Protecting Space Assets from Irregular Threats

Expanding the Scope of Space Risk Detection to Include Non-State Actors and Criminal Organizations

Abstract: As space continues to grow in importance as a commercial and national security domain, the US military and intelligence community (IC) have recognized the need to defend space assets from an increasingly broad and sophisticated range of threats from adversary nations. Countermeasures include threat detection across cyber and kinetic attack surfaces. The increasing role that space plays in economic and national security terms, however, also heightens the risks posed by non-state actors and criminal organizations. This paper explores the issue and offers an approach to detecting and mitigating threats of space crime and piracy using integrative system architectures and technologies, including artificial intelligence (AI).

Contact: Hugh Taylor, Director | The Center for the Study of Space Crime, Piracy, and Governance | hugh@cscpg.org | (310) 383-7041

INTRODUCTION

The US military and intelligence community (IC) have recognized the need to defend space assets from an increasingly broad and sophisticated range of threats from adversary nations. Countermeasures include threat detection across cyber and kinetic attack surfaces. As space grows in importance as an economic and national security domain, however, stakeholders also plan for risks posed by non-state actors and criminal organizations.

These entities may act independently for their own private gain, but they could also function as deniable agents of disruption working covertly for adversary nations. The history of piracy on the high seas offers many examples of this form of stealthy geopolitical aggression. This paper explores the issue and offers some suggestions on how the IC and others could benefit from new modes of cooperation. By leveraging new integrative system architectures and technologies like artificial intelligence (AI) to expand the scope of risk detection, stakeholders can improve their ability to respond to irregular threats to space assets, national security, and the broader space economy.

CURRENT SPACE RISK SCENARIOS

As the space industry grows towards a projected $1.8 trillion in revenue within a decade,[1] there is a growing awareness that attacks on its assets would have serious repercussions on critical infrastructure, the economy, and national security. A cyberattack that impairs an intelligence satellite, for example, could weaken the United States' readiness in wartime. Long-term national economic and military strategies that rely on space superiority are also at risk. Concerned stakeholders include space businesses, the aerospace and technology firms that support them, the military, and the IC.

The National Counterintelligence and Security Center (NCSC), which is part of the US Office of the Director of National Intelligence (DNI), spoke to this concern when it issued a warning bulletin in 2023. Titled "Safeguarding the US Space Industry," the bulletin calls attention to threats from foreign intelligence entities (FIEs). Risks include disruption of space operations, along with the loss of intellectual property that enables the US to stay ahead of its adversaries in space.

As reported in Space.com, the NCSC bulletin "offers a set of guidelines to help private companies mitigate any potential damage these espionage attempts might cause." Specific suggestions run the gamut from vetting suspicious insiders to being cautious about foreign companies that want facilities tours and joint ventures. The bulletin also recommends developing an "anomaly log" to "track peculiar incidents to potentially spot malicious trends against your organization."[2]

Writing on this subject for the Center for Strategic and International Studies (CSIS), USAF Major Generals Brian Garino and Jane Gibson expand the scope of awareness of threats to space assets. In "Space System Threats," Generals Garino and Gibson underscore the risks facing

[1] McKinsey & Company, "Space: The $1.8 trillion opportunity for global economic growth", 2024
[2] Tingley, Brett, "Spies and hackers are targeting the US space industry", *Space.com*, August, 2023

military capabilities and space operations. They also highlight how threats to space can occur in more earthly domains.[3] Malicious actors could target ground segments, uplink infrastructure, computer networks, and launch facilities. In their view, kinetic threats deserved attention, along with cyber. Their focus is on threats from nation state actors and FIEs.

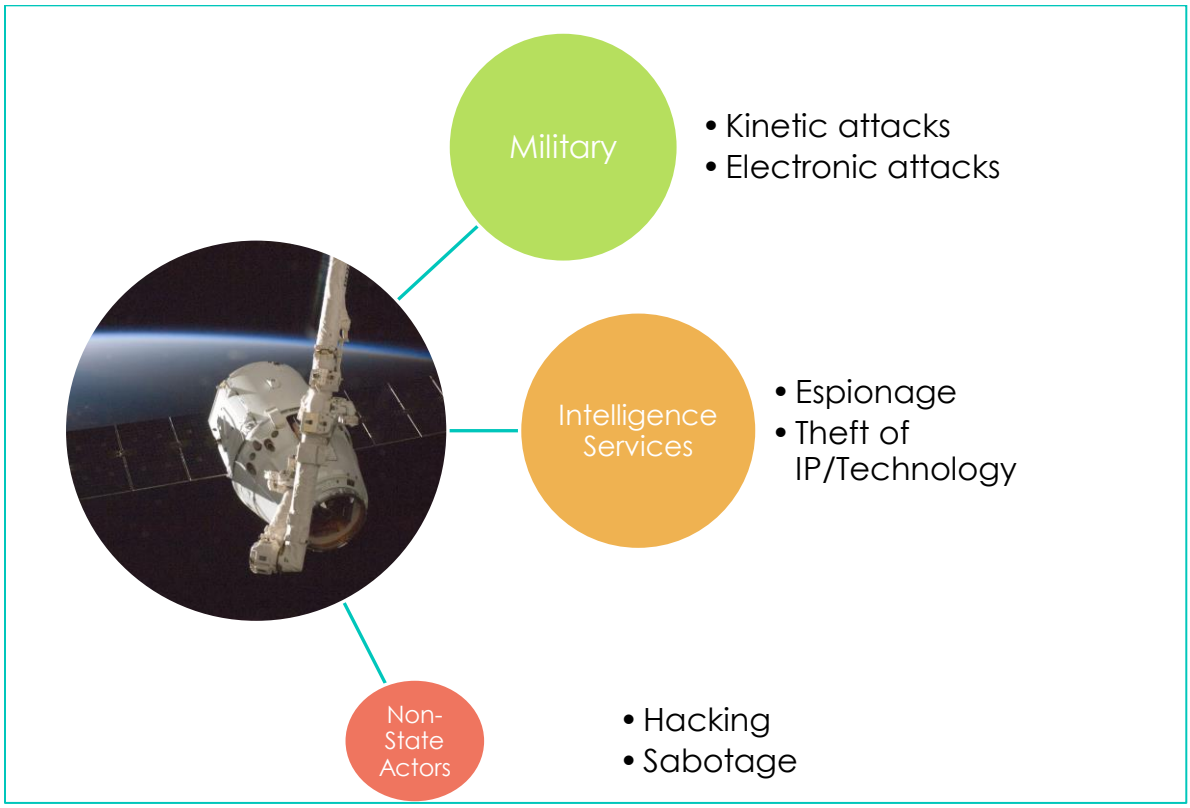

Figure 1 - The main threat actors in space today. (Photo by SpaceX)

As of today, there are two primary types of threat actors: military and intelligence services, often overlapping in terms of mission and operations. Figure 1 depicts this dynamic, with the military preparing to engage in kinetic and electronic attacks on space assets and intelligence services engaging in espionage related to space, and theft of space intellectual property. Non-state actors, such as hacking gangs based in foreign countries, are a present threat to space assets. They may or may not be connected to nation states.

[3] Garino, Brian (Gen USAF), and Gibson, Jane (Gen USAF), "Space System Threats", Center for Strategic and International Studies (CSIS), 2018

CURRENT SPACE RISK MITIGATION PROGRAMS

A great deal of effort is going into mitigating threats to space assets. The U.S. Space Force plays a key role in this work, as do each of the service branches and various intelligence agencies. The Space Force itself is a member of the IC. The private sector has its own security infrastructure, including cybersecurity programs and corporate security teams that work to prevent, detect, and respond to threats.

Many of these entities come together in the Space Information Sharing and Analysis Center (ISAC). The Space ISAC's mission is "to facilitate collaboration across the space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats." In this, the Space ISAC is similar to other ISACs, which operate in sectors like critical infrastructure, aviation, maritime, the chemical industry, and others. ISACs play an important role in risk mitigation because they enable fast, streamlined sharing of threat information between entities that may not normally communicate with one another.

In the Space ISAC, tech companies like Microsoft share threat intel with organizations like MITRE and Aerospace Corporation, along with aerospace vendors like Northrop Grumman and Lockheed Martin. This way, for instance, if Microsoft discovers a vulnerability that could put a ground station's computer systems at risk, they can quickly circulate information about the vulnerability so affected parties can remediate it.

The Space ISAC addresses itself to risks affecting operational technology, business systems, and missions. They look at the technology supply chain supporting these areas of activity, too. This helps its members identify and respond to threats that may be lurking deep in the software and hardware they use to power their operations. The process might include scanning code to spot malware embedded in open-source software (OSS) used to support space missions.

APPARENT GAPS IN CURRENT RISK MITIGATION PROGRAMS

It's difficult to say for sure how well risk mitigation programs like the Space ISAC and others are doing in their respective missions. On the one hand, there hasn't been a major space hacking incident or comparable disruption. On the other, it's not easy to know what they're up to. Their work is not public. Most countermeasures against space threats are classified, and it's probably best that this remains the case.

Based on a review of public information about risk mitigation programs, coupled with interviews with subject matter experts, it appears there are gaps in the defense of space assets. This is not a criticism of the current approach. Rather, it is an acknowledgement that existing systems and methods for risk mitigation are designed to focus on a narrow range of threat actors and a limited set of risk scenarios.

The bad actors are assumed to be nation states, e.g., Russia attempting to disrupt American satellites. The risk scenarios now being contemplated are those that impair space systems' functioning for purposes of geopolitical aggression. This is probably adequate for today's threat

landscape. In the near future, though, risk mitigation will be deficient if it does not address new classes of malicious actors and tactics:

- Acts of space piracy or disruption of ground systems committed by non-state actors, e.g., criminal cartels hijacking commercial satellites for ransom. Such attacks would likely extend far beyond mischief making or small-scale hacking for profit. Rather, they might involve the use of the most sophisticated technologies for exploits of sustained and significant scope.
- Money laundering involving space assets and space commerce, exploiting lax oversight and incomplete definition and enforcement of law in space.
- Smuggling of space commodities to avoid taxes or sanctions.
- Kidnapping of space tourists.
- Theft of space equipment, e.g., lunar mining robots.
- Theft of space cargoes.
- Ransoming of earth-based businesses that rely on satellites by space pirates, e.g., SatCom for aviation and commercial shipping.

Who might be committing such acts? They could be criminal organizations or violent non-state actors like terror groups which are in need of funding for their operations. Rogue insiders, such as employees of space agencies in economically challenged countries, could provide the know-how. Insiders might also emerge from the ranks of well-trained space forces and space industries in highly developed countries. Just as some former American military officers find employment with criminal cartels today, technically skilled space personnel could engage in similar illegal activity for profit.

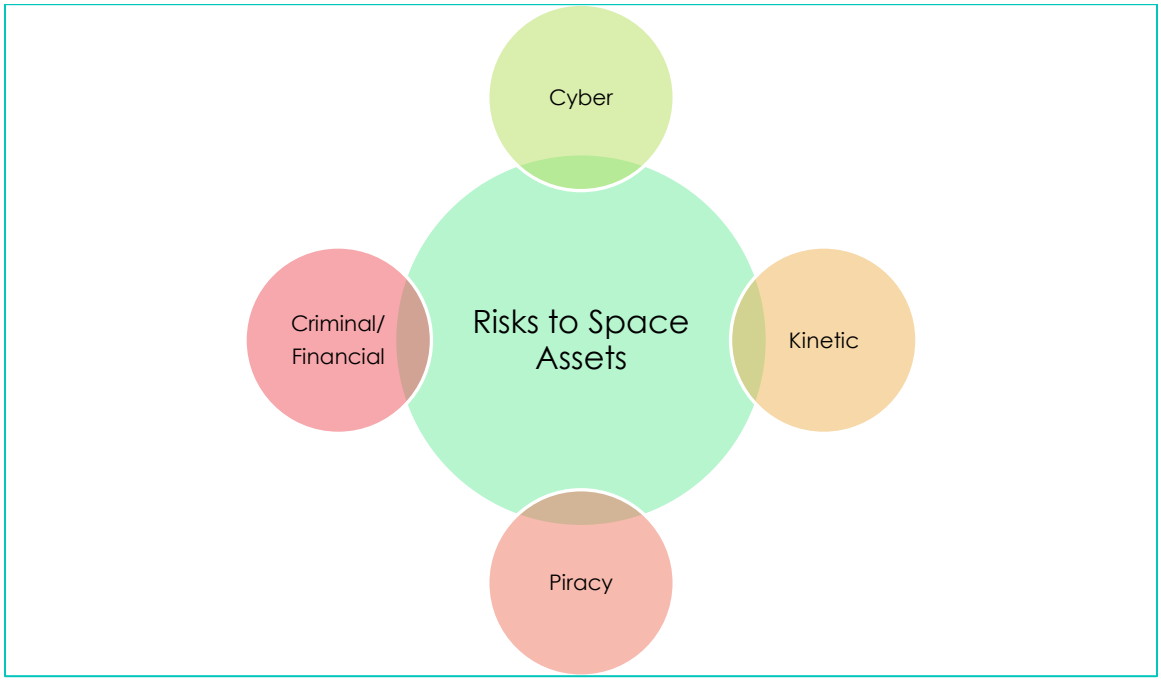

Figure 2 – In the future, it is likely that space assets will face risks of piracy and criminal/financial crimes in addition to existing cyber and kinetic risks.

Figure 2 depicts the four types of threats that pose risks to space assets. In addition to kinetic and cyberattacks, which are under the purview of today's risk mitigation methods and organizations, it would be wise to consider criminal/financial attacks and piracy.

Piracy in space might follow the template of piracy's historical role on the high seas: as a deniable form of attack used by nation states. In the "golden age" of piracy in the 17th and 18th centuries, for example, England utilized privateers, who were pirates acting with permission of the British crown, to plunder Spanish treasure galleons in the Caribbean. The results were devastating to Spain. The American revolution saw similar activities by American privateers operating against British vessels. We may witness such irregular warfare tactics in space.

Pushing further out into the future, the risk of piracy could affect lunar colonies and space-based commercial enterprises such as asteroid mining. Pirates could become key players in the commercial development of asteroids, Mars, and other planetary platforms. If history is any guide, pirates could actually be governing such enterprises, perhaps behind the scenes.

THIS IS A SOMEWHAT FUTURISTIC PROBLEM

Crime and piracy in space are admittedly not a serious problem today. Cyberattacks are affecting space assets today, but they are relatively rare. This is likely to change as satellites and other space systems shift from proprietary technologies and adopt more open architectures and commercial off the shelf (COTS) computer hardware and software, e.g., the Linux operating system. These technologies are more vulnerable to attack than the proprietary predecessors.

Space cyberattacks may feature non-state actors, but as of now, their impact is limited in scope. As the space industry grows, however, and becomes more economically critical to nation states, crime and piracy are likely to follow. World history bears out this prediction. Wherever valuable cargoes transit narrow passages, there will be piracy. Space meets this criterion. Despite its apparent vastness, desirable orbits and lunar landing spots are quite small and easily disrupted for gain.

THE NEED FOR AN EXPANDED SCOPE OF THREAT DETECTION

Futuristic or not, the risks of space crime and piracy deserve attention. Tomorrow's problem requires solution planning today. Now is the time to start thinking about ways to detect, prevent, and respond to space crime and piracy.

What will it take to succeed? To mitigate the looming risks of space crime and piracy, it will be necessary to expand the scope of threat detection and response from where it stands today. This will involve, to a great extent, a change in mindset about what constitutes a threat and whom those threats affect.

The future space threat landscape will be broader and more irregular than the one we face today. Figure 3 offers a glimpse at the potential for new threat actors on the scene. Space assets

are likely to face threats from criminal organizations, non-state actors, and space privateers. There is also the potential for criminals to hijack a seemingly legitimate corporation, such as an orbital servicing firm, for the purpose of space crime. The 2019 seizure of $1.8 billion in cocaine from the MSC container ship Gayane, which was crewed by members of a Montenegrin gang,[4] offers an example of how this risk may manifest in space.

Some current stakeholders are skeptical of the prediction that criminals will make their way into space any time soon. They suggest that the costs are too high, and the technological barriers are too steep for even large and sophisticated criminal organizations. The story of the MSC Gayane reveals the flaw in this argument. The drug smuggling gang didn't need to buy or build the ship. They simply took it over. Terror attacks like 9/11 also show that attackers need not own, or even understand the technology they use to commit criminal acts. Space piracy may follow a similar path, with criminal groups infiltrating space corporations and using their expensive assets for criminal purposes.

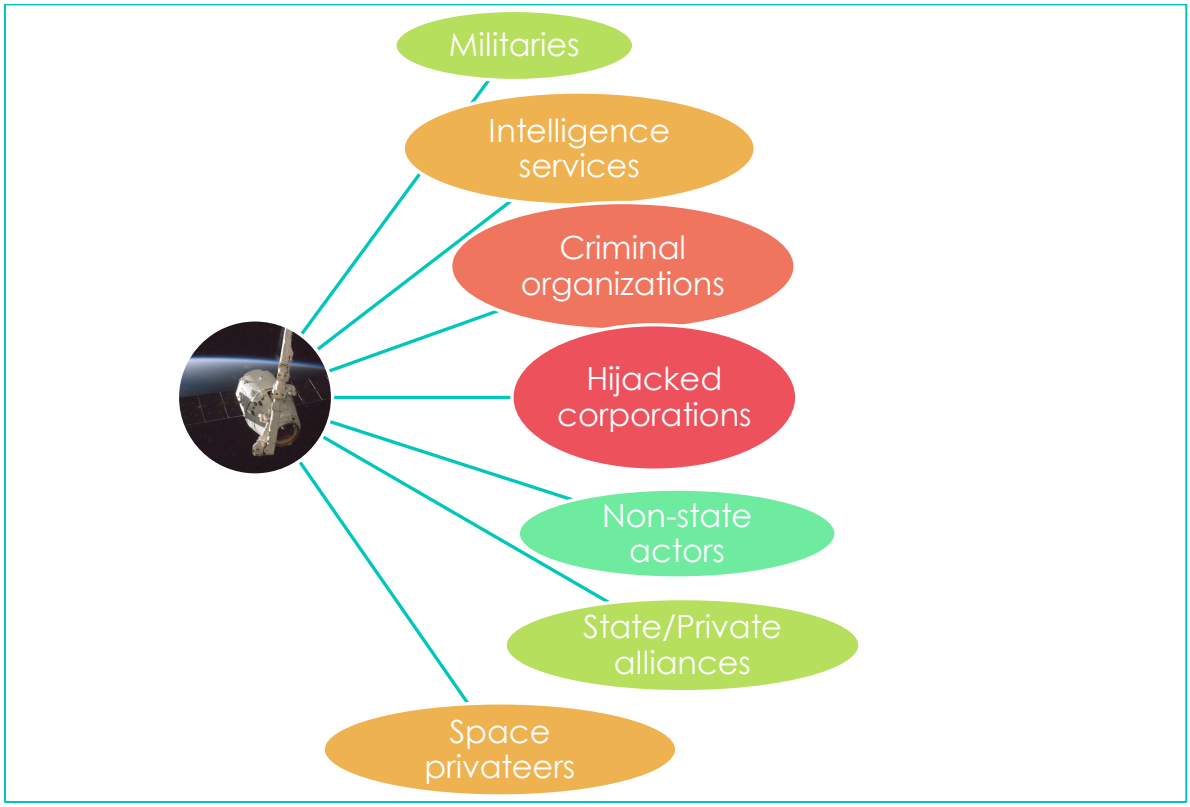

Figure 3 – The number and variety of threat actors posing risks to space assets is like to grow in the future, including hijacked corporations, space privateers, state/private alliances, and criminal organizations.

With more attackers and new types of threats comes a need to involve more stakeholders in risk detection and mitigation. In addition to cybersecurity teams and members of the military and

[4] Miller, Greg, "Case closed: How drug ring hid $1B worth of coke on a single ship" *FreightWaves.com*, September 2, 2021

IC, it will be insurance companies, law enforcement agencies, financial institutions, and government agencies who must also track and respond to space threats.

For example, the Commodities Futures Trading Commission (CFTC) may need to get involved in monitoring illegal handling of lunar minerals. Financial institutions that handle securities for space corporations may have a compelling need to stay abreast of risks affecting their investments, and so forth. Figure 4 shows the range of stakeholders who will be engaged in the work of space risk detection and mitigation.

Figure 4 - The evolving and growing set of stakeholders who should be concerned about the risk of piracy and crime in space.

MAKING SPACE THREAT DETECTION WORK IN A COMPLEX WORLD

It will be challenging to operationalize a threat detection system of the breadth and depth required to mitigate the risks of space crime and piracy for all stakeholders. Yet, it is essential. As a recent article in *Mother Jones* described the challenges of assessing the probability of someone committing a mass shooting, "You can't connect the dots if you don't collect the dots."[5]

Collecting the dots for space crime and piracy worldwide, across the full range of possible threat actors and attack types, will require a significant amount of advanced technology. A threat detection engine for this purpose would need to ingest data streams and analyze historical data from entities like the Space ISAC, but also from open-source intelligence (OSINT),

[5] Schulman, Jeremy, "A Mass Shooter's Mother Explains How She's Trying to Stop the Next Tragedy" *Mother Jones*, May 18, 2024

law enforcement, and the dark web. A powerful artificial intelligence (AI) capability would be essential to parse the data and spot suspicious activities and anomalies that could signify the presence of a threat. Figure 5 offers a simple representation of this idea.

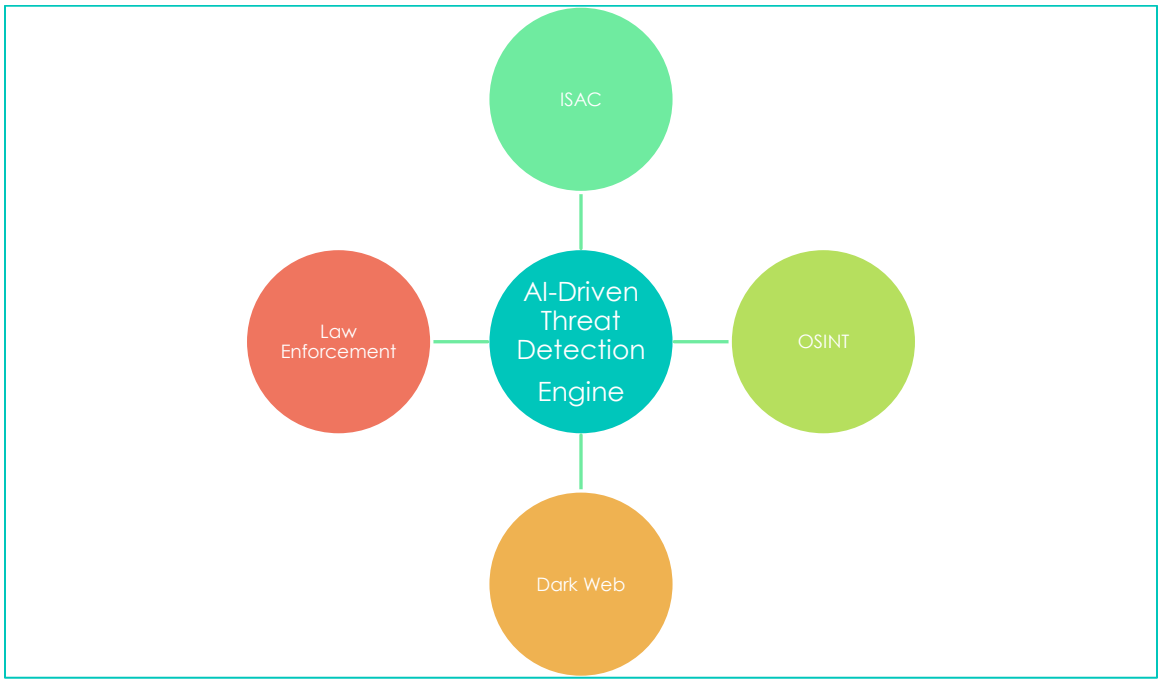

Figure 5 – The primary sources of data to feed into an AI-driven threat detection engine for mitigating risks of space crime and piracy.

The data feeds into this solution would include cyberthreats, but would go far beyond this one area of current focus. Data about crimes and the activities of criminal organizations would be an additional factor, as would business activities that might look normal on the surface, but in fact indicate the presence of people or situations that endanger space assets.

The data analytics process and algorithms required to make this work would be highly sophisticated and far from easy to develop and maintain. Building this solution would be a time-consuming and costly proposition. Keeping it running would also mean a commitment of resources. It is worth attempting, however, because the potential losses from acts of space crime and piracy would be high enough to justify the investment.

CONCLUSION

Space crime and piracy are largely theoretical problems as of today. However, now is an opportune time to start thinking about mitigating such irregular threats to the space economy and national security. The current threat detection and remediation entities are adequate for today's threat environment, but they will need to expand in scope if they want to address activities from criminal gangs, non-state actors, and the like. Possible solutions might involve

integrating threat data from novel sources, such as the dark web and OSINT—feeding them into an integrative system architecture that uses AI to detect suspicious but hard-to-spot attacks on space assets.

About The Center for the Study of Space Crime, Piracy, and Governance

The Center for Study of Space Crime, Policy, and Governance (CSCPG) is an independent, non-profit, nonpartisan think tank whose purpose is to serve as a policy resource for government officials and business executives on issues related to space governance, sovereignty, commerce, law, crime, and piracy. CSCPG seeks to serve as an actionable resource for government officials, and space industry players. The center's objective is to prevent and combat space crime/piracy, enhancing space governance, space sovereignty, and commerce.

CSCPG was founded by Marc Feldman and Hugh Taylor as an outgrowth of their research process in writing the book "Space Piracy: Preparing for a Criminal Crisis in Orbit" (Wiley, 2025). Marc Feldman is a space entrepreneur and space finance professional. Hugh Taylor has over 20 years of experience writing about cybersecurity, technology, and compliance.

For more information, visit https://cscpg.org