AUGUST 2025

How Can the U.S. Government Safeguard Commercial Satellites from Threats?

By Clayton Swope

Introduction

Though the Founding Fathers could not have anticipated today's global security landscape, they did navigate a complex threat environment with similarities to the twenty-first century. The young United States emerged in a world where state and nonstate actors posed security risks to U.S. commercial and civilian interests both domestically and abroad, leaving a long-lasting impact on U.S. defense policymaking. In the centuries since, in peacetime and war, the United States has repeatedly demonstrated its resolve to protect and safeguard its national equities—its people, territory, economic interests, and national infrastructure—using its combined military power and civil capabilities. There should be no doubt that those imperatives to protect and defend extend into space, no more or less than they extend into other areas beyond U.S. national borders, such as the high seas.

As of 2025, there are **around 10,000** active satellites orbiting the Earth, with the preponderance privately owned. Moreover, over 7,000 satellites are owned and operated by a single U.S. company—SpaceX. Over the next five years, the number of satellites in orbit will likely skyrocket, with tens of thousands of additional satellites—mainly for satellite communications—launched primarily by companies from the United States and China. As the number of satellites in orbits grows, so do the threats they face. The sharp growth in the number of satellites owned and operated by the private sector creates challenges as to how the U.S. government can best protect and defend private sector equities in space.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Fortunately, the United States government has many tools able to help protect U.S. interests in space from foreign and domestic threats that originate from nation-state and nonstate actors. Several agencies and departments, including the military, already perform central roles in those efforts, working to protect space-related elements of critical national infrastructure from physical and cyber threats. Law enforcement and judicial organizations at the federal, state, and local levels, intelligence agencies, and the military have responsibilities to help protect space systems and functions from threats.[1] Private sector operators of space systems share in the responsibility to help protect themselves, particularly by mitigating their vulnerabilities to cyber threats.

> *The federal government already has in place frameworks and policies to help protect commercial space systems, but it could be doing more to address the full spectrum of adversarial threats facing these systems.*

This paper examines the policy foundations and historical precedents from other domains for lessons on how the federal government could help protect and defend commercial space systems, discusses the threat environment confronting commercial space operators, and presents key considerations and recommendations for U.S. policymakers. The paper concludes that the federal government already has in place frameworks and policies to help protect commercial space systems, but it could be doing more to address the full spectrum of adversarial threats facing these systems.[2] The federal government should be thinking about deterring hostile actions against U.S. satellites, helping operators prepare for and respond to threats, and considering how insurance and best practices from other domains can help companies manage risks to their satellites from the increasing threat environment. Ultimately, the best approach to protecting commercial space systems is multilayered, necessitating close cooperation and coordination among government and industry partners.

Types of Threats

Many nations and some nonstate actors have **counterspace** capabilities that can be used both to disrupt and degrade space-based services and to damage or destroy space systems. For this paper, these counterspace tools are organized into four main categories: (1) kinetic; (2) non-kinetic; (3) radio-frequency electronic weapons, which produce effects in the physical world, and (4) cyber operations, which directly affect cyberspace but can also impact the physical world. Kinetic and some types of non-kinetic weapons produce nonreversible effects that damage or destroy hardware and equipment, while radio-frequency electronic weapons typically impart reversible effects, temporarily disrupting and interfering with systems when the capability is activated. Cyber operations can have both reversible and nonreversible effects and be used for espionage and data theft.

---

1 This white paper uses the definition of space system from Space Policy Directive 5 (SPD-5). "'Space system'" means a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service. A space system typically has three segments: a ground control network, a space vehicle, and a user or mission network. These systems include Government national security space systems, Government civil space systems, and private space systems."

2 Natural hazards and accidental collisions are not in scope of this paper, but the dangers they pose to satellites should also be kept in mind.

Kinetic weapons include bombs, bullets, missiles, and other munitions that are used to physically strike targets. This category includes direct-ascent (DA) anti-satellite (ASAT) missiles launched from Earth, such as the ones used by **China in 2007** and **Russia in 2021**. Kinetic weapons also comprise other physical means that can be used for attacks on terrestrial space infrastructure, such as ground stations, launch sites, rocket and satellite factories, critical elements of space-system supply chains, and space monitoring facilities. Orbital grappling satellites that physically handle targeted spacecraft to move them or do them harm are also included in the kinetic weapon category.

Non-kinetic weapons use radiated energy to destroy, damage, or interfere with space systems. This energy can be directed, such as with laser or microwave energy, or distributed through nuclear detonations or electromagnetic pulse (EMP) events. Nuclear detonations in near-space or space are included in this category because these attacks typically damage electronics in spacecraft through radiation and EMP effects. Terrestrial non-kinetic weapons can be used to target spacecraft in orbit. Satellites in space can also be equipped with non-kinetic weapons to target other satellites.

Radio-frequency electronic weapons—which conduct electromagnetic warfare—include systems designed for jamming and spoofing radio signals or other capabilities that use the electromagnetic spectrum to deny or interfere with a target's ability to use space services and capabilities. The Russian **R-330Zh "Zhitel"** is an example of a mobile jammer that is allegedly effective against certain commercial satellite communications receivers. These weapons cannot destroy their targets; they only impart temporary effects as long as the system maintains engagement with its target.

Cyber operations include any offensive cyberspace activity that targets space systems, which include ground infrastructure, satellite terminals, spaceports, and spacecraft. Such operations can destroy or damage equipment, erase code and software, temporarily disrupt access to networks and systems, and conduct espionage and information theft. For example, Volt Typhoon, a state-sponsored actor affiliated with China, has **targeted satellite systems** as part of its activities to pre-position a digital beachhead inside U.S. critical infrastructure so that it could disrupt that infrastructure early in a conflict.

The Current Threat Landscape

In today's world, U.S. and allied commercial satellites face many risks. Some, such as malfunctions, accidental collisions, and space weather events, do not result from malicious intent or action. However, an increasing number of risks stem from nation-states possessing—or developing—capabilities intended to cause harm. For example, in March 2024, Russia **warned** that it would consider commercial satellites that support U.S. military activities as legitimate targets for retaliation. This **followed** a similar warning from Russia in September 2022 concerning U.S. commercial satellites supporting military operations in Ukraine. In February 2022, Viasat—a private global communications company specializing in satellite communications—was the target of a cyber operation attributed to Russia at the start of its invasion of Ukraine, which **impacted** thousands of customers in Europe. The Viasat hack did not, however, target a satellite in space, but rather aimed to disable the modems on Earth relied upon by Ukrainian security forces. Radar images from a European remote sensing satellite **displayed** interference in 2021, though the interference may have been unintentional.

Though attacks on terrestrial infrastructure—such as user modems, ground stations, and launch facilities—can degrade or disrupt access to a space capability as effectively as attacks on systems in

space, this report mainly focuses on threats to satellites themselves. This paper assumes that satellites are exposed to greater or different risks from hostile actors than most infrastructure located on Earth due to several factors. Specifically, satellites

- operate outside of national borders;
- are uncrewed, with no human operator on board; and
- support U.S. government, allied, and partner government and military operations.

It should be noted that satellites are not the only type of infrastructure with one or more of these characteristics. For example, undersea telecommunications cables display the same three characteristics—they operate in extraterritorial locations, have no crews, and support government activities—and, moreover, are increasingly **threatened**. Like undersea cables, communications satellites are part of the United States' critical infrastructure. Though, as in the case of the maritime domain, the U.S. government has not designated the space domain as an official critical infrastructure sector, systems in space provide a variety of services (e.g., positioning, navigation, and timing, communications, and remote sensing) that are themselves included in or integral to the operation of officially designated critical infrastructure sectors.

Every day, the nation's critical infrastructure—especially dual-use capabilities like space systems that support both civilian and national security needs—faces a **constant barrage** of attacks in cyberspace, regardless of the physical location of the infrastructure. Though many of these attacks come from criminal and non-nation-state actors, numerous others come from nation-states. Recognizing their exposure to terrorist and criminal threats, critical infrastructure operators take measures to protect themselves from physical attacks and disruptions even during peacetime. In wartime, this type of infrastructure—such as power plants, manufacturing facilities, and transportation networks—even those located in the homeland, would undoubtedly face kinetic attacks, possibly from long-range missiles or terrorist attacks. The threat picture for satellites, including both physical and cyber threats, looks remarkably like the description of threats facing all critical infrastructure, though satellites are exposed to many of these threats in times of both peace and war.

It is tempting to assume that a decision to attack a satellite would come easier than attacking terrestrial infrastructure as there is no direct threat of death in damaging a satellite in space—as is also the case in cutting undersea cables. General John Hyten, then-head of the Air Force Space Command, **noted** this in 2016, saying: "Satellites don't have mothers." Yet there is no public evidence or historical data to suggest an adversary would sooner launch a missile at a U.S. commercial satellite than at a munitions factory, data center, or undersea cable. If anything, the undersea cable may be the easiest target, as it is more difficult to track undersea activities than those in orbit. Satellites are increasingly vulnerable to these and other **gray zone** attacks.

The U.S. government uses its own satellites, particularly for national security and military purposes, as well as satellites that are commercially owned. Satellites may also face threats because they provide service tied to a conflict zone outside of the United States, even without a direct link to the U.S. government—for example, even without an explicit contractual or procurement relationship with the U.S. government, Starlink would still have likely found itself in Russian crosshairs due to its **provision of service** to Ukraine. In a future conflict, other U.S. space operators may find themselves in an

adversary's crosshairs because of the possibility that they might provide service to the U.S. government, even if they were not currently doing so. This threat scenario is not unique to space. Because they **provide cloud services** to the Ukrainian government, Amazon and Microsoft are vulnerable to the same Russian threat, particularly in cyberspace.

If the threats facing satellites are no different from the ones facing other important infrastructure, there should be no reason for the U.S. government to treat satellites differently when assessing their vulnerabilities and need for defense. In peacetime, no one expects the U.S. government to provide special insurance for a cloud company providing information technology services to the national security community, just as they do not expect such insurance for a power plant providing power to a military base, though the cloud companies face near-constant threats in cyberspace. Cloud service providers and power plants may very well have different expectations during wartime, however. If their assets face sharpened attacks—such as kinetic attacks—cloud providers may call for some form of war-risk insurance or financial indemnification by the government.

> *Throughout its history, the U.S. government has taken special measures to protect certain assets . . . outside of its national territory. Satellites and other space-based capabilities should be similarly protected.*

Throughout its history, the U.S. government has taken special measures to protect certain assets, such as international maritime shipping, outside of its national territory. Satellites and other space-based capabilities should be similarly protected. Recognizing the nature of the threat and the need to protect commercial space capabilities that support its mission, the Department of Defense (DOD) **stated** in its 2024 Commercial Space Integration Strategy that it "will leverage a range of tools across all domains to deter aggression against and defeat threats to U.S. national security space interests, including all space segments and, where appropriate, commercial space solutions." Furthermore, the U.S. government has established an entire agency, the Cybersecurity and Infrastructure Security Agency (CISA), and a **framework**—currently being **reviewed and updated** by the Trump administration—to protect the nation's critical infrastructure. The following section outlines several historical situations in which the United States has provided increased protections for assets in international territories (i.e., outside of the homeland) facing increased threats, discusses the U.S. approach to safeguarding critical infrastructure, and describes how insurance has been used to offer financial protections for companies facing wartime risks.

Historical Precedent

Early leaders of the United States were clear-eyed about the security threats facing the young republic, worrying that the European powers would try to expand their colonial territories at the republic's expense. The Founding Fathers believed that the nation could reach its full potential by using its vast natural resources and agricultural output to play a greater role in global trade and maritime commerce. The **U.S. Navy** was created, not only to defend the United States from invasion by the European powers, but also to protect the nation's commercial interests at sea.

Outside of naval operations, the U.S. government has demonstrated its intention to protect and defend U.S. interests, including private property and citizens, from foreign threats at times of both peace and war. In addition to military responses, the U.S. government has **used tools** such as financial and diplomatic actions to deter and respond to threats, including those in cyberspace, from hostile foreign-state and nonstate actors. The U.S. military has even "imposed costs," which a *New York Times* article **described** as a "term military officials use to describe punitive cyberoperations," in response to cyber attacks targeting U.S. entities. Furthermore, in certain instances, the U.S. government has assumed liability for risks faced by U.S. companies from foreign threats through the provision of war-risk insurance or other financial compensatory arrangements.

NAVY FREEDOM OF THE SEAS MISSIONS

Not long after his inauguration as the third president of the United States, in March 1801, Thomas Jefferson ordered the Navy to confront and stop Barbary corsairs from attacking U.S. maritime commerce off the coast of north Africa. These attacks had begun after Jefferson refused to pay tribute demanded by the governor of Tripoli, ending a practice carried out under the two preceding U.S. presidents. Arguably, Jefferson had been waiting for this moment for a long time, having repeatedly argued that the United States should confront the state-sponsored pirates rather than pay off their leaders. Congress had also been preparing for this development, passing legislation that funded the construction of six frigates that **would be used**, in the event of a war with the Barbary States, to "protect our commerce and chastise their insolence—by sinking, burning or destroying their ships and vessels wherever you shall find them."

Beginning with its operations against the Barbary pirates, throughout the nearly 250 years of its existence, the U.S. Navy has retained the protection of U.S. worldwide seaborne commerce and trade during both times of peace and war as a core part of its mission. Along with allied powers, the Navy protected U.S. merchant shipping across the Atlantic Ocean during both world wars. Since the 1950s, the Navy's mission has expanded to include not just protection of U.S. commercial interests, but also the preservation of economic prosperity and freedom of the seas for U.S. allies and partners. Most recently this has included **protecting** global shipping from Iranian and Houthi threats in the Red Sea. In addition, the Navy **played a key role** in protecting U.S. and global maritime commerce from Somali pirates near the Horn of Africa in the late 2000s. In many cases, including the 2023 creation of the international **Operation Prosperity Guardian** in the Red Sea, the Navy's efforts to protect and defend global shipping involved a **retaliatory response** aimed at deterring future attacks or degrading the military capabilities of hostile actors.

PROTECTION OF CRITICAL INFRASTRUCTURE

Across all domains, national infrastructure is exposed to threats because that infrastructure, including the space-based elements, plays a critical role in the maintenance of U.S. economic and military power. Important infrastructure includes: (1) power generation and distribution systems, (2) telecommunications, (3) gas and oil pipelines and storage facilities, (4) financial networks, (5) water supplies, (6) emergency services, and (7) information technology systems. Beginning in 1996, the United States sought to identify specific critical infrastructure sectors, taking a domain-agnostic approach to identify key functions in need of protection.

With the establishment of the presidential **Commission on Critical Infrastructure Protection** in 1996, the United States began to **consider** the role of the federal government in protecting national critical infrastructure, which is often owned and operated not by federal agencies, but rather by the private sector or by state and local entities. Such an arrangement meant that the federal government's ability to directly influence the security measures taken by infrastructure operators was limited. Therefore, the commission's recommendations **emphasized** increasing voluntary cooperation and coordination with infrastructure operators as means for federal authorities to help infrastructure owners mitigate growing cyberspace threats.

In response to these recommendations, President Clinton **issued** Presidential Decision Directive No. 63 (**PDD-63**) in 1998, which aimed to develop an approach to protect critical infrastructure by 2003. PDD-63 listed eight categories of **critical infrastructure**, also identifying four government functions that needed protection. For each sector, PPD-63 identified one or more federal agencies—later called Sector Specific Agencies and eventually renamed **Sector Risk Management Agencies** (SRMAs)—which would serve as the main interface with the federal government and which would coordinate security and resilience activities for sector members. As part of that role, each SRMA develops and implements a sector-specific plan for protecting and maintaining resilient operations of the infrastructure providers and operators covered under each sector. These sector-specific plans **complemented** an overall national plan, directed by PPD-63, and provide guidance on how federal funding and resources are used to deter threats, protect infrastructure from threats, and respond to attacks and incidents. As part of these efforts, federal officials engage with owners and operators of key assets to help protect them from physical and cyber threats.

Following the 9/11 terrorist attacks, President Bush issued a number of executive orders and directives which touched on issues related to protecting national infrastructure and assets, the **most relevant** being Homeland Security Presidential Directive 7 (**HSPD-7**). Importantly, the directive underlined the central role that the newly established Department of Homeland Security (DHS) would play in efforts to protect critical infrastructure and increase the number of critical infrastructure sectors. HSPD-7 also placed greater focus on protecting infrastructure from physical threats than pre-9/11 directives had, which focused more on threats in cyberspace.

In 2013, President Obama issued Presidential Policy Directive 21 (**PPD-21**) on Critical Infrastructure Security and Resilience, which **emphasized** the need to develop a whole-of-government approach for strengthening and maintaining the security and operation of important national infrastructure. Though it made no major changes to any policies or initiatives begun under the Bush administration, PPD-21 stressed the importance of resilience and protection from all hazards and raised the profile of the energy and communications sectors due to the dependencies of other sectors on energy and communications functions. Established as an organization within DHS in 2018, CISA was given responsibility for the cybersecurity of federal government networks and helping to safeguard the nation's critical infrastructure.

Between 2017 and 2020, President Trump **issued** several executive orders aimed at improving the U.S. posture towards critical infrastructure, with a focus on cybersecurity. The Biden administration provided updated direction for protecting critical infrastructure when it issued National Security Memorandum 22 (**NSM-22**) in April 2024. NSM-22 directed DHS to coordinate "cross-sector risk management and resilience activities" and called for the creation of a list of systemically important

entities whose "disruption or malfunction . . . [would] . . . cause nationally significant and cascading negative impacts to . . . national security . . . national economic security, or national public health or safety." In March 2025, President Trump **issued an executive order** calling for review of NSM-22, as well as other policies related to state and local preparedness, and for the publication of a National Resilience Strategy.

Given the ubiquitous use of and reliance on space for the economic and national security of the United States, space-based capabilities and services play key roles in several designated critical infrastructure sectors. Satellite communications are explicitly identified as part of the communications critical infrastructure sector already. Space launch should be considered part of the transportation critical infrastructure sector. While not focused on space or any single domain, the defense industrial base (DIB) critical infrastructure sector should include space operators and manufacturers who provide services to or build space systems for the military. According to a **GAO description**, the DIB critical infrastructure sector includes any entity that "supplies the military with the means to protect the nation."

The DOD oversees the **DIB critical infrastructure sector**, and is also responsible for developing the DIB sector-specific plan. Last updated in 2010, this plan outlines a layered approach to protecting DIB critical infrastructure. The DIB is responsible for the first protection layer, obtained through compliance with contractual, legal, and regulatory security requirements. As the threat escalates, local, state, and federal law enforcement may be asked to provide additional protection. In serious situations, a state governor may employ the National Guard, either using state authorities and funding or, if approved by the president or the secretary of defense, **Title 32, section 502(f)** status. Finally, should these protections prove insufficient, the president can direct U.S. military forces to protect DIB critical infrastructure and key resources.

The DIB plan specifically notes that DIB functions are critical to military operations during times of peace, crisis, and war, which presumes a requirement for protection at all times. Additionally, the plan directs and describes the creation of an asset priority list, which is updated annually and is used for allocating protection resources. The **deputy assistant secretary of defense for defense continuity and mission assurance** manages all funding and programs aligned toward protecting DIB critical infrastructure and key resources. Government partners engage with the DOD on the sector-specific plan through the Government Coordinating Council, while industry partners engage through the Sector Coordinating Council.

Outside of its role in protecting the DIB from threats, the DOD has stated its intent to take certain measures to protect and defend commercial space systems, noting in its **Commercial Space Integration Strategy**: "In appropriate circumstances, the use of military force to protect and defend commercial assets could be directed." Furthermore, the strategy states that the DOD will "promote the security of commercial solutions through three lines of effort: norms and standards, threat information sharing, and financial protection mechanisms."

U.S. GOVERNMENT ACTIONS IN CYBERSPACE

In December 2021, Gen. Paul M. Nakasone, then-head of U.S. Cyber Command, publicly **acknowledged** that the U.S. military had taken actions against ransomware groups that had been targeting U.S. organizations. Nakasone said that prior to the cyberattacks on the Colonial Pipeline in May 2021 and

the JBS meat plants in June 2021, the federal government would have considered ransomware attacks the responsibility of law enforcement organizations. But because these attacks have been "impacting our critical infrastructure," Nakasone **indicated** a decision had been made to take a different approach. Additionally, in November 2021, a major ransomware organization **shut down** after reportedly being jointly targeted by Cyber Command and a foreign government. Prior to the 2020 presidential election, Cyber Command reportedly **conducted** an operation against a cyber threat actor called TrickBot, due to concerns about voting disruptions.

Cyber Command's alleged actions in these instances would seem to reflect Gen. Nakasone's strategy of **defending forward** and, if true, may signal increased military involvement in protecting U.S. interests from criminals and nonstate actors in cyberspace. Though these developments indicate increased military involvement in U.S. responses to criminal hackers, private sector partners have also cooperated on cyber operations. For example, Microsoft and the Justice Department, including the FBI, worked together on cyber operations aimed at disrupting malicious cyber threat actors, such as the **GameOver Zeus** botnet in 2014. More recently, in August 2023, the FBI removed malware from more than 700,000 computers around the globe to **disrupt** a botnet called Qakbot that facilitated ransomware cybercrimes.

The U.S. government has also attempted to disrupt state-sponsored hackers. In September 2024, employing a court order, the FBI seized control over hundreds of thousands of routers and other connected devices that were **being used** by Chinese state-sponsored hackers for cyber operations against U.S. critical infrastructure. The next month, the Department of Justice, working with Microsoft, **acted against** dozens of internet domains used by Russian intelligence agencies and their partners to target U.S. government agencies and companies with spear-phishing campaigns.

WARTIME MARITIME CONVOYS

Almost immediately after the U.S. entry into World War I, the U.S. Navy began participating in convoys protecting maritime commerce crossing the Atlantic Ocean. The Navy assumed nearly identical escort duties for transatlantic allied shipping during World War II. In both cases, the convoys protected primarily British, Canadian, and U.S. wartime shipping—transporting cargoes of soldiers and goods that were vital to the overall war effort—from German U-boat threats.

WAR-RISK INSURANCE

For over two centuries, **war risk was considered** one of many normal hazards associated with maritime transportation. Though previously included alongside coverage for fire and other risks at sea, starting around 1840, war risk was no longer automatically included in maritime risk insurance policies. In fact, insurers began to charge extra for insurance that covered war risk, noting the increased costs of ships and the goods they carried. In 1898, England's main insurer, Lloyd's of London, removed war-risk coverage from its standard maritime risk contract, creating a domino effect whereby major insurers in France, Italy, and the United States followed suit. Insurers, however, continued to offer war-risk insurance for maritime transportation as a policy separate from their standard contracts.

The onset of German U-boat warfare targeting commercial shipping in World War I caused maritime war-risk insurance premiums to skyrocket, making such coverage unaffordable for many shipping companies. Stepping in to ensure that U.S. maritime transportation firms could obtain affordable

coverage, Congress passed, and the president signed into law, the **War Risk Insurance Act of 1914**, which established a new bureau in the Department of the Treasury to issue insurance policies and pay claims. In 1917, the law was amended so that the program could also provide life insurance policies for U.S. merchant marines.

During World War II, the U.S. government again played a role in underwriting risk for merchant ships facing threats from German U-boats, **creating** an organization called the War Shipping Administration to handle maritime and war-risk insurance. At the conclusion of the war, the U.S. government sought to end its role in providing maritime insurance, though it retained authority to resume coverage during a future conflict or crisis. This meant that responsibility for providing maritime risk insurance rested solely with private sector underwriters, who continued to offer war-risk policies separate from their usual maritime risk contracts.

In 1949, leading insurance companies in the United States and the United Kingdom made it clear that they would stop issuing maritime war-risk insurance at the outbreak of another major war. This assertion eventually evolved into what became known as the **five powers war clause** within insurance policies, which "excludes [coverage for] loss, damage, liability, or expense arising from the outbreak of war—whether there be a declaration of war or not—between any of the following: United States of America, United Kingdom, France, the Russian Federation, the People's Republic of China." With minor changes, this clause remains in effect in 2025 for maritime risk insurance issued by U.S. underwriters, leaving open an opportunity for U.S. government assumption of risk in the event of an outbreak of war with Russia or China.

Even without a trigger to the five powers war clause, the U.S. government has used its authorities to insure merchant ships and sailors supporting U.S. actions in Vietnam, Haiti, and Iraq between 1975 and 1999. Additionally, President George W. Bush **approved** the issuance of government war-risk insurance for ships, cargo, and sailors "entering the Middle East region" in support of U.S. counterterrorism efforts if the commercial market did not offer reasonably-priced options. Later, in 2008, President Bush **approved** government-backed war-risk insurance for vessels supporting humanitarian operations in the Black Sea following Russia's invasion of Georgia.

In 2025, because maritime transport often faces risks associated with conflict around the globe, it is common for shipping companies to purchase war-risk insurance from commercial underwriters. Sometimes, such policies are **offered** through specialized entities and consortia. In times of conflict, the premiums for such coverage in certain geographical areas may significantly increase. The clause allowing the increase, named **NMA464**, states that:

> Notwithstanding anything to the contrary contained herein this Certificate does not cover Loss or Damage directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power, or confiscation or nationalization or requisition or destruction of or damage to property by or under the order of any government or public or local authority.

The DOD **Commercial Space Integration Strategy** addresses financial risks to satellite operators that support national security missions. The strategy lists the types of financial protection mechanisms that

could be available to operators, such as commercial insurance, commercial war-risk insurance, and U.S. government-provided insurance. Additionally, the document notes that the U.S. government has legal authority to indemnify companies doing business with government for damages **caused** by "unusually hazardous or nuclear risks" under **P.L 85-804**.

Though the U.S. government does not currently operate any programs providing government-backed insurance to commercial space operators, it does operate such programs for the air and maritime domains. With the approval of the president, the secretary of transportation has statutory authority to **provide** government-backed marine, war-risk, and liability insurance. Using this authority, the Maritime Administration's Voluntary Intermodal Sealift Agreement (VISA) **program** can provide non-premium government war-risk insurance to VISA participants when "commercial war risk insurance is not available on reasonable terms and conditions." The secretary of transportation also has **authority** to offer insurance for aircraft "owned or chartered by, or made available to" the U.S. government. This authority is used by the U.S. government to provide indemnification and liability **coverage** for commercial aircraft activated in support of the DOD's Civil Reserve Air Fleet program. The DOD is modeling its Commercial Augmentation Space Reserve (CASR) on these programs and is **considering offering** CASR participants access to U.S. government-back war-risk insurance.

Key Considerations

When facing threats from hostile foreign actors, there are a few things that the U.S. government could do to safeguard the interests of commercial satellite operators, taking cues and learning lessons from precedents in other domains. Firstly, the U.S. government should consider how to deter and respond to threats against satellites. Secondly, it can help satellite operators better secure and protect their own assets using resources available for the protection of critical infrastructure. Thirdly, the U.S. government should consider how it could facilitate mechanisms, such as insurance, that would help ensure that satellite operators are compensated for any losses incurred due to hostile actions against their satellites—the DOD is already thinking about this issue as part of the CASR initiative.

DETERRING (AND RESPONDING): CONSEQUENCES FOR HOSTILE ACTIONS AGAINST SATELLITES

The 2020 National Space Policy **states** that "any purposeful interference with or an attack upon the space systems of the United States or its allies that directly affects national rights will be met with a deliberate response at a time, place, manner, and domain of our choosing." Consistent with this policy, because Russia invaded Ukraine and subsequently threatened commercial satellites that support Ukraine's military efforts, the United States has said that it would **respond** to attacks on commercial satellites. On at least one occasion, a senior official **stated** that attacks on U.S. satellites—commercial or military—could provoke a military response. Similarly, in 2021, NATO leaders **announced** that attacks in space could lead to the invocation of **Article V**, a key element of the North Atlantic Treaty emphasizing that an attack on one NATO member will be treated as an attack on them all. However, it is not clear how strongly the U.S. government would respond to attacks on government satellites, let alone **attacks** on commercial ones. Moreover, as noted above, there is a wide spectrum of possible attacks, including through physical, electronic, and cyber means, complicating any effort to develop a one-size-fits-all response.

> *Failure to match action to rhetoric would undermine deterrence and embolden hostile actors to strike against U.S. satellites.*

In 2025, there is little public evidence—or indications of potential hostile actors' involvement—pointing to specific actions the United States would take in response to nation-state or non-nation-state attacks against U.S. satellites. Clarity on how the United States and its allies would respond to certain types of attacks on their commercial and government satellites would help deter hostile actions against those assets. A response need not occur in space and could be taken in other domains, including in cyberspace. Nor does the response necessarily have to be a military one, though it should be clear as much as possible which types of attacks against U.S. satellites would provoke a military response, as opposed to a law enforcement, diplomatic, or economic one. If the United States decides to make clear the types of actions it may take in response to certain attacks on satellites, it should not hesitate to take those measures in the event of an actual attack. Failure to match action to rhetoric would undermine deterrence and embolden hostile actors to strike against U.S. satellites.

As an example, one response to an attack against a satellite might be the use of a capability to actively stop or disable an attacker. Though there has been very little public discussion among U.S. and allied officials about developing and deploying technologies that can actively protect and defend satellites from physical attacks, there are exceptions. In September 2024, for instance, French defense officials **outlined plans** to build a demonstration satellite that can target other satellites in space. Though the satellite would not possess kinetic weapons, it might include a laser-dazzling capability, which could be used to respond to attacks on other satellites, as well as perform offensive actions. While this system is being developed for operation by a nation-state, commercial satellite operators may also want to deploy similar systems, such as dazzlers or signal jammers, that could protect their satellites from hostile kinetic or electronic attacks from other satellites. Commercial operators taking such measures would be akin to "**hacking back**" in cyberspace, a concept that has been debated but not sanctioned by the U.S. government and which would permit private sector entities to "fight back" against cyber intruders in their networks. Already, companies are developing **what appear** to be commercial counterspace capabilities.

SECURING AND SAFEGUARDING: APPROACH TO CRITICAL INFRASTRUCTURE

Following the Russia-Ukraine conflict, the Biden administration took a particular interest in coordinating national efforts to protect federal and private sector space systems from nation-state cyber threats. President Biden's **January 2025 cybersecurity executive order** articulated minimum cybersecurity requirements to protect federal space systems and outlined ongoing national-level space cybersecurity work. As part of its agency-level strategy to secure space systems and services, DHS has **outlined three** main lines of effort: (1) promoting cybersecurity planning for space systems, (2) mission assurance planning and execution for homeland security, and (3) contingency planning for impacts to the homeland from denied or degraded space environments. Central to DHS's goals, and cutting across all three lines of effort, is information sharing among the federal government; state, local, tribal, and territorial governments; and the space industry. Prior to the **termination** of the Critical Infrastructure Partnership Advisory Council (CIPAC) by the Trump administration, the CIPAC Space Systems Enterprise Critical Infrastructure Working Group (SSCIWG) had been the main avenue for DHS,

in conjunction with industry partners, to develop and disseminate policies and frameworks aimed at improving the security and resiliency of space systems.

Despite the above efforts, experts note a **lack of clarity** in many allied countries, including in the United States, about which agency is responsible for preventing and responding to cyber-attacks against space systems. In addition to agency-specific efforts like the SSCIWG, the **Space Information Sharing and Analysis Center** (ISAC) and the **National Defense ISAC** facilitate coordination between government and industry partners and provide cyber and physical threat information sharing to space companies. While these organizations can play critical roles, they are not government entities, but rather private sector organizations that may require private sector participants to pay membership dues to obtain threat information and data.

In 2022, DHS **started** the State and Local Cybersecurity Grant Program and the Tribal Cybersecurity Grant Program. Modeled after the Homeland Security Grant Program, the programs will have awarded around $1 billion to help state, local, tribal, and territorial government organizations improve their cybersecurity by 2026. Companies, however, are not eligible subrecipients of this grant funding, so commercial space operators would not have access to these federal resources. Arguably, this is not a unique limitation to space operators; private sector entities writ large are not eligible to receive grant funding from these programs.

This funding restriction speaks to the overall U.S. government approach toward protecting private sector critical infrastructure, including satellites. DHS, including CISA and the sector-specific plans to protect critical infrastructure, are focused on developing relationships with and disseminating information—including threat sharing—to private sector entities. DHS does not provide funding to private sector organizations to improve their security postures. Ultimately, this government approach is about enabling private sector partners to improve their own security postures, so that they can better defend themselves, using their own resources. But the U.S. government has and should continue to play an **active role** in protecting and defending infrastructure from threats. All DHS resources available to strengthen the cybersecurity of space systems and to improve threat sharing to the private sector should be fully utilized. To that end, the government should help clarify how commercial space operators engage with DHS and, furthermore, should develop a streamlined government-run interface and coordination mechanism.

While deliberating the Biden administration's policy update (NSM-22), federal departments and agencies extensively discussed whether to designate space infrastructure under a new seventeenth sector with an assigned SRMA—an option they ultimately decided against. Some **experts believe** such a designation could help address current coordination challenges across federal and industry space operators, while **others** argue sector designation might introduce coordination and regulatory burdens. In its review of federal policies aimed at protecting critical infrastructure, the Trump administration may again raise the question of whether space should be designated as its own critical infrastructure sector.

COMPENSATING FOR LOSSES: AVAILABILITY OF INSURANCE

The types of insurance products available for satellites are significantly more limited than those generally available for systems and infrastructure in non-space domains. Though insurers offer

coverage for satellites, they do not offer war-risk policies for satellites. Part of the issue—applicable also to cyberspace due to the lack of **agreed-to definitions** for cyber war and cyber terrorism—is the absence of an accepted vocabulary describing war in space and hostile actions against space systems. Without common terms and definitions that relate to war and other hostile acts against space systems, it is difficult for insurers to accurately assess and determine their exposure to risk and reasonably set insurance rates. Establishing a common language with respect to counterspace and space weapons, hostile acts against space systems, and the range of effects on those systems would help space operators, insurers, and government organizations better understand and define the scale of possible claims in the event of war from space operators.

Comprehending the scale of possible claims and the likelihood of certain types of hostile actions against space systems could create the foundation for a satellite war-risk insurance model wherein companies obtain private insurance up to a certain amount of damages, and the United States assumes liability for damages above that amount. This approach would somewhat mirror the existing third-party liability insurance framework for commercial launches in which the U.S. government requires launch providers to purchase a certain amount of insurance, with the government assuming liability beyond that amount up to a certain cap. As with maritime war-risk insurance, space war-risk insurance could also cover the equivalent to "hull" losses in the marine industry, be they physical losses or damages to the insured spacecraft themselves.

Any agreement between insurers and the U.S. government to share liability should address whether commercial insurers would continue issuing new war-risk policies during an actual war, or if insurers would cease issuing new coverage during wartime. To answer this question, the government and private sector would need to establish an agreed-upon understanding of what constitutes wartime, potentially specifically defining war in space or war against space systems. During actual wartime it may not be reasonable to ask a private sector insurer to issue new wartime coverage, as this would be akin to an insurer offering a fire-risk insurance policy for a structure already in the path of an approaching wildfire. Due to the increased likelihood and large scale of potential damage during wartime, the government may need to assume some level of risk, similar to its role during both world wars for marine insurance, at a minimum for the issuance of new policies.

Ultimately, the primary impediment to the development of commercially available space war-risk insurance is the lack of market interest from space operators in buying such insurance, with many operators forgoing even basic insurance, let alone liability coverage. Users (e.g., customers) of space-based services could also decide that they are willing to pay for some type of war-risk insurance. As with maritime war-risk insurance, however, space war-risk insurance would probably come at a significant cost, one that many space companies are likely to consider too high. But without work to identify agreed-upon definitions around space war and hostile acts against satellites, it is difficult to price space war-risk insurance with a degree of accuracy. Should there be market interest in space war-risk insurance, the first step ought to be to develop a common vocabulary and then determine a way to assess and price risk to satellites.

Conclusions

Both government and commercial satellites face a plethora of threats in space from nonstate actors and from nation-states. There are many precedents for the U.S. government, using law enforcement tools, homeland security resources, or military actions, to protect, safeguard, and defend important national assets, infrastructure, and networks on U.S. soil and in territory around the world. In most ways, satellites are no different from other elements of the nation's critical infrastructure and, like other infrastructure, serve government customers. And there are government resources available to help critical infrastructure prepare for and address threats.

But having the government actively defend commercial satellites would be something different. There is little clarity on how the U.S. government would respond to attacks on U.S. satellites, which makes deterring attacks on satellites difficult. There are also no insurance products covering war risks to satellites, meaning that operators are left holding all the risk should their systems face wartime threats.

The U.S. government has a role in establishing deterrence, making clear the response to hostile actions against U.S. satellites, and possibly subsidizing space war-risk insurance, especially providing new coverage needed during an actual war. The government should also work to clarify how satellite operators interact with the federal officials and organizations charged with safeguarding U.S. critical infrastructure, ensuring operators are engaged with the right resources, as part of its review of federal critical infrastructure policies. Commercial operators, too, must help themselves and seek out resources and convenings to stay cognizant of the latest threats. First and foremost, they should be willing, like the maritime industry, to pay for wartime risk insurance. Ultimately, protecting and defending the nation's commercial satellites and space infrastructure is a team sport—both industry and the government have roles to play. ■

Clayton Swope *is the deputy director of the Aerospace Security Project and a senior fellow in the Defense and Security Department at the Center for Strategic and International Studies (CSIS) in Washington, D.C. He previously served as a congressional staffer and at the Central Intelligence Agency.*

The author would like to thank Chris Kunstadter, John Plumb, and Lauryn Williams for their time and advice. Their expertise and insights greatly improved the final paper.

This white paper was made possible through general support to the Aerospace Security Project.