Evaluating Space as the Next Critical Infrastructure Sector

Mark Peters II

USAF Retired

ABSTRACT

When one considers critical infrastructure protection, the default discussion too often becomes discussing cyber vulnerabilities as the only way to defend the homeland without considering whether all correct critical infrastructure (CI) was identified. When created, the Department of Homeland Security (DHS) protected those critical U.S. infrastructure categories identified by the executive branch with all military space infrastructure becoming part of the category called Defense Industrial Base. Other potential space sectors including television, satellite manufacturing, commercial launch, and global positioning disappeared into other CI categories such as critical manufacturing, communications, or information technologies. Just as military space required a separate armed service in the Space Force, the time appears right to implement a space CI sector including from commercial satellite manufacturing through launch and ground control to on-orbit missions as critical to U.S. public health, public safety, economic benefit, and national security. Starting with historical approaches to selecting and protecting CI, this paper expands to what sectors are currently protected, which space infrastructure matters most, and provides a qualitative CI sector comparison based on a hypothesis-based design.

Keywords: evaluating space, critical infrastructure (CI), sector, Department of Homeland Security

Evaluación del espacio como el próximo sector de infraestructura crítica

RESUMEN

Cuando se considera la protección de la infraestructura crítica, la discusión predeterminada con demasiada frecuencia se convierte en discutir las vulnerabilidades cibernéticas como la única forma de defender la patria sin considerar si se identificó toda la infraestructura crítica (CI) correcta. Cuando se creó, el Departamento de Seguridad Nacional (DHS) protegió las categorías críticas de in-

fraestructura de los EE. UU. Identificadas por el poder ejecutivo y toda la infraestructura espacial militar se convirtió en parte de la categoría denominada Base Industrial de Defensa. Otros sectores espaciales potenciales, como la televisión, la fabricación de satélites, el lanzamiento comercial y el posicionamiento global, desaparecieron en otras categorías de CI, como la fabricación crítica, las comunicaciones o las tecnologías de la información. Así como el espacio militar requería un servicio armado separado en la Fuerza Espacial, parece que es el momento adecuado para implementar un sector de CI espacial que incluya desde la fabricación de satélites comerciales hasta el lanzamiento y el control terrestre hasta misiones en órbita que son críticas para la salud pública, la seguridad pública y la economía de los EE. UU. beneficio y seguridad nacional. Comenzando con enfoques históricos para seleccionar y proteger la IC, este documento se expande a qué sectores están actualmente protegidos, qué infraestructura espacial es más importante, y proporciona una comparación cualitativa del sector de la IC basada en un diseño basado en hipótesis.

Palabras clave: espacio, infraestructura crítica (CI), evaluación, sectores espaciales, infraestructura cualitativa, crítica

关于太空作为下一个关键基础设施部门的评价

摘要

当个体考量关键基础设施（CI）保护时，默认的辩论时常将网络脆弱性作为保卫国土的唯一方式加以探讨，而不考量是否识别了所有正确的关键基础设施。国土安全局（DHS）成立时，对那些被行政分支所识别的关键美国基础设施类别加以保护，所有军事空间基础设施都属于国防工业基地这一类别。其他潜在的空间部门，包括电视业、卫星制造、商业发射、全球定位等，转移到其他关键基础设施类别，例如关键制造、传播、或信息技术。正如太空军中的军事空间要求一个单独的军事服务，是时候启用一个包括从商业卫星制造、发射、地面控制到轨道任务（on-orbit missions）的空间关键基础设施部门，它对美国公共卫生、公共安全、经济利益和国家安全至关重要。从选择和保护关键基础设施的历史方法出发，本文扩展研究了哪些部门正在受到保护、哪些空间基础设施最重要、并基于一项基于假设的设计，提供了一个关于关键基础设施部门的定性比较。

关键词：太空，关键基础设施（CI），评价，太空部门，性

1. Introduction

The most terrible threat for any strategic planner is suffering a Pearl Harbor type event exceeding all previous expectations due to a lack of proper preparation. In all critical infrastructure (CI) debate, cyber vulnerabilities have reigned supreme as a panacea to protect the homeland. However, many systems vulnerable to cyberattacks have other inherent weaknesses demanding unique protections best addressed by dedicated bodies of experts. The central question then becomes whether analysts and strategic planners planning for homeland defense identified all correct critical infrastructure areas. Today, the answer should be no. Space infrastructure demonstrates critical contributions to U.S. public safety, provides clear economic benefit, and national security value but remains unaddressed by the Department of Homeland Security as a holistic sector. To understand why space critical infrastructure should be included, one starts with how DHS selects critical infrastructure, which existing areas are protected, identifying critical space capabilities, and validating U.S. benefits. As the Space Force's creation validates, if the U.S. fails defend space infrastructure, we will lose many benefits our citizens value today.

CI ownership has long been solely the executive branch's responsibility with informed opinions occasionally used to review and revise processes, usually when administrations change. Despite adding the Department of Homeland Security (DHS) as a cabinet

member, CI history and selection process are largely administratively driven by administrative decisions. The DHS defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters" (DHS, 2020). Sixteen sectors currently constitute the Critical Infrastructure and Key Resources (CIKR) identified by the DHS and seconded to the Cybersecurity and Infrastructure Security Agency (CISA). Rather than individually assessing each sector in detail, the employed method measured the sectors as groups against a potential space category. The five combined sectors are hazardous materials, life sustaining support, manufacturing, digital spaces and governance. Each sector was previously assessed as having sufficient impact to require protection with budget, dedicated groups, and processes to accomplish those goals. The five groups were compared to space with three hypotheses, first, comparing public health and economic benefits, second, comparing national security benefits, and finally, evaluating a counter-hypotheses that space facilities are sufficiently protected by other sectors as to not require unique protections.

This paper demonstrates space shows enough common characteristics in national security, economic benefit, public health, and public safety with other critical infrastructure areas to merit consideration as a separate func-

tion. Other sectors each cover portions of potential Space sector vulnerabilities through defending cyberspace networks, physical locations, and logistics transport yet fail to offer sufficient protection to space infrastructure. When first created, the Department of Homeland Security identified selected areas correlated from previous administrations as central to U.S. protection. All military defense requirements for acquisition, manufacturing and services were categorized as part of the Defense Industrial Base. This assumed all commercial-produced items necessary for military success were built in individual facilities or distinguishable within other facilities. As the Space Force begins operations, the time appears right to propose a space sector, from commercial build and ground control to on-orbit employment, should be considered a critical infrastructure area for the United States.

The next step to evaluating space as a separate sector considers two facets, what functions would be considered space infrastructure, and what risks do those facilities face? The first space function for considerations should be the launch facilities, ground control, and satellites. Without launch, there is no space but without control, any derived value may be greatly reduced. In different, U.S. located, spaceports are currently licensed by the FAA (FAA, 2018). Although the list begins in 1998, the newest construction was Spaceport America in New Mexico (America, 2020). Any list must also include the manufacture and transportation of space goods and services. Finally, any

space infrastructure includes the communication networks required to communicate between ground and on-orbit devices. The equation's other half considers potential risks as the threats and vulnerabilities faced by space CI. Threats to ground-based infrastructure likely remain the same as for other sectors while space will also inherit threats in the manufacture and communication sectors. Unique to space are features like space weather, orbital debris, direct action by adversaries, limited orbital slots, commercial interference as well as potentially unknown events. This area also considers whether the existing Space Information Sharing and Analysis Center (ISAC) provides sufficient protection to space facilities

Finally, the paper finishes through evaluating each hypothesis, discussing evidence, and making a recommendation for space as future critical infrastructure. Each hypothesis was qualitatively evaluated as an aggregate and individual sectors before comparing to the same results for space. These comparisons provide research integrity through demonstrating where each sector might stand during any future process. Additionally, the counter hypothesis offers a contrary opinion to see if other sectors may indeed provide sufficient coverage for space. While eventual decisions will lie at the federal level, comprehensive analysis should add substance any discussions. This last section makes some recommendations for further studies, protection theory, and potentially merging existing CI sectors to create additional budget room for space facilities.

2. History of Critical Infrastructure?

The critical infrastructure theory states identified structures are systems the American people depends on for daily life sustaining or improving services. Incapacitating or paralyzing any CI system either individually or in aggregate function could seriously damage the homeland through degrading national security, the U.S. economy, or public health. These parameters have changed over the years so David Reidman's clarifying work to assess fourteen different policy documents since 1986 uncovers common terms across multiple documents (Reidman, 2016). Although CI protection has been relatively common recently, the first federal usage for CI occurred less than 25 years ago. Reidman's search looked for key words including "nationally significant," "provide vital service," "interdependent system," "debilitating impact," and "safety of public." While these terms are useful during an assessment, this paper uses the definition for CI from the 2001 Patriot Act, Title X, Sec 1016 H, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Congress, 2001). This definition was selected as it also forms the basis for the DHS mission as a governmental agency. One can see the slight language variance from Reidman's study although the only

major difference lies only in the term, "interdependent."

Interdependence normally refers to the international relations viewpoint advocated by Joseph Nye and Robert Keohane (Keohane & Nye, 1997). The concept builds from when organizations demonstrate multiple connections, show a lack of hierarchy among those connections, and deemphasize military force. When applying interdependence to CI, one can use all three qualifications from a slightly different perspective. Critical infrastructure components offer a backbone to societal processes through multiple connections at various hierarchical levels. As an example, a recent Department of Treasury memo lists essential financial services as all those who process financial transactions and services, insurance services, financial operations, security and all underlying third-party providers (Mnuchin, 2020). The volume of included personnel demonstrates the multiple connections, and at the same time, the lack of hierarchy in which aspects work with which other connections and when. The memo reinforces the third point through the absence of any Department of Defense resource references.

Advocating for change to existing governmental processes like the DHS's Critical Infrastructure and Key Resource (CIKR) listing requires first discussing how previous changes occurred. Many believe Federal CI protection begins with the Patriot Act and 9/11 attacks, but the first attempts to protect U.S. infrastructure began five years earlier during the Clinton Administration.

President Bush used his mandate to make some significant changes, President Obama made more, and the recent administration continued the trend through President Trump's creation of the Cybersecurity and Infrastructure Security Agency (CISA). Change typically occurs at the point where an administration changes as well as several times during each administration depending on how internal and external pressures are applied.

The first, formal federal "critical infrastructure" definition was 1996 when President Clinton signed Executive Order 13010 (Listes, 2018). In typical government fashion, EO 13010 designated 10 agencies to contribute to a commission who reported to a Principal committee in the National Security Council structure. The order identified eight critical areas as vulnerable to either physical or cyber-attacks (Clinton, 1996).¹ The commission returned the report the following year and highlighted five sectors of each area most vulnerable to attack as; information and communications, energy, banking and finance, physical distribution, and vital human services. Several vulnerability areas overlap sectors as CI although were not treated as a distinct area at the time.

Two years later, in 1998, President Clinton signed Presidential Decision Directive 63 (PDD-63). PDD-63's aimed to develop improved protection capacity for U.S. CI and marks the first time cyber was defined as a CI compo-

nent. Further, PDD-63 designated federal agencies as lead for each specific sector in coordination with equivalent Sector Liaisons designated from private industry (Clinton, Presidential Decision Directive/NSC-63 "Critical Infrastructure Protection, 1998). This proved to be a continuing bedrock concepts for today's CI planning and will likely continue as vital for the space industry as large elements including launch and control shift into the private sector.

In 2001, the 9/11 attacks redefined the how the U.S. government defined protection, and CI was no exception. The 2001 Patriot Act discussed the requirements for CI protection and information sharing while leaving out calling for any specific areas. The 2002 Homeland security act adds definitions for key resources which were then used to write the Homeland Security Presidential Directive -7 (HSPD-7). Further, HSPD-7 reduces the CI sectors to five which were designated as information technology, telecommunications, chemical, transportation systems, emergency services and postal while including dams, government facilities, and commercial facilities as key resources. The directive adds several other requirements and coordination elements to homeland security including mandating the government responsible agents would liaise independently to each sector's private institutions. The Department of Homeland Security was also designated as the agency to change, modify, or otherwise update CI any re-

1 The eight identified sectors were: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

quired elements (Bush, 2003). While the DHS continued to monitor and track changes from below the policy level, the next significant change was 2013 when Presidential Policy Directive 21 (PPD-21) outlined federal infrastructure protection roles through clarifying functional relationships, enabling efficient information exchange, and implementing an integration and analysis functions (Goss, 2014). This directive accomplished two other key functions, establishing an independent analysis center for physical effects on infrastructure, and another center for cyber effects. Further, PPD-21 expanded the critical sectors to 16, where the number stands today.

The next CI security change was launching the Cybersecurity and Infrastructure Agency (CISA) as a DHS branch. On November 16, 2018, President Trump signed the 2018 Cybersecurity and Infrastructure Security Agency Act into law which elevated the former National Protection and Programs Directorate (NPPD) within DHS to establish CISA and included the National Cybersecurity and Communications Integration Center (NCCIC). CISA's priorities are federal network protection, comprehensive cyber protection, infrastructure resilience and field operations, and emergency communications. Prior to CISA, NCCIC had realigned in 2017 to integrating like functions previously performed by the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) independently (CISA, 2020). The changes

might lead one to consider whether any physical CI protection, or independent cyber defense are still being considered as vital components for the sixteen CI families, an interesting topic but outside this paper's scope.

Although the agency remains new, the assumed responsibilities include all features previously managed by DHS as the National Security Agency assumes all signal intelligence responsibilities for the Department of Defense. CISA's budget for 2020 was \$2B with the planned budget for 2021 as \$1.75B (DHS, Cybersecurity and Infrastructure Security Agency: Budget Overview, 2020). This contrasts sharply with the formal DHS budget for 2020 of \$51B (DHS, FY2020 Budget in Brief, 2020). CISA was included as part of the overall DHS budget but has the lowest budget rating of all designated areas. The CISA numbers match the budget requirement for the U.S. Secret Service but are surpassed by "Other" at 4% and then U.S. Citizenship and Immigration Services at 5%. The two highest budget areas for DHS are the Federal Emergency Management Agency at 31% and U.S. Customs and Border Protection at 23% (DHS, FY2020 Budget in Brief, 2020). The miniscule \$2B overall budget is only .5% when compared to the interest paid on national debt and only 30% of launch revenues as the lowest producing economic sector for space (Amadeo, 2020).

While centrally managing CI as a U.S. federal responsibility for almost 25 years, no consistent method exists to evaluate whether to included new CI areas discard old ones. Neither has

any discussion emerged regarding how sectors are categorized and evaluated as each set of approvals was recommended by congressional inquiry and then validated by Executive Order or Presidential Policy Directive from the four most recent Presidents. Seven of the sixteen areas are assigned directly to DHS and two more are shared, or were, prior to CISA's emergence. The Department of Health and Human Services owns one area and shares one, while the Departments of Defense, Energy, Treasury, and the Environmental Protection Agency each focus on one area. A framework similar to the one used later in the paper to evaluate space CI hypotheses could be equally enacted by a simple mandated congressional reporting structure based on economic value, public health, and national security to score yearly or biannually to validate infrastructure protection needs.

3. Comparing CI Sectors

Sixteen infrastructure protection categories currently exist and evaluating each in depth would take many more pages than available during each discussion so instead, this paper treated those functions largely as aggregated functions for hazardous materials, manufacturing, life sustaining services, digital spaces, and government and governance functions. Each section has been aggregated to cover 2-4 of the existing sectors based on their similarity to other functions. Only a top level look is considered for individual functions without considering individual economic revenues or unique capabil-

ities. Multiple ways probably exist to parse the existing sixteen sectors for different factors or integrations, and even parsed, some of the sectors are likely large enough to require multiple liaisons from government and commercial domains. Hazardous materials as the first grouping includes the chemical and nuclear sectors which covers a requirement to safely transport products. Both sectors contribute to space sector usefulness in terms of fuel or power while neither creates a direct dependent link. A second grouping designation would be life sustaining for water and wastewater, dams, food and agriculture, and energy. Dams and energy both provide power in a different manner from nuclear and requiring less waste transport although still support daily needs. At the same time, water and food again deliver necessities for daily life through public health and safety. The life sustaining grouping would more likely supply secondary dependent links to those working in space areas such as supporting ground control and manufacturing. Current satellites usually receive power from either internal fuel or solar power once launched. The below chart (Table 1) describes the grouping for all five aggregated sectors.

The third grouping, manufacturing includes commercial facilities, critical manufacturing, and the Defense Industrial Base. All three sections would tie tightly to space infrastructure aspects although no specific cross coordination emerges. The Cyber and Infrastructure Security Agency lists the four critical manufacturing components as primary metals, machinery, electrical

Table 1: Aggregated Groups for the Dept. of Homeland Security Critical Infrastructure Sectors

CI Group	CI Sectors
Hazardous	Chemical
	Nuclear Reactors, Materials and Waste
	Energy
Life Sustaining	Waste and Wastewater
	Dams
	Agriculture
Manufacturing	Critical Manufacturing
	Commercial Facilities
	Defense Industrial Base
Digital Spaces	Communications
	Information Technology
	Financial Services
Government and Governance	Emergency Services
	Government Facilities
	Healthcare and Public Health
	Transportation Systems

equipment and transformation equipment while commercial facilities has eight sub-sectors (CISA, Critical Manufacturing Sector, 2020).² Commercial facilities would more likely be tied to the private presentations associated with space commercial foundations or retail sites selling space-associated products. Finally, the Defense Industrial Base contains all those subsections who work under contract to the Department of Defense. This section would likely include the entire government space industry although like the other elements, no separate distinction

appears just for space infrastructure. In 2018, the U.S. spent \$47.5B on all space services while the global space, ground services market alone was \$60B (FAA, 2018). A fourth grouping, Digital Spaces, would include communications, information technology (IT), and Financial services. Communications involves all forms of voice and data transmission while the IT sector coordinates services provided by hardware and software components. The Financial sector depends on the previous two working successfully to push through their regular functions contributing to U.S. eco-

² Eight sub-sectors are Entertainment and Media (e.g., motion picture studios, broadcast media), Gaming (e.g., casinos), Lodging (e.g., hotels, motels, conference centers), Outdoor Events (e.g., theme and amusement parks, fairs, campgrounds, parades), Public Assembly (e.g., arenas, stadiums, aquariums, zoos, museums, convention centers), Real Estate (e.g., office and apartment buildings, condominiums, mixed use facilities, self-storage), Retail (e.g., retail centers and districts, shopping malls), Sports Leagues (e.g., professional sports leagues and federations).

conomic benefit. Like the third grouping, space will heavily depend on this sector but no specific identification for space related ground links, satellite television, or Global Navigation Satellite System (GNSS) are included in the initial discussions for these areas.

The last grouping for comparison would be government and governance. This section includes emergency services, government facilities, health-care, and transportation. All of these are government provided mitigation for daily concerns. These areas have little to nothing to do with any space CI sector although space might be potentially regulated under transportation systems through the aviation subsector for transportation (CISA, Transportation Systems Sector, 2020). Today, the Federal Aviation Administration (FAA) holds the responsibility for all space commercial transportation. Finding the FAA branch and webpage which manages space takes a little more difficulty. No links existed from the main page and the item required multiple specific searches on the page to locate the FAA's space page. U.S. space launch and transportation were categorized as \$1.7B in the FAA's 2018 Annual Space Compendium versus \$5.5B for global launch services (FAA, 2018). The largest commercial space providers in the U.S., SpaceX, claims their 2018 launch revenues topped \$2B, more than overall total for all 2017 launches, reaffirming space mission's economic impact. (Sheetz, 2019)

Categorizing the various sectors leads to considering how one assesses

risk. Although a common definition for risk suggests any total risk equals threat multiplied by vulnerability, other definitions may be used. Systemic protection for CI can skip right past risk assessments to focus on immediate protection shortfall like physical fences or background checks for employees. As another risk framework example, the European CI protection framework uses four pillars: readiness, detection, recovery, international cooperation, and information technology. These pillars are assessed against four protection levels each as primary loop, control loop, analyzing feedback and planning (Roman, 2016). Comparatively, the North American Electric Reliability Corporation (NERC) provides 11 standards for Critical Infrastructure Protection (CIP) but only for electric power. The NERC risk assessment occurs their standard, CIP 014, including performing an initial assessment, conduct third party review, notify owners, evaluate threats and vulnerabilities for physical attack, develop a plan, and have a third party review the plan. If Space becomes an additional CI sector, corporations and agencies within that sector will likely have to develop risk and industry standards for protection.

Space is not currently a CI sector although various industry pieces fall under different, currently protected areas. No government standard exists for comparison between CI sectors, so this paper uses a high-level qualitative assessment to compare space benefits to the other sectors. This assessment is based on two primary hypotheses and a counter hypothesis, included below.

H1. If space industry infrastructure is protected than significant value will be preserved to the general public safety, health and economic outcomes for U.S. citizens.

H2. If space industry infrastructure is protected than significant value will be preserved to the national security outcomes for U.S. citizens.

H3. If space industry infrastructure is currently protected by other DHS Critical Infrastructure and Key Resource than a unique designation is not required.

Each hypothesis was compared on a binary basis for the existing CI groups and for space. H1 examined the evidence supporting the U.S. population deriving economic and public health benefits from space sector. Economic benefit can be calculated through comparing to Gross Domestic Product numbers as reported by the U.S. Department of Commerce's Bureau of Economic Analysis (BEA) (Howells, Morgan, & Aversa, 2020). The BEA tracks 22 different sectors which overlap some, but not all, CI sectors. In this case, substantial positive revenues were used as evidence of economic benefit. Public health measurements are more difficult to measure and will be qualitatively assessed based on a binary summary of whether the various space sectors contribute to overall public well-being. The Center For Disease Control Foundation defines public health as, "the science of protecting and improving the health of people and their communities ... achieved by promoting healthy lifestyles, researching disease and injury prevention, and

detecting, preventing, and responding to infectious disease" (Foundation, 2020). Strictly based on the definition, space contributes little to public health but neither do many other CI sectors are likely similar.

The second hypothesis evaluated whether space increased positive national security outcomes. Again, a qualitative response was used to comparing the various sectors to space. The qualitative structure allowed determining whether space contributes to security relatively rather than defining an absolute value based on a measurable characteristic. The recently commissioned Space Force establishes national spacepower as, "the totality of a nation's ability to exploit the space domain in pursuit of prosperity and security ... comparatively assessed as the relative strength of a state's ability to leverage the space domain" (U.S. Space Force, 2020). This definition does establish a way to examine space contributions to national security although terms like relative strength and leveraging would have to be more concisely defined. Publicly, many space contributions are likely overlooked on a daily basis including functions such as satellite television, positioning services, and even timing.

The final hypothesis explores the counter position, one where the argument becomes whether any existing CI sectors already provide sufficient protection for space infrastructure. The two aggregate sectors likely to have the most overlap are Digital Spaces and Manufacturing with the other three having significant less. Government and

Governance would likely have the next most coverage with Life Sustaining and Hazardous having little to no direct overlap to space functions. This hypothesis will also be considered as a qualitative response based on existing CISA coverage definitions for each section. This final sector will be evaluated by comparing scores to other sections and assessing whether those sectors provide similar benefits to space.

The final evaluation step scored the three hypotheses. While using a qualitative standard, scores were produced from the a binary assessment of yes (1) or no (0) and then averaged across the board. Each section will be evaluated subjectively for whether significant damage to the sector from a threat or an attack could critically impact one of the four criteria. The four criteria from the critical infrastructure definition are public health, public safety, economic benefit, and national security. Each CI sector was evaluated as either a positive or negative for each category. Although each category was scored, the first three were grouped together based on the hypothesis structure. Positive results were scored as one while negative scores were regarded as zero. Scores were recorded for individual as well as the aggregated sectors. This provides the ability to objectively compare various sectors. A more extended or quantitatively focused study could establish monetary or other impact criteria within those sections for a more quantified comparison. Having established a method, the next step must be to consider what space industry aspects could be considered as critical infrastructure.

4. What Should be Space Critical Infrastructure?

When compared to other CI sectors, one must consider what elements are space infrastructure. Any infrastructure evaluation should start through the North American Industry Classification System (NAICS). NAICS provides a Federal agency standard to classify businesses with two-digit classifications and adds additional numbers up to six numerical digits for sub-sectors. This classification becomes the basis for collecting, analyzing and publishing statistical data about the economy with a category revision published every 5 years since 1997 (U.S. Census Office). A keyword search for “space” in the 2017 NAICS catalog finds 24 results from space simulation chambers (332313) to space research services, [for] government (927110). In selecting a topic from each aggregated sector for comparison, one can find four results for “Dam,” 26 for “nuclear,” 27 for communications, 87 for “health,” and 7,232 for “manufacturing.”

The broader space categories from the NAICS structure includes nine two-digit elements which make up the 24 six-digit elements to highlight contributed aspects and overlap. The current 24 elements are contained in broader two-digit elements for manufacturing (33), wholesale trade (42), transportation (48), Professional services (54) and public administration (92). Two sections are clearly missing from the broader category, information (51) and construction (23) with the possible addition of accommodation and

food services (72). Each of these sectors could include multiple other sectors for evaluation. Construction would cover building satellite receiving stations and launch facilities while Information would cover satellite telecommunications and most navigation or timing systems. The last addition for accommodation and food services covers the possibility of developing and deploying commercial residence or other forms of space tourism (Highfill, Georgi, & Dubria, 2019). These assessments are contained in a new BEA project launch document aiming to compile more detailed space economic references by late 2020 (Highfill, Georgi, & Dubria, 2019).

A more logical separation for space infrastructure would consider launch, ground control, orbital functions, and manufacturing as separate sub-sectors. Globally, the 2018 FAA Compendium of Commercial Space Transportation refers first to satellite and non-satellite industry as a roughly 3-1 margin globally, \$260B to \$84B. In a further breakdown, the same chart lists global investments as satellite television (\$97B), government budgets (\$82B), satellite ground equipment (\$60B), navigation (\$52B) fixed satellite service (\$17B) satellite manufacturing (\$13B) and launch (\$5.5B) (FAA, 2018). One of the biggest problems appears again as multiple government evaluators select different comparisons across the space industry. Regrouping these functions puts the global value as roughly \$160B for orbital functions, \$82B for government space, \$73B for ground control, and \$5.5B for launch. As government space functions were not segregat-

ed through this study the best option would likely consider government space a different section for infrastructure.

Over the next several years, space access and functions will probably decrease in per capita value while increasing overall space assets numbers. This cost reduction increase space functional impacts across societies as space-based possibilities emerge for previously unconsidered commercial solutions. A National Defense University presentation suggests increasing launch rates by a factor of 9 creates a 3x cost reduction per kg of payload (Stockdale, Aughenbaugh, & Boensch, 2018). This decrease will match with a lowering of individual asset costs and decreases in associated support costs as insurance and financing for space becomes better understood. Even further, new business models will likely open paths for investment and implementation opportunities which are not yet even envisioned, similar to if one could invest in digital music or smartphones in the 1980s (Partnership for Conflict, Crime, And Security Research, 2016).

In its present form, the National Space Council (NSC) was established in 1989 under the Bush administration, closed under the Clinton Administration and did not reappear under 2016 under the Trump administration. The Secretary of Commerce is a key member of this board whose designed mirrors previous National Security Council structures to raise space issues to the executive branch level within the government. Under most administrations, conflict between the DOD for military space, and the National Aeronautics and

Space Administration were key blockers to a unified U.S. policy (Vedda, 2016). The NSC looks to enact U.S. space policy for commercial development, sustainable human presence, and expanding opportunity for Americans to live and work in space. This matches long-term goals to achieve these same results not only in Earth orbits but also creating a human presence on the Moon, Mars and further (Office of Space Commerce, 2020). This governmental structure could be key to space's reconsideration as a critical infrastructure area.

Further evidence supporting establishing a U.S. space critical infrastructure sector was the recent establishment of a Space Information Sharing and Analysis Center (ISAC) (Space ISAC, 2020). The Space ISAC was added to the national council of ISACS which establishes cross-sector coordination for sharing information about cyber and physical threats, mitigation strategies, and bringing partners together (Miller, 2020). This organization looks to identify possible threats to the supply chain, business systems and missions associated with space. The early establishment of this ISAC could help reduce cost and administrative difficulties in nominating a space infrastructure sector. ISACs were established as part of the original critical infrastructure protection plan by PPD-63 (Clinton, Presidential Decision Directive/NSC-63 "Critical Infrastructure Protection, 1998). Some suggest the original ISAC intention was only to coordinate on cyber threats but the NCI mission statement suggests both cyber and physical threat informa-

tion are routinely reviewed (National Council of ISACs, 2020). As some organizations seem to exist to protect some space aspects, the next consideration should be what threats would routinely be faced by space critical infrastructure.

The term, "threat" drives protection discussion but thoroughness demands one also evaluate vulnerabilities. Active threats usually are driven by state, non-state, or criminal actors who intend to damage U.S critical infrastructure as part of economic or political goals. State actors are nations who can afford more advanced means to commit kinetic and non-kinetic actions either in orbit or against terrestrial sites (Bateman, 2020). High entry barriers to space conflict suggests the most likely U.S. opponents would be Russia or China (Edmonds, 2020). Non-state actors as terrorist groups, other political activists, or even corporate entities may also have unique goals for the space environment from destruction to establishing resource-yielding norms regarding extraterrestrial development. John Klein's close examination of terrorist group's potential capability to operate in the space environment proved largely negative (Klein, 2020). Criminal groups seek to obtain an illegal economic advantage through group. Terrorists and criminals are equally deterred from direct orbital actions based on the high entry costs for orbital operations but could still use cyber-attacks, sabotage, or influences on earth-based infrastructure to achieve desired effects.

The other half of risk, vulnerabilities, arise from the difficulties found naturally in the space environment.

Klein reflects three required functions shaped by orbital vulnerabilities: minimizing debris, coordinating proximity operations, and reducing electromagnetic interference (Klein, 2020). Some vulnerabilities may be caused from cascading events from threats or completely derived from external, and frequently unalterable, influences. All listed vulnerabilities are made more significant by distance since all space-based assets reside at least 62 miles above sea level. From the terrestrial side, either ground control installations or on-orbit functions means the vast distances create a vulnerable attack surface where threats may interject detrimental effects. Orbital debris from objects either snagged by Earth's gravity or manmade pieces remaining in orbit from either intentional or unintentional collisions can pose dangers to future mission. Coordinating space objects for mission events also poses dangers. All space objects possess velocity from their position and changing those vectors to maneuver near or around other objects can pose significant danger. These maneuvers can become more dangerous as one considers proximity and debris. Finally, space begins outside Earth's atmosphere which minimizes the protection terrestrial objects receive to interplanetary electromagnetic interference from celestial bodies or artificial signals (Moltz, 2019).

Any risk discussion would be remiss if not considering Black Swan principles. Accepted risks and vulnerabilities are largely based on known knowns or known unknowns, those concerns previously proven true or sus-

pected to occur. Black Swan methodologies, from Nassim Taleb, are those actions which cannot be predicted from previous events with any reasonable certainty (Taleb, 2010). An excellent example is Japan's 2011 earthquake measuring 9.1 on the Richter scale and the fourth largest quake since seismologists began recording in 1900 (Live Science Staff, 2011). Reconstructed seismic events from historical records suggest this was the first 9.0 or larger earthquake to ever hit Japan with the next largest event being a 8.6 quake in 1707 (Live Science Staff, 2011). The 2011 earthquake reshaped all previous assessments and the impact on protection appeared through the Fukushima nuclear reactor at Fukushima. The reactor successfully withstood the quake's initial impact but other safety estimates were based on being located 5.7m above sea level. The tsunami which hit the site was measured at 15m, rocking the site, and rendering it still unusable today (World Nuclear Association, 2020). This event shows how one Black Swan event can change all previous estimates.

The final risk step address mitigation by developing the means to reduce or eliminate risk. Establishing space as a CI sector would grow the consolidated structure to discuss and suggest future mitigations. The ISAC may be the first step towards those goals but additional coordination will certainly be necessary. Terrestrial mitigation will likely prove easier than reducing orbital risk although the imposition of industry standards and communication could accelerate these processes. recent congressional report to Congress on Space

Traffic Management even states the Department of Commerce should assume this responsibility from the DoD due to increasing orbital expansion. The report views the DoD as not capable of handling the expanded scale necessary to deal with orbital debris and control, then classified Space Situational Awareness as a public good (Hitchens, 2020). Mitigation works best when more views are involved and growing new federal and commercial partnerships could help develop excellent solutions to space's inherent threats and vulnerabilities.

5. The Case for Space

Making a case for space as an independent CI sector requires evaluating the three hypotheses. For the first hypothesis, a subjective assessment was made as to whether each sector contributed to public health, public safety, and an economic benefit. Public health was evaluated as to whether the general health and well-being of the public would deteriorate if the sectors were unavailable. Public safety was assessed as whether a lack of standardization, control, or limited resource usage would be detrimental to overall public safety. The final element, economic benefit, again considered subjectively whether the area proved beneficial to overall U.S. finances and production capability. The below chart collates the scores to evaluate the first two hypotheses and then ranks both aggregate and individual sectors for comparison.

The first hypothesis, H1, considers if space infrastructure provides

beneficial public health, safety and economic results. Space was evaluated as making no contribution to public health, a positive benefit to public safety and a positive benefit to the overall economy.

H1. If space industry infrastructure is protected than significant value will be preserved to the general public safety, health and economic outcomes for U.S. citizens.

This resulted in a combined score of .7 for the H1 hypothesis. Compared to the aggregated sectors, Space ranks above all except Digital Spaces, ranking two among the six aggregated categories. When compared to individual sectors, the rank for space scores below Energy, Communications, and Information Technology while ties with four of the remaining thirteen and outranks the final nine.

Space cannot currently be considered as beneficial to public health. No direct benefits derive from space which make public health better daily. However, GNSS must be considered beneficial to daily public safety from a navigation and mapping perspective. Most relate to GNSS through the more common aspect, Global Positioning Systems (GPS) as related to electronic mapping services. In 2019, global GNSS revenues were estimated at \$97B, just short of one-third of the overall space revenue (Satellite Industry Association, 2020). While individual navigation revenues may be limited, the RTI International group estimated that GPS has generated \$1.4T in economic benefits since its

Table 2: Critical Infrastructure Evaluation

CI Group	CI Sectors	Public Health	Public Safety	Economic Benefit	Score (H1)	National Security (H2)	Combined	Aggregate Rank	Sector Rank
Space		0	1	1	0.7	1	1.7	1	2
Hazardous		0.3	1	0.3	0.5	0.3	0.8	4	
	Chemical	0	1	0	0.3	0	0.3		5
	Nuclear Reactors, Materials and Waste	0	1	0	0.3	0	0.3		5
	Energy	1	1	1	1.0	1	2.0		1
Life Sustaining		0.7	0.7	0	0.5	0	0.5	5	
	Waste and Wastewater	1	1	0	0.7	0	0.7		4
	Dams	0	1	0	0.3	0	0.3		5
	Agriculture	1	0	0	0.3	0	0.3		5
Manufacturing		0	0.3	0.7	0.3	0.3	0.6		
	Critical Manufacturing	0	1	1	0.7	0	0.7		4
	Commercial Facilities	0	0	0	0.0	0	0.0		6
	Defense Industrial Base	0	0	1	0.3	1	1.3		3
Digital Spaces		0.7	1	1	0.9	0.7	1.6	2	
	Communications	1	1	1	1.0	1	2.0		1
	Information Technology	1	1	1	1.0	1	2.0		1
	Financial Services	0	1	1	0.7	0	0.7		4
Government and Governance		0.5	0.75	0	0.4	0.5	0.9	3	
	Emergency Services	1	1	0	0.7	1	1.7		2
	Government Facilities	0	0	0	0.0	0	0.0		6
	Healthcare and Public Health	1	1	0	0.7	0	0.7		4
	Transportation Systems	0	1	0	0.3	1	1.3		3

creation in the 1980s. They further assessed any loss of GPS services could result in a billion dollars per day loss to the U.S. economy. These results were commissioned by NIST in an interest to discover how GPS affected the ten U.S. economic sectors which used GPS on a day to day basis (Coraggio, 2019).

In addition to GPS' economic benefits, the space industry continues to expand other economic sectors which contributed to the positive score. One of the biggest global space economic sectors deals with improved commu-

nications. As an example, global satellite television was evaluated at \$92B in 2019 (Watson, 2019). The overall global pay T.V market in 2020 was evaluated at \$225B. Satellite TV in the U.S was tracked in 2017 as \$33.4B (Dziadul, 2020). This shows satellite television's importance as a U.S. market and global economic contributions. Satellite television offer significant entertainment as well as a means to communicate during external chaos which remains only minimally susceptible to terrestrial interference.

Overall, labelling and protecting space CI should be considered as a positive benefit for U.S. citizens and two of the three required areas for H1, proving this hypothesis as true. Space provide safety and economic benefits with this hypothesis score for space ranking significantly ahead of more than 50% of the remaining sectors. If this consideration alone was used, space should be added to the DHS CI listing as a funded protection area. The next hypothesis moves beyond public good to consider how space provides benefits to national security in protecting U.S. citizens from state and non-state threats.

The second hypothesis, H2, evaluates the benefit each CI sector brings to national security. A research inconsistency emerges here as space has no subsectors to consider so received a single score in a single sector.

H2. If space industry infrastructure is protected than significant value will be preserved to the national security outcomes for U.S. citizens.

Every aggregated section received a lower score than spaces their composite scores were averaged by the number of sectors. No aggregated sector appeared where all subsectors were assessed as having a positive benefit to national security. For the individual sectors, six sectors subjectively show importance to national security, when those scores are combined and averaged, no other section scores as high as space's full point. Of note, the critical manufacturing individual sector was considered not vital to national security

as the Defense Industrial Base sector is assumed to encompass any manufacturing areas which directly contribute to national security.

The seminal work by James Clay Moltz, *The Politics of Space Security*, suggest there are three areas where space contributes to national security; space science and exploration, space utilities, and military applications (Moltz, 2019). Advancing zero gravity manufacturing, unique experiments, and the harsh environments has directly contributed to many inventions initially featured as national security now contributing to public welfare daily. A short list of items derived from infrastructure would include solar cells, water filtration, LASIK surgery, insulin pumps, artificial limbs, camera phones, LEDs (Green, 2019). Many of these items are part of a number of U.S. citizens daily life.

The second contribution for national security, space utilities, includes previously discussed areas like communications, satellite TV and global positioning. Space utilities would likely extend into networked command and control, and Earth monitoring activities short of direct military applications. Future aspects could include transmitted power, orbital manufacturing, and coordinated frequency management. In the future, the potential exists to develop habitable and self-sustaining environments in orbit, on the Moon, or as far out as Mars. Expanding humanity beyond a single biome should certainly be considered vital for national security.

The last contributing area for national security, military applications,

evaluates the direct potential space brings to U.S. military strategy and implementation. The most significant gain from holding the ultimate high ground arrives from the advantage in reconnaissance, being able to observe the enemy and shorten one's own OODA loop for military actions.³ As of 2020, the U.S. possesses the only Space Force stood up as an independent military branch. Russia previously established an independent service arm as a Russian Space Force, but this was merged into the overall Aerospace Forces (VKS) in 2015 and never a fully independent service (Ministry of Defense of the Russian Federation, 2015). Finally, maintaining a space presence allows for early warning of adversary attacks and provides a command and control loop outside terrestrial interception. These three advantages combine to make space CI vital to national security and prove H2 as true.

The third hypotheses counters the previous two by stating the establishment of a space CI sector remains unnecessary as all required functions are covered by other sectors. If this evaluation were proved true than the H1 and H2 evaluation areas would be common across the scoring metric.

H3. If space industry infrastructure is currently protected by other DHS Critical Infrastructure and Key Resource than a unique designation is not required.

During the evaluation, space scored as positive for safety, health,

economic benefit, and national security. Of the other 16 sectors, only three show positive in the same areas; energy, communications, and Information Technology. Comparing the individual scores for each sector, the previous three areas again outscore space while space also ties with emergency services. A combined aggregate score of the previous two hypotheses places space as a the number one ranking, with the highest score, while the digital spaces score immediately behind.

Full spectrum analysis allows the possibility space may be ranked incorrectly by the combined scoring and lean towards an individual ranking. During the individual ranking, sectors with the same score were scored as tied. The top-three scoring sectors, and, ranked higher than space CI, were energy, communications, and information technology. Space tied for second place with emergency services and the remaining eleven infrastructure sections were all ranked lower. Some space aspects may be covered by either communications or infrastructure technology, those sectors are software and hardware, respectively. All CI aspects likely require some overlapping coverage from those two sectors just as all functions require energy. Additionally, economic scoring based on a quantitative metric might yield different results.

Space's unique structure means the cyber requirements under software

³ OODA is a common term in decision making processes and stands for Observe, Orient, Decide, and Act. In military tactics, the key is to able to complete one's own OODA loop before the enemy. Intelligence operations like reconnaissance make the OODA loop smaller than the adversaries and allows one to complete more cycles, faster.

and hardware for this sector may need to be considered differently. The Space ISAC establishment discussed earlier in the paper justifies this approach. Further, for any space orbital resources, much of their energy remains independent of terrestrial sources as orbiting satellites have the most direct solar potential and do not require as much support as ground-based energy sources. All ground-based stations and capabilities do require power with most sources from the terrestrial energy sector. The Defense Industrial base and critical manufacturing sectors currently cover some space aspects although these could be likely managed more efficiently as a direct space CI responsibility. Lacking any central governing body devoted to Space CI protection means unique facilities for launch, command and control, and positioning are likely left unprotected under current CI protection. All of these aspects lead to evaluate H3 as false since space CI does not appear to be effectively protected by overlapping CI sectors.

Conclusion

In conclusion, this paper evaluated a brief history of the CI process, to determine when CI was established and what factors were used to determine individual sectors. The next step proposed a method to evaluate whether space CI was needed and the metrics used before moving to consider what constituted space infrastructure. Those considerations lead to evaluating three hypotheses; whether space contributes to public safety, health, and the econo-

my, whether space contributes uniquely to national security, and if space CI today is sufficiently covered by other national resources. The first two proved to be true with space ranking number one in combined scoring and ranking above 11 of the remaining sectors during individual scoring. The third hypotheses was evaluated as false since no other sector adequately covers space CI. Some overlap does occur although those same areas also overlap numerous other CI sectors with none precisely matching space. These areas lead to the three recommendations, establishing a model for space CI interactions, developing a regular process for evaluating CI, and finally, including space as a CI sector as soon as possible. Finally, remaining potential gaps and areas for future study will be discussed.

One of Moltz's recommendations suggests any model for space should be a netocracy. his netocracy would be international, transparent, commercially lead, networked, with small resilient platforms and bottom-up innovation (Moltz, *The Changing Dynamics of Twenty-First-Century Space Power*). Several of these characteristics could benefit any future space CI protection structure. The first characteristic, international, does not translate to CI protection however international norms will be needed to manage orbital space both physically and electromagnetically. Standards must be established to control orbital debris as well as to manage orbital frequency usage to prevent losing control of functions vital to public health and national security. Transparency between commercial

and government sectors helps drive to the commercially led partnership similar again to other forms of CI. The last three elements clearly speak to building efficient CI protection for space through utilizing commercial successes to increase resilience through networking and innovation.

Moltz's clear path establishes while an agency may lead for protection, the commercial involvement will drive eventual success. The companies and development of local spaceports means the demand for space will continue to grow. As the demand grows, the sector must be protected and that protection between commercial and federal assets calls for efficient CI protection at all levels. Many companies today use complex, non-networked platforms which lack resiliency, coordinating U.S. efforts could increase control, and the economic return. While federal and commercial bodies exist to regulate various space functions, no central agency or networking function as required for CI protection. This body could also alleviate some responsibilities as the U.S. Space Force stands up, similar to how the Department of Commerce intends to assume Space Traffic Management responsibilities.

One key gap during this study was the lack of any coordinated body established to review and assess CI security areas for the U.S as an aggregate function. The areas selected since 1996 do not appear to undergo any active review or renewal process. Infrastructure changes, the pace of commercial technology like Space X, and even the grow-

ing Internet of Things suggest a more frequent and objective process is needed rather than the political vagaries from administration to administration. While the federal government must establish the process and timelines, the true work to defend U.S. space CI will likely fall mostly on the commercial sector. This will happen for two reasons, first, cyber actions will likely occur more under contractors and delivered equipment than as government actions. Second, expansions into the commercial market, private space travel for tourism, and the ease of maintaining low-cost satellites will create enhanced interest. Current satellite databases show just over 2500 satellites orbiting Earth but Space-X plans to launch over 42,000 in the next decade as part of their Starlink expansion (Union of Concerned Scientists, 2020); (Sheetz & Petrova, Why in the next decade companies will launch thousands more satellites than in all of the history, 2019).

As a final recommendation, the expansion of space, and the results of this evaluation suggest space should be included as soon as possible as a CI element for DHS. The study demonstrated space poses significant benefits to public safety through global navigation services and communication. The expanding space sector will continue to increase overall economic benefits as more and more corporations seek to secure space-based services. If nothing else, the sheer value of space-based assets to U.S. national security demand this sector should be evaluated and promoted to a DHS CI sector within the next 12 months. Any argument sug-

gesting other sectors adequately cover space industry is insubstantial at best, and a strawman at worst as any significant losses to the space industry will critically affect the United States safety, economy, and national security.

Any reasonable study should suggest other areas for future research. While this study measured space qualitatively against other CI sectors, a more detailed look could occur between space and any one other sector. Additionally, an examination could effectively measure whether CI considerations should be measured as aggregated and multiple sectors, using multiple links between the elements instead of a government liaison and commercial representative. A third and final recommendation would be to develop a metric, such as direct economic benefit, and use those considerations to provide a more detailed look into sector by sector comparison.

Overall, this study effectively used three hypotheses to demonstrate why space industry should be considered critical infrastructure by the Department of Homeland Security. This study used a qualitative comparison to demonstrate space shows more benefit to public health and safety, economic benefit, and national security than the majority of the current CI sectors. The study showed the need to establish a clear model for evaluating space infrastructure, working with federal agencies to create a body to regularly evaluate continuing need for all the CI sectors, and to include space infrastructure as a protected, and budgeted element of either CISA or DHS's consolidated infrastructure list. Space poses the ultimate high ground, with the commercial incentives and U.S. Space Force elevation, we should not let this sector be bypassed simply because it has not yet been included on a governmental list.

References

- Amadeo, K. (2020, Jun 17). *Interest on the National Debt and How it Affects You*. Retrieved from Thebalance.com: <https://www.thebalance.com/interest-on-the-national-debt-4119024>
- America, S. (2020). *About*. Retrieved from Spaceport America: www.spaceportamerica.com
- Bateman, A. (2020, Jul 30). America can Protect its Satellites without Kinetic Space Weapons. *War on the Rocks*. Retrieved from <https://warontherocks.com/2020/07/america-can-protect-its-satellites-without-kinetic-space-weapons/>
- Bush, G. (2003, Dec 17). *HSPD 7: Critical Infrastructure Identification, Prioritization and Protection*. Retrieved from Cybersecurity and Infrastructure Agency: <https://www.cisa.gov/homeland-security-presidential-directive-7>

CISA. (2020, Aug 2). *About Us*. Retrieved from US-Cert: <https://us-cert-cisa.gov/about-us>

CISA. (2020). *Critical Manufacturing Sector*. Retrieved from CISA.gov: <https://www.cisa.gov/critical-manufacturing-sector>

CISA. (2020). *Transportation Systems Sector*. Retrieved from CISA.gov: <https://www.cisa.gov/transportation-systems-sector>

Clinton, W. (1996, Jul 15). *Critical Infrastructure Protection*. Retrieved from Federation of American Scientists: <https://fas.org/irp/offdocs/eo13010.htm>

Clinton, W. (1998). *Presidential Decision Directive/NSC-63 "Critical Infrastructure Protection*. Federation of American Scientists. Retrieved from fas.org/irp/offdocs/pdd/pdd-63.htm

Congress, U. (2001). H.R. 3162. *Uniting and Strengthening America by Providing Appropriate Tools*.

Coraggio, M.-D. (2019, Oct 2). *Economic Benefits of the Global Positioning System to the U.S. Private Sector Study*. Retrieved from Nist.gov: <https://www.nist.gov/news-events/news/2019/10/economic-benefits-global-positioning-system-us-private-sector-study#:~:text=For%20the%20United%20States%20alone,day%20impact%20to%20the%20nation>

DHS. (2020). *Critical Infrastructure Sectors*. Retrieved from <http://www.dhs.gov/cisa/critical-infrastructure-sectors>

DHS. (2020). *Cybersecurity and Infrastructure Security Agency: Budget Overview*. Retrieved from DHS: https://www.dhs.gov/sites/default/files/publications/cybersecurity_and_infrastructure_security_agency.pdf

DHS. (2020). *FY2020 Budget in Brief*. Retrieved from DHS: https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_FY-2020-Budget-In-Brief.pdf

Dziadul, C. (2020, Feb 27). *\$50bn fall for North American pay-TV revenues*. Retrieved from Broadband TV News: <https://www.broadbandtvnews.com/2020/02/27/50bn-fall-for-north-american-pay-tv-revenues/>

Edmonds, J. (2020, Aug 14). *Russia and China Playing Musical Chairs in Zero Gravity. War on the Rocks*. Retrieved from <https://warontherocks.com/2020/08/russia-and-china-playing-musical-chairs-in-zero-gravity/>

FAA. (2018). *The Annual Compendium of Commercial Space Transportation, 2018*. Retrieved from FAA.gov: https://www.faa.gov/about/office_org/headquarters_offices/ast/media/2018_ast_compendium.pdf

Foundation, C. (2020). *What is Public Health?* Retrieved from cdcfoundation.org: <https://www.cdcfoundation.org/what-public-health#:~:text=Public%20health%20is%20the%20science,and%20responding%20to%20infectious%20diseases>

Goss, K. (2014, Sep 23). *Critical Infrastructure Protection: History, Overview & Update*. Retrieved from Domestic Preparedness.Com: <https://www.domesticpreparedness.com/preparedness/critical-infrastructure-protection-history-overview-update/>

Green, J. (2019, Jul 8). *Inventions we use every day that were actually created for space exploration*. Retrieved from USA Today: <https://www.usatoday.com/story/money/2019/07/08/space-race-inventions-we-use-every-day-were-created-for-space-exploration/39580591/>

Highfill, T., Georgi, P., & Dubria, D. (2019, Dec). *Measuring the Value of the U.S. Space economy*. Retrieved from Bea.gov: <https://apps.bea.gov/scb/2019/12-december/1219-commercial-space.htm>

Hitchens, T. (2020, Aug 20). *Commerce Should Take DoD Space Safety Mission*. Retrieved from Breakingdefense.com: <https://breakingdefense.com/2020/08/commerce-should-take-dod-space-safety-mission-study/>

Howells, T., Morgan, E., & Aversa, J. (2020, Jul 6). *Gross Domestic Profit by Industry*. Retrieved from Bea.gov: <https://www.bea.gov/sites/default/files/2020-07/gdpind120.pdf>

Keohane, R., & Nye, J. (1997). *Power and Interdependence* (4th ed.). Pearson Publishing.

Klein, J. J. (2020). *Understanding Space Strategy: The Art of War in Space*. New York: Routledge.

Listes, M. (2018, Mar 17). *CI Scoop: History of Critical Infrastructure Designation*. Retrieved from EAC: <https://www.eac.gov/ci-scoop-history-of-critical-infrastructure-designation/>

Live Science Staff. (2011, Apr 8). *Japan's Biggest Earthquakes*. Retrieved from Livescience.com: <https://www.livescience.com/30312-japan-earthquakes-top-10-110408.html#:~:text=1%20%2D%20Tohoku%20earthquake%2C%202011,largest%20ever%20recorded%20in%20Japan>

Live Science Staff. (2011, Apr 12). *The 10 Biggest Earthquakes in History*. Retrieved from Live Science.com: <https://www.livescience.com/30320-worlds-biggest-earthquakes-110412.html>

Miller, E. (2020, Jul 16). *Space ISAC Welcomed as Member of National Council of ISACs*. Retrieved from s-isac.org: <https://s-isac.org/s-isac-joins-nci/>

Ministry of Defense of the Russian Federation. (2015, Aug 3). Russian Defense Ministry Army General Segey Shoygu Holds Regular Teleconference.

Mnuchin, S. T. (2020, Mar 22). *Memorandum for Financial Services Sector*. Retrieved from aba.com: <https://www.aba.com/-/media/documents/incident-response/Financial-Services-Sector-Essential-Critical-Infrastructure-Workers.pdf>

Moltz, J. C. (2019). *The Politics of Space Security* (3rd ed.). Stanford: Stanford University Press.

Moltz, J. C. (n.d.). The Changing Dynamics of Twenty-First-Century Space Power. 12(1), pp. 15-43. doi:<https://doi.org/10.5038/1944-0472.12.1.1729>

National Council of ISACs. (2020). *About NCI*. Retrieved from nationalisacs.org: <https://nationalisacs.org/about-nci>

Office of Space Commerce. (2020, July 23). *White House Releases Moon-Mars Development Strategys*. Retrieved from Space.commerce.gov: <https://www.space.commerce.gov/white-house-releases-moon-mars-development-strategy/>

Partnership for Conflict, Crime, And Security Research. (2016, June). *The Road to Resilience- Critical Space Infrastructures and Space Security*. Retrieved from Paccs research.org.uk: <https://www.paccsresearch.org.uk/wp-content/uploads/2016/06/The-Road-to-Resilience-Critical-Space-Infrastructures.pdf>

Reidman, D. (2016, May). Questioning the Criticality of Critical Infrastructure: A Case Study Analysis. *Homeland Security Affairs*, 12(3). Retrieved from <https://www.hsaj.org/articles/10578>

Roman, D. (2016). Critical Infrastructure Protection from a Systemic Perspective. *Strategic Impact*(1)

Satellite Industry Association. (2020). *2020 State of the Satellite Industry Report*. Retrieved from <https://sia.org/news-resources/state-of-the-satellite-industry-report/>

Sheetz, M. (2019, May 20). *Space X is the No. 1 rocket company by revenue, with \$2 billion last year, Jefferies estimates*. Retrieved from CNBC.com: <https://www.cnbc.com/2019/05/20/spacex-revenue-2-billion-from-rockets-last-year-jefferies-estimate.html>

Sheetz, M., & Petrova, M. (2019, Dec 15). *Why in the next decade companies will launch thousands more satellites than in all of the history*. Retrieved from CNBC.com.

Space ISAC. (2020). Retrieved from S-Isac: www.s-isac.org

Stockdale, P., Aughenbaugh, S., & Boensch, N. (2018, Feb). Low Cost Access to Space. *Defense Horizons*(83). Retrieved from <https://inss.ndu.edu/Portals/68/Documents/defensehorizon/DH-83.pdf>

Taleb, N. (2010). *The Black Swan*. New York: Random House Trade Publications.

U.S. Census Office. (n.d.). *North American Industry Classification System*. Retrieved from Census.gov: <https://www.census.gov/eos/www/naics/>

U.S. Space Force. (2020, Jun). *Space Power*. Retrieved from Spaceforce.mil: https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf

Union of Concerned Scientists. (2020). *Satellite Database*. Retrieved from ucsusa.org: <http://ucsusa.org/resources/satellite-database#:~:text=In-depth%20details%20on%20the,purpose%2C%20and%20other%20operational%20details>

Vedda, J. (2016, Nov). *National Space Council: History and Potential*. Retrieved from Center for Space Policy: <https://aerospace.org/sites/default/files/2018-05/NationalSpaceCouncil.pdf>

Watson, A. (2019, Nov 27). *Revenue of cable and pay TV providers since 2005*. Retrieved from Statista.com: <https://www.statista.com/statistics/184187/revenue-of-cable-and-pay-tv-providers-since-2005/#:~:text=Revenue%20of%20U.S.%20cable%20and%20pay%20TV%20providers%202005%2D2018&text=In%202018%2C%20cable%20and%20subscription,85.5%20billion%20U.S.%20dollars%20re>

World Nuclear Association. (2020, May). *Fukushima Daiichi Accident*. Retrieved from World-Nuclear.org: <https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident.aspx>