Program will provide an overview of potential cyberthreats in space during a July 14 virtual program titled "Cybersecurity on the Final Frontier: Protecting Our Critical Space Assets from Cyber Threats." The Washington, D.C.-based center is holding the event in partnership with The Aerospace Corp. and the Space Information Sharing and Analysis Center.

Historically, the U.S. has been very dependent on space-based systems to power everything from global positioning systems to 5G networks and to provide the ability to take pictures of the Earth for weather information, said Melissa Griffith, a public policy fellow with the center's Science and Technology Innovation Program.

That reliance will only increase as rapidly evolving technology further enables satellite capabilities.

"There is an incredible range up there in terms of what we are using them for," Griffith said. "As our dependency increases on space-based systems, so does our need to protect those systems, to build out secure, defensible and resilient systems."

There have not been any publicly disclosed space security threats on the same level of, say, the SolarWinds Corp. breach, Griffith said.

But possible cyberspace threats could stem from nations such as Russia and China, which have considerable space technology capabilities, as well as criminal groups seeking to hack into systems that may result in the loss of critical connectivity with defense weapons and or communications systems. Those potential threats have increasingly become a concern as the U.S. intelligence community investigates reports of "unidentified aerial phenomena" that could indicate extraterrestrial activity. Griffith could not speak to that specifically as it is not her area of expertise.

But the cybersecurity issues are taking on extra significance at a time when a growing number of private companies are doing business in space with various business models and approaches to the way they manage security risk. As of January, there were a total of 1,897 operating U.S. satellites, 1,486 of which are commercial, according to the Union of Concerned Scientists. There are also a total of 411 government, military and civil U.S. satellites.

Among the companies doing business in space are Blue Origin LLC, which was founded in 2000 by former Amazon.com Inc. CEO Jeff Bezos, and Space Exploration Technologies Corp., which operates the Starlink satellite broadband service. Amazon Web Services Inc. helps commercial and government customers build satellites and conduct space and launch operations. Lockheed Martin Corp. is the prime government contractor building NASA's Orion spacecraft.

Thus far, companies have generally focused less on security threats in space and more on ensuring system functionality in one of the harshest conditions known to mankind, Griffith said.

But the Wilson Center is encouraging policymakers and industry players to create frameworks for cybersecurity best practices, including identifying vendors in the supply chain that are high risk and pinpointing locations where ground-based stations — the brains of the satellites — can be more secure.

"One of the things that we are doing is saying, 'You're worried about this, we're worried about this, here are some questions you need to start asking industry to understand risk in this space,'" Griffith said.

#### Solves better --- implementation of cyber norms at all levels of the supply chain is uniquely key --- that requires collaboration with the private sector that the plan can’t access.

Amber Gillette 21, Staff Assistant Intern, Science and Technology Innovation Program, September 16 2021, “From Supply Chains to Spacecraft: Taking an Integrated Approach to Cybersecurity in Space”, https://www.wilsoncenter.org/blog-post/supply-chains-spacecraft-taking-integrated-approach-cybersecurity-space \\SYang

In his opening remarks, Morin noted key ways in which the average American interacts with space systems, including timing synchronization, banking systems, and emergency service provisions. “Space is really fully integrated into our society and it’s becoming more so everyday,” said Morin. “Both U.S. national security and our economic prosperity are dependent on space to a degree that most people just don’t fully appreciate.”

Space systems are not one of the 16 critical infrastructure sectors that are recognized as vital to U.S. national security and economy. However, developments in space technology, from advancing rocket designs to commercial deorbit services, are elevating space systems towards an official critical infrastructure designation, according to Erin Miller, Executive Director of the Space ISAC. “Even before Richard Branson travelled, space systems were and are critical infrastructure… It’s not necessarily the degree to which we’re dependent that makes the case, it’s just the fact that we are dependent upon space systems,” she said.

At the same time that our dependence on space has grown, the increased threat of cyberattacks has become a frightening reality for governments and individuals alike. “If you’ve even modestly been following the news, it’s clear that adversaries—criminal adversaries, state adversaries, a melange of both—are using cyberattacks that have an increasing sophistication and they are reaching a wider impact then they have before,” said Morin. “There is no reason to believe that trend isn’t going to continue.”

Space systems are not exempt from cyberattacks by any means, whether the ground stations to satellites in orbit, or the data links in between. This begs the question Morin posed to the speakers: “What needs to be done, both from a policy standpoint but also at the technical level—where the metaphorical rubber meets the road—to protect our space systems from cyberattacks?”

Tackling the Unique Vulnerabilities of Space Technologies & Systems

Space systems—which are composed of the vehicles and infrastructure needed to complete a task in the space environment, including but not limited to ground stations, data links, and satellites—are vulnerable to cyberattacks at multiple points, noted several speakers. “Satellites present a unique challenge: [they] have a limited amount of storage, memory and power on board and once you launch it, that’s what you get,” explained Prashant Doshi, Associate Principal Director of the Cyber Security Subdivision. “You have to run the mission on the hardware that’s already there. So there’s not a lot of extra hardware leftover to run McAfee or some other anti-virus [software].”

When thinking about protecting space infrastructure, you have to look at the entire space system, according to Miller, because all elements involved are vulnerable to cyberattacks. For example, low costs to entry and a wide pool of capable adversaries—from “script kiddie” hackers to sophisticated state actors—fosters an environment where an attack against a ground station could come from anywhere.

Additionally, as more and more adversaries place spacecraft in orbit and establish their capacity to conduct command link intrusions, the risk of satellite disruption or even loss of operational control to an adversary increases. The consequences of a cyberattack on space infrastructure can be “anything from temporary disruption to complete mission failure,” noted Brandon Bailey, The Aerospace Corporation’s Cybersecurity Senior Project Leader in the Cyber Assessments and Research Department.

The commercialization of the supply chain introduces new risk as well. Satellites used to be built according to a “boutique” model, where one satellite was uniquely designed for its purpose. However, with space becoming more accessible to a greater number of operators, it is now more common to use off-the-shelf components. This means that all satellites are vulnerable to cyber intrusion if even one part of their shared supply chain is corrupted. This threat of supply chain intrusion, alongside the nature of cyberattacks in general, means that the consequences of supply chain attacks by adversaries could be wide-reaching. “It may not be practical to fire hundreds of thousands of missiles at once, but it may be possible, with a single [cyber]attack, to attack multiple spacecraft,” said Ryan Speelman, Principal Director of The Aerospace Corporation’s Cyber Security Subdivision.

Fortifying the Supply Chain through Information Sharing

One of the conclusions reached by the panel was that unique threats to space systems are not being addressed to the same extent as unique threats to other critical infrastructures. In order to address these vulnerabilities and prevent such attacks from taking place, several panelists noted that the U.S. must incorporate cybersecurity planning into all stages of space system development. The first step to reaching this goal is increasing collaboration and information sharing among government organizations, commercial companies, and international partners in the space industry.

According to Speelman, the government uses a higher standard of defense and security requirements for space systems than private companies do. This becomes a problem when commercial companies do not fortify their space system components against cyberattacks. “It may be easy for DOD missions and the military to say, ‘well we don’t care.’ But when we’re buying a bunch of services, potentially bandwidth and other things from them, it becomes a really big deal,” he said.

This alludes to a problem faced by space system developers: due to the different regulations and requirements used by firms and within the government, it is difficult to ensure that components from all levels of the supply chain have the same quality of cyber protection. Miller explained that promoting transparency across the industry will be vital to securing the entire supply chain for space technologies. “I’m not asking that we specifically regulate those companies, I’m asking that in the Space ISAC that we come together and we collaborate,” said Miller. “So that we’re all aware of the baseline expectation for cybersecurity and we have active information sharing, so we have actionable intelligence around the threats.”

With the increasing prevalence of threats like ransomware attacks, information sharing across sectors and stakeholders will only become more critical. “We need to be very concerned and aware of whether or not the space industry has visibility on these different types of attacks and [when] they’re getting the information in a timely manner, it’s going to the right people who can take action,” Miller stated.

Overcoming Classification Barriers: Sharing What You Can

Transparency can be a difficult goal to reach in an industry where classification and intellectual property protection are salient concerns. However, there are ways to address potential vulnerabilities without divulging sensitive information. “To help somebody, you don’t necessarily need to right away share everything you have. Just the fact that you believe something is going on and it affects this particular subsystem—you don’t necessarily have to say what it is—that could be really useful for a lot of people… A little bit of information early on can help quite a bit.” said Speelman.

The Space ISAC and other government agencies are working to provide as much information as possible even with classification restrictions. Designating space systems as a critical infrastructure would help the flow of information. As Miller noted, “There’s a concerted effort towards making sure that the information that doesn’t need to be classified, that needs to be out there in the global space community, is reaching the global space community... We need to empower them, those space system critical infrastructure owners and operators, and give them the information they need.”

For successful prevention, information sharing must take place all the way down the supply chain, taking special effort to share information with small and medium sized companies involved in space system development. It’s not enough to target the large companies and organizations in this effort, because “if you’re not sharing that with your supply chain, then you’re introducing additional unnecessary risk,” said Miler.

Building Resilience in Space Using a Defense-in-Depth Model

On a more technical level, the panelists discussed strategies to build resiliency by fortifying space systems at multiple levels and leveraging new modeling technologies to test space systems. According to Bailey, the U.S. must incorporate a defense-in-depth model within its space systems to ensure that multiple layers, from the software to the encryption, are fortified against attack. “That’s another way to look at [defense-in-depth]: redundancy in your defenses,” he explained, noting that these defenses should provide not only preventative measures, but detection and recoverability capacity as well.

Penetration testing is another critical component to finding and mitigating vulnerabilities before they become problems, according to Speelman. “If we are not constantly attacking and finding holes and vulnerabilities in our own systems, our adversaries will do it for us,” he said. “I don’t think you can ever say your system is secure unless you're willing to try and break it yourself.” While project managers are hesitant to put their systems at risk, additional system engineering around the test itself and evolving digital twin technology allow penetration tests to be conducted without significant risk to the space asset itself.

Next Steps: Moving the Space Industry Towards Greater Cyber Awareness

Cybersecurity is not an issue that can be ignored or glossed over. If the U.S. is not proactive in securing its space systems against cyberattack, our adversaries will undoubtedly take advantage of our vulnerabilities. “We make ourselves as a country so vulnerable to a disruption in our space systems that it really will affect our society and quality of life. On that day when we get into a conflict, we will not be ready for [it].” said Doshi.

In order to fortify space systems, policymakers, engineers, and private corporations must make a concerted effort to change the way we develop and operate spacecraft. Cybersecurity must be built into each layer of the spacecraft’s design and at each stage of the supply chain, an endeavor that will require an entire industry to adjust its operating procedures. “If we can get as many people as possible pushing in that direction, I think we can make some big progress,” concluded Speelman.

### 2NC – Solves NC3

#### Solves NC3---forensics techniques, backdoor reduction, shift in architecture, honeypots can be implemented solely by the US.

Dr. Jared Dunnmon 17, postdoctoral fellow in the Computer Science Department at Stanford, xx/xx/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

One approach to the above scenarios would be an in-depth analysis of each question to determine exactly how the United States should respond. However, in light of substantial modernization to the NC3 system currently planned and under way, it is perhaps most useful to consider technological and policy avenues that could be pursued with the goal of ensuring that the above scenarios, each of which is fraught with uncertainty around nuclear intentions and appropriate U.S. response, would never come to pass. Distinct sets of technology and policy recommendations intended to inform discussion around modernization and design of the future nuclear enterprise are presented below. Technological Directions Several concrete technological initiatives would help reduce operational uncertainty and ensure resilient NC3 functionality. Apply Advanced Forensics Techniques All NC3 satellites should be outfitted with advanced forensics capability. Motion sensors, heat sensors, and EM intensity sensors should be emplaced in order to assess whether any given satellite inoperability resulted from external physical attack. For protection from cyber attack, domestic control over supply chains should be pursued to reduce the possibility of backdoors, insecure or undocumented protocols, and hard-coded credentials. Finally, in addition to traditional antivirus scans of satellite software, commercially available assessments based on computationally efficient code-level machine learning tools that proactively detect both new variants and repackaged versions of existing malware should be implemented.48 Such methods should prove powerful in reducing the possibility of a successful cyber attack on NC3 systems. Emphasize Modern Network Defense Techniques in NC3 Traditionally, network defense has focused on keeping attackers outside of a virtual “wall,” while keeping all critical functionality accessible to those with valid credentials. In today’s democratized cyber environment, cost to attackers is substantially lower than cost to defenders. Thus it is useful to consider moving toward an architecture that is more akin to a building with all of its doors open, but riddled with traps and misdirection. As NC3 is modernized to utilize Internet-based protocols,49 for instance, considering widespread implementation of mechanisms designed to increase costs to attackers via such methods as honeypots, script white-listing, and address scrambling would help to deter and frustrate potential attackers. Honeypots, or environments that look like useful targets to an attacker but are in fact benign, can be particularly useful in enabling U.S. personnel to identify candidate attack vectors and enact defenses before critical systems are compromised. Script white-listing entails using efficient data structures to enable a computer to run only code with a bit representation that has been explicitly pre-specified as part of an allowed execution set. Finally, address space scrambling methods such as address space layout randomization (ASLR) protect from common buffer overflow attacks by randomly arranging address space positions of key portions of a process, such that an attacker cannot jump between dif­ferent points reliably. As a higher-level consideration, the United States should consider the idea that it is generally not possible to be completely sure that a networked computer system has not been compromised. If an adversary informed the United States that it had compromised U.S. NC3 and that surety of the nuclear deterrent had been affected, it would be extraordinarily difficult for the United States to prove otherwise, which fundamentally undermines the strength of the U.S. deterrent posture. Thus, it is imperative that the United States be able to viably make the argument that compromising the entirety of NC3 would be a statistical impossibility; and for this to occur, there must exist no possible mechanism for a single point of failure. While the command, control, and communications triad architecture ensures this posture adequately from a physical standpoint, it is imperative that NC3 systems be constructed with the same ideas in mind. Specifically, the United States should consider a fractionated NC3 network design, with a large number of sub-networks, each secured via dif­ferent sets of protocols or standards. In this case, it would be nearly impossible for an adversary to convince either itself, the United States, or third parties that the surety of the U.S. nuclear deterrent could be fully compromised by what would effectively be a first cyber strike. Minimize Code Base Size As systems are modernized to take advantage of twenty-first century information technology (IT), the temptation will exist to implement a great deal of additional functionality. While there may exist substantial operational benefits to additional features, these should always be balanced with the reality that more code almost always equates to more vulnerability—and NC3 is an area wherein a vulnerability could result in mistakes of nuclear import.50 Thus, the usual analysis around the cost-benefit trade-off of IT upgrades may not apply to NC3 systems, and this reality should be taken into account in system design processes. Maintain Small-Scale Launch and Inexpensive NC3 Communications Hardware A particularly interesting suggestion put forth by Dr. John Harvey, former principal deputy assistant secretary of defense for nuclear, chemical, and biological defense, is that “small, single-purpose ‘cheap-SATs’ to replenish lost communication or GPS [global positioning system] functionality” could improve system-level resilience of space-based NC3 assets. Instead of or in addition to large, multifunctional satellites, leveraging the widespread proliferation of small, inexpensive CubeSats51 that cost on the order of $100,00052 to construct and launch could substantially reduce overall system cost and improve reliability. In addition to allowing inexpensive system updates as technology improves, these small satellites would be extremely difficult to target for ASAT operators. Further, since Dr. Harvey’s address in 2014, small-scale launch technology has seen significant advances. In fact, several commercial entities currently have the technology to offer 150-kilogram payloads to sun-synchronous orbit (500-kilometer altitude) on a single dedicated rocket costing only $5 million.53 These rockets could be retained specifically for emergency NC3 launches as backups to current satellites. In this way, expensive AEHF satellites that would require an expensive, large-scale launch to reconstitute would be supplemented or ultimately replaced by a small satellite and dedicated launch ecosystem that would result in a substantially more resilient NC3 system. Moving to a reserve of small satellites as a backup for the NC3 network would also have the advantage of increasing the number of possible launch sites the United States can use. At present, only a handful exist, and these are well-known to any potential adversary.54 Decrease Reliance on Space-Based NC3 In addition to shoring up the reliability of space-based NC3, ultimately decreasing U.S. reliance on these assets would likely enhance overall NC3 surety.55 In particular, relying more on the various airborne components of the NC3 system and deploying “long-range airborne communications relay networks that could be stood up on short notice” would potentially mitigate the vulnerabilities posed by cyber threats to space-based assets. This risk reduction would result not only from the ability to more rapidly deploy space-based systems, but also from the simple reality that 50. Danzig, Surviving on a Diet of Poisoned Fruit. 51. A variety of companies (e.g., Planet Labs), universities, national labs (e.g., Los Alamos National Laboratory), and research institutions already fly multiple CubeSats. 52. “Commercial Space Launch Schedule and Pricing,” Spaceflight.com, accessed 31 July 2016, http://www.spaceflight .com/schedule-pricing/. 53. “Space Is Now Open for Business,” Rocket Lab, accessed 31 July 2016, https://www.rocketlabusa.com/. 54. Ellis, personal conversation with the author. 55. Rose, “Using Diplomacy to Advance the Long-Term Sustainability and Security of the Outer Space Environment.” This content downloaded from 67.194.16.231 on Fri, 24 Jun 2022 18:46:22 UTC All use subject to https://about.jstor.org/terms 30 Project on Nuclear Issues performing diagnostics and updates on hardware that is not in outer space is a far simpler process than the reverse.56 Policy Considerations Carefully Consider Unilateral Action: Anticipatory Self-Defense and Belligerent Reprisal Given the Tallinn Manual’s clear authorization of anticipatory self-defense and the potentially dire consequences of the scenarios outlined above, it would be prudent to pursue a national policy that enables U.S. intervention to combat the development of cyber capabilities that would compromise NC3. In the context of peacetime international law, this would likely entail either claiming extraterritorial jurisdiction over those developing anti-NC3 cyber capabilities and/or claiming anticipatory self-defense if an attack is imminent. Were the United States to already be engaged in an armed conflict, the functional equivalent of anticipatory self-defense would be legally termed belligerent reprisal.57 In this case, if the United States views attacks on NC3 as outside the boundaries established by the LOAC, the question would become whether a proportional attack on opponent (potentially on their NC3) would be appropriate, and, if so, what form that proportional response would take. Even in the case that U.S. NC3 is compromised, for instance, it is still desirable from the U.S. point of view for the adversary’s NC3 systems to be able to verify that the United States has not launched a nuclear attack. Thus, in the context of belligerent reprisal, it is critical to make a clear policy decision on what constitutes a proportional, but practically optimal response to an attack on U.S. NC3.

### 2NC – Solves Deterrence

#### Solves deterrence

Micah Zenko 14, Whitehead Senior Fellow on the US and Americas Programme at Chatham House, April 16, 2014, “Dangerous Space Incidents”, https://www.cfr.org/report/dangerous-space-incidents, Council on Foreign Relations \\SYang

The United States could issue clear and specific public warnings to deter malicious activity in space. As of yet, U.S. deterrent threats are confined to Pentagon planning documents, or have been applied with little specificity to cyber and space domains contemporaneously. If the space event was detected during the planning stage by the U.S. intelligence community, or it became clear that a country developing space capabilities intended to use them maliciously and the resultant space debris could be predicted by JSpOC, the United States could publicize the costs that such debris would pose to the world’s satellites in an attempt to marshal international condemnation to prevent it.

### 2NC – Decentralization Key

#### International de-centralized cooperation key---over-centralization and nationalist efforts both fail.

David Livingstone and Patricia Lewis 16, associate fellow in the International Security program; leader of the International Security program at Chatham House, September 2016, “Space, the Final Frontier for Cybersecurity?”, https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf, International Security Department \\SYang

The response to a complex and specifically internationalized cybersecurity problem needs to be based on an international coherent approach, which can be defined as a regime – that is, a set of: … implicit or explicit principles, norms, rules and decision-making procedures around which actors’ expectations converge in a given area of international relations. Principles are beliefs of fact, causation and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action, decision-making procedures are prevailing practices for making and implementing collective choice. There is an urgent requirement to develop a space cybersecurity regime that will inform and organize policy efforts and subordinate strategies, while remaining federally networked rather than controlled from a centre or hierarchically driven. Too centralized an approach would give the illicit actors, who are generally unencumbered by process or legislative frameworks, an unassailable advantage simply because their response and decision-making time is more flexible and faster than that of their legitimate opponents. To be successful and durable, the space cybersecurity regime should be one that functions intelligently and responsively, and possesses enough flexibility to be able to react in a coordinated way as the environment and circumstances alter. As noted above, over-zealous central direction by regulators in a market-driven sector tends to lead to the supply chain finding ‘workarounds’, leading to the risk of developing a general culture of cyber insecurity in which the default condition is simply to identify the best way to dodge the rules. This hands another advantage to the adversaries of legitimate users of the space domain. However, the international space community has not yet acted as a coherent system in the area of cybersecurity. This problem is compounded by the fact that the nature of space and its relationship to society are entering a period of fundamental change. The stakeholders required for the space cybersecurity discourse remain essentially segregated (apart from occasional meetings at events such as conferences), and are only concerned with managing risks within their narrow fields of interest. Left unaddressed, this dynamic will in all likelihood continue unless there is an external stimulus. As a result, there will be little recognition that each stakeholder can be affected by another’s security, or lack of it, unless there is a change in perceptions. A significant element of self-help is required to make up for the shortcomings of the regulatory cadre. A space cyber regime, based on a lightly regulated initiative from the supply chain, seems to offer the most suitable and sustainable basis for channelling multinational contributions to an internationalized space cybersecurity capability which has to include an ever greater number of different stakeholders. Such a regime must be agile enough to meet the rapidly evolving security challenge facing the space domain, and to continue to develop as the market is transformed over the next decades. Policy requirements Ideally, the policy needed to establish a space cybersecurity regime would align the needs of all the various concerns: on an already complex international stage this would include the millions of end users, individual scientists, the corporate sector and the military; address technical, political, economic and social interests; and combine the tactical with the strategic and the bottom-up with the top-down approach. To align across and within all sectors, one approach is to adopt a single focus – such as the provision of assured broadband via space – and make that the driving force, organizing all other initiatives around it. But the space domain is now becoming so intrinsic to every human activity, whether government, private-sector or individual, that the foundation of a more robust and coherent space cybersecurity regime requires a common understanding of what is essential to determine both the nature of the problem and threat mitigation responses. The approach must be non-hierarchical, where each stakeholder is empowered by knowledge provided by the regime and feels valued as a contributor. Ensuring security in space must correspondingly be a common ambition for all concerned players. Thus a common approach to cybersecurity can be developed and encouraged by applying the principles of governance, management and inclusiveness as outlined below. Governance There are three paramount dimensions in the governance of a space cybersecurity regime. First, whatever is done to combat space cyber insecurity, policy should be adopted and applied in order to enable legitimate users of space-related capability, while increasing the costs (of entry, for example, or discovery and being subject to law enforcement action) for illegitimate users. A culture of space cybersecurity must lead to the development of an innate instinct for what is safe and what is risky throughout the supply chain. Second, the governance of space cybersecurity needs a collective approach, involving as many legitimate stakeholders as possible and practical. This will also create a progressive and dynamic environment where knowledge is a key ingredient; if participants can share experiences and lessons learned, cybersecurity will become increasingly instinctive, from the boardroom down to the shop floor, and its sum will increase. Third, the regime needs to be based on a self-governing and lightly regulated effort by a wide range of legitimate users of space capability. This is because space infrastructure, with its multiple uses, is a complex and constantly adapting area that defies control, centralized management and oversight by any single stakeholder (except for some very specific processes such as orbit or communications frequency allocation). Experience suggests that there is no other option but to deliver this effort within a business environment of transparency and accountability involving collaboration designed to share knowledge. Effective and durable governance of cyberspace requires a shared awareness that implies a dynamic, common approach to raising cyber capability. A culture of space cybersecurity must lead to the development of an innate instinct for what is safe and what is risky throughout the supply chain.

### 2NC – Grid Plank

#### Plank: The United States federal government should create and fund the Institute for Electric Grid Cybersecurity.

#### Solves -- the IEGC will develop and enforce cybersecurity standards regarding the electric grid.

Bipartisan Policy Center 14, Washington, D.C.–based think tank that promotes bipartisanship, February 2014, “Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat”, https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2019/03/Cybersecurity-Electric-Grid-BPC.pdf \\SYang

NERC should continue to develop and enforce cybersecurity standards in a manner that is consistent with a risk-management approach and that provides affected entities with compliance flexibility. FERC and applicable authorities in Canada should be supportive of this approach in their review of NERC standards. n The electric power industry should establish an organization, similar to INPO, that would develop cybersecurity performance criteria and best practices for the entire industry. This organization would be intended to complement the standards process that is in place at NERC. We encourage the industry to establish such an organization before a significant cybersecurity event occurs and requires a rapid response. A centralized, industry-governed institution may be in the best position to promote effective strategies for managing cyber threats that could have broader systemic impacts. This effort should include the full range of generation, transmission, and distribution providers and market operators in the North American power sector, including municipal utilities and electric cooperatives. It should be funded through member dues. We envision that this organization—which we will call, for purposes of this discussion, the Institute for Electric Grid Cybersecurity (hereafter, the institute)— would be charged with several activities: • Development of performance criteria and cybersecurity evaluations. The institute would develop performance criteria and best practices for cybersecurity and perform detailed evaluations of individual facilities according to these criteria. Performance criteria and best practices should be tailored to address conditions for individual companies and systems, taking into account their contribution to larger systemic risks. • Analysis of systemic risks. With industry’s assistance, the institute should conduct analyses to identify facilities or locations on the system, and in particular the distribution system, where a localized cyber event could have disproportionate implications for the broader electric grid or for economic or national security. For example, there may be places on the grid where, because of system interdependencies, the loss of a particular substation could trigger a cascade of impacts in multiple critical infrastructure sectors. While many utilities have taken inventories to identify critical facilities or customers, a broader national inventory, combined with modeling and scenario analysis, should help to identify priority areas for cybersecurity investment from the perspective of protecting the grid as a whole. • Event analysis. While NERC, FERC, state and provincial agencies, and potentially federal law enforcement or intelligence agencies are likely to be involved in analyzing significant cybersecurity events, the institute should play a role in understanding the cause of such events and disseminating lessons learned. • Technical assistance. The institute should provide technical support to entities that need assistance implementing performance criteria. It should also facilitate the use of cybersecurity tools—such as the ES-C2M2—produced by industry and government partnerships. • Training and accreditation. The institute should engage in efforts to define positions and career paths for utility cybersecurity professionals. The institute could partner with, or potentially house, ongoing efforts to develop cybersecurity certifications.

# DA

## Ambiguity DA

### 1NC – DA

#### The squo is goldilocks – locks in strategic ambiguity over both cyber thresholds and responses as official policy – but there’s a strong norm against activating Article 5 against non-violent attacks.

Justin Lynch 18; Associate Editor at Fifth Domain, contributor to the New Yorker, Foreign Policy, the Atlantic; 7/10/18, "Cyber ambiguity: NATO’s digital defense in doubt amid unstable alliances," https://www.fifthdomain.com/international/2018/07/09/cyber-ambiguity-natos-digital-defense-in-doubt-amid-unstable-alliances/

Today, the alliance counts cybersecurity as one of its core missions. It has placed a new cyber research center in the heart of the Baltic nation.

But amid what is viewed as a sustained campaign of Russian digital warfare on the West and the trans-Atlantic alliance ― whose foundations are being questioned through a surge of populism ― the very future of NATO’s cyber strategy is left intentionally murky.

During a May speech, NATO Secretary General Jens Stoltenberg said he is often asked under what circumstances the organization would trigger Article 5 in the case for a cyberattack.

Article 5 is the alliance’s principle of collective self-defense; an attack on one member nation is considered an attack on all member nations.

“My answer is: We will see. The level of cyberattack that would provoke a response must remain purposefully vague, as will the nature of our response,” Stoltenberg said. “It could include diplomatic and economic sanctions, cyber responses, or even conventional forces, depending on the nature and consequences of the attack.”

Questions over how NATO will respond to a cyberattack come as the alliance takes steps to bolster its digital protocols. In its joint air power strategy, unveiled in late June, NATO added cyberwarfare to its joint operations programs. The document boasts of the historic threat the organization faces: “For the first time since the end of the Cold War, the Alliance has to be able to conduct operations.”

In 2014, the alliance said for the first time that a cyberattack could trigger the organization’s collective-defense mechanism. It has proven a successful deterrent to combat large-scale digital attacks like the reported Russian cyber assault on Estonia in 2007, said Sorin Ducaru, a former assistant secretary general of NATO. But he added that the alliance has to be more creative in deterring medium- and low-grade cyberattacks “because that is the world we are living in.”

For Estonia, an aggressive NATO cyber policy could be the difference between the smooth withdrawal of cash or a disturbing “error” sign flashing on an ATM screen. An Estonian intelligence report from earlier this year predicts Russia will continue its campaign of aggression in Eastern Europe and the Baltic states through a combination of cyberattacks and information warfare.

When it comes to digital threats, “each country has faced them alone. NATO has not adopted a unified response,” former Estonia President Toomas Hendrik Ilves said during a May conference.

Today, nations are still loath to share information on cyberattacks, Ilves said, recounting a story about how as president he reported a hack on Estonia to NATO. “The response was: ‘Oh, you, too.’ I don’t think that’s how we should be doing things.”

Ilves is among those who have called for a cyber NATO ― an alliance of nations cooperating in digital defense.

The top civilian of Estonia’s Ministry of Defence also told Defense News that international cooperation could help thwart cyberattacks.

“I think people are realizing that we need international cooperation, and without international cooperation we simply cannot succeed in this new domain,” Jonatan Vseviov said.

Yet a bolstered NATO cyber response could mean a wave of new tension with Russia and China, which are seen as two of the alliance’s biggest digital challengers.

It is unclear under existing NATO rules how the alliance could be more aggressive in response to cyberattacks, said Alex Crowther, a senior research fellow at the National Defense University.

“In order for Article 5 to be voted on, it has to be something major. It pretty much has to be an armed attack or a use of force as discussed in the U.N. Charter. The most commonly adopted point of view is that people have to be hurt or killed, or property is damaged or destroyed,” Crowther told Fifth Domain, a sister publication of Defense News. “I have met people who say that the only attack that meets that criteria was the Stuxnet attack because it caused damage to Iranian centrifuges.”

Even the hack on Estonia did not meet the criteria for triggering the principal of collective self-defense, Crowther added.

#### Cyber defense is intentionally ambiguous – the plan removes flexibility and encourages adversary probing – current Article 5 threshold properly responds to armed attacks.

Z’hra Ghavam 16; Navy Lieutenant Commander; September 2016, "NATO’s Preparedness for Cyberwar," https://www.hsdl.org/?abstract&did=801548

NATO’s publicly declared policy on cyber threats is consciously and purposefully vague.207 Why? Strategic ambiguity has its benefits. According to the Atlantic Council panel, there is no “redline” or “determined threshold” that would automatically define a cyber act as an act of war.208 Leaving the rules undefined affords NATO ample room in which to operate. For a 28-member multinational organization that operates on the principle of consensus, time and latitude for solidifying strategic-level decisions are critical. If NATO publicized a cyber redline, it would box the Alliance into a corner. This kind of policy could embolden cyber offenders and provoke massive intrusions that target NATO’s networks at just below this threshold. Having a defined redline could also invite nefarious cyber actors to cross it to test NATO’s resolve, damage its reputation as a leader in Euro-Atlantic security, and undermine the credibility of its Article 5 commitments.

Following the Wales Summit in 2014, NATO affirmed its stance on law and cyberspace while refusing to address cyber redlines:

Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm, therefore, that cyber defense is part of NATO’s core task of collective defense. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.209

However, an invocation of Article 5 does not necessarily mean that a NATO response would include force. Article 5 of the Washington Treaty states the following:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.210

Thus, as long as each Alliance member takes “such action as it deems necessary,” it cannot be found in violation of the collective defense principle.211 In the case of a major act of cyberwar against one of its members, NATO could invoke Article 5 as a show of solidarity but opt to refrain from employing kinetic military force; instead, the Alliance could use purely cybernetic means or a hybrid alternative that combined cybernetic tools with military force to fulfill its objectives.

In all, NATO’s establishment, organization, and employment of its sophisticated cyber response agencies and IT resources like the NCIRC, NCIO, NCIA, and RRT are indicative of how seriously the Alliance has implemented its cyber defense policies at the operational level. NATO’s cyber policy, standard operating procedures, and ambiguous thresholds for the use of military force make the Alliance highly prepared to respond effectively to major acts of cyber aggression against one or more of its members. If an act of cyberwar met the threshold of an armed attack, NATO would probably be prepared to manage, counter, and resolve the issue in cyberspace; still, one cannot exclude the possible need to take kinetic measures. Out of a numerical ranking of 1–3, the Alliance earned a preparedness score of 3 in cyber strategy.

### 2NC – Turns Case

#### This solves their offense – a general consensus is good but shouldn’t be official policy – ambiguity stops miscalculation and preserves flexibility for unanticipated threats.

Ken Jones 15; MS in Cyber Systems and Operations from the Naval Postgraduate School; March 2015, "Cyber War: The Next Frontier for NATO," https://calhoun.nps.edu/bitstream/handle/10945/45201/15Mar\_Jones\_Ken.pdf?sequence=1&isAllowed=y

Finally, NATO needs to maintain ambiguity on what justifies an Article 5 response. As mentioned previously, ambiguity has served NATO well. A set threshold for when NATO will invoke an Article 5 response to a cyber-attack on a member country is not necessary. This ambiguity has historically served the alliance well, as demonstrated by the 9/11 attacks. If the alliance had said weapons were only include guns, bullets, tanks, and bombs, it would have set a threshold precluding a NATO response to attacks that turned four planes into improvised missiles. The larger issue of ambiguity is that there is no set definition of what constitutes an armed attack and what circumstances dictate a collective response, as per Article 5. Remaining ambiguous on the severity threshold of a cyber-attack allows the alliance to act in cases of future cyber-attacks that cause severe damage, but also allow NATO to refrain from over-reacting, even if an event is a cyber, or kinetic, attack as per a definition. It would be a mistake to set a threshold for attacks that cannot currently be anticipated.

When NATO was originally formed, it was with the purpose to be unambiguous, with the promise of “massive retaliation” by Eisenhower. This was meant to constantly act as a reminder to the Soviet Union and the Red Army that if they were to surge into Western Europe, in no uncertain terms NATO would respond with nuclear weapons. Ambiguity is useful in times, and at other times, it is not. Had NATO been ambiguous in dealing with the Soviet Union, there could have been opportunity for the Red Army to advance further across Europe, to test and see what NATO, and the United States, would allow them to get away with, without an attack. Ambiguity can also cause problems, particularly in the event of a cyber-attack with some members feeling an attack might warrant retaliation through Article 5, with others feeling that the necessary thresholds have not been met. It is important for NATO to have a clear understanding, or general belief, of what would constitute a serious enough cyber-attack in order to respond, but not through official policy or rules to ensure proper consideration.

### 2NC – ! – Non-State

#### Ambiguity specifically solves non-state actors – spills over to responding to state actors which solves case.

Łukasz Kulesa 19; Deputy Head of Research at the Polish Institute of International Affairs, MA in International Relations from the Faculty of Law of Jagiellonian university; 11/28/19, "The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures," https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440

NATO needs to be careful about defining and signaling its redlines. Making these boundaries too specific could embolden adversaries to intensify their actions below NATO’s declared threshold of response. Being deliberately ambiguous and raising the fear of retribution may be more useful for encouraging adversaries’ self-restraint.

At the same time, NATO should aim to deter specific types of particularly threatening unconventional activities. These include major and sophisticated cyber attacks against allies’ military forces and critical military and civilian infrastructure, proxy military and special forces operations, and state-sponsored terrorism. NATO could declare that such activities may lead it to invoke Article 5 and respond in various ways, including asymmetrically (for example, the response to a cyber attack may not involve only cyber capabilities).

The alliance must be able to identify early whether and when unconventional and hybrid gray-zone actions have become a more substantial and coordinated campaign. In such a case, NATO should aim to deter the adversary from escalating further. This requires increasing the alliance’s capacity to share early-warning intelligence and pool national intelligence-gathering, investigation, and attribution capabilities. NATO should not shy away from attributing ongoing operations to state adversaries, relying on national data as needed. The alliance and its members should be prepared to use direct channels of communication and other means to deliver immediate deterrence signaling in specific cases.

On the Southern flank, NATO faces state actors that use unconventional tactics and proxy forces (for example, Iran and Syria); state collapse and the emergence of ungoverned spaces in Libya, Yemen, and parts of the Sahel; and the activities of a range of nonstate actors, from loose groups to terrorist and criminal networks to highly organized quasi-state structures like Hezbollah. Cooperation with regional partners in addressing these threats will be vital. NATO’s primary task, as elsewhere, should be to deter states in the region from using unconventional tactics against NATO and its allies, using signaling and attribution tools. When possible, the alliance should aim to affect the calculus of nonstate actors to prevent them from harming alliance interests. This may not work with jihadist groups but may be possible with actors motivated by political or economic interests.

Since many of the unconventional threats are not linked to specific regions or actors, a more general approach is called for. The alliance and its members need to continue investing in passive and active measures to neutralize unconventional threats, including in peacetime. Further developing cyber defense and offensive capabilities—NATO’s toolbox for countering hybrid tactics—and strengthening resilience can affect adversaries’ willingness to use unconventional means against NATO and thus help establish deterrence by denial. The toolbox—counterterrorism, special forces, information operations, disruption of terrorist groups’ cyberspace activities—that allies develop for dealing with nonstate and quasi-state entities posing unconventional threats can also be used to deter state adversaries that rely on such tactics.

### 2NC – Link – Deterrence

#### Ambiguity deters attacks – clarification encourages attackers and causes alliance disputes.

Susan Davis 19;General Rapporteur to the NATO parliamentary Assembly Science and Technology Committee; 4/18/19; "NATO in the Cyber Age: Strengthening Security & Defense, Stabilizing Deterrence," https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087\_STC\_19\_E%20-%20NATO.pdf

60. NATO maintains a cyber deterrence policy of ambiguity. First, it does not draw a clear line for when a cyber attack is sufficiently harmful to cross the threshold to an armed attack. Second, it does not currently have an operational definition of what the collective response would be if that threshold were to be crossed. Such a cyber deterrence policy offers several advantages, but also poses distinct challenges.

61. A certain degree of ambiguity is beneficial because it could make opponents wary of going too far in their cyber attacks. The opponent always fears stepping over the invisible line, and thus prefers treading lightly. A similarly vague deterrence posture arguably worked well during the Cold War. However, ambiguity on where the threshold lies could indeed lead an opponent who is sufficiently comfortably with taking risks, to continuously exploit the ‘grey zones’, test the defender’s resolve, and conduct ever more daring cyber attacks.

62. If the Alliance were to set a clear threshold, the opponent would better understand how to stay below that threshold. This would strengthen deterrence of threats above the threshold but would encourage the opponent to increase attacks just below the threshold. Arguably, the solution for such attacks cannot be found in deterrence, but rather in clearly defined policy response for hybrid operations. Despite its best efforts, the Alliance continues to struggle to develop such options. Setting specific thresholds without strong options for hybrid operations would only encourage more of them. Moreover, the Allies could also find it hard to agree on and perhaps also credibly commit to a specific threshold. Thus, on balance, the policy of ambiguity on thresholds makes sense.

63. NATO’s ambiguity also extends to the type of punishment it threatens were it to suffer a cyber attack. The Alliance has made clear that it neither limits punishment to similar cyber attacks nor excludes them. Instead, it keeps the option open to use the full range of Allied capabilities to deter and counter cyber attacks. Once again, this introduces useful doubt in an opponent’s mind. While NATO would retaliate in a proportional manner, it could do so through similar cyber attacks, air strikes, or worse. A more technical reason for the difficulty of restricting retaliation to cyber attacks is that it is hard to credibly threaten the assets of the attacker in a similar fashion. If an attacker shuts down a power plant, would the Alliance have cyber options to attack an opponent’s power plants or similar infrastructure? Would NATO even want to if it could?

64. On balance, NATO’s ambiguity on the type of retaliation serves a convincing purpose. It produces doubts in the would-be attacker’s mind and presents more options to tailor and scale a response to re-establish deterrence. That being said, in practice, this so-called cross-domain deterrence can be complicated, problematic, and difficult to control (Nye, 2017). For example, proportional response in the mind of the defender might look escalatory to the attacker.

#### The plan gives adversaries impunity to confidently act below the threshold – case-by-case evaluation is intentional and advantageous.

Mustafa Canbolat and Emrah Sezgin 16; PhD in Management Science from McMaster University, Associate Professor of Operations Management and Business Analytics at the State University of New York; MBA as an International Military Officer from the Naval Postgraduate School, Senior Program Manager at Amazon; December 2016; "Is NATO Ready for a Cyberwar?" https://www.hsdl.org/?view&did=810939

One of the most discussed issues in the international arena after the 9/11 attacks was the Digital Disaster scenario that could be experienced in a member country (Bicakci, 2014). Many countries have incorporated cyber security strategies in their national security strategies in order to address cyber-attacks that could threaten the state. The role of NATO in the case of a serious cyberattack against a member country has been a conundrum.

Due to the difficulty of attributing a cyber-attack, NATO appears to have a pragmatic cyber security posture that handles each attack on a case-by-case basis (Burton, 2015). However, NATO officially stated that “NATO will consider (and potentially implement) a collective Article 5 response to cyber-attacks against NATO members, just as it did in response to the terrorist attacks on 9/11” (Burton, 2015, p. 308). Nevertheless, the threshold for the cyber-attacks that could invoke Article 5 is not certain. The head of NATO’s Emerging Security Challenges division, Jamie Shea stated that “[w]e are keeping that ambiguous so a potential aggressor does not get the idea they can carry out cyber-attacks up to a certain level with impunity” (Ashford, 2014, para. 8). Even though setting a specific and certain threshold would make it easier for NATO to determine when to invoke Article 5 against a cyber-attack, keeping it ambiguous gives an advantageous flexibility to the alliance regardless of the attack or adversary (Jones, 2015).

Article 5 was purposely left vague to give NATO more flexibility to assess a threat and determine a response. Therefore, it is also uncertain what kind of a response NATO would give against a cyber-attack. Would it be a cyber or a kinetic operation against the adversary if Article 5 were triggered? The answer to this question is deliberately left ambiguous, reinforcing NATO’s position that it will evaluate cyber-attacks on case-by-case basis.

#### Closing the window of escalation encourages adversaries – their choice of grey-zone threats signals sensitivity to escalation.

Sugio Takahashi 19; Chief of Policy Simulation at the National Institute of Defense Studies, MA in Political Science from Waseda University; 1/9/19; "Development of gray-zone deterrence: concept building and lessons from Japan’s experience," The Pacific Review, Vol. 31, Issue 6, p. 787-810

Third aspect of gray zone deterrence is that deterring states should never close the window for escalation. The main reason why the challengers use gray zone threats to change the status quo is that, first, they are discontent with the status quo and, second, they recognize their inferiority in conventional military challenge (Mazzar, 2015). The challenger may choose gray zone creeping expansion, rather than conventional military challenge, because the cost of conventional military challenge would easily exceed potential gain. Therefore, they may refrain from launching the challenge in the first place if they realize that their expansion has plausible risk of escalating to military conflict. The tripwire definitely has an effect that the challenger estimates higher possibility for escalation. If deterring states absolutely refrain from escalating countermeasures, the challenger side can continue gray zone creeping expansion eternally without taking any risk accompanied with escalation. In order to stop them, the deterring side needs to develop robust posture to win the possible war in the case of escalation, and make the challengers recognize the possibility of unfavorable military conflict. The critical role of military force, which cannot be substituted by other toolkit of statecraft, exists in this aspect of gray zone deterrence. And in this context, war-fighting capabilities still have an irreplaceable role to play.

### 2NC – AT: New Domain/Inexperienced

#### Cyber being distinct is a reason to err neg – ambiguity’s necessary to respond to unpredictable threats with maximum flexibility.

Ken Jones 15; MS in Cyber Systems and Operations from the Naval Postgraduate School; March 2015; "Cyber War: The Next Frontier for NATO," https://calhoun.nps.edu/bitstream/handle/10945/45201/15Mar\_Jones\_Ken.pdf?sequence=1&isAllowed=y

To answer this question, it is important to look at the first (and only) time NATO invoked an Article 5 response; namely, following the 9/11 attacks on the United States. When the partners of the alliance first wrote the Washington Treaty, it was initially to deter the Russians from expanding and to deter nuclear warfare at the onset of the Cold War. Article 5 is purposefully vague to give NATO considerable room to maneuver. Before the 9/11 attacks led by Al Qaida, it would have been nearly impossible for anyone, anywhere, including the framers of the Washington Treaty, to imagine such an attack. Likewise, at the 2014 summit in Wales, NATO announced that it would and could invoke an Article 5 response to a cyber-attack, and that the ambiguity would stand.158 NATO’s Ambassador Sorin Ducaru, NATO’s assistant secretary general for “emerging security challenges,” made the following remarks:

[T]here’s no predetermined threshold…there was a conscious decision by the allies in this policy that there is benefit in keeping flexibility and ambiguity…article 5 was by design something that should be invoked politically by [member] nations in a specific context, on a case by case basis…article 5 was never designed to be triggered by a certain threshold. The only time it was invoked was after 9/11, which was a scenario that had never been contemplated by the founding partners.159 In this same vein, Christopher Painter, the U.S.’ State Department cyber coordinator said:

The NATO leaders’ declaration that international law including the UN Charter, the Law of Armed Conflict, international humanitarian law, etc. applies in cyberspace just like it does in the physical world…[t]his is a clear statement that this is not a lawless space. There was some doubt before. There was some thought you had different rules entirely for the cyber world than the physical world, which made no sense and in fact would be very destabilizing.160

In light of the recent developments of NATO, it would seem to be in NATO’s best interest to remain ambiguous and allow the organization to approach its response to a cyber-attack on a case-by-case basis. For instance, the attacks on Estonia might require intervention on behalf of the Estonian people due to the fact they are a smaller, lesser defensible state. Estonia would not be successful standing up against Russia, and as Russia becomes more aggressive in the former-Soviet bloc region, small states like Estonia are at risk. If another attack were to occur against Estonia, the attacks would have to be more severe to invoke an Article 5 response. Such a response would enable NATO states to act as if they too have been attacked as per the mutual defense announcement against cyber-attacks at the Wales Summit. Yet, if the United States is attacked in a similar manner, there likely does not need to be the same scale of defense taken, because the United States has more resources and capabilities to respond on its own. Remaining ambiguous allows NATO to choose the best opportunities for supporting and defending member states.

#### Article 5 is appropriately flexible – builds in discretion and empirically works for traditional and cyber threats.

Sydney Freedberg 14; Deputy Editor at Breaking Defense, MA in Security Studies from Georgetown University; 11/7/14; "NATO Hews to Strategic Ambiguity on Cyber Deterrence," https://breakingdefense.com/2014/11/natos-hews-to-strategic-ambiguity-on-cyber-deterrence/]

NATO is now taking cyber threats as seriously as the Russian tanks and nuclear weapons it was created to deter. But the alliance has a long way to go just to shore up its own network defenses, and it explicitly eschews any role on the offense. NATO has not even written a formal policy on how it would deter a cyber attack. The net result is a certain degree of strategic ambiguity — but then NATO has survived and even thrived on ambiguity for decades.

The crucial development: September’s NATO summit declaration that the alliance’s hallowed Article 5 — which says an attack on one member is an attack against all — applies equally to virtual attacks as to physical ones.

“[In] linking cyber defense to collective defense and Article 5, the declaration says that cyber attacks…could be as harmful to modern society as conventional attack,” said Amb. Sorin Ducaru, NATO’s assistant secretary general for “emerging security challenges.”

That said, the Romanian diplomat emphasized at an Atlantic Council panel this week, “there’s no predetermined threshold,” no defined “red line” beyond which a cyber attack counts as an act of war. But then NATO never defined an automatic trigger for conventional or nuclear conflict either, even during the height of the Cold War. Article 5 only commits a NATO member to “assist” allies under attack by “such actions as it deems necessary, including the use of armed force” — which leaves vast amounts of wiggle room.

There was always doubt whether the United States would really risk nuclear escalation against its homeland to defend West Germany, and, for that matter, whether West Germany would stick with the alliance once wartime commanders started using tactical nuclear weapons on its soil to slow the Soviet horde. Yet despite these uncertainties, the Soviets were ultimately still deterred.

So when it came to cyber, Ducaru said, “there was a conscious decision by the allies in this policy that there is benefit in keeping flexibility and ambiguity.”

“Article 5 was by design something that should be invoked politically by [member] nations in a specific context, on a case by case basis,” Ducaru said. “Article 5 was never designed to be triggered by a certain threshold. [In fact,] the only time it was invoked was after 9/11, which was a scenario that had never been contemplated by the founding partners.

Despite that one area of (arguably inevitable) strategic ambiguity, the NATO summit made the situation in cyberspace much clearer, argued Christopher Painter, the State Department’s cyber coordinator. Beyond Article 5, “the NATO leaders’ declaration [stated] that international law including the UN Charter, the Law of Armed Conflict, international humanitarian law, etc. applies in cyberspace just like it does in the physical world,” Painter said at the Atlantic Council event. “This is a clear statement that this is not a lawless space — [and] there was some doubt before. There was some thought you had different rules entirely for the cyber world than the physical world, which made no sense and in fact would be very destabilizing.”

“Cyber seems so weird and different [that] it’s really inhibited seeing which of the old laws and ways of thinking about it might apply,” said Jason Healey, the Atlantic Council’s in-house cyber strategist. In fact, he argued, “the more strategically significant the conflict, the more similar it is to conflict in the air, land, and sea.”

### 2NC – AT: Attribution

#### Predictive technology solves attribution – AI means it’ll only get more accurate.

Justin Lynch 19; Associate Editor at Fifth Domain, contributor to the New Yorker, Foreign Policy, the Atlantic; 2/8/19; "The struggle behind predicting a cyberattack," https://www.fifthdomain.com/industry/2019/02/08/the-struggle-behind-predicting-a-cyberattack/

The idea that public data can point to future cyberattacks has been embraced by several government agencies.

The intelligence community’s research arm, the Intelligence Advanced Research Projects Activity, is researching how data can help forecast a cyberattack by using sensors that predict when a target is vulnerable to hackers. BAE Systems, Charles River Analytics, Leidos, and the University of Southern California are the prime contractors on the project.

There is a “significant link between hackers use of social media platforms, especially Twitter and Facebook, and the volume of web defacement attack,” according to 2017 research backed by the Office of the Director of National Intelligence and IARPA.

But experts have had mixed results with predicting cyberattacks with machine learning and open data.

By analyzing conversations of known criminals on the dark web, researchers from the University of California also tried to create an early warning system for incoming cyberattacks in 2017. That approach was 84 percent effective at predicting current or imminent cyberattacks.

Also in 2017, three researchers used historical attack count data to predict future cyberattacks to some success. It was 14 percent more effective than other models.

However, others believe the future of predicting cyberattacks through artificial intelligence will combine both humans and computers.

Researchers from the Massachusetts Institute of Technology created a computer system in 2016 that continuously incorporated information from human experts with a success rate of 85 percent while also decreasing false positives by a significant factor.

“The more attacks the system detects, the more analyst feedback it receives, which, in turn, improves the accuracy of future predictions,” said Kalyan Veeramachaneni, a research scientist at MIT in a release. “That human-machine interaction creates a beautiful, cascading effect.”

## Politics DA

### 1NC – Cybersecurity link

#### Cyber security reform is seen as authoritarian surveillance legislation.

Peter Hess 16, writer for Scienceline, "Controversial new cybersecurity law may compromise privacy"; Scienceline; Published: 1-24-2016; Accessed: 2-5-2022; https://scienceline.org/2016/01/controversial-new-cybersecurity-law-may-compromise-privacy/

The recent, highly publicized cyberattacks on Sony and the U.S. government’s Office of Personnel Management exposed sensitive data about millions of people. In Congress, lawmakers responded by approving the Cybersecurity Information Sharing Act, or CISA. But some critics say the bill, which President Obama signed into law on Dec. 18, not only would have done nothing to prevent those attacks, but also erodes personal privacy.

CISA encourages companies to share digital signatures — unique codes that track the origins of electronic communications, including the sender’s IP address — associated with possible security threats, both with each other and with the U.S. government. Supporters say this information sharing makes it easier for companies and the government to quickly get out ahead of security threats by alerting each other to the origin and nature of potential breaches. Opposition to the new law has come from technology companies, along with advocacy groups, such as the American Civil Liberties Union, that are worried about protecting privacy.

Critics say CISA’s focus on digital signatures is invasive and fails to include more current and relevant threats. Some even question whether the slow-moving machinery of lawmaking can ever keep up with the breakneck pace of the online world, where entirely new kinds of security threats regularly arise in an instant, seemingly out of nowhere.

“It was the intention of our founding fathers that policy should be slow because it prevents tyranny,” says Elissa Shevinsky, head of product at Brave, a company that focuses on easy-to-use privacy software. “If policy were fast, we’d be in a surveillance state. We’d have CISA already. It’s on us to fight hackers at the pace of hacking.” Private cybersecurity companies like hers, she adds, are better positioned to handle these security issues.

Privacy concerns are a key issue for critics like Shevinsky, who say CISA erodes privacy rights by going too far in encouraging companies to share private information with the U.S. government. An important element of the bill would protect companies from liability if they shared such data. According to Shevinsky, that would encourage companies to flout their own privacy policies by sharing their customers’ personal information. Before the bill passed, federal agencies could penalize companies for betraying their privacy policies, she says. CISA in its current form would not require companies to scrub customers’ identifying information from the data before sending it to other companies or the government. “CISA makes it so they can [share private information] in broad daylight,” Shevinsky says.

### 2NC – Cyber Link

#### Committee will derail any cybersecurity bill, unless Biden uses PC to get him on board

Tim Starks & Eric Geller 19, writers for Politico, 2/11/2019, “Where cybersecurity legislation 'goes to die' in Congress”, Politico, https://www.politico.com/story/2019/02/11/cybersecurity-ron-johnson-1160081

Wisconsin Republican Sen. Ron Johnson leads the committee with broad oversight over the nation’s most important cybersecurity issues, including protecting consumers and U.S. elections from hackers.

But he’s also a major reason little legislation on these topics ever passes, according to lobbyists, cybersecurity policy experts, lawmakers and congressional aides from both parties who spoke with POLITICO.

Johnson or members of his staff have derailed many of the most significant cybersecurity-related bills in the past four years, including legislation to secure elections, study whether the growing use of encrypted apps hampers law enforcement, and hold companies accountable for the proliferation of insecure connected devices, people who track the legislation told POLITICO.

His panel “is the place where legislation goes to die on cybersecurity,” said Mieke Eoyang, a former Hill aide and vice president for the national security program at Third Way, a centrist think tank in Washington that works on national technology policy issues.

While no official accounting exists of cybersecurity bills in Congress, Third Way counted 15 in the last Congress that passed the House and didn’t advance through the Senate Homeland Security and Governmental Affairs Committee, which Johnson has led since 2015.

“The record speaks for itself,” former House Homeland Security Chairman Michael McCaul (R-Texas) told POLITICO, expressing frustration over the fact that Johnson hasn’t advanced cybersecurity bills that his panel approved.

Many of the 15 people POLITICO spoke with for this story refused to be named for fear of angering a chairman who holds sway over legislation now pending in Congress. But all agreed that Johnson either actively stymied cybersecurity matters or has shown little interest in advancing them in his committee, which oversees the Department of Homeland Security, one of the government agencies most focused on digital security.

Johnson came to Congress in 2010 touting his background in manufacturing as the basis for his strong anti-regulatory bent, which critics say is a chief reason he’s resisted cyber bills that could enforce new standards on industry. And since Donald Trump won the White House in 2016, the senator has adopted many of the president’s views — such as downplaying Russian interference in the last presidential election — and sought to focus on topics favored by conservatives.

“I think he’s more interested in the waste, fraud and abuse, and more the political issues,” a former committee staffer told POLITICO. “Immigration — that’s a political issue. Border security — that’s a political issue. Rooting out government fraud and waste — that’s a political issue.”

## Spaceforce DA?

### 1NC – Link tradeoff

#### Space force steals NASA’s budget and prioritizes military goals.

Robert Farley 20, Senior Lecturer in Security and Diplomacy at the University of Kentucky, 12/1/2020, "Space Force: Ahead of Its Time, or Dreadfully Premature?," https://www.cato.org/policy-analysis/space-force-ahead-its-time-or-dreadfully-premature, sg

The ties between NASA and the military agencies managing space are extensive and cross‐​cutting, including personnel, technology, and various communications platforms. The establishment of the Space Force is not expected to have any direct impact on NASA, although second‐​order effects associated with the militarization of space may have some effect on how the agency handles its responsibilities.59 The Space Force could also draw funding and expertise from NASA if it takes responsibility for any dual‐​hat civilian‐​military missions. Some space infrastructure could also contribute to both the Space Force and NASA missions.60 Undoubtedly, a tighter relationship between NASA and the Space Force carries some dangers, as existing civilian missions could become targets for enemy action if they are too closely associated with the Space Force. Pressure from the Space Force could also compromise elements of NASA’s scientific mission by prioritizing military goals.

### 1NC – Link – Domain Awareness

#### Militarization causes space war.

Bryan Bender 22, senior national correspondent for POLITICO and adjunct professor at the Walter Cronkite School of Journalism, 3/12/2022, "Moon battle: New Space Force plans raise fears over militarizing the lunar surface," https://www.politico.com/news/2022/03/12/space-force-moon-pentagon-00016818, sg

The Pentagon maintains these new pursuits, all launched since the creation of the Space Force three years ago, are primarily designed to help secure a growing private space economy and safeguard civilian astronauts. In all, the newest branch believes nation-states and commercial companies will fly nearly 100 missions — both crewed and uncrewed — to the moon between now and 2030.

But space policy and security experts also fear that the armed forces could outstrip NASA in space exploration and thrust what has largely been a peaceful competition into a military contest.

Aaron Boley, co-director of Outer Space Institute at the University of British Columbia, says the Pentagon already plays an outsized role in Earth orbit, where satellites are used to support military operations and global security.

“But once we move to the moon, this should really be driven by civilian organizations to ensure that peaceful purposes are maintained,” he said.

Some leading military strategists, however, say there is simply too much at stake in the space race to leave it to civilians, and that the Pentagon will likely be compelled to take on a bigger role.

China’s space agency has made significant strides in its plan to develop the moon, including landing the first spacecraft on the south pole in 2019. It also plans at least three additional robotic missions, beginning in 2024, to build a lunar base, with missions involving taikonauts to follow.

In this photo released by Xinhua News Agency, the Shenzhou-13 manned spaceship onto of a Long March-2F carrier rocket prepares to be transferred to the launching area of Jiuquan Satellite Launch Center in northwestern China, Oct. 7, 2021.

DEFENSE

Proponents for a more muscular U.S. military say they fear China cannot be trusted to pursue only peaceful aims and could use its space program for both economic and military advantage, including a new partnership with Russia to build a moon base.

“Power abhors a vacuum,” said Peter Garretson, a retired Air Force lieutenant colonel and space strategist who is now a senior fellow in defense studies at the American Foreign Policy Council. “You should expect that other actors will act in ways that favor their interests to the exclusion of others.”

“I think we all hope that NASA will rise to the occasion again and be able to perform that traditional exploration role,” he added. “But with the slipping of budgets and slipping the timelines, I think there is some concern as to whether or not NASA is scaling its efforts and will be able to rise to the occasion.”

The Space Force maintains it is interested only in developing the means for “domain awareness,” not exploration.

### 1NC – Impact

#### Space Force involvement causes militarized arms races AND undermines multilateral governance.

Robert Farley 20, Senior Lecturer in Security and Diplomacy at the University of Kentucky, 12/1/2020, "Space Force: Ahead of Its Time, or Dreadfully Premature?," https://www.cato.org/policy-analysis/space-force-ahead-its-time-or-dreadfully-premature,

The primary legal instrument for managing the militarization of outer space is the 1967 Outer Space Treaty.64 The treaty regulates space exploration and colonization and establishes rules for the peaceful use of space and the heavenly bodies therein, including the moon. The treaty bans the deployment of weapons of mass destruction in space, although it does not prohibit military operations altogether.65 While the prospects for multilateral governance of space seem grim, especially in context of current American policymaking, the inception of the Space Force necessarily raises questions about the future of multilateral management of space. Will the institutionalization of the Space Force make it easier or more difficult to develop mechanisms for multilateral space governance?

Military services tend to warily view arms control arrangements that affect their auto­nomy in their specialized domains. The events described in the 1964 film (and 1962 novel) Seven Days in May, in which an Air Force general seeks to topple an arms control–minded American president in a coup, are overstated, but services have historically opposed arms control limitations that affect their core priorities. The Royal Air Force’s preference for offensive bombing doctrines during the interwar period, and its belief that the realities of war would rapidly blow past any legal limitations, undoubtedly influenced the United Kingdom’s approach to international law in the 1920s and 1930s.66 Similarly, the U.S. Navy (and its counterparts in Britain, Japan, and elsewhere) resented the Washington Naval Treaty process because it limited the construction of their most prized vessels.67

Even in the prehistory of the U.S. Air Force, Billy Mitchell warned about the threat that international arms control might pose for aerial bombardment. However, opposition to arms control was not always automatic or immediate; the Army Air Forces chiefs offered qualified support for nuclear arms control in the immediate aftermath of World War II.68 By the early 1960s, however, the Air Force senior hierarchy resolutely opposed most multilateral arms control, including the Limited Test Ban Treaty, the Outer Space Treaty, and the Nuclear Nonproliferation Treaty.69 In part because of generational change, the Air Force had minimal influence over the early Strategic Arms Limitation Talks negotiations between the United States and the Soviet Union. Later activism on the part of the Air Force and of the Navy focused on the protection of specific systems, such as the B‑1 Lancer bomber, the LGM-118 Peacekeeper ballistic missile (then the Missile, Experimental, or MX), and the Trident submarine‐​launched ballistic missile.70

The reasoning behind this opposition is clear: Strategic bombing (and later the delivery of nuclear payloads through intercontinental ballistic missiles) provided the rationale for the autonomy, independence, and primacy of the Air Force. Limitation of these weapons would not only require significant revision of doctrine and force structure but also would strike at the core cultural stories that undergirded the services. Moreover, compliance with the restrictions of a multilateral governance regime can be onerous in terms of financial, human resources, and intelligence demands.71 Most modern arms limitation regimes demand transparency on the part of the participants, which services tend not to welcome.

Given that services tend to pursue autonomy, the Space Force could pose some obstacle to future efforts for multilateral arms control in space. To be sure, neither the navies nor the air forces of the 20th century managed to prevent arms control. Nevertheless, if the Space Force manages to acquire the bureaucratic heft it needs to accomplish its core missions, it could act as an interest group within government to prevent the execution of strong multilateral arms control agreements. The record offers qualified reasons for concern about the role that the Space Force could play in future arms control negotiations. Services tend to resent the imposition of external limits on their procurement and force structure, although the extent of this resentment depends on organizational priorities. Still, the Space Force is unlikely to spearhead a drive for arms control within the U.S. government and probably will resist limitations imposed by such arms control on its core interests.

#### Space wars!

UCS 19, The Union of Concerned Scientists, national nonprofit organization founded more than 50 years ago by scientists and students at the Massachusetts Institute of Technology, 12/10/2019, "Creating a Space Force Would Trigger a Space Arms Race and Threaten US Satellite Security, Science Group Says," https://www.ucsusa.org/about/news/space-force-would-trigger-arms-race, sg

WASHINGTON (December 10, 2019)—A congressional conference committee has agreed to include the creation of a space force in a must-pass defense bill in exchange for paid parental leave benefits for federal workers. What is missing from the debate over the horse trade, according to the Union of Concerned Scientists (UCS), is the fact that a space force is a very bad idea

Below is a statement by Laura Grego, a physicist and senior scientist in the Global Security Program at UCS.

“At best a space force is a distraction from what is necessary to ensure space security in the face of rapid technological and geopolitical changes. At worst, it would prompt a space arms race that would threaten U.S. military and civilian satellites, not protect them. Diplomacy, not bureaucratic reorganization is urgently needed.

“The Pentagon insists that keeping space predictable and safe is the core purpose of whatever reorganization they do. To be sure, that mission is important and stabilizing, but it doesn’t need a new military service. Creating a new military service focused on space will create bureaucratic incentives to hype the space weapons threat and build new weapons. Pentagon officials emphasize that Russia and China are developing anti-satellite technology, but they leave out the fact that the United States is far ahead in sophistication as well as capacity of such technology.

“In fact, having anti-satellite weapons will do very little to keep one’s own satellites safe from attack. And unconstrained space weapons development will lead to a competition that makes space more dangerous, costly and unpredictable to use.

# K

## Capitalism

### 1NC – Link

#### Modern satellite infrastructure has functioned as the panoptical architecture of surveillance capitalism and the security state, enabling the surrender of all agency, accelerating the transfer of information, furthering globalization of liberal capitalism, and augmenting geopolitical competition.

Jocelyn Wills 17, assistant professor of history at Brooklyn College, City University of New York, Tug of war: Surveillance capitalism, military contracting, and the rise of the security state, Introduction: Satellites and Surveillance Capitalism \\SYang

On 4 October 1957, the Union of Soviet Socialist Republics launched Sputnik, the world’s first artificial satellite. Humiliated by the Soviet feat, the United States quickly countered, launching its Explorer satellite on 31 January 1958. On 29 July 1958, the US Congress then passed the National Aeronautics Space Act, declaring that “activities in space should be devoted to peaceful purposes for the benefit of humankind.”1 Signed into law by US President Dwight D. Eisenhower, the Act established the National Aeronautics and Space Administration (NASA) to conduct all non-military activity in outer space while also incorporating elements of the US Army Ballistic Missile Agency and Naval Research Laboratory. NASA began its official operations on 1 October 1958, with a mission to create a space program based on non-military and commercially promising satellites for scientific research, communications, terrain mapping, meteorological and environmental monitoring, and other Earth resource applications. Knowing that NASA’s satellites would collect images from countries other than the United States, the agency’s representatives also entered into cooperative agreements with US allies, assuring other countries’ representatives that NASA had peaceful intentions.2 Sputnik-1, Explorer-1, the creation of NASA, and a quick succession of additional satellite launches by the United States and the USSR captured the imagination of technological enthusiasts around the world. As conspicuous political acts performed on the world stage during the Cold War, those launches also inaugurated a global space race, accelerated the arms race, and encouraged other nations to compete for the military and commercial spoils of satellite surveillance.3 In an agreement with the United States, the United Kingdom soon entered the space race, sending its Ariel satellite into orbit on 26 April 1962. Constructed by NASA at the Goddard Space Flight Center in Maryland, and launched aboard an American rocket from Cape Canaveral Air Force Station in Florida, Ariel distinguished the United Kingdom as the third nation to send a satellite into orbit. Damaged by an American high-altitude nuclear test, Ariel never lived up to its promise. Nevertheless, the launch signalled the United Kingdom’s commitment to the development of a space program, including a pledge to devote its efforts to peaceful scientific research and commercial applications.4 On 29 September 1962, Canada followed the United Kingdom into outer space, sending its Alouette satellite into orbit aboard an American rocket launched from the Pacific Missile Range at California’s Vandenberg Air Force Base. Built by the Special Products Applied Research (SPAR) division of de Havilland Aircraft of Canada, and assembled by the Electronics Division of Canada’s Defence Research Telecommunications Establishment (DRTE), Alouette distinguished Canada as the fourth country to launch and the third one to build a satellite. Although several more years passed before satellite technologies reached beyond military, government, and scientific communities, Canada announced its stake in peaceful Earth observation, including its intention to develop remote sensing technologies (to acquire information via aerial photographs, satellite images, and other observation systems, and to detect and classify objects and phenomena without making physical contact with them). The country’s policymakers also tied Canadians to American developments, both signing continental trade and defence sharing agreements as well as vigorously promoting space exploration, scientific research, and the engineering disciplines as vital for protecting both national and continental interests.5 As other nations joined the space race over the next thirty years, developments in computing, digitization, and satellite reconnaissance, imaging, and communications pushed the boundaries of surveillance capitalism. Following the formal dissolution of the USSR on 26 December 1991, Americans then moved swiftly to commercialize the Internet, deregulate communications and financial industries, and assist in the further liberalization of the global economy and the evolving space industry. By the end of 2012, NASA’s National Space Science Data Center confirmed that more than 6,600 satellites had launched into orbit since Sputnik, with the vast majority of them reaching outer space after 1993.6 By 2012, Space Security Index (SSI) reported that artificial orbiting objects had reached approximately 8,300. The United States owned about half of all active satellites, with fifty other countries and several international consortia and nongovernmental organizations (NGOs) owning the others. Although satellites have declined in price, launching them remains expensive. As a result, by the end of 2012, only nine countries and one intergovernmental organization (the European Space Agency) had launching capabilities, with the United States dominant. In 2011 alone, global actors had embarked upon eighty space launches that placed 126 new satellites into orbit, with participating nations contributing billions of dollars to the effort. SSI further revealed that the International Space Station (ISS) had already cost US$100 billion, with most of it paid for by the taxpayers who helped to fund billions of dollars’ worth of other space initiatives. “Advanced and developing economies alike depend on these space-based systems,” SSI observed, with commercial space revenues “steadily” increasing “since the mid-1990s. From satellite manufacturing and launch services to advanced navigation products and the provision of satellite-based communications,” SSI declared, “the global commercial space industry is thriving, with estimated annual revenues in excess of $200 billion.”7 SSI also disclosed that operational satellites accounted for fewer than 5 per cent of the objects orbiting the Earth during 2012, while the remaining 95 per cent represented orbital debris due to anti-missile testing, accidents, and dead batteries.8 One of China’s older weather satellites is among that debris, blown out of the sky in January 2007 when the Chinese conducted their first test of an anti-satellite weapon (ASAT) and, according to one commercial space writer, put “other nations on notice that their commercial and military space assets were vulnerable to attack.”9 As part of an article on Sapphire, Canada’s first military satellite, the commercial space writer mentioned neither the fifty-year history of US and USSR anti-missile testing nor the more recent space-based collisions and accidents cited by Space Security Index as central to the creation of orbital debris. Regardless, the article reflected a trend among business-friendly space writers employing national security concerns to justify increased budgets and private-public initiatives for ASAT detection, “collision avoidance maneuvers,” and “debris mitigation efforts.”10 All of these initiatives now promise to become as significant as satellite launches and what their information-gathering capabilities have revealed about the Earth and its people, with “rapidly increasing revenues associated with satellite services” and the protection of commercial space systems linked to the government contractors who manufacture and maintain the satellites, ground receiving stations, advanced navigational products, and security systems that receive data for both civilian and military users.11 This book weaves the history of one of those government contractors – Canada’s MacDonald, Dettwiler and Associates (MDA) – into a larger narrative about the ways in which the forces of surveillance capitalism integrated Canada into regional, industrial, academic, and military alliances, particularly but not exclusively with the United States. Founded in Vancouver, British Columbia, during 1969, MDA evolved from a four-person software consultancy into a multinational supplier of space-based systems. A significant provider of the world’s ground stations that receive, process, archive, and exploit satellite data, MDA received global recognition in the 1970s for its pioneering work in the commercial applications of remote sensing and synthetic aperture radar (SAR, a high-resolution device that provides surface mapping no matter the weather conditions, cloud cover, or levels of darkness). MDA also became the prime contractor for Canada’s powerful Radarsat-2 Earth observation satellite and the official data distributor for Radarsat images worldwide. Other notable feats include MDA’s global delivery of the navigational systems that support aircraft and unmanned aerial vehicles (UAVs, commonly known as drones), as well as its role as primary builder of Sapphire, and central contributor to Canadarm-2 (the remote manipulator component of the robotic, mobile servicing system that moves equipment and supplies around the International Space Station and supports astronauts working in space). MDA has additionally received credit as the incubator for Vancouver’s high-technology corridor, with many of the firm’s former employees launching some of British Columbia’s most successful technology ventures. Of the surviving firms, most work as important surveillance-related government contractors in their own right.12 As Canadians celebrated the fifty-year anniversary of Alouette-1, and the Canadian Space Agency (CSA) readied the nation for the launch of Sapphire at the end of 2012, MDA’s strategies culminated in the acquisition of the US Space Systems/Loral (SS/L), a global provider of communications satellites and subsystems. According to industry analysts, the SS/L acquisition furnished MDA with a “critical mass in the commercial satellite manufacturing industry.”13 When the deal closed on 2 November 2012, MDA had also created one of the world’s most significant communications and information systems integrators, an achievement that promised “to boost estimated earnings” and provide “a platform to win upcoming space contracts” and more “defence and intelligence work” from the US government. The US government soon fulfilled that promise, in multiple contracts that gave MDA the market value and visibility its executives and shareholders had long craved as “the top technology stock in Canada over the past year.”14 Although financial news reports finally acknowledged MDA’s significance to Canada’s place within the global surveillance power core, the firm still remains largely invisible in the historical record and to the general public. According to David Ebner of the Globe and Mail, MDA’s obscurity has much to do with the ephemeral nature of systems engineering. Whereas one can touch and see products, MDA’s “technology isn’t widely recognized by most people because” the firm “generally operates unseen, in the background,” Ebner argued. As a result, “when MDA’s Radarsat satellites monitor Canada – the surveillance can spotlight down to a single metre – there isn’t any obvious MDA or Made in Canada stamp that people can see or cheer.”15 Operating “unseen, in the background,” MDA has played a critical role in the long-term development of the information systems and products that proliferate in global positioning devices, flight navigation systems, drones, mobile satellites, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR, also known as “Battle Command”), and a host of other networks that dominate various industries, from communications and financial services to environmental monitoring and resource extraction. Although they did not initially work on surveillance technologies for overtly political reasons, MDA’s scientists and engineers also played a part in turning satellites into a multi-billion-dollar commodity and outer space into a competitive, militarized zone. Along with other technological enthusiasts, they embraced satellites, the commercialization of space, and a notion of the “end of ideology.” In practice, however, their work has contributed to the expansion of the neoliberal project of privatization, fiscal austerity, deregulation, free trade, and reduced social spending, as well as the use of more efficient data mining systems, precision surveillance, first-strike capabilities, and the use of robotics for commerce as well as war. Engineering systems such as the ones they developed have also helped to remove the last barriers to routine aerial surveillance and the monitoring of everyday life. It would be a mistake, however, to see MDA’s founders, executives, scientists, and engineers as principal architects of this change; recent scholarship on the importance of social capital networks as well as ongoing revelations about surveillance and military-industrial adventurism have exploded the myths that a bright line divides business from government and the “great” man or woman from the socially constructed universe in which they operate. That MDA existed at all made it an entrepreneurial enterprise: the first of its kind in Vancouver, the firm helped to establish a hightechnology presence in BC’s Lower Mainland. But MDA’s history also reveals that business enterprises succeed or fail not simply on technological innovation, the personal qualities of those who lead them, the first-mover advantages that early entrants enjoy, or the “visible hand” of executives and managers who develop strategies and structures for continued expansion. Indeed, business survival always reflects the contingencies of larger social structures and cultural tropes, government priorities and changing educational, legal, and political policies, and unanticipated events and exogenous shocks beyond the control of any inventor, business founder, investor, executive, worker, government bureaucrat, or policymaking body. No different, MDA depended on these phenomena as well as the taxpayers who supported government spending on surveillance and those who hoped to profit from enhanced information-gathering techniques. “Without the benevolence” of the Canadian government, one long-time employee suggested, “MDA would never have grown beyond the size of a very, very small company.”16 MDA’s history therefore reminds us that corporations are juridical constructs and entrepreneurs instruments of state power, with both providing ways for governments to spread risk and for gatekeepers to favour certain individuals and businesses over others. By placing surveillance capitalism at the centre of Canada’s political economy, this book argues that MDA matters to our understanding of poilcymaking and business-government relations during the Cold War and into the twenty-first century. Reflecting the assumptions of capitalism’s culture of individual striving, people at MDA hoped to profit from living and working in a society where government officials promised to nurture their technical skills, reward their surveillance-based work, and bail them out when they stumbled. No matter their technical, business, or political skills, some realized their ambitions while others did not. Some had the ability to sell their ideas and motivate others, but lacked the skills to make the firm a profitable one. Others had excellent negotiating, managerial, and marketing skills, but still failed to realize returns from the “best practices” they had learned from management literature and the experiences of others in similar circumstances. Always, they engaged in complex negotiations with the capitalist system and government policies that provided incentive for some activities and discouraged others. MDA survived because members of the firm’s evolving executive team ultimately embraced MDA’s role as a systems integrator and procurement contractor for governments worldwide. Over time, they also understood that power resided not in the technologies they developed but rather in Ottawa and Washington, DC. Once done, they learned how to lobby the government to keep Canada’s space program on the budgetary agenda. In turn, the federal government encouraged MDA’s surveillance-based work because it promised to expand Canada’s influence as a significant, albeit junior member of the international power club. Canadian policymakers also appreciated that “countries which have less competitive industrial strengths in the areas of information technology face an increasing risk of losing trade, influence and economic power both within the community of developed nations and in the broader context of trade with developing countries.”17 MDA therefore provides more than a case study about how one particular firm managed to survive in the competitive space industry; it serves as a window into a corporate world girded by potent forces at the nexus of state, capital, and geopolitical power games. That nexus has included myths about space exploration’s peaceful purposes as well as competitive posturing for the spoils of surveillance-based commerce. Largely well-intentioned and with little interest in war, people at MDA nevertheless got caught up in the excitement of technological development, capitalist ambitions, and state incentives for both. Their eventual move into military work also reflects the unique security but problematic cultural relationship that integrated Canada into a continental defence economy with the United States while members of each country struggled to define their national identities and the imperial role each would play during the Cold War and beyond. As that relationship played out, Canadians consistently feared the overwhelming influence of their more powerful southern neighbours. Whether Conservative or Liberal, policymakers thus attempted to protect Canadian sovereignty and an autonomous international identity while simultaneously enjoying the benefits of their geographical proximity to as well as trading relationship with the United States. They also concerned themselves with foreign investment in the Canadian economy and the brain drain of technical talent that such investments might engender. Hoping to realize a “fair share” of the bounty promised by participation in world trade organizations and international governing bodies, they additionally wrestled with balancing desires to project Canada’s peacekeeping role and the realities of the country’s place within the American military-industrial complex. Satellites played a prominent role in that struggle. THE SIGNIFICANCE OF SATELLITES, SOVEREIGNTY, AND SURVEILLANCE STUDIES Artificial satellites, those ubiquitous “eyes in the sky,” twinkle as stars in various orbits. Some stand alone; others work in constellations. All contain powerful computers and subsystems, including those for propulsion, power, and communications. They vary in size and purpose, but ultimately they all gather information, with each of them launched to perform particular jobs for military and commercial purposes, often both. Whether for reconnaissance, remote sensing, or communications, satellites track assets, map resources, and communicate information to users on Earth and in outer space. In constant competition, those who own satellites seek to create more powerful features and capture more information for their own uses and profit, for “without a comparable capability,” one Canadian task force on satellite surveillance stressed, “we may never learn what other nations know about us, which must be viewed as a serious non-military threat.”18 Governments and their private contractors use reconnaissance (or spy) satellites to gather intelligence on military and other activities in outer space and on Earth. Launched into polar orbit, the most powerful among them can cover the entire globe every fourteen days. They come in four basic varieties and interact with each other. Optical-imaging satellites use light sensors to detect missile launches and weapons on the ground. Radar satellites use synthetic aperture radar to see through clouds and darkness. Signals-intelligence satellites employ powerful receivers to capture radio and microwave transmissions from every foe and friend. Relay satellites quickly move data from spy satellites to military bases on Earth, thereby speeding up the communications process for engagement. As surveillance studies scholars remind us, reconnaissance satellites are very useful tools for militaries and the police-security state.19 Remote sensing (also known as Earth observation) satellites measure and photograph the surface of the Earth and oceans as well as the atmosphere. Like most non-military satellites, Earth observation satellites typically launch into geostationary orbit over the equator. They use sensor technologies to detect objects and other phenomena via electromagnetic radiation signals from aircraft, satellites, and other systems, taking pictures of and classifying those objects without having to make physical contact with them. With SAR onboard, remote sensing satellites can map the entire surface of the Earth in the same ways that sonar technologies map the oceans, day or night, in all weather. Google Earth provides just one example of their power. Because they are very expensive to launch, Earth observation satellites are funded and used mainly by governments, to detect mineral and oil deposits, changes in agricultural activities and forests, weather damage, military bases, submarine wakes in the ocean, and other assets. MDA’s Radarsat-2, launched into the sun-synchronous polar orbit during 2007, can cover the Arctic daily, Canada every seventy-two hours, and the entire Earth every twenty-four days. The Canadian government has given MDA the right to sell Radarsat images to others around the world, as an export for economic development. MDA can downlink images to multiple ground stations in real time, or store them in the satellite’s computer until within range of a ground station. Once other countries, companies, and individuals have those images, they too can see resources, thereafter exploiting them for various applications, including city and regional planning, resource extraction, market segmentation, intelligence work, warfare, and a host of other reputable and nefarious activities.20 Most communications satellites also launch into geostationary orbit so they can circle the Earth within the same time that the Earth rotates just once. With their powerful antennas, these satellites send radio, television, and telephone transmissions, so that the Earth-bound can receive live broadcasts, use cellular telephones, and communicate by e-mail, among other activities. All of these devices record activities, making it easier for their owners to share information with each other. 21 There are many other satellites, including those used for astronomy, meteorology, navigation, search and rescue, space exploration, and other scientific applications. Working interactively with the space stations that make living in outer space possible, as well as with aircraft (including drones), ground-based computers, multimedia platforms, geographical positioning systems (GPS), and other technologies, satellites have created the panoptical architecture for the global surveillance state we experience and serve, all the while increasing the power of the elite who own and control the technologies and firms that produce them. As Michel Foucault observed, surveillance networks make us self-policing subjects. We daily use technologies we can no longer seem to do without, whether on the job, through the cash register, or at the ballot box. We “check in” with authority figures, even perform for them. We congregate with online communities because we have few public spaces left to meet. We trade civil liberties for protection because we receive daily reminders that we live in a dangerous world. We consign our control to the awesome power of the networks and inanimate objects created to extend shareholder value and the power of the elite. Ultimately, we even connect our identities to machines, watching, touching, and speaking into them, inviting them to become one with us.22 Investigative journalist Christian Parenti has argued that we do all of these things because surveillance techniques developed in earlier eras have gone global, become ubiquitous, “mundane, decentralized, and even convenient.”23 The conveniences of surveillance technologies come at a price, just as earlier conveniences came at a price to those enthralled by railroads and telegraphs, automobiles and radios, and airplanes and televisions. Technological revolutions have created great wealth, but they have not necessarily effected a greater distribution of that wealth or a more peaceful and inclusive world. “If the twentieth century has shown us anything,” Joel Mokyr concluded in his intellectual history of technology and the “useful” knowledge economy, “it is that the capacity of humans for intolerance, stupidity, and selfishness has not declined as their technological power has increased.” He also conceded, “The institutional setup of the world is such that holdouts that reject modern technology or cannot adopt it will eventually have to change their minds.” Canadian policymakers therefore embraced space exploration and surveillance technologies as a way to maintain Canada’s sovereignty and relevance, marketing both on their abilities to create a “new” world order of economic and social opportunities without end.24 Sociologist Vincent Mosco captured the force of such strategies a decade ago while tracing the dot-com bust of the late 1990s to the seductive power of the Internet. With Internet enthusiasts demonstrating “a remarkable, almost willful, historical amnesia,” Mosco observed that each generation “has renewed the belief that, whatever was said about earlier technologies, the latest one will fulfill a radical and revolutionary promise.” As a result, when the dot-com bubble burst, many Internet enthusiasts were shocked to learn that the power structures they thought they had overthrown remained remarkably resilient.25 MDA’s history resonates with these findings. Thanks to the mythological power of space exploration, MDA’s engineers and scientists thought they were different from previous generations, that their technical expertise could insulate them from past imbroglios. After all, they reasoned, they were well-educated, scientifically adept, computer-literate professionals, the vanguard of a new economy. 26 People from all walks of life rationalize their decisions and choose selective memories to make sense of their current circumstances and imagine themselves as active agents of the systems they develop and the structures they support. But as social anthropologist Hylton White recently observed, in an environment structured for competition and unending expansion, capitalism inevitably turns each new wave of technological enthusiasm, every gadget and new profession from an exotic first to a ubiquitous necessity. 27 This is just one of the consequences of the willful innocence people at MDA and elsewhere possess. In her study of engineering and the legitimacy of state power, sociologist Chandra Mukerji has argued that “the intelligence of engineering is not just pragmatic, but also deeply invested in social, legal, and moral conceptions of power” that privilege efficiencies over ecological awareness and quality-of-life issues as well as “produce an engineered world that shapes our lives – in ways we systematically ignore.”28 Surveillance studies scholars concur, including David Lyon, whose work continues to stress that surveillance is a “morally and politically loaded activity,” with what “we disclose to whom, and under what conditions” a highly significant act of state power. 29 Sociologists and surveillance studies scholars have contributed a great deal to our understanding about the synergies between capitalism, state power, military aims, academic research, and technological change, particularly in the Internet era. With few exceptions, however, most tend to focus on the United States, the United Kingdom, and other “great powers” while remaining remarkably silent on the history of the secondary powers that have helped to serve the interests of capital and the hegemonic ambitions of the United States. They also have the propensity to explore the state without examining the businesses involved in the space-faring enterprise. This omission flows, in part, from the classified nature of defence-related work; however, disparate sources can help to connect the dots between governments and their surveillance contractors. Tug of War draws upon interviews I conducted with MDA’s founders, employees past and present, and government patrons during 1992–93, and prior to MDA’s larger leap into the secret world of international defence/military contracting. Once transcribed, the tapes of those interviews produced an oral history of more than 1,000 pages. As I reread and reflected on that oral history after the heady dot-com boom had busted, terrorists had flown airplanes with sophisticated flight information systems into the World Trade Center and Pentagon, and the US government had stepped up its war footing, ultimately invading Iraq in 2003 on manipulated intelligence derived from military briefings and private contractors, I knew I had a larger story to tell. I therefore turned to archival material at Library and Archives Canada (LAC), some of it received through several requests under the Freedom of Information and Protection Act, as well as publicly available business records, government documents, and other sources that could place MDA’s trajectory within the larger context of surveillance capitalism’s expansion, the Cold War’s emphasis on permanent military preparedness and continental integration, and the rise of the North American security state. Interviewees who spoke about MDA’s first decade focused on the excitement of their technological innovations. Those who discussed the 1980s and early 1990s emphasized the business strategies and structures MDA had instituted to survive the winds of technological change and global competition, including the pull of military contracting. And documents collected after MDA went public in 1993 disclosed the ways in which the firm capitalized on neoliberalism, systems integration, and the expansion of the world’s surveillance architecture. Together, these sources have given me the luxury of hindsight, an increasing appreciation about the concatenation of events that pulled MDA into surveillance capitalism and a larger tug of war, and a better understanding about the ways in which time, memory, and selective amnesia shape the histories we tell ourselves and others over time.30 The MDA case therefore demonstrates that historians have much to contribute to the field of surveillance studies, particularly when they search for sources that allow them to trace how those asserting no particular interest in gaining military power nevertheless get drawn into the promises of space exploration, larger state objectives, and the US military-industrial complex.31

### 2NC – Link

#### Space serves as a spacial fix for capitalism by averting the crisis over overaccumulation --- the aff’s desperate cry for space is a last-ditch attempt to resolve inherent contradictions within the capitalist framework that render it terminally unsustainable.

Victor L. Shammas & Tomas B. Holen 19, associate Professor of Sociology at the Department of Sociology and Social Work, University of Agder, Norway; journalist for Nature, January 29, 2019, “One giant leap for capitalist kind: private enterprise in outer space”, <https://www.nature.com/articles/s41599-019-0218-9> \\SYang

The universalization of capitalism

The 2010s may very well be remembered as the ‘Age of NewSpace', the decade when outer space was turned into a capitalist space, when private corporations pushed the price of launches, satellites, and space infrastructure downwards, exerting what industry insiders call the ‘SpaceX effect' (Henry, 2018), centered on the technological achievement of ‘reusability', recovering used rocket boosters for additional launches, promising to drastically reduce the price of going to space (Morring, 2016). As one report observes, ‘Not only has the number of private companies engaged in space exploration grown remarkably in recent years, these companies are quickly besting their government-sponsored competitors' (Houser, 2017). What the rockets, shuttles, ships, and landing pods will carry beneath their payload fairing or in their cargo hold, however, along with supplies and satellites, is the capitalist worldview, a particular ideology—just as Robinson Crusoe, in Marx’s ironic retelling in Capital, ‘having saved a watch, ledger, ink and pen from the shipwreck… soon begins, like a good Englishman, to keep a set of books' (Marx, 1976, p. 170), brings with him English political economy—'Freedom, Equality, Property and Bentham', as Marx (1976, p. 280) says elsewhere—to his desert island.

In early 2018, astronomers across the world learned that a New Zealand start-up, Rocket Lab, which aimed to launch thousands of miniature satellites into orbit around Earth (so-called ‘smallsats'), had planned to launch a giant, shining ‘disco ball'—the ‘Humanity Star'—into orbit around Earth. It was an elaborate marketing stunt masked by humanistic idealism. ‘No matter where you are in the world, or what is happening in your life', said Rocket Lab CEO Peter Beck, ‘everyone will be able to see the Humanity Star in the night sky' (Amos, 2018). Many astronomers expressed outrage at these plans, fearing that the light from the Human Star would threaten their ability to carry out scientific observations. But while these astronomers were incensed by the idea of a bright geodesic object disrupting their ability to carry out observations, concerns with the effects of the arrival of capitalistkind on their ability to collect data were non-existent. The astronomical community was angered by the idea of a material, concrete, visible object polluting “pure” scientific data, but it paid less attention to the (invisible and abstract) recuperation of the night sky as it was brought into the fold of capitalism.

In an interview, Beck was quizzed about the Humanity Star and asked by a reporter about the difficulties of generating profits in space (Tucker, 2018). To this Beck replied, ‘It has always been a government domain, but we’re witnessing the democratization of it…[I]t [is] turning into a commercially dominated domain'. Beck established an equivalence established between the dissolution of space as the rightful domain of states and the advent of profit-making ventures as signs of ‘democratization'. In space, according to Beck’s logic, democratization involves the disappearance of the state and the rise of capital. The argument, of course, is impeccably post-statist: on this account, states are monolithic, conservative Leviathans beyond the reach of popular control; corporations, on the other hand, are in principle representatives of the everyman: in the age of the start-up, any humble citizen could in theory become an agent of disruption, a force for change, an explorer of space, and a potential member of the cadre of capitalistkind. Following this logic, the question for the entrepreneurs of NewSpace is how to monetize outer space, which means turning space into a space for capital; their question is how they can deplanetarize capital and universalize it, literally speaking, that is, turn the Universe into a universe for capital. In this light, Peter Beck’s distortion of democratic ideals appears eminently sensible, equating democratization with monetization, that is, capital liberated from its earthly tethers.

Emblematic of this capitalist turn in space was the founding of Moon Express in 2011, composed of a ‘team of prominent Silicon Valley entrepreneurs…shooting for the moon with a new private venture aimed at scouring the lunar surface for precious metals and rare metallic elements' (Hennigan, 2011). Following Google’s Lunar XPRIZE—an intertwining of Silicon Valley and NewSpace’s capitalistkind—which promised a $20 million prize for the first private company to land a spacecraft on the Moon, travel 500 meters, and transmit high-definition images back to Earth, all by March 2018,Footnote9 Moon Express claimed that it would be capable of landing on the lunar surface and earn the cash prize. Their stated goal was twofold: first, to mine rare resource like Helium-3 (a steadily dwindling scarce resources on Earth), gold, platinum group metals, and water, and, second, to carry out scientific work that would ‘help researchers develop human space colonies for future generations' (Ioannou, 2017). The ordering is telling: first profits, then humanity. These were the hollow, insubstantial promises of a venture-capitalized NewSpace enterprise: in early 2018, Google announced that none of the five teams competing for the Lunar XPRIZE, including Moon Express, would reach their stated objectives by the 31 March deadline and they were taking their money back (Grush, 2018). In this sense, it was typical for NewSpace in its formative years: a corporate field populated by (overly exuberant) private enterprises who promised more than they could deliver. But the belief in NewSpace is real enough. In a tome bursting with the optimism of NewSpace, Wohlforth and Hendrix claim that ‘the commercial spaceflight industry is transforming our sense of possibility. Using Silicon Valley’s money and innovative confidence, it will soon bring mass space products to the market' (2016, p. 7).

The trope of humanity plays a key role in the rhetoric of the adherents of NewSpace. To fulfill the objectives of NewSpace, including profit maximization and the exploitation of celestial bodies, the symbolic figure of a shared humanity serves a useful purpose, camouflaging the conquest of space by capitalism with a dream of humanity boldly venturing forth into the dark unknown, thereby also providing the legitimacy and enthusiasm needed to support bolster the legitimacy of NewSpace. So long as the stargazers and SpaceX watchers are permitted their fill of ‘collective effervescence', to use Durkheim’s (1995, p. 228) concept, capitalist entrepreneurs will be able to pursue their business interests more or less as they please. The spectacle of outer space is crucial in this regard.

Crucially, however, and despite this spectacle, SpaceX’s technology might not necessarily be more sophisticated than its competitors or predecessors. Some industry insiders have rebuffed some of the more the spectacular claims of NewSpace’s proponents, arguing that launch vehicle reusability requires a (perhaps prohibitively) expensive refurbishing of the rocket engines involved in launches: ‘The economics will depend on how many times a booster can be flown, and how much the individual expense will be to refurbish the booster…each time' (Chang, 2017). Reusability may be a technological dead-end because of the inherently stressful effects of a rocket launch on the launch vehicle’s components, with extreme limitations on reusability beyond second-use as well as added risks of malfunctions that customers and insurers are likely to wish to avoid. Furthermore, the Falcon Heavy still has not matched the power and payload capacity of NASA’s Saturn V, a product of 1960s military-industrial engineering and Fordist state spending programs. What SpaceX and other NewSpace corporations do with great ingenuity, however, is to manage the spectacle of outer space, producing outpourings of public fervor, aided by a widespread adherence to the ‘Californian Ideology' (Barbrook and Cameron, 1996), or post-statist techno-utopianism, in many postindustrialized societies.

The very centrality of these maneuvers has initiated a new phase in the history of capitalist relations, that of ‘charismatic accumulation'—certainly not in the sense of any ‘objective' or inherent charismatic authority, but with a form of illusio, to speak with Bourdieu, vested in the members of capitalistkind by their uncanny ability to spin mythologizing self-narratives. This has always been part of the capitalist game, from Henry Ford and onwards, but the charismatic mission gains a special potency in the grandiose designs of NewSpace’s entrepreneurs. Every SpaceX launch is a quasi-religious spectacle, observed by millions capable of producing a real sense of wonder in a condition of (legitimizing) collective effervescence.

Outer space necessarily reduces inter-human difference to a common denominator or a shared species-being. An important leitmotiv in many Hollywood science fiction movies, including Arrival (2016), is that a first encounter with an alien species of intelligent beings tends to flatten all human difference (including ethnoracial and national categories), thereby restoring humankind to its proper universality (see also Novoa, 2016). Ambassadors of Earth as a whole, not representatives of particular nations, step forth to meet alien emissaries. But even in the absence of such an encounter, the search for habitable domains (or rather, profitable locales) beyond Earth will necessarily forge a shared conception of the human condition, initiated with the Pale Blue Dot photograph in 1990. Typical of this sentiment are the words of the astronomer Carl Sagan, who famously observed of this photograph: ‘On it everyone you love, everyone you know, everyone you ever heard of, every human being who ever was, lived out their lives'.

This naïvely humanistic vision has been one of the dominant tropes in the discourse on space since the 1950s, and it remains strong today, as with the claims of the United Nations Office for Outer Space Affairs (UNOOSA) that their task is to ‘uphold the vision of a more equitable future for all humankind through shared achievements in space'. This representational tendency mobilizes humanism to generate enthusiasm about space-related activities. But such representations are increasingly being recuperated by capitalist enterprise, so that it is not humankind but its modulation by space capitalists that will launch into the dark unknown. It is not humankind but capitalistkind that ventures forth. In early 2018, NASA was set to request $150 million in its 2019 budget to ‘enable the development and maturation of commercial entities and capabilities which will ensure that commercial successors to the ISS…are operational when they are needed', only one of many signs that space is becoming a space for capitalism. According to one estimate, the value of just one single asteroid would be more than $20 trillion in rare earth and platinum-group metals (Lewis, 1996), a precious prize indeed for profit-hungry corporations.Footnote10 Even the UNOOSA spoke vociferously in favor of the commercialization of space, appealing variously to the ‘industry and private sector' and elevating the ‘space economy' to a central pillar in its Space2030 Agenda (including the ‘use of resources that create and provide value and benefits to the world population in the course of exploring, understanding and utilizing space'), even as the UN agency falls back on a humanistic, almost social-democratic vision of the equitable distribution of benefits (and profits) from space mining, exploration, and colonization (UNOOSA, 2018).

We find evidence of this strategic humanism in all manner of pronouncements from NewSpace entrepreneurs. To take but one example: Naveen Jain, the chairman and co-founder of MoonEx, a lunar commercialization firm, has claimed that ‘from an entrepreneur’s perspective, the moon has never truly been explored'. The moon, Jain has claimed, ‘could hold resources that benefit Earth and all humanity' (Hennigan, 2011). We should note the recourse to the trope of all of humanity by this NewSpace entrepreneur, mimicked in the 1979 Moon Agreement, a UN treaty, which also held that the Moon’s resources are ‘the common heritage of mankind' (Tronchetti, 2013, p. 13).Footnote11 In a purely factual sense, of course, Jain is wrong: Google Moon offers high-resolution images of the lunar surface,Footnote12 and the moon has already been explored, in the sense of being mapped, albeit rudimentarily and with room for further data collection. Crucially, however, these cartographic techniques have not been put to capitalist uses: mapping minerals, for instance, or producing detailed schemata that might one day turn the Moon into a ‘gas station' for commercial space ventures, as Wilbur Ross, Trump’s Secretary of Commerce, has proposed (Bryan, 2018). What is lacking, in short, are capitalist maps of the Moon, i.e., a cartography for capital. But as Klinger (2017: 199) notes, even though no one is ‘actively mining the Moon' at present, at least ‘six national space programs, fifty private firms, and one graduate engineering program, are intent on figuring out how to do so'; furthermore, Klinger draws attention to mapping efforts that have revealed high an abundance of rare earth metals, thorium, and iron in the Moon’s ‘Mare Procellarum KREEP' region (Klinger, 2017, p. 203).

We have already noted that it is not humanity, conceived as species-being, a Gattungswesen, that makes its way into space. The term Gattungswesen, of course, has a long intellectual pedigree, harking back to Hegel, Feuerbach, Marx, and others. The term can ‘be naturally applied both to the individual human being and to the common nature or essence which resides in every individual man and woman', Allan Wood (2004, p. 17) writes, as well as ‘to the entire human race, referring to humanity as a single collective entity or else to the essential property which characterizes this entity and makes it a single distinctive thing in its own right'. Significantly, the adherents of NewSpace often resort to the idea of humanity in its broad universality (e.g., Musk, 2017), but this denies and distorts the modulation of humanity by its imbrication with the project of global (and post-global, i.e., space-bound) capitalism. It is precisely the sort of false universality implied in the humanism of the supporters of NewSpace that Marx subjected to a scathing critique in the sixth of his Theses on Feuerbach. Here Marx noted that the human essence is not made up of some ‘abstraction inherent in each single individual' (1998, p. 570). Instead, humans are defined by the ‘ensemble of social relations' in which they are enmeshed. Under NewSpace, it is not humanity, plain and simple, that ventures forth, but a specific set of capitalist entrepreneurs, carrying a particular ideological payload, alongside their satellites, instruments, and supplies, a point noted by other sociologists of outer space, or ‘astrosociologists' (Dickens and Ormrod, 2007a, 2007b).

The spatial fix of outer space

No longer terra nullius, space is now the new terra firma of capitalistkind: its naturalized terroir, its next necessary terrain. The logic of capitalism dictates that capital should seek to expand outwards into the vastness of space, a point recognized by a recent ethnography of NewSpace actors (Valentine, 2016, p. 1050). The operations of capitalistkind serve to resolve a series of (potential) crises of capitalism, revolving around the slow, steady decline of spatial fixes (see e.g., Harvey, 1985, p. 51–66) as they come crashing up against the quickly vanishing blank spaces remaining on earthly maps and declining (terrestrial) opportunities for profitable investment of surplus capital (Dickens and Ormrod, 2007a, p. 49–78).

A ‘spatial fix' involves the geographic modulation of capital accumulation, consisting in the outward expansion of capital onto new geographic terrains, or into new spaces, with the aim of filling a gap in the home terrains of capital. Jessop (2006, p. 149) notes that spatial fixes may involve a number of strategies, including the creation of new markets within the capitalist world, engaging in trade with non-capitalist economies, and exporting surplus capital to undeveloped or underdeveloped regions. The first two address the problem of insufficient demand and the latter option creates a productive (or valorizing) outlet for excess capital. Capitalism must regularly discover, develop, and appropriate such new spaces because of its inherent tendency to generate surplus capital, i.e., capital bereft of profitable purpose. In Harvey’s (2006, p. xviii) terms, a spatial fix revolves around ‘geographical expansions and restructuring…as a temporary solution to crises understood…in terms of the overaccumulation of capital'. It is a temporary solution because these newly appropriated spaces will in turn become exhausted of profitable potential and are likely to produce their own stocks of surplus capital; while ‘capital surpluses that otherwise stood to be devalued, could be absorbed through geographical expansions and spatio-temporal displacements' (Harvey, 2006, p. xviii), this outwards drive of capitalism is inherently limitless: there is no end point or final destination for capitalism. Instead, capitalism must continuously propel itself onwards in search of pristine sites of renewed capital accumulation. In this way, Harvey writes, society constantly ‘creates fresh productive powers elsewhere to absorb its overaccumulated capital' (Harvey, 1981, p. 8).

Historically, spatial fixes have played an important role in conserving the capitalist system. As Jessop (2006, p. 149) points out, ‘The export of surplus money capital, surplus commodities, and/or surplus labour-power outside the space(s) where they originate enabled capital to avoid, at least for a period, the threat of devaluation'. But these new spaces for capital are not necessarily limited to physical terrains, as with colonial expansion in the nineteenth century; as Greene and Joseph (2015) note, various digital spaces, such as the Internet, can also be considered as spatial fixes: the Web absorbs overaccumulated capital, heightens consumption of virtual and physical goods, and makes inexpensive, flexible sources of labor available to employers. Greene and Joseph offer the example of online high-speed frequency trading as a digital spatial fix that furthers the ‘annihilation of space by time' first noted by Marx in his Grundrisse (see Marx, 1973, p. 524).

Outer space serves at least two purposes in this regard. In the short-to medium-term, it allows for the export of surplus capital into emerging industries, such as satellite imaging and communication. These are significant sites of capital accumulation: global revenues in the worldwide satellite market in 2016 amounted to $260 billion (SIA, 2017, p. 4). Clearly, much of this activity is taking place ‘on the ground'; it is occurring in the ‘terrestrial economy'. But all that capital would have to find some other meaningful or productive outlet were it not for the expansion of capital into space. Second, outer space serves as an arena of technological innovation, which feeds back into the terrestrial economy, helping to avert crisis by pushing capital out of technological stagnation and innovation shortfalls.

In short, outer space serves as a spatial fix. It swallows up surplus capital, promising to deliver valuable resources, technological innovations, and communication services to capitalists back on Earth. This places outer space on the same level as traditional colonization, analyzed in Hegel’s Philosophy of Right, which Hegel thought of as a product of the ‘inner dialectic of civil society', which drives the market to ‘push beyond its own limits and seek markets, and so its necessary means of subsistence, in other lands which are either deficient in the goods it has overproduced, or else generally backward in creative industry, etc.' (Hegel, 2008, p. 222). In this regard, SpaceX and related ventures are not so very different from maritime colonialists and the trader-exploiters of the British East India Company. But there is something new at stake. As the Silicon Valley entrepreneur Peter Diamandis has gleefully noted: ‘There are twenty-trillion-dollar checks up there, waiting to be cashed!' (Seaney and Glendenning, 2016). Capitalistkind consists in the naturalization of capitalist consciousness and practice, the (false) universalization of a particular mode of political economy as inherent to the human condition, followed by the projection of this naturalized universality into space—capitalist humanity as a Fukuyamite ‘end of history', the end-point of (earthly) historical unfolding, but the starting point of humanity’s first serious advances in space.

What role, then, for the state? The frontiersmen of NewSpace tend to think of themselves as libertarians, pioneers beyond the domain of state bureaucracy (see Nelson and Block, 2018). ‘The government should leave the design work and ownership of the product to the private sector', the author of a 2017 report, Capitalism in Space, advocates. ‘The private companies know best how to build their own products to maximize performance while lowering cost' (Zimmerman, 2017, p. 27). One ethnographer notes that ‘politically, right-libertarianism prevails' amongst NewSpace entrepreneurs (Valentine, 2016, p. 1047–1048). Just as Donald Rumsfeld dismissed the opponents to the Iraq War as ‘Old Europe', so too are state entities’ interests in space exploration shrugged off as symptoms of ‘Old Space'. Elon Musk, we are told in a recent biography, unlike the sluggish Big State actors of yore, ‘would apply some of the start-up techniques he’d learned in Silicon Valley to run SpaceX lean and fast…As a private company, SpaceX would also avoid the waste and cost overruns associated with government contractors' (Vance, 2015, p. 114). This libertarianism-in-space has found a willing chorus of academic supporters. The legal scholar Virgiliu Pop introduces the notion of the frontier paradigm (combining laissez-faire economics, market competition, and an individualist ethic) into the domain of space law, claiming that this paradigm has ‘proven its worth on our planet' and will ‘most likely…do so in the extraterrestrial realms' as well (Pop, 2009, p. vi). This frontier paradigm is not entirely new: a ‘Columbus mythology', centering on the ‘noble explorer', was continuously evoked in the United States during the Cold War space race (Dickens and Ormrod, 2016, pp. 79, 162–164).

But the entrepreneurial libertarianism of capitalistkind is undermined by the reliance of the entire NewSpace complex on extensive support from the state, ‘a public-private financing model underpinning long-shot start-ups' that in the case of Musk’s three main companies (SpaceX, SolarCity Corp., and Tesla) has been underpinned by $4.9 billion dollars in government subsidies (Hirsch, 2015). In the nascent field of space tourism, Cohen (2017) argues that what began as an almost entirely private venture quickly ground to a halt in the face of insurmountable technical and financial obstacles, only solved by piggybacking on large state-run projects, such as selling trips to the International Space Station, against the objections of NASA scientists. The business model of NewSpace depends on the taxpayer’s dollar while making pretensions to individual self-reliance. The vast majority of present-day clients of private aerospace corporations are government clients, usually military in origin. Furthermore, the bulk of rocket launches in the United States take place on government property, usually operated by the US Air Force or NASA.Footnote13

This inward tension between state dependency and capitalist autonomy is itself a product of neoliberalism’s contradictory demand for a minimal, “slim” state, while simultaneously (and in fact) relying on a state reengineered and retooled for the purposes of capital accumulation (Wacquant, 2012). As Lazzarato writes, ‘To be able to be “laissez-faire”, it is necessary to intervene a great deal' (2017, p. 7). Space libertarianism is libertarian in name only: behind every NewSpace venture looms a thick web of government spending programs, regulatory agencies, public infrastructure, and universities bolstered by research grants from the state. SpaceX would not exist were it not for state-sponsored contracts of satellite launches. Similarly, in 2018, the US Defense Advanced Research Projects Agency (DARPA)—the famed origin of the World Wide Web—announced that it would launch a ‘responsive launch competition', meaning essentially the reuse of launch vehicles, representing an attempt by the state to ‘harness growing commercial capabilities' and place them in the service of the state’s interest in ensuring ‘national security' (Foust, 2018b).

This libertarianism has been steadily growing in the nexus between Silicon Valley, Stanford University, Wall Street, and the Washington political establishment, which tend to place a high value on Randian ‘objectivism' and participate in a long American intellectual heritage of individualistic ‘bootstrapping' and (allegedly) gritty self-reliance. But as Nelson and Block (2018, p. 189–197) recognize, one of the central symbolic operations of capitalistkind resides in concealing its reliance on the state by mobilizing the charm of its entrepreneurial constituents and the spectacle of space. There is a case to be made for the idea that SpaceX and its ilk resemble semi-private corporations like the British East India Company. The latter, “incorporated by royal charter from Her Majesty Queen Elizabeth I in 1600 to trade in silk and spices, and other profitable Indian commodities,” recruited soldiers and built a ‘commercial business [that] quickly became a business of conquest' (Tharoor, 2017). SpaceX, too, is increasingly imbricated with an attempt on the part of a particular state, the United States, to colonize and appropriate resources derived from a particular area, that of outer space; it, too, depends on the infrastructure, contracts, and regulatory environment that thus far only a state seems able to provide. Its private character, like that of the East India Company, is troubled by being deeply embedded in the state. As one commentator has observed of SpaceX, ‘If there’s a consistent charge against Elon Musk and his high-flying companies…it’s that they’re not really examples of independent, innovative market capitalism. Rather, they’re government contractors, dependent on taxpayer money to stay afloat' (cit. Nelson and Block, 2018, p. 189).

Perhaps this should not come as a surprise. As Bourdieu (2005, p. 12) observed, ‘The economic field is, more than any other, inhabited by the state, which contributes at every moment to its existence and persistence, and also to the structure of the relations of force that characterize it'. The state lays out the preconditions for market exchanges. Under neoliberalism, the state is the preeminent facilitator of markets. The neoliberal state is not so much a Minimalstaat, night watchman state, or slim state as it is the prima causa of market society (see, e.g., Wacquant, 2012). Similarly, in the political theory of Deleuze and Guattari, any economic development presupposes the political differentiation caused by the state (Deleuze and Guattari, 2004a, p. 237–238). Even in the global environment of contemporary capitalism, the market cannot operate without the state becoming integrated with capitalism itself, as ‘it is the modern state that gives capitalism its models of realization' (Deleuze and Guattari, 2004b, p. 480). For capitalism to survive in outer space, the state must create a regulatory environment, subsidize infrastructure, and hand down contracts – in short, assemble outer space as a domain made accessible in legal, technical, and economic ways.

Universalizing capital

As Earth’s empty spaces are filled, as our planet comes to be shorn of blank places, capitalistkind emerges to rescue capitalism from its terrestrial limitations, launching space rockets, placing satellites into orbit, appropriating extraterrestrial resources, and, perhaps one day, building colonies on distant planets like Mars. But why limit ourselves to Mars? As of mid-2017, NASA’s Kepler observatory had discovered more than 5000 exoplanets—planets that seem like promising alternatives to Earth, located at an appropriate distance from their respective suns in the famed ‘Goldilocks zone'. These ‘planetary candidates', as they are known—that is, candidates for the replacement of Earth, capable of supporting human life with only minimal technological augmentation or cybernetic re-engineering—are above all viable candidates for selection by specific capitalists seeking to discover new profitable ventures beyond the limits of an Earth-bound capitalism. Space reveals the impotence of the neoliberal, post-Fordist state, its incapacity and unwillingness to embark on gigantic infrastructural projects, to project itself outwards, and to fire the imagination of (actual) humankind. Capitalistkind steps in to fill the vacuum left behind by a state that lacks what Mann (2012, p. 170) calls ‘infrastructural power'. The old question, the question of Old Space, was quite simply: is this planet a viable site for humankind, a suitable homeland for the reproduction of human life away from Earth? But the new question, the question for NewSpace, will be: can this celestial body support capitalistkind? Will it support the interests of capitalist entrepreneurs, answering to the capitalist desire for continued accumulation?

While some elements of the astrosociological community, such as the Astrosociology Research Institute (ARI),Footnote14 insist on elucidating the “human dimension” in outer space, Dickens and Ormrod recognize that this humanization-through-capitalism really involves the ‘commodification of the universe' (2007b, p. 2). While Dickens and Ormrod develop similar arguments to those sketched here—from their concept of an ‘outer spatial fix' to their argument about outer space becoming woven into circuits of capital accumulation—they were writing at a time when their remarks necessarily remained speculative: the commercialization of space was still in its infancy. In an inversion of Hegel’s owl of Minerva, reality has since largely confirmed their ideas and caught up with theory. Above all, when considering the various ventures ongoing in space today, it is not so much the universalizing human dimension as the specifically capitalist dimension that is striking. With the advent of NewSpace, outer space is becoming not the domain of a common humanity but of private capital.

The arguments laid out above mirror an ongoing turn in critical scholarship away from the notion of the Anthropocene towards a more rigorously political-economic concept of Capitalocene, premised on the ‘claim that capitalism is the pivot of today’s biospheric crisis' (Moore, 2016, p. xi). Just as the exponents of the concept of Capitalocene emphasize that it is capitalism, and not humanity as such, that is the driving force behind environmental transformation, so too does the notion of capitalistkind emphasize that it is not humankind tout court but rather a set of specific capitalist entrepreneurs who are acting as the central transformative agents of and in outer space, with the ‘ever-increasing infiltration of capital' into what was formerly the domain of the state (Dickens and Ormrod, 2007a, p. 6). We can also think about these issues in terms of what Philippopoulos-Mihalopoulos (2015) terms ‘spatial justice'. This concept captures the fact that struggles over justice are often struggles to occupy space, as the term is more conventionally understood, as with urban battles over the ‘right to the city' (Harvey, 2008), to provide just one example. But the same also holds true for outer space: there is an ongoing struggle over the right to take up space in outer space. So far, the capitalist side appears to be winning. As the proto-communism of the Cold War-era Outer Space Treaty is abandoned—in tandem with the increased technological feasibility of exploiting resources and accumulating profits in outer space—spatial justice in outer space increasingly comes to mean the ‘justice' of capital, capitalistkind taking the place of humankind. It is comparatively easy to declare that outer space is a commons, as the Outer Space Treaty did in the late 1960s, when that domain is, for all practical purposes, inaccessible to capital; with the heightened accessibility of outer space, however, it is unsurprising that central political agents, such as President Trump’s administration, should seek to dismantle this regulatory framework and ensure the smooth functioning of capital accumulation beyond the terrains of Earth.

What kind of capitalism is being projected into space? The complexity of state-market relations is sufficient to force us to hedge against a simplified reading of space commercialization: it is not a matter of states against markets, as if the two were mutually exclusive. Instead, as Bratton (2015) suggests, we are witnessing the emergence of a ‘stack', a complex intertwining of commercial, geopolitical, and technological concerns, which challenges previous notions of state sovereignty. This can be seen as a hybridized state-market form, with technology playing a central role in reciprocal processes of political and economic transformation. On the one hand, outer space was in some sense always already the domain of marketization, albeit to a limited extent, even during the Cold War, from the first commercial satellite launch in the early 1960s to President Ronald Reagan’s implementation of the Commercial Space Launch Act of 1984, which aimed to encourage private enterprise to take an interest in an emerging launch market. As Hermann Bondi, the head of the European Space Organization, wrote in the early 1970s, ‘It is clear…that there must be three partners in space, universities and research institutions on the one hand, the government on the second and industry on the third' (Bondi, 1971, p. 9).

On the other hand, outer space still remains firmly within the domain of the state and is likely to do so for the foreseeable future, with the likely continued importance of military uses of satellite technology and the weaponization of Earth’s orbit—crucially, the Outer Space Treaty only prohibits nuclear arms and other ‘weapons of mass destruction' in space, not conventional weapons, such as ballistic missiles. One novel element in this phase of capitalism-in-space is the interrelationship between Silicon Valley, NewSpace, and the state (see, e.g., Vance, 2015). Silicon Valley’s capitalist class, including Amazon’s Jeff Bezos, play an outsize role in NewSpace. Behind and around these figures, however, remains the state—through its weighty fiscal, regulatory, military, and symbolic investments.Footnote15 To take but one example: In June 2018, SpaceX won a $130 million contract with the U.S. Air Force to launch an ‘Air Force Space Command' satellite onboard a Falcon Heavy rocket (Erwin, 2018).

Fredric Jameson’s (2003, p. 76) oft-quoted observation that it is easier to imagine the end of humankind than the end of capitalism, is realized in the ideals and operations of capitalistkind. Elon Musk has observed that the goal of SpaceX is to establish humankind as a ‘multiplanetary species with a self-sustaining civilization on another planet' whose purpose is to counteract the possibility of a ‘worst-case scenario happening and extinguishing human consciousness' (Vance, 2015, p. 5). But couldn’t we view this idealistic assertion on behalf of humanity in another way? It is not human consciousness, over and against what the writer Kim Stanley Robinson (2017, p. 2) calls ‘mineral unconsciousness' (i.e., the mute, geological reality of the natural universe), so much as a specifically capitalist consciousness that is at stake. While the actions of capitalistkind may primarily be aimed at ensuring the future survival of the human species, an additional result is to ensure that the very idea of capitalism itself will outlive a (distantly) possible extinction event. Capitalism is a self-replicating system, pushing to expand ever outwards, using a territorializing strategy of survival. As David Harvey notes, ‘a steady rate of growth is essential for the health of a capitalist economic system, since it is only through growth that profits can be assured and the accumulation of capital be sustained' (1990, p. 180). In this respect, outer space is ideal: it is boundless and infinite. As Earth comes to be blanketed by capital, it is only to be expected that capital should set its sights on the stars above. The actions of capitalistkind serve to bolster the capitalist mode of production and accumulation: it is not only life but capital itself that must outlive Earth—even into the darkness of space.

## Security

### 1NC – Link

#### Satellites, and specifically environmental monitoring systems, fuel environmental security rhetoric through the use of the visual as a uniquely distinct medium.

Delf Rothe 17, senior researcher at the Institute for Peace Research and Security Policy at the University of Hamburg, June 23, 2017, “Seeing like a satellite: Remote sensing and the ontological politics of environmental security”, https://journals.sagepub.com/doi/full/10.1177/0967010617709399?casa\_token=StJp7\_PKhUkAAAAA%3Ac\_wg-VURPt3gATjXf35OGB5PQZ85Int99mWbYn1AZptShG7WJmCASah20h2sqqHIqZ9iXCxCjcmF#\_i2 \\SYang

In the aftermath of the so-called linguistic turn in the social sciences, an increasing number of scholars in International Relations studied how environmental problems have been discursively framed as security problems. Starting from the assumption that security threats are not simply objectively given, they showed how different authorized actors – including politicians, scientists, and military officials – have successfully reframed environment problems like climate change as security concerns (Buzan et al., 1998; Floyd, 2010). The merit of these works has been to demonstrate that ‘framing matters’ (Dalby and O’Lear, 2016: 5): that the way in which environmental problems are perceived and treated politically depends on how they are framed discursively. They revealed that different discourses of environmental security identify different threats (e.g. climate-induced migration, scarcity-induced conflicts, or natural disasters), multiple referent objects to be protected (e.g. the environment vs. the nation-state vs. vulnerable populations), and heterogeneous policy responses to organize this protection (Detraz and Betsill, 2009; McDonald, 2013; Trombetta, 2008).

Notwithstanding these merits, the literature on the securitization of the environment has been criticized for its narrow focus on securitizing speech acts and linguistic threat constructions and for drawing a stark boundary between the physical reality (which is not directly perceivable) and the socially constructed world (the meaningful representation of reality). By concentrating on ‘threat perceptions rather than an actual danger emanating from objective factors’ (Mayer, 2012: 167), linguistic constructivist approaches might thus unwillingly play into the hands of climate skeptics. Furthermore, the one-dimensional relation between discourses and practices implied by linguistic constructivist works has been criticized (Rothe, 2016). Asking how certain speech acts unidirectionally shape policy responses to environmental threats, they would fail to acknowledge the mutually constitutive relationship between discourses and practices.

A broader understanding of environmental security is provided by governmentality approaches (Oels, 2013; Rothe, 2016). In this perspective, environmental security is understood not so much as a discourse but as a particular field of government shaped by competing political rationalities, subjectivities, practices, and technologies. Some of these works, for example, have shown how environmental problems such as climate change have been turned into security problems through a range of expert practices including risk assessment, scenario development, and hotspot modeling (Mayer, 2012; Methmann and Rothe, 2014). Others have shown that practices of environmental security cohere with different ideal-typical governmentalities such as liberalism, biopolitics, or neoliberalism, each of which produces a different set of assumptions on the subjects, objects, and means of government (see Oels, 2013). Governmentality studies, however, have been criticized for their tendency to simply assign practices and discourses of environmental security to ideal-typical governmentalities (Corry, 2014). This would risk overstating the coherence of existing governmentalities and treating practices and political technologies as epiphenomenal to the broader political discourses that shape them.

A further important extension of discourse-analytical works on environmental security has been provided by works that focus on the role of visuality in the construction of security threats and risks. As nicely expressed by Bleiker (2015: 874): ‘Images … frame what can be seen, thought and said. In doing so, they delineate what is and is not politically possible.’ Two features are said to distinguish pictures and other visuals from words in the construction of security. First, pictures and satellite images are taken as authoritative sources of knowledge, as they apparently represent reality in an objective manner (Dodge and Perkins, 2009: 498; Shim, 2014: 156). The authority of visuals is particularly evident in the realm of environmental security. Here, a whole range of visualization techniques – from colorful data visualizations to computer models or satellite images – make abstract and complex phenomena such as climate-induced migration (Methmann and Rothe, 2014) or the geopolitics of climate change (Manzo, 2012) visible and sizable. Second, images are particularly suitable for invoking certain emotive reactions, such as fear, horror, or grief, that are crucial for the creation of urgency and danger in security discourses. Again, this is mirrored in the debate on environmental security, where powerful icons – such as images of polar bears on retreating ice sheets – or colors in data visualizations are used to invoke emotive reactions and a sense of risk (see Liverman, 2009; Schneider and Nocke, 2014).

The emerging body of literature on visual security represents a promising way to broaden the analytical scope of environmental security beyond the narrow realm of language and speech acts. However, I hold that it often follows a too narrow understanding of visuality – as simply a particular form of discursive representation – that ignores the complex materiality of the visual. This materiality is to be found in the visual economies in which images are produced, circulated, and interpreted (Dodge and Perkins, 2009; Parks, 2009). Furthermore, images and pictures are not only semiotic systems of signs but also physical objects that can be printed, circulated, blocked, (re-)combined, and reproduced. Finally, looking at, seeing, touching, or interpreting visuals are material bodily practices – which are increasingly supplemented with technological practices such as algorithmic pattern detection or automated image analyses (see Brannon, 2013).

Environmental security as ontological politics

To account for the materiality of the visual and for the special role of visual technologies in the construction of environmental security, I reread the existing literature on environmental security through the lens of ANT and the notion of ontological politics. In short, ANT radicalizes the assumptions of linguistic or visual constructivism. Instead of viewing texts, images, and other semiotic systems as representations of a pre-existing single reality, it holds that the interplay of expert practices, scientific discourses, technologies, and visuals constitutes multiple realities (Hind and Lammes, 2016: 81–82). Annemarie Mol (2002), for example, shows through her long-term ethnographic research in Dutch hospitals how different medical practices and diagnostic tools produce multiple versions of atherosclerosis. To assume that phenomena are multiple implies they are ‘more than one but less than many’ (Mol, 2002: 55). According to this understanding, ontology ‘is not given in the order of things but … ontologies are brought into being, sustained, or allowed to wither away in common, day-to-day, sociomaterial practices’ (Mol, 2002: 6). As Ingunn Moser (2008: 99) puts it, natural realities become ‘matter-real’ and are ‘mattering’ only through their ‘continued enactment and re-enactment in situated practices’. Following these assumptions, environmental security can be understood as a form of ontological politics, in which the ontological status of phenomena such as climate change, deforestation, or natural disasters – as well as the ways of knowing them – becomes the subject of debate (Barry, 2013: 7; Schouten, 2014).

I argue that visual technologies such as satellite remote sensing play a crucial role in the ontological politics of environmental security. Consider Mol’s seminal work in the ontological politics of disease. A large share of the practices that render a disease such as atherosclerosis ‘matter-real’ are based on visual technologies: X-ray units, MRI scanners, microscopes, molecular imaging techniques, etc. The same holds true for the realm of environmental security. Here, visual technologies, including computer modeling, satellite remote sensing, data visualization, hotspot mapping, and graphs of future scenarios, enact different versions of ‘the environment’ as security risk (Randalls, 2014). Rather than producing mere representations of pre-existing environmental risks, visual technologies essentially bring them about: ‘The world does not exist before these ways of sensing’ (Hind and Lammes, 2016: 90). For, as Mitchell (2013: 233) crucially reminds us, ‘Nature is unable to speak for itself…. The facts of nature speak only with the help of measuring devices and tools of calculation’. To render a phenomenon such as climate change visible, intelligible, and thereby ‘matter-ing’ and ‘matter-real’, a global assemblage of visual technologies – including satellites, weather stations, computer simulations, researchers, and mechanisms of international cooperation – is required (Edwards, 2010; Wark, 2015: 166–182).

To study visual technologies as part of the ontological politics of environmental security, I first draw on the notion of immutable mobiles (Latour, 1986). Bruno Latour has coined this term to explain the power effects of ‘technologies of visualisation and inscription’ (Latour, 2013: 77), such as the printing press, cartography, photography, or the computer, that allow inscribing parts of the real world into flat and mobile artifacts (Latour, 1986: 17). Through these technologies, reality becomes flattened, mobile but immutable. Inscribed into pictures, maps, or charts, inscriptions of local realities – such as a piece of soil – can be circulated globally, reproduced, or combined with other inscriptions of reality. Pictures of different origin and different scale can be layered (Latour, 1986: 7).

Second, I draw upon the notion of visual assemblage (Bleiker, 2014: 76) to account for the fact that environmental risks and threats are never produced by a single technology – never become visible on a single image – but become enacted by a complex web of linked inscription devices, practices, and discourses (Latour and Hermant, 2006: 29). The notion of assemblage refers to a temporary form of order of heterogeneous elements ‘whose unity comes solely from the fact that these items function together, that they “work” together as a functional entity’ (Patton, 1994: 158). The visual assemblage of environmental security can be understood as exactly such a heterogeneous network of visual technologies and related infrastructures, people, laws and regulations, discourses, and practices (van Munster and Sylvest, 2016: 2). The immutable mobiles (satellite pictures, global climate models, vulnerability maps), which circulate through this assemblage, create new associative relations between actors as diverse as satellite operators, climate scientists, environmental activists, or military officials (Mayer, 2012). Together they turn ‘nature’ into a range of calculable, perceivable, and governable risks through a series of calculations, transformations, and translations (Hind and Lammes, 2016). The notion of visual assemblage makes it possible to account both for the socio-material character of the visual and for the messiness and multiplicity of practices and discourses of environmental security.

Using the framework in practice

The perspective of assemblage calls for a pluralization of methods in the study of visual politics (Bleiker, 2014). To grasp the social/technical/discursive/visual character of visual assemblages, I combine three analytical layers. The first analytical layer is a semiotic visual analysis (Rose, 2016: 106–146). A corpus of highly visible demonstration images – provided on websites, in demonstration reports, in social networks, or in demonstration videos – has been compiled in each case. Such showcase images are particularly promising for the objectives of this article because they are pre-selected by the respective actors to demonstrate the whole range of possible applications and capabilities of satellite imagery. A set of heuristic questions helps to structure the analysis: What do the images show and what is hidden? Are there common visual characteristics or patterns? How are images arranged and how are colors used? And what are the aesthetic and political effects of decisions on the composition, color, framing, or resolution of images?1 Second, a discourse-analytical layer reveals the interdiscursive context of images through a study of the reports, homepages, flyers, or policy documents in which they are embedded (Rose, 2016: 186–219). Here, I ask how the different texts ascribe meaning to the images, and how the latter become linked to broader concepts, narratives, and storylines in environmental security discourse. A third layer focuses on the performativity of images as immutable mobiles and their function in broader visual assemblages. So, here the question is what visuals do rather than what they show: How are images produced by broader visual assemblages? How are they circulated or blocked? And how do they enact different versions of the environment? To study this third layer, I draw on a comprehensive review of the relevant secondary literature, combined with a thorough document analysis of legislation, regulations, and related policy documents in each case.

The co-evolution of remote sensing and environmental security

The roots of the visual assemblage of environmental security can be traced back to the militarization of geophysical research in the early years of the Cold War (Dalby, 2013: 41). With its successful launch of the Sputnik satellite in 1957 during the so-called International Geophysical Year, the Soviet Union fired the starting pistol for a technological and scientific race between the two superpowers. As a crucial part of this race, satellite remote sensing emerged as a dual-use technology, or ‘cyborg science – the result of an irreparable fusion of scientific and military concepts, materials and skills’ (Elam, 1999: 106). At the same time, the strategic communities’ interest in the atmospheric impact of nuclear weapons boosted advancements in numerical weather modeling, which in the 1960s were further developed into the first simulation models of global climate change. The ever more detailed global models at the same time produced ‘an insatiable thirst for data from every corner of the world’ (Edwards, 2010: 24), which since the late 1970s and 1980s was increasingly satisfied by satellite-based remote sensors. In addition, in 1972 the US administration established the Landsat program within the US National Aeronautics and Space Administration (NASA) as the first civilian satellite remote sensing program. The program’s eight satellites provided multispectral Earth imagery at moderate spatial resolution – perfectly suited for land (change) monitoring – and thereby contributed considerably to the discovery of macro-scale environmental problems, including deforestation, land degradation, and the ozone hole (DeLoughrey, 2014: 261).

NASA’s Landsat and other emerging remote sensing programs can be considered as parts of an emerging visual assemblage of heterogeneous human and non-human components (Barry, 2013: 14; Edwards, 2010). This assemblage includes hardware such as satellites, sensors, ground stations, and data centers; imagery-processing-and-analysis software; data such as images or digital maps; human actors like system operators, policymakers, scientists, and national security personnel; and legal and regulatory frameworks (Thompson, 2007: 2). The capacity to ‘see’ environmental problems, and to see the planet from a distance, is distributed across this visual assemblage. Neither the satellites, which translate the electromagnetic radiation reflected from the Earth’s surfaces into numerical grey-values, nor the operators in the control room, which process ‘wavelengths in false colours’ (Latour and Hermant, 2006: 8), nor the software tools that turn the data into realistic true-color images, nor the analysts or algorithms that interpret the resulting images would be able see anything were it not for the other elements in the assemblage.

A securitization precursor

I would argue that there was a close co-evolution between the emergence of a global visual assemblage of satellite remote sensing and the emerging discourse on environmental security in the 1980s and 1990s. The notion of co-evolution stresses the reciprocity of this development. While the satellite gaze made it possible to conceive of environmental change as a global threat in the first place (Van Munster and Sylvest, 2016: 6), environmental security also became inscribed into technical decisions, for example when Landsat’s remote sensors were optimized to monitor land change and resource degradation. The mutual imbrication of satellite technology and environmental security played out at several levels. First, the militarization of geophysical research during the Cold War created new associations between geoscientists and security actors that were crucial for the emerging imaginary of the environment as a security problem. Marzec (2014: 244) describes how this emerging actor-network led, for example, to the US defense and intelligence community’s interest in climate change in the early 1990s:

In 1992 the Central Intelligence Agency (CIA) began to establish relations with climate scientists in the program Measurements of Earth Data for Environmental Analysis, or MEDEA, when it declassified satellite imagery for ‘patriotic’ climate scientists.

Second, the described visual assemblage enabled a new ‘way of seeing’ the Earth and the human environment, which might be called a planetary gaze (DeLoughrey, 2014; Jasanoff, 2004: 44). The new possibility to look at the planet from the outside produced a sense both of the earth’s singularity and of its radical fragility. The planetary gaze produced a certain uncanniness – a feeling of being detached from planet Earth (DeLoughrey, 2014: 264). In so doing, the planetary gaze invoked deep-rooted ‘apocalyptic fears about the end of the earth’ (DeLoughrey, 2014: 266). This sense of urgency created by satellite remote sensing resonated well with the early environmental security debate in the 1990s and its alarmist tone (Marzec, 2014: 235). Yet the planetary gaze of the described visual assemblage did not simply produce another discursive frame of a pre-existing environment. Rather, it constituted a whole new reality of the Earth as a singular, interconnected, and fragile system (Van Munster and Sylvest, 2016: 4–8). This fragile Earth system became ‘matter-real’ through the immutable mobiles – such as true-color satellite images, simulation models, graphs, or numerical calculations – produced by two central inscription technologies: satellite remote sensing and computer modeling (Edwards, 2010: 2). By developing these technologies into a comprehensive global monitoring system, it was believed it would be possible to monitor, predict, control, and manage the Earth system (Jasanoff, 2004: 42; Marzec, 2014: 245). This global monitoring approach, which highlighted the role of national leaders as planetary or environmental managers, considerably influenced the early environmental security debate.

Third, the focus of the early environmental security debate in the 1990s was on large-scale global problems such as scarcity-induced conflict or migration (Rothe, 2016). The detection of these large-scale problems was closely linked to the technical capabilities of satellite remote sensing, for to detect large-scale, slow-onset changes like land degradation and resulting scarcities, an abstracted, distant view from above was required. What is more, multispectral sensors, such as those carried by Landsat satellites, made it possible to visualize processes of plant degradation in the infrared range of radiation. To be precise, these large-scale environmental changes were considered as drivers of conflict and migration in the early environmental security discourse. Remote sensors and their planetary gaze thus considerably influenced the epistemological horizon of environmental security thinking.

Opening and commercializing remote sensing

During the Cold War, access to the visual assemblage of satellite remote sensing was restricted to a closed ‘club’ of a few geoscientists, military research centers, and international bureaucrats (Elam, 1999: 98). The monopolization of space technology and security concerns imposed heavy restrictions on the circulation of the immutable mobiles of satellite sensors. Landsat is a good case in point: while the civil Landsat program was used by the USA to promote ideals of transparency and international scientific cooperation, the US government at the same time restricted the permitted spatial and spectral resolutions of Landsat images (Thompson, 2007: 8). Furthermore, the inaccessibility of satellite images and their abstract, scientific enactment of the environment further limited the number of potential users.

Shortly before the end of the Cold War, however, this picture began to change. The USA reacted to privatization efforts in France and the Soviet Union and decided to open and commercialize its remote sensing industry with the Land Remote Sensing Policy Act of 1992 (Elam, 1999: 99). The commercialization process was accompanied by the triumphal march of the personal computer and the spread of geographic information system (GIS) software to read, process, and interpret geodata, which further increased the number of users of commercial satellite imagery. As a result, satellite remote sensing grew into a massive and complex global market with a projected size of US$2.6 billion by 2020. The current global market is characterized by the dominance of a few global players, such as DigitalGlobe, and national space agencies as well as the emergence of myriad medium- and small-sized enterprises that are turning satellite data into maps, GIS products, or data visualizations.

The opening and commercialization of remote sensing technology happened at the same time as a shift in environmental security discourse towards human security and resilience (Corry, 2014; Detraz and Betsill, 2009; Trombetta, 2008). Increasingly, the focus of environmental security was shifted from the international system or the nation-state towards individuals’ and local communities’ vulnerabilities and local environmental risks (McDonald, 2013: 46–47). A global managerial command-and-control approach to environmental problems made way for more regionalized approaches of risk management and other measures to enhance the adaptive capacities of vulnerable populations against environmental shocks (Oels, 2013: 24–26).