FDD

UVA | FRANK BATTEN SCHOOL *of* LEADERSHIP *and* PUBLIC POLICY

Countering the People's Republic of China's (PRC) Cyber Enabled Anti-Satellite (ASAT) Capabilities

David King

Applied Policy Project: Frank Batten School of Leadership and Public Policy with the Foundation for Defense of Democracies

Professor Andrew S. Pennock, PhD

Spring 2020

ACKNOWLEDGEMENTS

I would like to thank Trevor Logan and Annie Fixler at the Foundation for Defense of Democracies for their thoughtful feedback and guidance during my research process. Thank you for allowing me the opportunity to learn from and leverage your expertise over the past year.

Special thank you to my thesis advisor, Andrew Pennock, your lessons on life and leadership have already impacted my life and will continue to do so. Your tireless support and constant feedback made this project possible.

I would also like to thank Professor Brad Carson for introducing me to Space Policy last year in your one credit short-course, Space Power, and for providing feedback on my research process over the past year.

Finally, I would like to thank my friends, family, and colleagues at the Batten School and beyond for supporting me throughout my academic career. Special thank you to my colleagues Daniel Durgavich, Zach Diamond, Seneca Tsang, and James Reed for your countless proofreads, edits, feedback, and support throughout this process.

Client

This report was prepared for the Foundation for Defense of Democracies (FDD). The Foundation for Defense of Democracies is a nonprofit, nonpartisan 501(c)(3) research institute focusing on foreign policy and national security. FDD conducts in-depth research, produces accurate and timely analyses, identifies illicit activities, and provides policy options – all with the aim of strengthening U.S. national security and reducing or eliminating threats posed by adversaries and enemies of the United States and other free nations.

Disclaimer

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy, University of Virginia. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. The judgments and conclusions are solely those of the author, and are not necessarily endorsed by the Batten School, by the University of Virginia, or by any other agency.

Honor Pledge

On my honor as a student, I have neither given nor received unauthorized aid on this assignment.

David King

UVA | FRANK BATTEN SCHOOL *of* LEADERSHIP *and* PUBLIC POLICY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Modern cyber capabilities pose a grave threat to critical United States satellite infrastructure. In the 21st century, satellite infrastructure is a critical component of the United States economy and national defense and is a top target for US adversaries.[1] While protecting satellites and deterring anti-satellite weapons is already a top priority for national security professionals, unique characteristics of both cyber space and outer space leave satellites vulnerable to severe damage from a motivated and capable adversary.

The People's Republic of China has both the capabilities and the incentive to deploy cyber-weapons to neutralize the US strategic advantage in outer space. Furthermore, the People's Republic of China has a history of deploying cyber means to advance their strategic interests in both the economic and national security realms. Rational deterrence theory further increases concern because it provides an academic framework describing China's incentives to proactively strike US space infrastructure and suggests that options to deter such an attack are severely limited. While the People's Republic of China may not deploy these capabilities today, tomorrow, or even next year, the threat will only continue to increase and the United States needs to prepare itself accordingly.

To address this problem, we recommend a multifaceted policy approach to reduce the probability of a successful attack and mitigate the national security costs in the event of a successful attack. Specifically, we recommend expanded that both government and commercial entities expand their compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework to limit the chance of a successful attack. Furthermore, additional training and resources should be devoted to mitigating the human element risk factor of cyber security, which seems to present the greatest risk.

Additionally, the United States should preserve ground-based GPS back-up infrastructure eLORAN so that critical military and national security functions can continue in the event of a cyber-attack against US satellite infrastructure. Finally, think-tanks, academic institutions, and government contracting firms should continue to research the both the technical and theoretical facets of the threat to and inform the federal government when the threat and recommended policy responses inevitably change.

UNDERSTANDING THE THREAT

Critical US Satellite infrastructure is particularly vulnerable to a cyber-attack from a technologically advanced adversarial state due to several unique features of both the cyber and outer space domains. Cyber-attacks are relatively cheap and easy to deploy relative to conventional military capabilities. Furthermore, when well executed it can be nearly impossible to attribute the source of the attack. Compounding these risks, satellites face many risks common to other critical infrastructure. Both hardware and software in satellites is frequently outdated in terms of security due to the high-costs of updating and patching in space. Similarly, as with other industries, the human element remains remain the weakest link in securing satellites from cyber threats. Additionally, since satellites must communicate with infrastructure on earth to be useful, they cannot be "air-gapped"[i] as is often recommended for critical infrastructure. Finally, since satellites perform unique functions, there is often no terrestrial back-up for satellite capabilities. To more deeply understand the vulnerability of US satellite infrastructure to attack, each of the above risk-factors will be discussed below.

> In a 2019 simulation, a cyber ASAT "tested in orbital spaceflight simulations and successfully attacked 93% of the strategically vital Iridium satellite constellation, all without firing a single rocket."[2]

Cyber capabilities are relatively cheap, easy, and accessible.

In contrast to conventional warfare, the high accessibility and low cost of cyber-attacks enables an asymmetric warfare approach where an adversary is able to cause grave damage without fear of a proportional response.[3] Cyber capabilities are far more widespread than orbital launch technology and NSA estimates that over "100 countries could harm the US with offensive cyber capabilities."[4] This number is over 10 times the number of independent spacefaring nations and over 50 times the number of countries with proven anti-satellite capabilities.[5] While conventional attacks require significant infrastructure and personnel costs, cyber-attacks can be executed remotely with little to no infrastructure support.[6] In fact, while both space technology and military technology often costs millions, cyber weapons are often cheap or even free to download from the public web. [7]

As a result, cyber offensive capabilities are generally regarded as easier and more cost-effective than cyber defense.[8] Defenders must be able to defend an entire network 24/7 while a cyber attacker only needs to find individual points of vulnerability.[9] While cyber attackers are

[i] A cyber "air gap" refers to a system disconnected from other networks and the internet to improve security.

constantly discovering new exploits, cyber defenders must invest significant time and money into patching each individual vulnerability while also working to anticipate new threats.

Cyber-attacks can be nearly impossible to attribute.

Another key challenge posed by cyber weapons is that, when they are well executed, it can be nearly impossible to attribute the source of the attack and the identity of the attacker. If the US cannot confidently identify the source of an attack, then its ability to respond effectively will be severely limited. From a structural standpoint, the architecture of the internet and most modern computing technology was not designed for identifying attributing the actions of a competent hacker.[10] As a result, cyber attackers can evade detection through a wide range of possible techniques.

There are countless techniques that hackers can use to obscure their identity. Hackers can spoof their digital identity using stolen credentials.[11] They can use a step stone attack where they route their attack through innocent machines before attacking the victim.[12] They can use a short "Time to Live" attack such that the program terminates before the victim's computer can gather location data or even a Zombie attack method, where malware isn't executed until the hacker is long gone.[13] While this list is by no means exhaustive, it demonstrates the variety of means that hackers have to obscure their identity and make attribution difficult. Exacerbating this problem further is the fact that, even if the United States is able to effectively trace an attack back to its geographic location, it is impossible to confidently assert that such an attack is state-sponsored.[14] In such a situation, the US wont' be able to determine whether a hacker is simply an unaffiliated cybercriminal or a third-party operating on behalf of his state government. This attribution challenge clouds policy decisions and makes it exceedingly difficult to effectively respond to state-sponsored cyber-attacks.

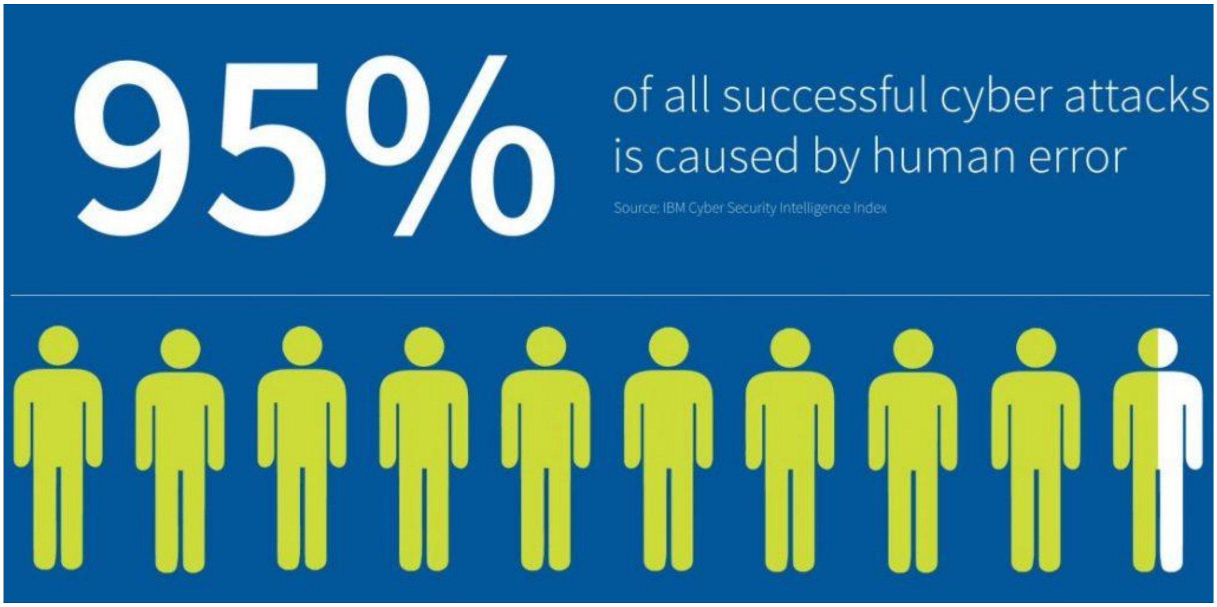
Satellite hardware and software is often outdated and insecure.

Continued use of outdated and insecure technology is a problem across the federal government. In 2019, the Government Accountability Office Identified, 65 legacy systems across 10 government agencies ranging from 8 to 51 years old operating with known hardware and software vulnerabilities, outdated languages, and obsolete hardware.[15] In the Department of Homeland Security alone, 168 high or critical risk vulnerabilities were discovered in 2018. This same pattern holds true for US satellite infrastructure. Both satellites and ground-based infrastructure often operate using outdated or insecure hardware and software. In summer 2019, Chatham House identified the use of old proprietary IT hardware and software and the failure to address known vulnerabilities in these technologies as key risk factors threatening NATO's space-based strategic assets.[16] While hardware attacks, which require physical access, against satellites are highly unlikely, outdated software and hardware leave satellites vulnerable to attack.[17] Patching for these vulnerabilities is often delayed because, as mentioned above, physical access to existing satellites for hardware update is cost prohibitive, and there are often high costs associated with taking a satellite "offline" for a software patch. As a result, many satellites remain vulnerable to old cyber threats long after a patch has been released.

The Human-Element Challenge

No conversation surrounding cyber threats is complete without acknowledgement of the human element. People still constitute the weakest link in cybersecurity and the space industry is no exception.[18] As Figure 1 shows below, social engineering and human error can be used to gain access to even the most technically secure systems. This includes critical satellite infrastructure. Human error threats include both careless mistakes by honest employees and the actions of malicious insiders who seek to cause harm. Most government agencies and commercial satellite companies have training and other measures in place to mitigate this challenge but, this is not the case with all companies and, as such, it remains a serious risk to our nation's satellite infrastructure.[19]

Figure 1. The Human Element of Cyber Threats



Statistic Source: IBM Security Intelligence Index
Graphic Source: Cyber Aware Magazine, https://cyberaware.com/cybercrime-the-human-element-beyond-it/

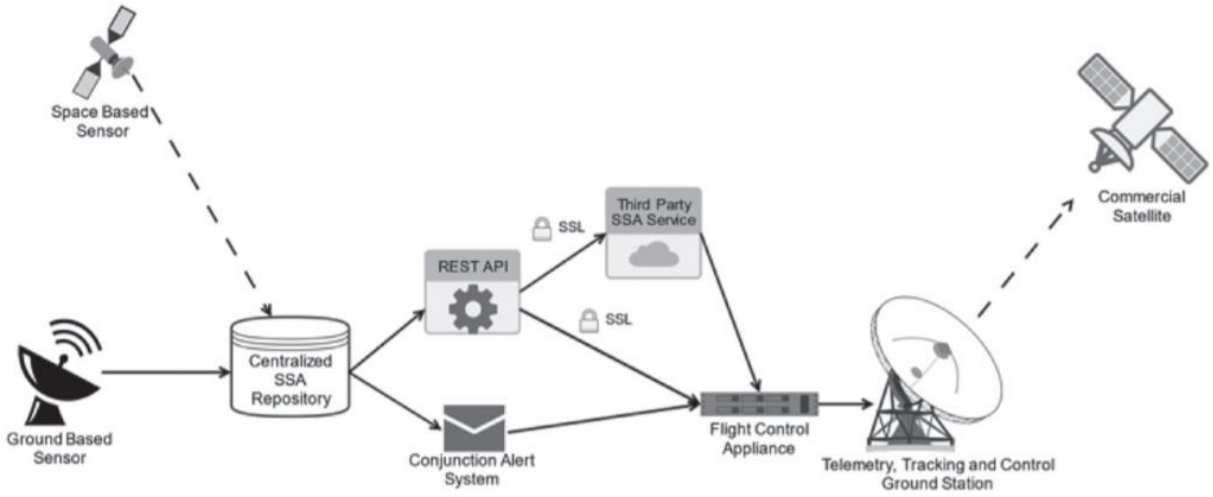
Satellites cannot be "air-gapped."

One of the most common recommendations for securing critical control systems is the "air gap." "Air gapping" describes the principle that if a system is disconnected from the internet and other business networks, one can theoretically prevent any exposure to malware or other cyber-attack.

While air-gapping is far from 100% effective and hackers have discovered a variety of means to bypass airgaps, air gaps remain the most cost-effective means of securing critical infrastructure.[20]

Unfortunately, due to the nature of satellite functionality, satellites cannot be "air gapped" in the traditional sense. To be useful to humans on the ground, satellites must communicate with networks based on the Earth's surface. This means that satellites are vulnerable to both direct and indirect attacks that other critical infrastructure can mitigate through air-gapping. Attackers have the option to attack satellites, ground-based support infrastructure, or the lines of communication between both parties. Figure 2 below shows what this data flow looks like and gives several examples of where attackers may choose to target. One example of such an attack can be found in Russia's jamming of civilian GPS signals during NATO's 2018 Trident Juncture exercise in Europe's High North region.[21] According to the Consultative Committee for Space Data Systems, the most common cyber threats to space infrastructure include but are not limited to: data corruption/modification; ground system loss; interception of data; jamming; denial of service; masquerade (spoofing); replay; software threats; and unauthorized access.[22]

Figure 2. Diagram of Space Situational Awareness Data Flow and Potential Targets



Source: Pavur, James and Martinovic, Ivan. (2019). "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space." *International Conference on Space Conflict*. Retrieved from: https://ccdcoe.org/uploads/2019/06/Art_12_The-Cyber-ASAT.pdf

Cyber anti-satellite weapons can mitigate collateral damage.

One of the greatest deterrents to the use of anti-satellite weapons is the potential for collateral damage that could impact one's own space assets. The physical destruction of satellites results in the production of space debris, which poses a grave risk to other satellites in orbit. This presents a threat to both current space infrastructure and any future space assets that could be impacted by this debris.[23] As a result, countries are deterred from using conventional anti-satellite capabilities that may hinder their own access to outer space. However, cyber threats to satellites allow countries to incapacitate, damage, or destroy satellites without producing space debris. This enables them to conduct anti-satellite cyber operations with impunity without concern for limiting their own access to Outer Space.

Satellites perform critical functions not duplicated by terrestrial tech.

One of the primary reasons we are concerned about an anti-satellite attack is that satellites perform many critical functions that cannot be duplicated using existing terrestrial capabilities.[24] Satellites perform communications, navigation, and imagery functions that cannot be perfectly replicated using assets on the ground. This means that the potential costs of an attack on space infrastructure are high, and correspondingly the relative gains for an adversary are equally high. Both critical functions performed by space assets and the options for terrestrial back-ups will be discussed more thoroughly in subsequent sections.

BACKGROUND AND LITERATURE REVIEW

To more fully understand why a cyber-attack on satellite infrastructure poses a grave threat to the United States and why the People’s Republic of China is particularly well poised to take advantage of this vulnerability, a brief background on the domain of Outer Space and the Strategic Approach of the People’s Republic of China is necessary. Furthermore, a brief summary of the academic literature on rational deterrence theory will explain both why the PRC is incentivized to act and how the United States might respond to mitigate the risk of attack.

Importance of Space

In short, the strategic importance of outer space to the United States can be divided into two main categories: the national security relevance and economic relevance.

National Security Importance of Outer Space

Satellite infrastructure plays a key role in broader US national security and military policy and strategy. Almost all modern military engagements rely on space-based assets in some capacity. For example, during the US invasion of Iraq in 2003, 68% of munitions were guided using space-based means; a large increase from 10% in 1990-1991 during the first Gulf War.[25] In addition to munitions guidance, space plays a role in United States “intelligence; surveillance and reconnaissance; disaster response; troop movement tracking on land, at sea, and in the air; classified and unclassified telecommunications; refugee movement tracking; identification of evidence of war crimes, genocide, or other mass human rights violations; drone operations; GPS-guided weapons; and cyber operations.”[26] As a result, space has been described as the “ultimate high ground” for information age warfare.[27] Modern space power has created a world in which ‘no enemy can withstand a frontal assault upon U.S. forces due to the American ability to sense, move, and strike with precision.’[28]

Space is the “ultimate high ground” for information age warfare. [29]

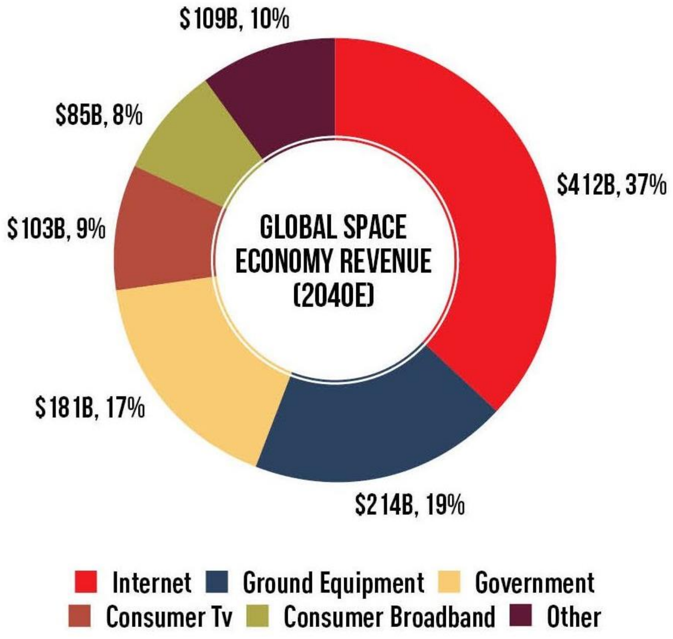
In addition, to the military capabilities that satellites provide they also provide the United States with vital intelligence to defend the homeland. GPS and imagery satellites play a critical role in tracking enemy troop movements and nuclear tests so that the US can prepare for future conflicts.[30] In addition to tracking nuclear tests, satellites play a vital role in the United States nuclear defense. In the event of a nuclear attack, a combination of ground-based radars and infrared sensors on satellites would be used to detect the launch of a missile and warn the US in time to launch one of its Ground-based Midcourse Defense Missiles to intercept the missile.[31]

The military and intelligence advantage that the United States holds in outer space – and its perceived dependence on it – will drive actors to seek ways to grow their own capabilities or to develop new ways to neutralize this advantage with anti-satellite weaponry.[32]

Economic Relevance of Outer Space

In addition, to its military and intelligence applications, outer-space has incredible economic relevance. In In 2018, the value of the space economy was valued at $414.75 billion after experiencing 8.1% growth from the previous year.[33] In the same year, the global satellite industry generated $277 billion in revenues, with United States companies owning the largest share of this revenue. [34] This value will only continue to grow and experts predict that by 2040 the global space economy revenue will exceed $1.1 trillion.[35] Figure 3 provides a helpful visualization of what the future space economy is likely to look like.

Figure 3. Projected Space Economy Revenue (2040)



Graphic Source: *Geospatial World*, https://www.geospatialworld.net/article/whos-buying-all-that-satellite-imagery/

Data Source: *Satellite Industry Association, Morgan Stanley Research, and Thomson Reuters*

US economic interests in space make it a top priority for US policy makers. The United States National Security Strategy of 2017 cites protection of "the American people, the homeland, and the American way of life" and promoting "American prosperity" as the top two priorities of the United States national security community.[36] United States space infrastructure plays a vital role in both the American way of life and in promoting American prosperity.

Commercial Applications of the US Satellite Infrastructure include but are not limited to:

- **Telecommunications and Network Services**
  Satellites enable access to communications services including phone and video calls, email, and other internet services in remote areas, without fiber optic connection.[37] Many rural Americans depend on satellite radio, television, and internet.

- **Navigation**
  GPS is the primary navigation technology in use not only within the US but globally. This service is freely available to all users on continuous, worldwide basis and is a critical part of the American way of life.[38]

- **Banking**
  The global financial system is dependent on timing services of the GPS satellite system. Precise timing is vital to maintain a global financial system of stock and currency exchange and GPS is the primary provider of this timing service.[39]

- **Agriculture**
  NOAA satellites play a vital role in agriculture monitoring. These satellites forecast drought conditions, map greenness and plant health, and are used to estimate soil-water availability, and crop yield.[40] As such, satellites play a critical role in modern agriculture.

- **Weather Forecasts and Disaster Mitigation**
  NOAA satellites are used to measure and predict weather patterns around the world in real time. These forecasts are used to predict and prepare for natural disasters, which is able to both save lives and mitigate economic consequences.[41] In the event of a disaster, satellite imagery is used to estimate damages and coordinate rescue and relief efforts.[42]

- **Environmental Impact Analysis and Resource Management**
  Satellite Imagery is a vital tool in conducting environmental impact analysis. Satellite imagery is used to track a wide range of environmental problems from deforestation to coastal ecosystem destruction.[43] This data can then be used to manage natural resources effectively to optimize both their current and future potential.[44]

- **Geology and Mining**
  Hyperspectral satellite imagery can be used to detect deposits of natural minerals, a valuable asset for mineral exploration. Satellites owned by the US geological survey, NASA, and private mining companies provide data that mining companies analyze to determine likely locations for mineral exploration and mining.[45]

- **Urban and Transportation Planning**
  Satellite mapping and imagery can be used to aid both urban and transportation planning. Satellites have been used to assess road safety design and analyze the frequency of car accidents to improve city road structure and traffic flow.[46] Similarly, satellite imagery can be used to track urban growth and plan city development to meet the needs of an urbanizing world.[47]

While the above list is by no means exhaustive, it demonstrates the wide range of important applications for satellites in the United States economy. Satellites play an important role across various sectors of the national economy and, as such, should be considered critical national infrastructure. The combined military and economic importance of satellites to the United States points to the ultimate conclusion that vulnerable satellites are a grave concern to the United States. Adversaries of the US also recognize this fact and are incentivized to develop the capabilities to exploit this weakness and neutralize the advantage of the United States in outer space.[48]

Understanding People's Republic of China Core Interests and Strategy

In 2019, Undersecretary of Defense for Policy, John C. Rood, identified the People's Republic of China "the largest long-term threat" to both US national security and to the American way of life.[49] The cyber capabilities and national interests of the People's Republic of China make them the greatest threat to US space infrastructure. To understand why China represents a threat to the United States, a brief background on Chinese grand strategy and foreign policy is necessary.

Historical Context

According to the Chinese view, China was the world's preeminent civilization for millennia, serving as an economic, intellectual, and cultural hub for the rest the world.[50] However, in the 19th century, China fell behind western superior technology and lost its dominant position in the world. This resulted in a "Century of Humiliation," where China was "diplomatically and militarily dominated by Western Colonial powers."[51] "The Century of Humiliation" inspired China to vow never to be dominated by foreign powers and to "rejuvenate" China to its past glory. [52] This history is the foundation of China's grand strategy and strategic aspirations.

Chinese Core Interests and Grand Strategy

In short, Chinese core interest can be summarized as follows:

1) Preservation of the Chinese Communist Party Regime,[53]
2) Restoration of China to a self-perceived status as the world's premiere civilization,[54]
3) and Protection against foreign influences.[55]

Each of these core interests supports both Chinese space interests and its cyber anti-satellite program.

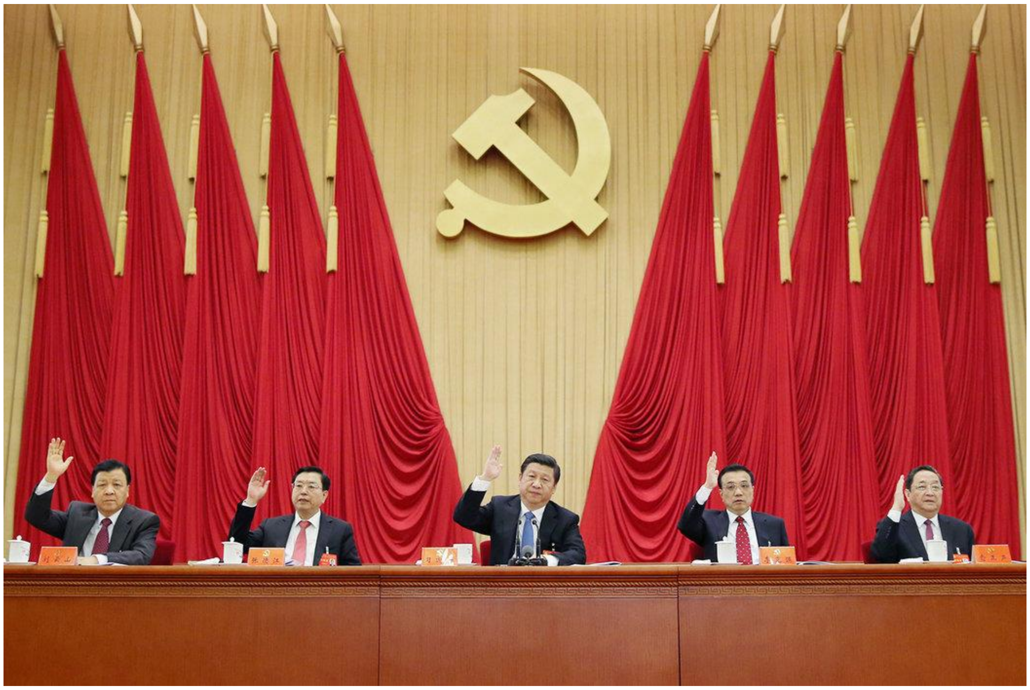
1) Preservation of the Communist Party Regime

First and foremost, the PRC desires to preserve the Chinese Communist Party (CCP) Regime. The CCP is the founding and ruling political party in China and has maintained a political monopoly over China for over 70 years.[56] The CCP are the primary decision-maker in the PRC and have a strong interest in retaining their position in the Chinese government. Rapid economic growth is the foundation of the CCP's legitimacy in China the basis of its popular support.[57] Therefore, to preserve stability of CCP rule the PRC must continue to fulfill its promises of economic growth to the Chinese people by whatever means necessary. [58]

2) Restoration of Historic Chinese Primacy

China's "Grand Strategy" outlines its plan to restore Chinese primacy on the world stage. This is a broad goal encompassing a desire to expand economic and cultural influence, expand geopolitical power, and restore historic land and institutions.[59] For the purposes of this paper, we will focus primarily on China's economic aspirations. China's economic strategy has two prongs: technological supremacy and the export of the Chinese economic model. Both China's space and cyber programs advance China's goals of technological supremacy and economic growth. The image below depicts a CCP meeting where President Xi Jinping outlines the Chinese economic strategy.

Figure 4. Chinese Communist Party Meeting



Source: Belt and Road News, https://www.beltandroad.news/2019/01/16/chinas-grand-strategy/

3) Protect Against Foreign Influences

The PRC seeks, without exception, to preserve domestic sovereignty and to prevent foreign influence in "internal affairs." Following "The Century of Humiliation," China is deeply opposed to foreign influence in their nation. [60] The PRC confirmed this national priority this year, when it called for the end of foreign interference related to "internal affairs" involving the governance of Hong Kong and Taiwan. [61] Similarly, the PRC seeks prevent influence through tight control of information by censoring online, print, and television media using “The Great Firewall.”[62] If China believes that US space infrastructure poses a threat to Chinese internal affairs, it would be greatly incentivized to neutralize US space advantage to mitigate the threat to its own sovereignty.

People's Republic of China Space Aspirations

The People’s Republic of China views outer space as key to its economic and military future. Outer space has traditionally been the domain of global super powers, and as such the United States and Russia dominated outer space during most of the 20th century.[63] However, as China has progressed as a global superpower, so too has its space program. In 2003, China became only the third nation in history to achieve independent manned- spaceflight and has since radically expanded its space program. [64] In China a 2015 internal white paper, China declared “commanding height of international strategic competition” and affirmed their desire to achieve “major progress towards informatization by 2020.”[65]

China’s actions in the domain of outer space match its rhetoric. Since the early 2000s, China has developed a wide range of advanced space capabilities, including “space-based C4ISR[*] capabilities, a growing fleet of modern launch vehicles, the BeiDou satellite navigation program, … and a manned space program.”[66] The Chinese C4ISR program and BeiDou satellite navigation systems are both intended to increase Chinese military and economic power and to decrease its reliance on foreign powers. Establishing national space independence will reduce the deterrence pressures on China and reduce the costs it would face from attacking US space assets.

Concurrent with developing its own space program, China has developed anti-satellite capabilities to neutralize the space advantage of its adversaries. Famously, China tested its first anti-satellite weapon in 2007.[67] Launching a simple kinetic anti-satellite weapon against one of its own satellites was both an internal test of China’s own capabilities and a signal to other countries that China had the capability to neutralize space assets in the event of conflict. Today, China’s ASAT arsenal is far more dangerous.

In 2015, the People’s Liberation Army of China restructured its operations and created the Strategic Support Force, which centralizes the space, cyber, and information warfare components of the People’s Liberation Army under one a single organization.[68] This shift signals a Chinese understanding of the intersection between cyber space and outer space and the potential for

[*] C4SIR is a national security acronym which stands for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, and describes how technology supports military and intelligence purposes.

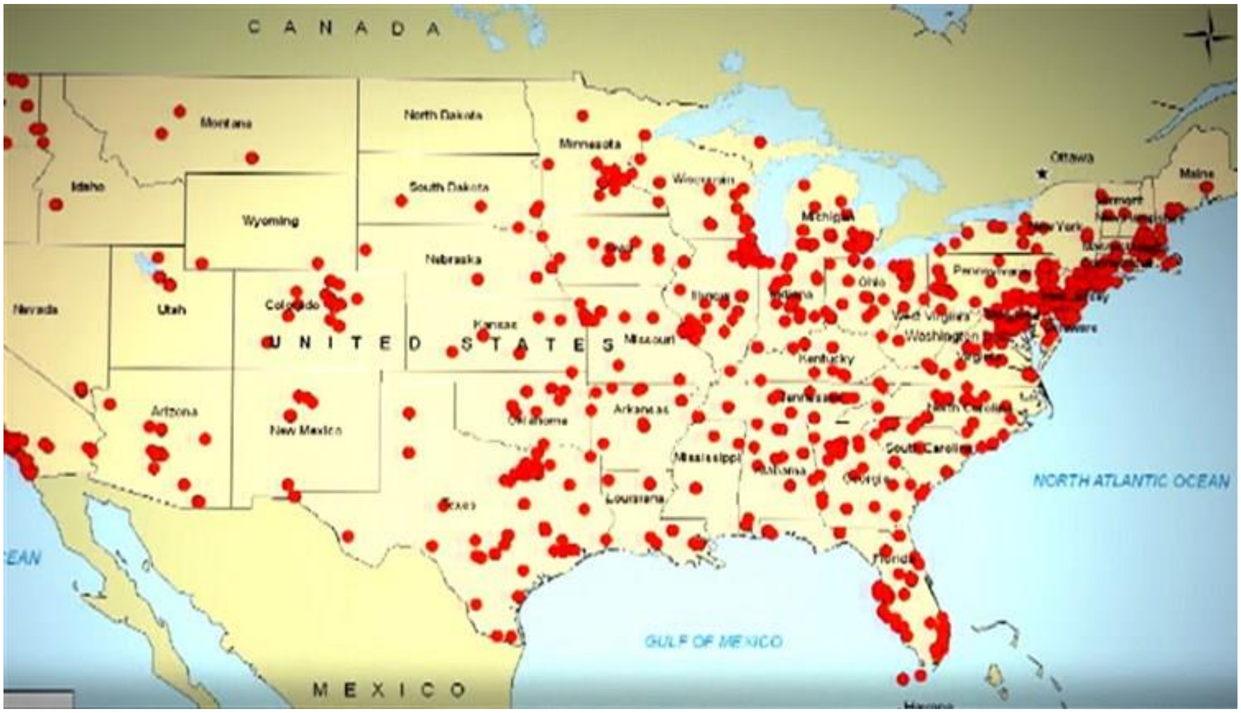
Chinese exploitation of the cyber vulnerabilities of US space assets. Chinese military doctrine highlights a belief that information dominance and is the key to winning conflicts and that this can be done by denying or disrupting the equipment of competitors.[69]

Role of Cyber in Achieving China's Strategic Goals

For decades, China has used cyber capabilities to advance its strategic goals. To date, these operations have been focused primarily on intellectual property theft and corporate espionage rather than aggressive acts of sabotage, but these campaigns reveal to key factors: 1) China possesses advanced cyber capabilities and 2) China is willing to deploy its cyber capabilities to advance its national interests.

To put this into perspective, former National Security Agency Director Keith Alexander has called China's cyber theft of economic information "the greatest transfer of wealth in human history."[70] In July 2018, FBI Director Christopher Wray revealed that the FBI has corporate espionage investigations linked to China in every US state.[71] In 2013, Verizon concluded that China conducted 96% of espionage motivated cyber intrusions through its networks.[72] The map shown in Figure 5 highlights the range of targets of Chinese cyberespionage.

Figure 5. Dot Map of US Victims of Chinese Cyberespionage (2010-2015)



Source: NBC News, https://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211

The first major reported Chinese cyber-attack, Titan Rain, occurred in 2003 and targeted US Department of Defense laboratories, NASA, and aerospace companies and their counterparts in the United Kingdom. Today, Chinese hackers target a wide range of sectors, but seem to match closely with the priorities identified in China's Made in China 2025 initiative. These areas are reported to be information and communications technology, military technology, civilian and dual use technologies, advanced materials, healthcare, manufacturing techniques, and agriculture.[73] Notably, many of these targets also align closely with the areas supported by US satellite infrastructure. While there is no indication that China intends to deploy its cyber capabilities to sabotage US space infrastructure in the near future, this pattern of use suggests both a motive and potential for deployment of Chinese cyber capabilities against US satellites in the future.

The most prolific Chinese cyber actors have historically been Units 61398 and 61486 of the People's Liberation Army.[74] Unit 61398, also known as APT 1, is one of the most persistent of China's Cyber threat actors and is credited with compromises of 141 companies across 20 industries between 2006-2013.[75] Unit 61486, also known as APT 2, is believed to support the Chinese space surveillance network and is associated with multiple attacks against satellite, aerospace, and communications firms since 2007.[76] Since 2015, both of these organizations are believed to be under the direction of the aforementioned Strategic Support Force. In the event of a Chinese cyber-attack against US satellite infrastructure, it is likely that one of these two groups would be responsible.

Failure of Conventional Deterrence in Cyber Space and Outer Space

In addition to the historical basis for a Chinese cyber-attack against US satellite infrastructure, a critical analysis of the academic literature on Rational Deterrence suggests that under current conditions China may be incentivized to proactively strike US space infrastructure with a cyber-attack.

Overview of Rational Deterrence Theory

Rational deterrence theory is rooted firmly in the academic disciplines of economics and criminology. The basic principle is that a rational actor will take an action if and only if the perceived benefits of the action outweigh the perceived costs of an action.[77] As a result, an individual can be "deterred" from taking an unwanted action by either raising the perceived costs or lowering the perceived benefits until the benefits no longer exceed the costs of an action.[78] The two main ways of accomplishing this are known as deterrence by denial and deterrence by punishment. Deterrence by denial involves taking preventive measures to lower the probability of a success for an undesired action and deterrence by punishment involves threatening a swift and sever punishment in response to an undesired action in order to discourage it.

While the rational deterrence model is far from perfect, this simple logic model is useful in understanding the actions of countries in the domain of international relations. Unfortunately, states do not always behave as rational actors. This is because states are not unitary actors but rather the amalgamation of different groups with distinct interests of their own that ultimately define state priorities and interests.[79] Nevertheless, the basic principles of rational deterrence theory serve as a useful logic model for generating policy options implementing a deterrence strategy on the world stage. Accordingly, the Joint Chiefs of Staff have adopted the lessons of this model as the cornerstone of US deterrence strategy.[80]

Deterrence Considerations in Outer Space

Moving past the broad theoretical framework of deterrence, there are a number of key considerations that make deterrence particularly complicated in the arena of outer space. At its core, classical deterrence in space would be defined as the idea that an actor would be incentivized not to deploy counter-space weapons because the perceived costs of such an attack would be greater than perceived benefits. This could be as a result an attack would have a low chance of success, an attack would have low impact or benefit, an attack would be exceedingly costly, or because the anticipated punishment would be too great to justify any benefit. Unfortunately, the conditions are unfavorable for successful deterrence on any of these dimensions in the context of space.

First, space assets are incredibly difficult to defend. Due to regular, predictable orbits, satellites are easy to track and easy targets for any adversary with space-capable technology.[81] Similarly, due to the high cost per pound of putting objects into space, it is extremely expensive to outfit satellites with defensive measures such as armor, additional fuel, or other technology.[82] As a result, defending space assets is both extremely difficult and extremely expensive and implementing satellite defenses is highly unlikely to be cost-effective on any dimension.

Second, the United States military and economy are highly reliant on space infrastructure and are far more reliant than any other nation.[83] As such, development and deployment of ASAT technology is likely to have high returns for any actor with an interest in hurting the United States.[84] Similarly, the US has very little option for direct, proportional retribution since no other country is as reliant on space infrastructure as the United States. As a result, unlike nuclear deterrence where the threat of mutually assured destruction is sufficient to deter use of nuclear weapons, space deterrence cannot be an independent construct within US policy. Rather space deterrence must likely involve a comprehensive set of responses including economic, conventional military, or even nuclear responses that would be sufficiently costly to deter potential adversaries.[85]

Third, space is an interesting domain because it is a common-resource that, in many instances lacks clear norms and regulations. While the history of regulation in space is beyond the scope of this paper, a few key documents provide valuable insight into the understanding the intricacies of deterrence in space. The Outer Space Treaty, born out of the Cold War, of which both the US and China are signatories, "bans the stationing of weapons of mass destruction (WMD) in outer space, prohibits military activities on celestial bodies, and details legally binding rules governing the peaceful exploration and use of space."[86] Notably, this treaty does not ban the use of anti-satellite weaponry or conventional weapons in space. As a result, Russia and China jointly proposed a Prevention of an Arms Race in Outer Space (PAROS) Treaty to the United Nations.[87] The US has been largely resistant to this treaty because it would restrict its own space capabilities including the US Anti-Ballistic Missile Defense system and conventional military technology with de facto ASAT capabilities and because it does not believe that Russia and China will truthfully adhere to the terms of the agreement.[88] However, this lack of consensus agreement surrounding ASATs in space makes deterrence of their development and use extremely challenging. Without a clear set of communicated norms and expectations, it is unclear how one would reasonably deter the development and use of ASAT technologies at all.

Amidst all the challenges that space poses to deterrence, it does have a few unique characteristics favorable to deterrence. First, due to the common nature of outer space, all nations with an interest in outer space bear the consequences of any conflict in space. Specifically, space debris pose a long-term threat to the safety of satellites in space and are indiscriminate in how they affect the satellites of different nations. The use of kinetic anti-satellite technology is associated with a substantial increase in the volume of dangerous debris in space.[89] As a result, the threat of space debris poses a strong deterrent to the deployment of ASAT technologies by any country who hopes to make use of space in the future. By some estimates, a significant space conflict could render parts of earth's orbit functionally unusable and would "ruin space for everyone."[90] Much like the threat of Mutually Assured Destruction in the nuclear context, this seems to be a very effective deterrent to the use of kinetic ASATs. Unfortunately, this does not help to deter cyber-enabled anti-satellite capabilities because these weapons can cause grave damage without generating high levels of space debris.

Deterrence Considerations in Cyberspace

Much like outer space, cyberspace poses some unique challenges for the application of classical deterrence theory. Common criticisms include low cost of entry, high number of non-state actors, and lack of clear attribution for attacks.[91] There is substantial theoretical logic behind these criticisms that makes deterrence in the cyber arena, very challenging but not impossible.

Since cyber-attacks are extremely cheap and easy, it is exceedingly challenging to modify the incentives so that the costs of conducting a cyber-attack exceed the potential benefits.[92] Unfortunately, this challenge is only greater in space because security is harder to implement. Hardware security updates are nearly impossible on a satellite in orbit, and as a result, vulnerabilities discovered decades ago may still be present in satellites today. Similarly, while software updates are possible, remote updating can be highly costly and highly risky. In fact, a corrupt software patch resulted in the destruction of a $268 million Japanese satellite as recently as 2016.[93] Furthermore, even if satellites themselves secured, ground based control systems and other aspects of the supply chain may still be vulnerable making total cybersecurity nearly impossible. Since cyber-attacks are relatively cheap and defense is exceedingly costly, deterrence in cyber space poses an extreme challenge.

Further exacerbating the problem is the fact that cyber-attacks can be extremely hard to attribute. Due to the malleable nature of digital identifiers, use of intermediary systems, and the prevalence of VPN technology, attributing a cyber-attack to a specific actor can extremely challenging.[94] Even when an attack can be attributed to a specific country, it can be hard to know whether or not an attack was state-sponsored.[95] Finally, much like in the outer space context, even if nation-state actor attribution is achieved. It is unclear what a proportional response looks like and/or if it is internationally acceptable to escalate conflict to conventional military action in response to a cyber-attack.[96] While China's advanced space and cyber infrastructure provide the US strong targets for proportional response, it remains unclear what this response would look like or whether the threat would be sufficient to deter an attack ex-ante. In summary, there is considerable uncertainty surrounding the role of deterrence in the cyber realm. Despite this uncertainty, the United States has doubled down on its emphasis on deterrence in the cyber realm, an action highlighted in both the National Cyber Strategy and the Department of Defense 2018 Cyber Strategy.[97]

POLICY ANALYSIS AND RECOMMENDATION

Assessment Criteria

An effective policy solution must meet the following criteria:

1. **Effective in Mitigating the Threat**
   Effectiveness refers to the degree with which a specific policy solution is able to address the threat. In this case, effectiveness refers to two specific measures:
   a. Mitigating the Chance of an Anti-Satellite Cyber Attack through Deterrence
   b. Mitigating the Damages in the Event of a Successful Anti-Satellite Cyber Attack

2. **Cost-Effective**
   A good policy solution must not only be effective in absolute terms but also generate strong value in relation to its cost. In this case, we will focus primarily on the financial cost of a policy solution, but it is also important to consider the potential economic opportunity costs of a policy recommendation.

3. **Political and Technological Feasibility**
   A policy must be both politically and technologically feasible to be considered as a recommendation. These measures will be evaluated qualitatively, but will consider factors including but not limited to, whether or not the proposed policy will be able to achieve sufficient bipartisan support in the legislature, the number of government agencies that will need to be involved, the complexity of the program in terms of rules and initiatives to successfully implement, and the technological complexity and technical expertise required to implement.

Recommendation

Based on our analysis and consideration of the criteria above, we recommend a multifaceted approach designed to reduce the probability and potential damages of a successful cyber-enabled anti-satellite attack.

This recommendation includes the following points:

1. Increase Compliance with Basic Cybersecurity Practices Defined Under the NIST Cybersecurity Framework
2. Continue Operations of Ground-Based GPS Back-Up System, eLORAN (Expand if Possible)
3. Continue Think-Tank, Academic, and Commercial Research into the Evolving Threat of Cyber-Enabled Satellite Weapons

1) Increase Compliance with Basic Cybersecurity Practices Defined Under the NIST Cybersecurity Framework

In evaluating deterrence by denial, it is important to note that many of the same denial measures used in conventional cybersecurity are effective in protecting satellite infrastructure. Satellite companies have long been leaders in the cybersecurity field, but it is impossible to be fully secure in the world of cybersecurity.[98] To ensure the highest level of security for its satellites, the US government should increase standards for satellite contractors and require that all US government contractors in Space be compliant with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The NIST cybersecurity framework is a "voluntary framework consisting of standards, guidelines, and practices to promote the protection of critical infrastructure."[99] Additionally, the Federal Communications Commission, the primary regulator of space companies, should highly encourage all US companies with space infrastructure to adopt and comply with the voluntary NIST framework as well.

Furthermore, security measures should focus on addressing the most common risk in cybersecurity, human error. While advanced zero-day vulnerabilities and complex malware certainly poses a grave danger, they are often not possible to address in a timely or cost-effective manner. Instead, the focus should be on mitigating the human element. IBM's 2014 Cyber Security Intelligence index found that 95% of successful attacks are the result of human error. [100] While the US government already has extensive training program in place to mitigate this threat, many newer satellite companies lack robust human-element cybersecurity training programs. As a result, mitigating the human element threat is one of the most cost-effective avenues to reduce the threat posed to US satellite infrastructure.

2) Continue Operations of Ground-Based GPS Back-Up System, eLORAN (Expand if Possible)

To mitigate the costs in the event of a successful attack, the United States needs to preserve contingency infrastructure to replace critical satellite operations in the event of a successful attack. To accomplish this, the US should continue to support legacy, ground based navigation technology such as LORAN-C or E-LORAN. LORAN-C, which stands for long range navigation technology, is a hyperbolic radio navigation system that allows a receiver to determine its position based on low frequency radio transmissions from fixed radio beacons.[101] LORAN-C was deemed obsolete and defunded in May 2009, however, increasing concerns about the vulnerability of GPS led to the introduction of an enhanced LORAN as a complement to and backup for both military and civilian uses of GPS "in the event that GPS timing signals are corrupted, degraded, unreliable, or otherwise unavailable."[102] In the context of deterrence, eLORAN accomplishes two key functions. First, it mitigates the potential impact of a successful cyber-attack on critical US space infrastructure because critical functions can and will be performed by the ground-based infrastructure. Second, since it reduces the potential strategic advantage of a first-strike in space, it mitigates the risk of any attack on US space infrastructure. Notably, eLORAN is not a full replacement for GPS but it is the best available back-up system to GPS and is a useful tool to verify information from other intelligence sources.[103] While current users of the eLORAN system are limited, the military, telecommunications, energy, and finance sectors are exploring its applications. Findings suggest that an eLoran solution for the financial sector may be less costly and less technically challenging than the current recommended atomic clock-time stamps.[104] Similarly, findings by the Alliance for Telecommunications Industry solutions and the University of Tennessee in Knoxville suggest that complementary eLORAN solutions improve reliability and accuracy of telecommunications and energy sector applications respectively.[105]

Under existing statute, eLORAN is under the authority of the US Coast Guard and is expected to increase net direct spending by $121 million over the 2018-2027 period. [106] While $121 million is by no means cheap, it is small in comparison to operating costs of the GPS system which totaled $1.42 billion in FY2019 alone.[107] As such, eLORAN is an extremely cost effective means of providing positioning, navigation, and timing services that can provide a complementary role to GPS and should be prioritized in the budget process rather than as current policy dictates, "subject to available appropriations."[108]

3) Continue Think-Tank, Academic, and Commercial Research into the Evolving Threat of Cyber-Enabled Satellite Weapons

Perhaps the most important recommendation is to do additional research and continue monitoring the threat. The cyber-threat to space infrastructure is a relatively new development and information about the threat is constantly evolving. New technologies such as quantum computing are expected to radically transform cyber, both offensively and defensively and it remains to be seen how this technology will impact the security of US satellites.

Similarly, the behavior, motives, and capabilities of the PRC are constantly evolving and any change in this arena will alter the threat level to US space infrastructure. In the same way, US-China relations are directly correlated with PRC incentive to deploy cyber enabled anti-satellite weapons. As such, each of these areas should be carefully monitored and analyzed to assess whether the degree to which they will alter the threat and appropriate responses.

Since the threat to US space infrastructure is an interdisciplinary problem, a coordinated effort across a variety of stakeholders will be required to stay ahead of the threat. Commercial cybersecurity firms, universities, and government agencies should continue to independently research the technical aspects of the cyber threat to satellites and should share this information whenever possible. Similarly, think-tanks should continue to conduct research and timely analyses of the threats posed by foreign adversaries and should share them with the intelligence community.

Notably Omitted Policy Response: Deterrence by Punishment

At this time, we do not recommend that the US pursue a strategy of deterrence by punishment as its primary strategy to mitigate the threat its space assets. Such a strategy might involve signaling to China that the US is able and willing to respond with force in the event of a cyber-attack on US space infrastructure. As discussed above, a lack of international norms and lack of historical background in this arena makes credible signaling of punishment difficult in this arena. If the threat of punishment is not viewed as credible, then deterrence by punishment is highly ineffective. Compounding this problem, it remains unclear what a proportional response to an anti-satellite cyber-attack would look like and it is not clear whether a potentially escalatory response would be in the best interest of the United States

Nevertheless, changes in technology, international norms, or credible signaling in the future may improve the viability of a deterrence by punishment strategy. As such policymakers and national security professionals, should reassess the viability of this strategy moving forward.

Implementation

The final section of this report seeks to briefly explain how the federal government might effectively implement the recommendations defined above.

Role of the Foundation for Defense of Democracies

Notably, FDD does not have policymaking power of its own, so the first step is to simply bring awareness to the problem. FDD can accomplish this by publishing a modified version of this APP to the FDD readership and National Security Alumni Network to raise awareness about the threat. Next, FDD should reach out to its partners on Capitol Hill and in the media to bring the problem onto the legislative agenda. This process may be furthered by National Security Alumni Network Members placed throughout the executive branch and private sector in positions of influence.

Role of the Federal Government

Legislative Branch
First and foremost, successfully securing our nation's satellite infrastructure will require support from the US Senate and House of Representatives to achieve the necessary funding. Representatives Kendra Horn (D) and Brian Babin (R) of the House Science Subcommittee on Space and Aeronautics, Representatives Sheila Jackson Lee (D) and John Ratcliffe (R) of the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Innovation, Senators Mike Rounds (R) and Joe Manchin (D) of the Senate Subcommittee on Cybersecurity, and Senators Joni Ernst (R) and Gary Peters (D) of the Senate Subcommittee on Emerging Threats and Capabilities may be particularly interested and useful allies in moving forward legislation on this issue.

Executive Branch
The National Space-Based Positioning, Navigation and Timing Executive Committee is the key stakeholder within the executive branch. The committee is chaired by the Deputy Secretaries of Defense and Transportation and also includes members of equivalent level from the Departments of State, Commerce, and Homeland Security, the Joint Chiefs of Staff, and NASA with a sitting representative from the Federal Communications Commission. This body has representation from key decision-making stakeholders from the key federal agencies with interest in securing space infrastructure. On this committee, representatives from the Department of Defense and the

Federal Communications Commission will be the most important players to reach because they are responsible for management, regulation, and security of government and commercial satellites respectively.

In addition to the top level decisionmakers, special mentions should be given to the United States Coast Guard and National Institute of Standards and Technology, housed within the Department of Homeland Security and Department of Commerce respectively. The US Coast Guard is the primary custodian of the eLORAN GPS backup system and their cooperation will be vital to the maintenance and expansion of the system. Similarly, the National Institute of Standards and Technology publishes the NIST Cybersecurity Guidelines, which form the basis for the basic cybersecurity practices recommendation.

Commercial Companies

Successful defense of our nation’s satellites will require the cooperation of private companies as well as public agencies. As of 2018, private companies controlled more than 75% of total space revenues and they are the default security providers for the majority of US satellite infrastructure. [109] Hence, their cooperation with federal initiatives and compliance with NIST Cybersecurity guidelines will be vital to the security of our nation’s satellite infrastructure. The Federal Communications commission is the governing body for these companies and, as such, will be the most effective way to communicate with these stakeholders.

Conclusion

Ultimately, while the threat of cyberweapons to United States satellite infrastructure is grave, an attack is unlikely to occur in the near future. Nevertheless, such an attack is both possible given current capabilities and the People’s Republic of China is incentivized to execute such an attack. The risks related to this threat will only continue to increase in the future. While defending against an anti-satellite cyber-attack, should not be the top priority of the national security, the US should use discretionary funding to take proactive measures to defend against the threats of the future.

Bibliography

[1] Cordesman, Anthony H. (August 19, 2019). "China Space Strategy and Developments" *Center for Strategic and International Studies*. Retrieved from: https://www.csis.org/analysis/china-space-strategy-and-developments

[2] Pavur, James and Martinovic, Ivan. (2019). "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space." *International Conference on Space Conflict*. Retrieved from: https://ccdcoe.org/uploads/2019/06/Art_12_The-Cyber-ASAT.pdf

[3] Yunos, Zahri. (September 2008). The Reality of Cyber Threats Today. *Cybersecurity Malaysia*. Retrieved from: https://www.cybersecurity.my/data/content_files/13/420.pdf

[4] M. Levine. (19 May 2017). "Russia Tops List of Countries that could Launch Cyberattacks on US", *ABC News*, Retrieved from: https://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacksus/story?id=47487188

[5] Pavur, James and Martinovic, Ivan. (2019). "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space." *International Conference on Space Conflict*. Retrieved from: https://ccdcoe.org/uploads/2019/06/Art_12_The-Cyber-ASAT.pdf

[6] Denning, Dorothy E. (2009). "Barriers to Entry: Are they lower for cyber warfare?" *Calhoun Institutional Archive of the Naval Postgraduate School.* Retrieved from: https://core.ac.uk/download/pdf/36729636.pdf

[7] Brown, Gary. (2000). "How Satellites Work." *How Stuff Works*. Retrieved from: https://science.howstuffworks.com/satellite10.htm;

Denning, Dorothy E. (2009). "Barriers to Entry: Are they lower for cyber warfare?" *Calhoun Institutional Archive of the Naval Postgraduate School.* Retrieved from: https://core.ac.uk/download/pdf/36729636.pdf

[8] Baylon, C. (2014), Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/2014

[9] Goldman, Emily. (2014). Cyber Analogies. *Calhoun Institutional Archive of the Naval Postgraduate School.* Retrieved from: https://core.ac.uk/download/pdf/36732393.pdf#page=109

[10] Goutam, Rajesh. (2015). The Problem of Attribution in Cyber Security. *University of Lucknow*. Retrieved from: https://pdfs.semanticscholar.org/3ea2/a54f8d5b473f0c261c2be45f741e040fa6f3.pdf

[11] Goutam, Rajesh. (2015). The Problem of Attribution in Cyber Security. *University of Lucknow*. Retrieved from: https://pdfs.semanticscholar.org/3ea2/a54f8d5b473f0c261c2be45f741e040fa6f3.pdf

[12] Goutam, Rajesh. (2015). The Problem of Attribution in Cyber Security. *University of Lucknow*. Retrieved from: https://pdfs.semanticscholar.org/3ea2/a54f8d5b473f0c261c2be45f741e040fa6f3.pdf

[13] Goutam, Rajesh. (2015). The Problem of Attribution in Cyber Security. *University of Lucknow*. Retrieved from: https://pdfs.semanticscholar.org/3ea2/a54f8d5b473f0c261c2be45f741e040fa6f3.pdf

[14] Chivvis, Christopher and Dion Schwarz. (2017). Why It's So Hard to Stop a Cyberattack – And Even Harder to Fight Back. Rand Corporation. Retrieved from: https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

[15] *Government Accountability Office*. (June 2019). Agencies Need to Develop Modernization Plans for Critical Legacy Systems. Retrieved from: https://www.gao.gov/assets/700/699616.pdf

[16] Unal, Beyza. (July 2019). "Cybersecurity of NATO's Space-based Strategic Assets." *Chatham House*. Retrieved from: https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets#

[17] Kallberg, Jan. (2018). "Why older satellites present a cyber risk." *Fifth Domain*. Retrieved from: https://www.fifthdomain.com/opinion/2018/12/28/why-older-satellites-present-a-cyber-risk/

[18]Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2016). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. doi:10.1016/j.chb.2016.12.040;

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011, 60–68. doi:10.1109/STAST.2011.6059257

[19] *Federal Information Systems Security Education Association*. (2017). Cybersecurity – the Human Element. Retrieved from: https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf

[20] Taylor, Hugh. (2018). "Industrial Information Security Policy: Rethinking The 'Air Gap.'" *Journal of Cyber Policy*. Retrieved from: https://journalofcyberpolicy.com/2018/04/04/industrial-information-security-policy-rethinking-air-gap/;

Coranet. (2019). How Secure are Air Gapped Computers from Intrusion? Retrieved from: https://www.coranet.com/network-air-gapping/

[21] Tigner, B. (2018), 'Electronic Jamming Between Russia and NATO is Par for the Course in the Future, But it Has its Risky Limits', Atlantic Council, 15 November 2018,

http://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-inthe-future-but-it-has-its-risky-limits ;

Unal, Beyza. (July 2019). “Cybersecurity of NATO’s Space-based Strategic Assets.” *Chatham House*. Retrieved from: https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets#

[22] The Consultative Committee for Space Data Systems (CCSDS) (2015), Report Concerning Space Data System Standards – Security Threats against Space Missions, https://public.ccsds.org/Pubs/350x1g2.pdf;

Livingstone and Lewis (2016), Space, the Final Frontier for Cybersecurity? Print.

[23] Andrew M. Bradley, Lawrence M. Wein, Space debris: Assessing risk and responsibility, *Advances in Space Research,* Volume 43, Issue 9, 2009, Pages 1372-1390, https://doi.org/10.1016/j.asr.2009.02.006.

[24] Steer, Cassandra. (8 January 2020). “Why Outer Space Matters for National and International Security. *Center for Ethics and the Rule of Law – University of Pennsylvania.* Retrieved from: https://www.law.upenn.edu/live/files/10053-why-outer-space-matters-for-national-and

[25] Unal, Beyza. (July 2019). “Cybersecurity of NATO’s Space-based Strategic Assets.” *Chatham House*. Retrieved from: https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets#;

UK Parliamentary Office of Science and Technology (2006), ‘Military Uses of Space’, Postnote, Number 273, December 2006, http://www.parliament.uk/documents/post/postpn273.pdf

[26] Lopez, C. (March 29, 2019). “DOD Official: Maintaining Space Dominance ‘Pivotal’ for U.S. Warfighters.” *US Department of Defense*. Retrieved from: https://www.defense.gov/Newsroom/News/Article/Article/1800891/dod-official-maintaining-space-dominance-pivotal-for-us-warfighters/;

Steer, Cassandra. (8 January 2020). “Why Outer Space Matters for National and International Security. *Center for Ethics and the Rule of Law – University of Pennsylvania.* Retrieved from: https://www.law.upenn.edu/live/files/10053-why-outer-space-matters-for-national-and;

Stephens, Dale and Steer, Cassandra. (2015). “Conflicts in Space: International Humanitarian Law and its Application to Space Warfare,” Annals of Air And Space Law, 2;

Steer, Cassandra. (2017). “Cosmic Commons: Implications of Military and Security Uses of Outer Space,” 18 *Georgetown Journal of International Affairs* 9–16, 9.

[27] Pollpeter, K. (Sep. 2016). “Space, the new domain: Space operations and Chinese military reforms.” *J. Strateg. Stud.*, vol. 39, no. 5–6, pp. 709–727. Print.

[28] Brown, T. (Dec. 2012). “Space and the Sea: Strategic considerations for the commons.” Astropolitics, vol. 10, no. 3, pp. 234–247. Print.

[29] Pollpeter, K. (Sep. 2016). “Space, the new domain: Space operations and Chinese military reforms.” *J. Strateg. Stud.*, vol. 39, no. 5–6, pp. 709–727. Print.

[30] Higbie, Paul and Blocker, Norman. (1993). The Nuclear Detection System on the GPS Satellites. *Los Alamos National Laboratory*. Retrieved from: https://www.osti.gov/servlets/purl/10185731

[31] Berkowitz, Bonnie, and Steckelberg, Aaron. (2017). If North Korea fires a nuclear missile at the US, how could it be stopped? *The Washington Post.* Retrieved from: https://www.washingtonpost.com/graphics/2017/world/north-korea-missile-defense/

[32]*Defense Intelligence Agency*. (January 2019). "Challenges to Security in Space." Retrieved from: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

[33] Lively, Carol. "Global Space Economy Exceeded $400 Billion for the First Time in 2018 as Revealed in The Space Report." *Space Ref.* July 15, 2019. (http://www.spaceref.com/news/viewpr.html?pid=54370).

[34] Wagner, I. (September 9, 2019). "Global space economy in 2018, by sector (in billion U.S. dollars)." *Statista*. Retrieved from: https://www.statista.com/statistics/662231/space-economy-breakdown-globally-by-sector/

[35] Mazareanu, E. (December 3, 2018). "Global space economy revenue in 2016 and 2040, by segment (in billion U.S. dollars)." *Statista*. Retrieved from: https://www-statista-com.proxy01.its.virginia.edu/statistics/946358/space-economy-global-revenue-segment-2040/

[36] *The White House. (*December 2017). National Security Strategy of the United States of America. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[37] Frempong, S. (2008). The Impact of Satellite on Telecommunications Industry Around the World. Retrieved from: https://peer.asee.org/the-impact-of-satellite-on-telecommunications-industry-around-the-world.pdf

[38] *GPS.gov*. (2019). GPS Overview. Retrieved from: https://www.gps.gov/systems/gps/

[39] Fernholz, Tim. (2017). The entire global financial system depends on GPS, and it's shockingly vulnerable to attack *Quartz*. Retrieved from: https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/

[40] *National Oceanic and Atmospheric Administration*. (2020). "Agriculture." Retrieved from: https://www.nesdis.noaa.gov/content/agriculture

[41] *National Weather Service.* (2019). "Satellites." Retrieved from: https://www.weather.gov/about/satellites

[42] WALTER, L.S. (1990), "The Uses of Satellite Technology in Disaster Management. Disasters," 14: 20-35. doi:10.1111/j.1467-7717.1990.tb00969.x

[43] Moufaddal, Wahid. (2005). Use of Satellite Imagery as Environmental Impact Assessment Tool: A case Study from the Nw Egyptian Red Sea Coastal Zone. *Environm Monit Assess.* https://doi.org/10.1007/s10661-005-3576-2

[44] Pettorelli, Nathalie. (2019). Satellite Remote Sensing and the Management of Natural Resources. *Oxford University Press.*

[45] Baumann, Jim. (January 2020). Mineral Exploration from Space. *ESRI Newsroom.* Retrieved from: https://www.esri.com/about/newsroom/arcwatch/mineral-exploration-in-the-hyperspectral-zone/

[46] Zubair, Salman. (2016). Evaluating the Road Safety Design through High Resolution Satellite Image: A Case Study of Karachi Metropolitan. *University of Karachi.* Retrieved from: https://www.researchgate.net/publication/309450959_Evaluating_the_Road_Safety_Design_through_High_Resolution_Satellite_Image_A_Case_Study_of_Karachi_Metropolitan

[47] Makhamreha, Z., & Almanasyeha, N. (2011). Analyzing the state and pattern of urban growth and city planning in Amman using satellite images and GIS. European journal of Social sciences, 24(2), 252-264.

[48] *Defense Intelligence Agency*. (January 2019). "Challenges to Security in Space." Retrieved from: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

[49] Cronk, Terri. (September 2019). "China Poses Largest Long-Term Threat to U.S., DOD Policy Chief Says." *US Department of Defense*. Retrieved from: https://www.defense.gov/Explore/News/Article/Article/1968704/china-poses-largest-long-term-threat-to-us-dod-policy-chief-says/

[50] Schiavenza, M. (2013). How Humiliation Drove Modern Chinese History. *The Atlantic.* Retrieved from: https://www.theatlantic.com/china/archive/2013/10/how-humiliation-drove-modern-chinese-history/280878/

[51] Soho, T. (2018). China's Second Century of Humiliation. *The Diplomat*. Retrieved from: https://thediplomat.com/2018/06/chinas-second-century-of-humiliation/

[52] Kissinger, H. (2011). On China. *(*New York, *Penguin Press*, 2011). Print.

[53] Tellis, A. J. and Swaine M. D. (2000). Interpreting China's Grand Strategy: Past, Present, and Future. *RAND Corporation.* Retrieved from: https://www.rand.org/pubs/monograph_reports/MR1121.html.

[54] Tellis, A. J. and Swaine M. D. (2000). Interpreting China's Grand Strategy: Past, Present, and Future. *RAND Corporation.* Retrieved from: https://www.rand.org/pubs/monograph_reports/MR1121.html;

Kissinger, H. (2011). On China. *(*New York, *Penguin Press*, 2011). Print.

[55] Tellis, A. J. and Swaine M. D. (2000). Interpreting China's Grand Strategy: Past, Present, and Future. *RAND Corporation.* Retrieved from: https://www.rand.org/pubs/monograph_reports/MR1121.html.

[56] Schiavenza, M. (2013). How Humiliation Drove Modern Chinese History. *The Atlantic.* Retrieved from: https://www.theatlantic.com/china/archive/2013/10/how-humiliation-drove-modern-chinese-history/280878/

[57] Shullman, D. (2019). Protect the Party: China's growing influence in the developing world. *Brookings Institute*. Retrieved from: https://www.brookings.edu/articles/protect-the-party-chinas-growing-influence-in-the-developing-world/

[58] McGregor, R. (2010). The Party (New York: Harper Collins, 2010), 269. Print.

[59] Kissinger, H. (2011). On China. *(*New York, *Penguin Press*, 2011). Print.

[60] Anthony, Ted. (2010). Analysis: Are China's Internal affairs' going more global? *Associated Press*. Retrieved from: https://www.apnews.com/a04291c370b64eba86e2855f1c1d94b1

[61] Ng, M. (2018). Stay out of Hong Kong's affiars government warns, after US report highlights 'chilling effect of political protest' in city. Retrieved from: https://www.scmp.com/news/hong-kong/politics/article/2142740/stay-out-hong-kongs-business-government-warns-after-us

[62] Bloomberg News. (2018). The Great Firewall of China. *The Washington Post*. Retrieved from: https://www.washingtonpost.com/business/the-great-firewall-of-china/2018/11/05/5dc0f85a-e16d-11e8-ba30-a7ded04d8fac_story.html

[63] Mann, Adam. (August 7, 2019). "What is the Space Race?" *Space.com*. Retrieved from: https://www.space.com/space-race.html

[64] *Space.com*. (2005). "Making History: China's First Human Spaceflight" Retrieved from: https://www.space.com/1616-making-history-china-human-spaceflight.html

[65] Cordesman, Anthony H. (August 19, 2019). "China Space Strategy and Developments" *Center for Strategic and International Studies*. Retrieved from: https://www.csis.org/analysis/china-space-strategy-and-developments

[66] Cordesman, Anthony H. (August 19, 2019). "China Space Strategy and Developments" *Center for Strategic and International Studies*. Retrieved from: https://www.csis.org/analysis/china-space-strategy-and-developments

[67] Zissis, Carin. (February 22, 2007). "China's Anti-Satellite Test." *Council on Foreign Relations*. Retrieved from: https://www.cfr.org/backgrounder/chinas-anti-satellite-test

[68] Pomerleau, Mark. (2019). New report explains how China thinks about information warfare. *C4ISRNET*. Retrieved from: https://www.c4isrnet.com/c2-comms/2019/05/03/new-report-explains-how-china-thinks-about-information-warfare/

[69] Office of the Secretary of Defense (2018), Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018, US Department of Defense, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF;

Pomerleau, Mark. (2019). New report explains how China thinks about information warfare. *C4ISRNET*. Retrieved from: https://www.c4isrnet.com/c2-comms/2019/05/03/new-report-explains-how-china-thinks-about-information-warfare/

[70] Emil Protalinski, (2012). "NSA: Cybercrime is 'the Greatest Transfer of Wealth in Human History." *ZDNet*. Retrieved from: http://www.zdnet.com/article/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history/

[71] Tara Francis Chan, (July 2018). “FBI director calls China ‘the broadest, most significant’ threat to the US and says its espionage is active in all 50 states,” *Business Insider*. https://www.businessinsider.com/fbi-director-says-china-is-the-broadest-most-significant-threat-to-the-us-2018-7;

Cooper, Zack. (September 2018). “Understanding the Chinese Communist Party’s’ Approach to Cyber Enabled Economic Warfare. *Foundation for Defense of Democracies*. Retrieved from: https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf

[72] *Verizon*. (2013). “2013 Data Breach Investigations Report.” http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf;

Cooper, Zack. (September 2018). “Understanding the Chinese Communist Party’s’ Approach to Cyber Enabled Economic Warfare. *Foundation for Defense of Democracies*. Retrieved from: https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/REPORT_China_CEEW.pdf

[73] Office of the National Counterintelligence Executive, (October 2011)., “Foreign Spies Stealing US Economic Secrets in Cyberspace,” *Office of the Director of National Intelligence* https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf

[74] Mikk Raud, (2016). “China and Cyber: Attitudes, Strategies, Organisation,” *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf;

Crowdstrike. (June 2014). “Hat-tribution to PLA Unit 61486,” https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/;

Mandiant (February 2013). “APT1: Exposing One of China’s Cyber Espionage Units,” https://www.fireeye.com/content/dam/fireeyewww/services/pdfs/mandiant-apt1-report.pdf

[75] *Mandiant*. (February 2013). “APT1: Exposing One of China’s Cyber Espionage Units,” https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[76] *CrowdStrike*, (June 2014). “CrowdStrike Intelligence Report: Putter Panda,” https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

[77] Bentham, J. (1988 [1789]). The principles of morals and legislation. *Prometheus Books*.

[78] Beccaria, C. (1986 [1764]). An essay on crimes and punishments. Indianapolis, IN: *Hackett Publishing Company, Inc.;*

Tomlinson, Kelli D. (2016). An Examination of Deterrence Theory: Where Do We Stand? *US Courts*. Retrieved from: https://www.uscourts.gov/sites/default/files/80_3_4_0.pdf

[79] Fearon, James D. (1998). Domestic Politics, Foreign Policy, And Theories of International Relations *Annual Review of Political Science* 1998 1:1, 289-313.

[80] Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations, Incorporating Change 1*, 2018, xx

[81]Kopec, Rafal. (2019). Space Deterrence: In Search of a "Magical Formula". *Space policy*, 47, 121;

Scharre, Paul. (2018). The US Military Should Not Be Doubling Down on Space. *Defense One*. Retrieved from: https://www.defenseone.com/ideas/2018/08/us-military-should-not-be-doubling-down-space/150194/

[82] Kopec, Rafal. (2019). Space Deterrence: In Search of a "Magical Formula". *Space policy*, 47, 121;

Scharre, Paul. (2018). The US Military Should Not Be Doubling Down on Space. *Defense One*. Retrieved from: https://www.defenseone.com/ideas/2018/08/us-military-should-not-be-doubling-down-space/150194/

[83] Haller, Linda and Sakazaki, Melvin. (2006). Commercial Space and United States National Security. *Commission to Assess United States National Security Space Management and Organization.* Retrieved from: https://fas.org/spp/eprint/article06.html

[84] Lamrani, Omar. (2016). What the U.S. Military Fears Most: A Massive Space War. National Interest. Retrieved from: https://nationalinterest.org/blog/the-buzz/what-the-us-military-fears-most-massive-space-war-16248

[85] Kopec, Rafal. (2019). Space Deterrence: In Search of a "Magical Formula". *Space policy*, 47, 121.

[86] Kimball, Daryl. 2017). The Outer Space Treaty at a Glance. *Arms Control Association.* Retrieved from: https://www.armscontrol.org/factsheets/outerspace

[87] Vasani, Harsh. (2017). How China is Weaponizing Outer Space. *The Diplomat*. Retrieved from: https://thediplomat.com/2017/01/how-china-is-weaponizing-outer-space/

[88] Vasani, Harsh. (2017). How China is Weaponizing Outer Space. *The Diplomat*. Retrieved from: https://thediplomat.com/2017/01/how-china-is-weaponizing-outer-space/

[89] Kelso, T. S. (2007, September). Analysis of the 2007 Chinese ASAT Test and the Impact of its Debris on the Space Environment. *In 8th Advanced Maui Optical and Space Surveillance Technologies Conference*, Maui, HI (Vol. 7).

[90] Koebler, Jason. (2014). All it takes is one missile to ruin space for everyone. *Vice*. Retrieved from: https://www.vice.com/en_us/article/4x3x43/all-it-takes-is-one-missile-to-ruin-space-for-everyone

[91] Fischerkeller , Michael P. and Harknett, Richard J. (2017). Deterrence is Not a Credible Strategy in Cyberspace,

Orbis. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0030438717300431

[92] Fischerkeller , Michael P. and Harknett, Richard J. (2017). Deterrence is Not a Credible Strategy in Cyberspace,

Orbis. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0030438717300431

[93] Jaxa. (2016). Hitomi Experience Report: Investigation of Anomalies Affecting the X-ray Astronomy Satellite "Hitomi." Retrieved from: https://global.jaxa.jp/projects/sat/astro_h/files/topics_20160524.pdf

[94] Goutam, Rajesh. (2015). The Problem of Attribution in Cyber Security. *University of Lucknow*. Retrieved from: https://pdfs.semanticscholar.org/3ea2/a54f8d5b473f0c261c2be45f741e040fa6f3.pdf

[95] Chivvis, Christopher and Dion Schwarz. (2017). Why It's So Hard to Stop a Cyberattack – And Even Harder to Fight Back. *Rand Corporation.* Retrieved from: https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

[96] Chivvis, Christopher and Dion Schwarz. (2017). Why It's So Hard to Stop a Cyberattack – And Even Harder to Fight Back. *Rand Corporation.* Retrieved from: https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

[97] *The White House*, National Cyber Strategy of the United States of America, 2018, https://nsarchive2.gwu.edu//dc.html?doc=4936882-The-White-House-National-Cyber-Strategy-of-the;

Department of Defense, Summary: The Department of Defense Cyber Strategy, 2018, https://nsarchive2.gwu.edu//dc.html?doc=4936880-Department-of-Defense-Summary-Department-of

[98] Shuman Ghosemajumder. (2017). You Can't Secure 100% of Your Data 100% of the Time. *Harvard Business Review* Retrieved from https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time

[99] National Institute of Standards and Technology. (2019). *Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework

[100]IBM. (2014). IBM Security Services 2014 Cyber Security Intelligence Index. Retrieved from https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

[101] Gallagher, Sean. (2017). Radio navigation set to make global return as GPS backup, because cyber. *Ars Technica.* Retrieved from https://arstechnica.com/gadgets/2017/08/radio-navigation-set-to-make-global-return-as-gps-backup-because-cyber/

[102] GPS.gov. (2019). LORAN-C Infrastructure & E-LORAN. *GPS.gov.* Retrieved from https://www.gps.gov/policy/legislation/loran-c/;

GPS World Staff. (2015). "Bill Supports eLORAN as GPS Backup. *GPS World.* Retrieved from: gpsworld.com/bill-supports-eloran-as-gps-backup/

[103] *Resilient Navigation and Timing Foundation.* (2015). "An eLORAN Primer." Retrieved from: https://rntfnd.org/wp-content/uploads/eLoran-Primer-RNTF-Submission-to-DOT.pdf

[104] Barlett, Stephen. (2015). "A Wide-Area Multi-Application PNT Resiliency Solution." *GPS World.* Retrieved from: https://www.gpsworld.com/innovation-enhanced-loran/

[105] Barlett, Stephen. (2015). "A Wide-Area Multi-Application PNT Resiliency Solution." *GPS World.* Retrieved from: https://www.gpsworld.com/innovation-enhanced-loran/

[106] Congressional Budget Office. (2017). Coast Guard Authorization Act of 2017. *115th United States Congress.* Retrieved from https://www.cbo.gov/system/files/115th-congress-2017-2018/costestimate/hr2518.pdf

[107] GPS.gov (2019). Funding. *GPS.gov*. Retrieved from https://www.gps.gov/policy/funding/

[108] GPS.gov. (2019). LORAN-C Infrastructure & E-LORAN. *GPS.gov*. Retrieved from: https://www.gps.gov/policy/legislation/loran-c/

[109] Wagner, I. (September 9, 2019). “Global space economy in 2018, by sector (in billion U.S. dollars).” *Statista*. Retrieved from: https://www.statista.com/statistics/662231/space-economy-breakdown-globally-by-sector/