Emerging Cybersecurity Threats to LEO Space Assets: Incentives for Market-Driven Cyber Defense

GEORGETOWN UNIVERSITY
SPACE INITIATIVE

Carly Glickenhaus
April 2020

Introduction

The escalation of cyber risk to space systems poses an existential threat to U.S. security and democracy. Computer network exploitation and attack undermine the confidentiality, integrity, and reliability of data systems in an age where disinformation campaigns distort public perception of truth and corrupt governing institutions.

As the space industry makes rapid advances, cybersecurity policy is struggling to keep pace. The proliferation of low-Earth orbiting (LEO) satellites has democratized space, hosting an array of new actors and creating an urgent demand for commercial governance. U.S. policy has explicitly acknowledged both cybersecurity and space as critical discussions but has not fused them in an integrated assessment of cyber vulnerabilities in space. This paper examines the cyber threat landscape across LEO assets and offers policy recommendations for cyber governance in the commercial space market.

U.S. Dependence on Space Assets

Cyber breaches in space systems could have disastrous implications on the ground. Satellite constellations offer critical services like communications (SATCOM), remote sensing, imaging, IoT, and cloud storage.[1] GPS satellites enable coordinated universal time, financial timestamping, and positioning for constant defense, civilian, and commercial applications.[2] If GPS functions were compromised, an adversary could undermine global banking and precision navigation. COVID-19 may pose a risk to the scheduled deployment of technologies like GPS. In April, Space Force SMC postponed the launch of the third GPS 3 satellite to minimize the potential of COVID-19 exposure to the launch crew and operators.

The U.S. military relies on space for C2, ISR, and missile defense. Inadequate interception of incoming ballistic missiles tracked by flawed space systems could result in innumerable civilian casualties.[3] In 2001, 60% of munitions employed in Afghanistan were guided by space technology. Just two years later, nearly 70% of American weapons in Iraq relied on space-based systems like SATCOM. Between 2003 and 2011, there was a 560% increase in U.S. military use of *commercial* satellites. As 5G implementation exponentially increases the quantities of data supported by a network, IoT and AI will be force multipliers in space-based military intelligence,[4] representing a growing challenge to ensuring data integrity. As DoD moves more data to the space-enabled cloud, space cybersecurity should be a top budget priority.

Space Governance and National Security

The space market has been growing faster than the accompanying cyber regime. American culture seems to have an instinctual respect and admiration for space, allowing the space economy to grow relatively unchecked. Since the Cold War era, space presence has been perceived as a signal of state power. For decades, space science was a proxy battlefield. When Russia beat the U.S. into orbit in 1957, the U.S. reacted by invigorating domestic space research, beating the world to the moon in 1969. Successful space programs allowed the U.S. and Russia to signal that they had explicit space doctrines, state funding, prestigious academics, and manufacturing infrastructure. Space innovation projected power through military resources, economic capacity, and a compelling cultural narrative. In the last few decades, a new kind of space race has emerged: the duty to maintain a competitive technological advantage, at the core of the U.S. security paradigm, rests in private hands.

Cyber Vulnerabilities in Space Assets

While certain resources in the space economy have recently become more affordable, like small launch vehicles and launch services, other resources remain scarce, intensifying competition. System vulnerabilities may emerge from this competition. For example, there is a finite supply of electromagnetic band allocations, creating high demand for ITU spectrum licenses. Supply restrictions block many

[1] Fidler, David. "Cybersecurity and the New Era of Space Activities." *Council on Foreign Relations Digital and Cyberspace Policy Program* (2018).
[2] "GPS Applications." GPS.gov. https://www.gps.gov/applications/ (November 2019)
[3] Unal, Beyza. "Cybersecurity of NATO's Space-based Strategic Assets." *Chatham House: The Royal Institute of International Affairs* (2019)
[4] Unal

hopeful entrants, leading some university-operated satellites to use "open frequencies" of the spectrum, which are much easier to manipulate.[5]

Orbital property itself is a limited resource; the proliferation of LEO assets and mega-constellations has already crowded orbital paths. SpaceX has deployed the world's largest active satellite constellation plans to launch up to 42,000 by 2027, nearly eighteen times the number of operational satellites in orbit today.[6] Already, astronomers claim Starlink's prolific reflectivity interferes with scientific observations.[7] Potential environmental impact means FCC licensing of Starlink may violate international law and even expose the agency to litigation.[8] Simultaneously, the number of IoT devices is projected to grow at an annual compound rate of 21% to 2022,[9] resulting in 18 billion IoT devices worldwide, 1.5 million on mobile networks. IoT deployment in businesses has increased from 13% in 2014 to 25% in 2019,[10] suggesting Internet Protocol 6 will heavily depend on SATCOM for growing network infrastructure. IoT growth appears highly resilient; despite compressed demand for space services as COVID-19 chokes revenue streams, major IoT deals have gone through. In early April 2020, Thales Alenia was contracted to design and build an initial two NGSO satellites to support 3GPP-defined narrow-band IoT radio interface for Omnispace, who envisisions deploying the world's first global 5G non terrestrial network.[11] Globally, the expansion of digital infrastructure to support 5G demand increases the *cost* of cyber defense, which may deter many small space companies from investing in cybersecurity, leaving their vulnerabilities undetected.

Targeting Satellite Systems

To execute a cyberattack, an aggressor must insert a threat vector within the satellite system.[12] Hackers are most likely to target ICS and SCADA systems, which are broken up into three components: computers that control and monitor operations, field devices like programmable logic controllers to govern sensors, and human-machine interfaces.[13]

Terrestrial components of the satellite system are connected by internet and operated by humans, who can be easier to 'hack' than computers. Like physical security, many cyberattacks are traced to insider breaches, intentional or accidental. Hackers often use open-source platforms like Google, LinkedIn, and Facebook to identify employees with privileged access credentials at the most vulnerable point in the network, the ground station. A simple phishing campaign via email or social media can be sufficient to manipulate personnel into inadvertently providing access to their workstation and, subsequently, satellite control systems. Once inside the network, hackers can control satellite functions or gain access to data.[14]

Chinese Cyber Capabilities

During conflict, one country's ability to disable or destroy its opponent's satellites would be a significant tactical advantage. The risk of cyberattacks seizing physical control of satellites has received scant attention[15] in government reports and academic literature. Our adversaries' hybrid cyber-kinetic attack capabilities have tremendous strategic importance. In particular, U.S. cyber defense should reflect Chinese state incentives for cyber aggression. In 2015, Chinese military strategy designated both space and cyber as commanding domains, signaling a realistic and credible space-cyber threat.[16] Two years

---

[5] Suzuki
[6] European Space Agency. http://www.esa.int/Safety_Security/Space_Debris/Space_debris_by_the_numbers
[7] Hall, Shannon. "As SpaceX Launches 60 Starlink Satellites, Scientists See Threat to 'Astronomy Itself'." November 2019. https://www.nytimes.com/2019/11/11/science/spacex-starlink-satellites.html
[8] McFall-Johnsen, Morgan. "SpaceX's license to launch hundreds of internet satellites may have violated the law, experts say. Astronomers could sue the FCC." January 22, 2020. https://www.businessinsider.com/spacex-starlink-satellite-license-fcc-environmental-law-2020-1
[9] Squire Technologies. "IoT Whitepaper." https://www.squire-technologies.co.uk/docs/IoT_whitepaper.pdf
[10] McKinsey & Company. "Growing Opportunities in the Internet of Things." July 2019. https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things
[11] "Omnispace Selects Thales Alenia Space to Develop Satellite Infrastructure for its Global Hybrid Network Vision." https://www.prnewswire.com/news-releases/omnispace-selects-thales-alenia-space-to-develop-satellite-infrastructure-for-its-global-hybrid-network-vision-301037600.html
[12] Livingstone, David. "Space, the Final Frontier for Cybersecurity?" Chatham House (2016). 21.
[13] Livingstone: 22
[14] Livingstone
[15] Livingstone: 23
[16] State Council Information Office of the People's Republic of China. "China's Military Strategy." *USNI News.* 2015.

later, a Chinese anti-satellite test produced over 3,000 pieces of debris, which remain in orbit today. Even if the resource-intensive task of cataloguing and tracking orbital debris succeeds, effectively identifying and communicating with the appropriate operators would be nearly impossible. Even if operators receive complete and accurate data, and their large satellites have maneuver capabilities to avoid debris, small satellites would not have the maneuver abilities needed to avoid collision.[17]

According to CSIS, *86%* of Americans[18] would have a more positive impression of a company if it relocated manufacturing away from China and back to the U.S.[19] In the wake of a trade war and protests in Hong Kong, the threat of declining U.S. demand and stunting Chinese growth could threaten to escalate tensions. China's growing incentives to fire a first warning shot makes it more urgent than ever to identify cyber vulnerabilities in U.S. space assets.

Russian Cyber Capabilities

As intelligence officials confirm evidence of Russian election interference in 2016 and beyond,[20] virtual campaigning during the COVID pandemic has offered hackers new vectors for attack and influence. Assessing Russian cyber capabilities in telecommunications ought to be a top national security priority. Low-budget, Russian-based "Turla" malware has proven successful attacking older communications satellites that used encrypted data links.[21] The malware package cost just $75 to build, which covers a satellite receiver card, open-source Linux applications, and widely available "network-sniffing" tools.[22] These tools are cheaper than kinetic alternatives, offering low risks and high rewards.

Frequent reports of GPS interference in the Black Sea indicate that Russia exploits Ukraine as a testing ground for cyber weapons. For example, Russia has experimented with jamming GPS signals to ground remotely piloted aircraft and execute DOS attacks on radio and phone equipment. Russia is a key player in a growing trend of blending electronic warfare and cyber warfare, with increasingly sophisticated tools for denial and degradation of C4ISR networks.[23]

State Governance of Cybersecurity Falls Short

In response to major data breaches like Target and CapitalOne, cyber governance has somewhat evolved from an emphasis on endpoint and perimeter defense to a more holistic risk-based approach, but stakeholder jurisdiction remains unclear. According to the GAO, 60 distinct organizations manage DoD space acquisitions, fragmenting responsibility for cyber governance.[24] Dispersed, unclear authority prohibits a consistent methodology for evaluating cyber threats to space systems.

Space cybersecurity will be fundamentally different from terrestrial cybersecurity. Joshua Hartman of Renaissance Strategic Advisors[25] makes a questionable claim that "space systems are an extension of our existing networks, so we should be able to take the mindset that we use on terrestrial cyber and project that into space."[26] This kind of linear thinking in the aerospace sector is dangerous; nothing is easily projected into space. First, space assets cannot be accessed and serviced on-demand yet. Second, space cybersecurity presents a double attribution problem. The first layer is the classical cyber attribution problem; it is more difficult to trace cyberattack's perpetrators than a kinetic attack. The second layer is the high burden of proof in space: a victim has to establish causation between a cyber event and satellite damage.

---

[17] Harrison, Todd, et. al. "Space Threat Assessment 2019. "*Center for Strategic and International Studies* (2019).
[18] The Harris Poll. April 3-5, 2020. https://theharrispoll.com/the-coronavirus-crisis-is-turning-americans-in-both-parties-against-china/
[19] Kennedy, Scott. Online Event: US-China Tech Competition and Cooperation in the COVID-19 Era. April 8, 2020. https://www.csis.org/events/online-event-us-china-tech-competition-and-cooperation-covid-19-era
[20] Goldman, Adam et al. "Lawmakers Are Warned That Russia Is Meddling to Re-elect Trump." February 20, 2020. https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html
[21] Harrison
[22] Weeden, Brian and Victoria Samson. "Global Counterspace Capabilities: An Open Source Assessment." *Secure World Foundation* (2019).
[23] Weeden

[24] Dwyer, Morgan. "Bad Idea: Assuming that Small Satellites Will Solve Big Satellites' Problems." CSIS Defense360. https://defense360.csis.org/bad-idea-assuming-that-small-satellites-will-solve-big-satellites-problems/ (November 2019)
[25] Renaissance Strategic Advisors is one of the leading consultancies supporting aerospace, defense, space, intelligence, and government services.
[26] Russell

Space cybersecurity requires a novel approach to remote system governance. Thus far, the U.S. regulatory landscape has been guided by the NIST framework, which offers common language to communicate requirements like supply chain analysis, privacy considerations, and cyber risk management practices.[27] Concrete NIST guidance is a crucial *foundation* for cyber governance, but implementation and enforcement fall short.

Alternatives to State Governance: Commercial Self-Regulation of Space Cyber

Corporations often perceive compliance efforts as intrusive obstacles to capitalist freedom. Despite moral and democratic objections to Russian and Chinese defense industrial bases, policymakers should admit that Chinese and Russian innovation are allowed to thrive under regimes free from government arbitration and bureaucratic delays.[28] The U.S. is not a global hegemon in a multipolar cyberspace and does not necessarily wield agenda-setting power to set the terms of engagement in cyberspace. Therefore, future regulatory efforts in the U.S. should prioritize commercial autonomy and leadership.

Engineering Reliable Incentive Structures for Cyber Governance

In 2018, the White House National Cyber Strategy formally acknowledged space cybersecurity as a priority, but is powerless without attractive paths for implementation.[29] With institutional backing from Air Force Space Command, the Missile Defense Agency, NASA, and the NSC, the Space Information Sharing and Analysis Center (S-ISAC) can bridge this gap. In theory, building alliances under NDA should enable an organization like ISAC to counter the deterrents to sharing that publicly traded companies typically face: publishing vulnerabilities undermines shareholder confidence and drives a stock price down. In practice, ISAC incentives are distorted. Companies, particularly small startups, may remain reluctant to share information with any potential competitors. For a profit-driven firm, announcing any vulnerability, even in private, can be just as dangerous as penetration of that vulnerability. The following recommendations offer tangible ways ISAC can incentivize participation and ensure impact through market-driven incentives.

Recommendation 1: Managing the Collective Action Problem

In a crowded LEO, governance demands precise commercial coordination of intersecting flight paths. Under existing international law, states are directly responsible for all national space activities, whether that activity is conducted by the government itself or by its companies.[30] Spacefaring states are internationally liable for "damage to another state party to the treaty or its natural or juridical persons by such object."[31] When considering collective threats to LEO assets, there is a precedent for addressing collective action in space, the Inter-Agency Space Debris Coordination Committee (IASDCC).[32] The threat of indiscriminate destruction by space debris means wealthier market incumbents are not necessarily safer than small entrants. ISAC can appropriate IASDCC's security model to build a cybersecurity regime resolving today's cyber deficits. The collective action problems for both space debris and cyber vulnerability escalate as more assets are deployed.

Under the classic economic model, the best product competes well and prevails above substitutes. This Darwinian explanation for product survival does not apply to LEO space. In LEO, even the most robust cyber defense can be vulnerable to variables outside the operator's control. For example, an attack on a university-launched CubeSat could send it spinning into a SpaceX COMSAT. This means cybersecurity of a military constellation is just as critical to collective security as a tiny CubeSat. Today, any LEO stakeholder could be affected by another's vulnerabilities.[33] The slight manipulation of code could alter function in the sky and enact massive system failures on earth.

[27] National Institute for Standards and Technology. "Cybersecurity Framework."
[28] Livingstone
[29] Office of the President of the United States. "National Cyber Strategy of the United States of America." White House, 2018.
[30] Secure World Foundation, 9
[31] Secure World Foundation, 27
[32] Fidler
[33] Livingstone, 24

Collective action requires participation of *all* relevant stakeholders. ISAC may incentivize more participation by rebranding the process of "information sharing" as a"threat exchange marketplace." The term "sharing" has linguistic associations with more social, voluntary practices, and might deter some for-profit companies, particularly smaller space players.

Recommendation 2: Prioritize Inclusivity and Accessibility

To promote inclusivity of small business, ISAC should develop widgets and training programs to empower businesses to feel directly responsible[34] for their cyber protections instead of just outsourcing all cyber defense to blind trust in cybersecurity firms. For participation to be sustainable, ISAC should revise its fee structure to make the organization accessible to small firms and startups. The pool of threat information represents a public good. If all stakeholders stand to benefit from that public good, the cost burden should be shared. The laws of probability would mandate a greater financial burden on behemoth veteran space companies with a larger fraction of LEO property. S-ISAC offers founding memberships at $75,000, platinum memberships at $50,000, and a starting fee of $10,000, which may be prohibitive for the smallest, and arguably most vulnerable, satellite operators.[35] The pricing scheme could be adjusted to start with a free "trial" membership, and then a "student discount" model for startups, which would align more closely with the venture capital investment cycle. Not only are there moral and economic imperatives to empower the weakest players, but excluding them also poses a grave security risk.

Recommendation 3: Experiment with Supply Web Management Tools

Military and commercial assets are entangled not in a singular "supply chain" but in a global supply web.[36] As COVID-19 disrupts and displaces supply flows, new webs will emerge, with novel security questions, making asset tracking ever more important. The UN mandates that any launching state share certain parameters with an international registry, including registration number, launch date, territory, and location, orbital parameters,[37] and function.[38] ISAC should explore opportunities to aggregate existing public registry data in a blockchain for distributed database management. Lockheed was the first major defense contractor to introduce blockchain to their own systems. Blockchain offers instant verifications, timestamping, and an immutable record of transactions that would help build credible relationships between vendors and their customers. By enhancing the trust built into the supply chain, space companies would be more likely to invest time and resources to comply with cyber norms. For example, operators may not prioritize constant software updates to patch vulnerabilities on satellite terminals, potential granting hackers access to the network. Trusted vendor relationships encourage those managing the software to treat cyber risks seriously and instantly respond to bug fixes.

Recommendation 4: Develop Quantitative Tools for Evaluating Space Cybersecurity

To build incentives for private firms to prioritize cybersecurity, the first step is mapping organizational decision-making from the stakeholders' perspectives. Behavioral economics helps explain firms' hesitance to invest in cybersecurity when framed through loss rather than gain. It would be wise to promote cybersecurity as an economic *good* rather than uncertain protection against an economic *bad* like data loss. Firm attitudes toward cybersecurity are modeled by prospect theory, which claims firms assess their loss and gain perspectives asymmetrically:[39] to some firms, the perceived loss of $1,000 can only be compensated by the perceived gain of $2,000. This means it may be more useful to emphasize discussing cybersecurity as a gain rather than cyber risk as a loss. While expected utility theory models decisions that perfectly rational agents would make, prospect theory describes real firm behavior, which deviates from perfect rationality. Prospect theory is essential to resolving conflicts of interest between government regulators and companies because risk-versus-reward evaluations by one actor could be very different to

[34] Livingstone, 26
[35] Hitchens, Theresa. "NSC Makes Cyber Security For Space Industry 'Top Priority.'" *Breaking Defense*, 2019.
[36] Livingstone 21
[37] Basic orbital parameters would include nodal period, inclination, apogee, and perigee.
[38] Secure World Foundation,11
[39] Kahneman, Daniel and Amos Tversky. "Prospect Theory: An Analysis of Decision Under Risk," 1979.

those imagined by others.[40] Parameters of risk vary across the target set of ground stations and satellites, the attacker's strategy of random or ordered selection, the compromise rate, and the malware effectiveness ratio.[41] By examining the space insurance industry, we can develop quantitative models of these risk vectors.

Recommendation 5: Incremental Discounting in Insurance Markets

Insurance markets offer a tangible way to incentivize small companies to participate in governance efforts like S-ISAC. Insurance incentives would prime cybersecurity as an *investment* with returns rather than a regulatory *burden.* Assigning market value to cybersecurity raises the reputational value of compliance and, conversely, the costs of defection. Many countries, including the U.S., *require* space entities to carry insurance,[42] creating a mandatory fixed cost. Following R&D and launch costs, insurance is usually the third-highest cost associated with satellite activities.[43] This means that space companies, particularly small businesses and startups, have a strong incentive to reduce their insurance premiums.

According to Richard Parker, the Managing Director of Assure Space,[44] space insurers are forced to address cyber but flinch at such a broad and unquantifiable risk vector. Assure Space operates in the Lloyd's of London insurance syndicate,[45] which employs a reverse auction such that the lowest premium offered wins the contract. By selecting the clients who best comply with cybersecurity standards, an insurance company could mitigate cyber risk and afford to price premiums more competitively. Insurance companies could reward adherence to prescribed cyber requirements with discounts, cheaper policies, and preferential treatment would enhance corporate compliance. Parker confirmed space insurance companies would certainly have an interest in such a plan if it could be developed. I will outline such a plan, which S-ISAC can leverage its network to execute.

In November 2019, the House reauthorized the terrorism risk insurance act, including a provision calling for a study of whether the current risk-share system is appropriate for a cyber terrorism attack, and whether cyber risk coverage can be adequately priced by the private market. Space insurance companies must be equipped to assess cybersecurity. ISAC can develop universal benchmarks and a industry-accepted framework that aggregates NIST and CIS controls, eliminating redundancies and vague clauses. From this document, objective third-party audits can conduct the risk assessment reports that insurance companies need to write effective policies. These reports would allow insurance companies to develop incentives for the insured entity to change its behavior, creating an economic "nudge." For example, a satellite operator would be prompted to implement system segmentation to make it more difficult for hackers to "crawl" laterally across a network. Investing in this practice would have a compression effect on net risk, reducing the cost of insurance coverage for the customer and mitigating the probability of a massive payout by the insurer. This process would be facilitated by threat information exchange between ISAC constituents.

Uncertainty and ambiguity with regards to cyber norms will accumulate costs for insurers and their customers over time, creating an urgent need for S-ISAC to establish its role in cyber governance. Insurance plans like homeowner's insurance list "perils" defining boundaries of coverage.[46] At the intersection of space and cyber insurance sectors, such boundaries remain unclear. Under many space insurance plans, a customer could forget to install an entire engine on its launch vehicle and still be covered. While kinetic attacks are covered, a cyberattack producing a kinetic effect, by changing the orbit of a satellite or depleting its propellant, would *not* be covered.[47]

---

[40] Livingstone, 26
[41] Lee
[42] Also the U.K., France, Australia, Brazil, Japan, and South Korea
[43] Secure World Foundation, 74
[44] Assure Space is an underwriting agency providing space insurance products including traditional launch, in-orbit, and third-party liability insurance
[45] Assure Space uses syndicates to insure high-valued property and high-hazard liability exposures.
[46] Insurance Information Institute. "Which disasters are covered by homeowner's insurance?" 2019.
[47] Parker, Richard.. "Space and Cyber: Bolstering the Two Domains." Interview by Carly Glickenhaus. October 2019

This irrational market failure is a product of the "war-like act" exclusion clause in insurance law. Since NotPetya, insurers have denied claims related to state-backed hacks, citing war exemption. Resolving this conflict will require determining the degree of responsibility companies have to protect their own networks. Because of the double cyber attribution problem and the designation of cyber as a military domain, essentially *any* cyber manipulation could be considered a war-like attack. In 2015, the Obama administration labelled the SONY hack a "very costly" act of cyber "vandalism" but not an act of war.[48] In 2017, the Trump administration labelled NotPetya a cyber "strike." This linguistic distinction is critical to insurance law because an "attack," especially by a state enemy, is categorically "war-like." Even if the perpetrator is not a state actor, a cyberattack on a satellite system is likely to be considered "war-like."

Recommendation 6: Leveraging Industry Transformation for Cyber Attention

COVID-19 exacerbates financial pressures on the space industry, where many small and medium-sized businesses may already be operating at low or variable margins. In late March, OneWeb, one of the leading companies attempting to build a mega-constellation for global broadband service, filed for bankruptcy. OneWeb's failure presents an opportunity for firms like Rocket Lab to grow their satellite business and fill demand gaps for low Earth orbit constellations.[49] However, the financial loss to Ariane Space and others strategically positioned to support OneWeb may constrain decades of space growth. The restructuring of market players, adapting business models, and delayed launch timelines makes the COVID crisis an ideal time for firms to reevaluate their cybersecurity standards and practices. Even the biggest players in space, like Airbus, have paused production. Despite widespread financial distress, COVID could be a massive opportunity for long-term space security. Space companies, linked by ISAC, should implement new cyber protections as they revise their business models and product development for a post-COVID world.

Today's new business practices expose unforeseen cyber vulnerabilities. While government agencies may have security restrictions demanding physical mission control centers, some private companies, particularly those working on smallsats, are using the pandemic to examine how they can operate their spacecraft remotely. CEO of Kubos[50] Marshall Culpepper said, "With current technology, there's no technical reason to require operators to be within visual range of a satellite dish, or even in the same time zone." Other companies have already adopted remote satellite operations, including Planet, which operates the largest remote sensing satellite system in the world.[51] Remote operations will increase the cost of cyber defense across an expanded attack surface.

Next Steps

Securing space assets is urgent. In an election year and pandemic, public trust in data is at stake. In the coming decade, climate change will produce ice-free summers in the Arctic, creating demand for telecommunications to support new industrial activities. Today, the momentum of 5G and IoT technology will not wait for cybersecurity policy to catch up. The tendency to default to an exclusively technical perspective has historically eroded cybersecurity efforts. The solution to today's governance deficit is not purely technical. The next step is to commission a study modeling the economic consequences of a hypothesized cyberattack on U.S. space assets to build smart incentive structures for the future. These recommendations will help establish norms, develop instincts, and enforce standards to create a habitual cybersecurity culture in the space industry.

[48] "Obama Called the Sony attack an act of 'cyber vandalism.'" *Washington Post, 2014.*
[49] Erwin, Sandra. "Rocket Lab executive says company is well positioned to weather crisis." April 1, 2020. https://spacenews.com/rocket-lab-executive-says-company-is-well-positioned-to-weather-crisis/
[50] a company that develops both spacecraft flight software and a cloud-based mission control system
[51] Foust, Jeff. "Coronavirus raises interest in remote spacecraft operations." March 27, 2020. https://spacenews.com/coronavirus-raises-interest-in-remote-spacecraft-operations/