DECISION SUPPORT SYSTEMS FOR CRITICAL SPACE INFRASTRUCTURE ASSETS

Devon L. Brown
Danielle Ciesielski
Duli Chand

Persistent regional and global power dynamics will ensure that adversaries will continue to push boundaries in the geopolitical, economic, technological, intelligence, and military arenas. Improved tactics, techniques, and procedures are needed to address, mitigate, and counter behaviors critical to the United States, as nations and nonstate actors test new norms across all warfighting domains, space in particular. In order to analyze and process multidomain signatures in support of operational decision-making, the United States can harness artificial intelligence and machine learning decision support system statistical models to augment collection capabilities, data repositories, and threat analysis.

On January 28, 2023, a People's Republic of China (PRC) surveillance balloon entered US airspace near the Aleutian Islands and traveled over the continental United States and Canada. On February 4, it was shot down off the coast of South Carolina by the US Air Force.[1] Two days prior to the incident, the US government reported the object was making its way toward US airspace, but given the threat analysis, the report was not flagged as urgent. The incursion provides further evidence that as strategic competition increases, adversaries will continue to push boundaries in a number of arenas, including technology, geopolitics, economics, intelligence, and military. The balloon incident also emphasizes the importance of adequately characterizing the threat level of reporting in the diplomatic, homeland defense, military, and intelligence sectors, specifically for national and international security professionals in the air and space domains.[2]

Devon Brown is a special assistant to the principal deputy chief information officer at the US Department of State and holds a master of science in information systems technology from George Washington University.

Dr. Danielle Ciesielski is an applied mathematician and data scientist in the computational biology group on the data science and biostatistics team, Pacific Northwest National Laboratory, Richland, Washington.

Dr. Duli Chand is an earth scientist with specialty in instruments, observations, satellites, and ground remote sensing at the Pacific Northwest National Laboratory, Richland, Washington.

1. Jim Garamone, "F-22 Safely Shoots Down Chinese Spy Balloon off South Carolina Coast," Department of Defense (DoD) (website), February 4, 2023, https://www.defense.gov/.

2. Katie Bo Lillis et al., "Initial Classified Balloon Report Wasn't Flagged as Urgent, Drawing Criticism," CNN, February 8, 2023, https://www.cnn.com/.

Governments and private organizations around the world are gradually embedding artificial intelligence (AI) into their systems to solve emergent problems with untested technologies. Adversaries are advancing technologically and challenging the United States, its Allies, and partners with aggressive space asset maneuvering, while also funding innovative ideas that disrupt markets to gain strategic advantage over competitors.[3]

As these new capabilities come online, it is critical now more than ever to employ more than just a dashboard with analytics. The Intelligence Community must harness the vast amounts of data collected to supply probabilistic correlation, outcomes, and insights where none existed in the past. Using this understanding, analysts can more effectively identify anomalies and present probabilistic outcomes in support of contingency planning.

Background

Since the passage of the Intelligence Reform and Terrorism Prevention Act of 2004, the decision space has evolved to include numerous emerging threats, particularly adversary space operations.[4] Improved tactics, techniques, and procedures are needed to characterize such behaviors as nations test new norms across warfighting domains. The government's timely and effective response to these events is critical.

Measurement and signature intelligence (MASINT) serves as a technical concentration for intelligence officers and technical staff who focus on collecting scientific and technical intelligence on any given target. In the space domain, radio, electro-optical, geophysical, and other types of signatures collected from targets are essential when combined with operational data. Due to the fact that human interaction is limited in space, MASINT plays a critical role when analysts characterize space assets. By harnessing a decision support system (DSS) with robust threat analysis data, the US government will be able to accurately characterize these threats and inform senior leadership with the most accurate threat-level analysis.

The lack of transparency and automation in disjointed systems hinders the time from collection and analysis to a final decision. A decision support system—an information system that analyzes and synthesizes vast amounts of information to assist in the decision-making process—that encompasses accurate multidomain signatures is vital. A DSS will allow analysts to identify anomalies and advise decisionmakers when considering kinetic, nonkinetic, electromagnetic, or cyber defenses.

This article recommends a change to space-threat analysis strategy by applying AI and machine learning (ML) DSS statistical models that harness US collection capabilities and the interagency information-sharing environment. These models can streamline decision-making processes by determining probabilistic outcomes from disparate

3. Nicholas Deschenes, "Enabling Leaders to Dominate the Space Domain," *Military Review* (May-June 2019), https://www.armyupress.army.mil/.

4. Intelligence Reform and Terrorist Prevention Act of 2004, P. L. No. 108-458 (2004), https://www.govinfo.gov/.

datasets. A robust decision support system can assist with distributing resources effectively and analyzing trends between disparate datasets and systems where anticipatory probability analysis is not available. Now is the opportunity for the Intelligence Community to employ advanced analytical techniques to adapt to the ever-changing security environment.

After the 9/11 attacks on the United States, the Intelligence Reform and Terrorism Prevention Act of 2004 was enacted in order to enhance national security information-sharing between departments and agencies. Given the focus on strategic competition between nations and the effort to "enhance the resilience of US space systems" necessary for "critical national and homeland security functions" in the 2022 *National Security Strategy*, the intelligence sector should also shift to offer analytical support in these areas.[5]

Data and the Space Domain

The creation of the US Space Force and threat testimony from senior leaders has eased the learning curve for decisionmakers in the space domain. As additional parties such as private organization and nonstate actors participate in the space domain, combatant command commanders will need to provide presidents, defense secretaries, the Joint chiefs, and congressional representatives timely, accurate reporting on threats and vulnerabilities. Equipping commanders and operators with a decision support system that captures the relationship between threat analysis and operational atmospherics will enable commanders to give readily available accurate threat analysis to inform national-level strategic decision-making.

Emerging AI/ML analytical models connected to multidomain systems can build knowledge and understanding throughout the decision chain of command. Yet disruptive technologies, such as generative AI, acting to amplify misinformation and disinformation, affect how decisionmakers in the US government ingest indicators from multiple domains. This makes it difficult for senior leadership in the executive and legislative branches to build consensus around threats and formulate an inclusive national security strategy. A dependable and robust DSS that includes statistically probabilistic models will encourage national leaders to invest in robust threat analysis using internal mechanisms.[6]

Resources are scarce in the space domain. It is difficult for stakeholders to characterize how the geopolitical environment affects the relationship between operational planning and critical infrastructure in space. Nations are challenging international norms by pushing boundaries, including the tolerance for kinetic war and the use of disruptive technologies. As the United States, its Allies, and partners strategically position their countries for the next 15 to 20 years, based on the Artemis Accords and

5. Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: White House, October 2022), 8–9, 45.

6. Tom Di Fonzo, "What You Need to Know about Generative AI's Emerging Role in Political Campaigns," Tech Policy Press, October 12, 2023, https://techpolicy.press/.

planned space missions, these nations have an opportunity to rethink policy and strategy in an already congested space domain.

Commercial, government, and Ally activities in the space domain complicate the decision space when dual-use assets are involved. With orbital assets dependent on critical ground infrastructure, collaboration with the private sector becomes paramount.[7] Artificial intelligence/machine-learning DSSs provide strategic advantage by distributing resources effectively. Decision support systems take large amounts of unstructured data and assist with mid-level analysis when building relationships between datasets manually by analysts is unfeasible. By building out known variables within the DSS and adding new threats as they arise, the statistical models will be able to adjust as the threat landscape changes.

Values

During the developmental phase of any national-level system, the US Constitution and international law norms must be integrated to eliminate biases and outright violations of the Law of Armed Conflict in the system's recommendations to decisionmakers. Ethics and bias concerns in AI/ML models stem from priorities and data abnormalities when training such models. When discussing values and ethics, it is important to consider the drivers for innovation and technological advances.

Today, commercial and economic indicators propel technology development and innovation.[8] Economic gain, patents, and selling access to technology drive technology development in the private sector while government-funded labs are more focused on bleeding-edge research, standards, science, and technology. The space race to the moon from the 1950s to the 1960s is a prime example. National security and strategic competition were the motivators for obtaining the high ground. In response, the United States mobilized resources and personnel in its space race against the Soviet Union.

Fast forward to the 1980s and 1990s, when funding for technology and innovation was channeled through labs or advanced programs focused on long-term research and development, leading to the current state of affairs where private organizations drive innovation and are deeply ingrained in government operations and systems. For example, SpaceX initially supported communications and operations by supplying broadband services to Ukraine's military during Russia's invasion. Yet, at a February 2023 conference, SpaceX's president and chief operating officer noted, "Ukrainians leveraged the systems in ways that were unintentional and not part of any agreement" by using SpaceX's Starlink satellite system to weaponize drones.[9] This raises a valid question on how dual-use systems in the private sector are employed to support

7. Biden, *National Security Strategy*, 45.

8. Ash Carter, "The Moral Dimension of AI-Assisted Decision-making," *Daedalus* 151, no. 2 (Spring 2022), https://www.jstor.org/.

9. Joey Roulette, "SpaceX Curbed Ukraine's Use of Starlink Internet for Drones," Reuters, February 9, 2023, https://www.reuters.com/.

military efforts and on the ethical considerations for using commercial services in the support of war campaigns.

In another modern example, Open AI's ChatGPT motivated Microsoft and Google to invest in large language models. Microsoft's preliminary test with the Bing search engine raised concerns among ethicists who questioned if chat-enabled search was premature for the market.[10] The examples of SpaceX and Microsoft show how private-sector competition for technological advantage may hastily move products to market without considering all the applications for the technology. For the US government, such examples offer an opportunity to consider how AI/ML models affect national security, information operations, and geopolitical strategy. Government policy, standards, and research on these technologies will not only aid the private sector in developing ethical systems, but also encourage innovation.

Historical evidence shows the US government is heavily dependent on commercial space technologies. This can be a problem in terms of national security. For example, in the 1990s, US companies Loral Space & Communications Ltd. and Hughes Electronics violated export controls laws, and as a result, inadvertently transferred technological insights to China.[11] This subsequently led to satellite systems' export licensing moving from the Department of Commerce to the Department of State under International Traffic in Arms Regulations.[12] While protecting US dual-use space technologies from adversaries is paramount, it will be imperative to balance the benefit of US space export policies and controls as emerging technologies and techniques start to integrate into critical space infrastructure.

As this article investigates these strategic and ethical considerations, it will highlight applications for DSSs in the space domain and current research into AI/ML models, and it will examine the evolving space/counterspace efforts as a stage for strategic competition.

Decision Support Systems

Strategic Approach

Analysts rely on community knowledge, expertise, and collection taskers to prepare briefing materials. For the Biden administration, under the structure of the National Security Council, the most senior civilian and military decisionmakers regularly meet to receive numerous briefings from the Department of Defense and

10. Cindy Gordon, "Why Is Microsoft's New Bing ChatBot Raising Ethical Eyebrows?," *Forbes*, February 21, 2023, https://www.forbes.com/.

11. *Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China*, Rpt. 105-851, 105th Cong. (1999), xiv–xxi, https://www.govinfo.gov/.

12. *China: Possible Missile Technology Transfers under U.S. Satellite Export Policy – Actions and Chronology*, 98-485 (Washington, DC: Congressional Research Service, updated October 6, 2003), https://www.everycrsreport.com/; and Chad J. R. Ohlandt, "Competition and Collaboration in Space between the U.S., China, and Australia: Woomera to WGS and the Impact of Changing U.S. National Space Security Policy," *Asian Survey* 54, no. 2 (2014): 406–7, https://doi.org/.

other departments and agencies. Armed with this national-level unclassified and classified information, the National Security Council formulates national security policy.[13] Equipping these national security leaders with correlated information from diplomatic, science, economic, technical, military, and health sectors will enable officials to better understand the decision space and accurately characterize how each decision may affect a given sector.

Each agency has its own taxonomy for classified material. These systems identify how the agency stores, classifies, and structures classified data. Decision support systems can harness those taxonomies to build relationships between legacy systems and cut redundant processes. Intelligence Community Directive 203 provides analytic standards to ensure reporting is transparent, timely, and accurate, as well as ethically aligned in terms of "objectivity, bias, politicization, and other issues" with the Intelligence Community.[14] Incorporating AI/ML-enabled DSSs into analytical standards will ensure analysts can effectively use all-source intelligence to build correlations from common indicators throughout government and open-source channels.

The Augmenting Intelligence using Machines (AIM) strategy from the Office of the Director of National Intelligence emphasizes that "closing the gap between decisions and data collection is a top priority for the intelligence community."[15] Collection strategies over the past 20 years accumulated massive amounts of data in disparate systems. These systems have grown organically to share information on common platforms; however, logging into multiple systems and synthesizing the information manually slows down the analysis process and is inconsistent from analyst to analyst.

The Department of Defense classifies AI/ML efforts for decision support as systems of systems to wargame, calculate mission success, measure risk, and provide command and control for warfighters and commanders.[16] Systems of systems brings together disparate systems to offer insights that may not be available during the speed of battle. These insights allow commanders to make more informed decisions. Further, the Department of Defense implemented five ethical principles through its responsible AI doctrine: responsible, equitable, traceable, reliable, and governable. It also created the Joint Artificial Intelligence Center to implement this guidance throughout the Department.[17]

---

13. Memorandum on Renewing the National Security Council System White House (website), February 4, 2021, https://www.whitehouse.gov/.

14. James Clapper, "Analytic Standards," Intelligence Community Directive 203, January 2, 2015, 2, https://www.dni.gov/.

15. Office of the Director of National Intelligence (ODNI), *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, DC: ODNI, January 16, 2019), 3, https://www.dni.gov/.

16. K. C. Miller et al., "Merging Future Knowledgebase System of Systems with Artificial Intelligence/Machine Learning Engines to Maximize Reliability and Availability for Decision Support," *Military Operations Research* 26, no. 4 (2021), https://www.jstor.org/.

17. Deputy Secretary of Defense, Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoD Field Activity Directors, Subject: Implementing Responsible Artificial Intelligence in the Department of Defense, May 26, 2021, https://media.defense.gov/.

In comparison, the AIM initiative in the Intelligence Community focuses on narrow AI in the short term to leverage private-to-government relationships and investments. Medium-term investments will focus on AI assurance and basic research to fuse data and information from disparate domains or intelligence sectors to create a better understanding of collected data.[18] Ultimately, however, the AIM initiative and DoD systems-of-systems efforts in AI/ML are both needed to address issues particular to their sector. One overarching policy or initiative is not enough to account for all government agencies.

Research and resources are key to advancing AI/ML initiatives, but partnerships and foreign policy are critical since these technologies have global reach. Due to the increased number of countries implementing AI into autonomous systems, the Bureau of Arms Control, Verification, and Compliance at the Department of State issued the *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy* to push countries to implement risk/benefit analysis and responsible human chain of command and control when dealing with weapon systems.[19]

As the Department of Defense and the Intelligence Community invest in AI/ML infrastructure, talent, and capabilities, the Department of State would also benefit by facilitating conversations with partners and Allies, especially when considering AI/ML in the space domain.

US Space Command

In March 2022, Commander of US Space Command General James Dickinson identified Russia and the People's Republic of China as major security challenges and persistent threats, outlining examples of kinetic, antisatellite (ASAT) weapons tests, and adversary AI/ML systems designed to achieve space superiority.[20] Threats include China's Shijian-17 and Shijian-21 satellites, multiple ground-based laser systems, and the Russian direct ascent-ASAT missile demonstration that created 1,500 pieces of space debris.[21]

During the same Congressional hearing, Dickinson noted US Space Command initiatives maximizing "artificial intelligence, modeling, and simulation to inform space domain awareness." Dickinson informed Congress that in order for the command to be fully operational in this effort, it required "an integrated platform with fully trained modeling, simulation, and analysis personnel, with in-place hardware

18. ODNI, *AIM Initiative*, 5.

19. Bureau of Arms Control, Verification and Compliance, "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy," Department of State (website), February 16, 2023, https://www.state.gov/.

20. *Hearing on National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2023 and Oversight of Previously Authorized Programs, Before the Committee on Armed Services House of Representatives*, 117th Cong., 2nd session (2022) (statement of General James H. Dickinson, commander, US Space Command), 3, https://www.armed-services.senate.gov/.

21. *NDAA for FY 2023*, 7.

and software tools, with resources required to provide high performance computing across all classification levels" in support of "unbiased and timely assessments."[22]

Dickinson's priorities are driving the command to research AI/ML models in support of defending critical space infrastructure by analyzing capabilities, threats, vulnerabilities, and criticality of orbital assets.

Space Critical Infrastructure Decision Support Systems

US Space Command led efforts in developing an interagency coalition to quantify and assess malicious behavior in the space domain with the goal of defending orbital assets from aggressive/malicious actors in space.[23] The command's educational outreach to professional military education programs focused on key space defense research topics to understand competition, support relationships, and digital superiority, and to integrate commercial and interagency organizations.[24]

The Massachusetts Institute of Technology–Lincoln Laboratories is one of the labs exploring how to characterize capabilities, threats, vulnerabilities, and criticality of orbital assets in the space domain using AI/ML. Their preliminary research explored how AI/ML-enabled DSSs use Bayesian network models to decide criticality for orbital assets.[25] The National Intelligence University undertook research efforts in the fall of 2022 to explore comparative models on criticality and risk management strategies for orbital assets.

Quantifying Space Threats and Vulnerabilities in Contingency Planning

Calculating defensive strategies for orbital assists requires knowledge of defended asset lists (DALs) and critical asset lists (CALs), which are essential during risk and contingency planning at the combatant-command level. Both dynamic lists are essential in determining priorities for all stakeholders in the space domain.[26] Decision support systems in the space domain focus on the highest prioritized assets and forecasting threats and vulnerabilities for those assets in order to develop defense strategies.

It is impossible to defend all assets from every threat in the space domain. The priority critical asset list (PCAL), risk management, and contingency planning are

22. *NDAA for FY 2023*, 14–15.

23. Headquarters, US Space Force (USSF), *Spacepower: Doctrine for Space Forces*, Space Capstone Publication (Washington, DC: USSF, June 2020), https://www.spaceforce.mil/.

24. Brook J. Leonard, Memorandum for Professional Military Education Programs: Space Defense and War Studies Outreach for Professional Military Education Programs – Academic Year 2023, 1.

25. Michael B. Hurley, Dan Castellarin, and Jenna Hallapy, "U.S. Space Command Critical Infrastructure Decision Support System (UCIDS): Bayesian Network Overview" (unpublished white paper, Massachusetts Institute of Technology–Lincoln Laboratories, 2022).

26. Scott Douglas Applegate and Christopher L. Carpenter, "Searching for Digital Hilltops: A Doctrinal Approach to Identifying Key Terrain in Cyberspace," *Joint Force Quarterly* 84, no. 1 (2017): 8, https://ndupress.ndu.edu/.

necessary for the DSS: these elements define government assets and relate them to threats and vulnerabilities. A PCAL drives the development of the DAL and is scored annually during an interagency conference including partners such as the Space Force, the Army, the National Aeronautics and Space Administration, and other departments and agencies. There are six steps in creating the PCAL:[27]

1. Assets/locations given priorities and criticality based on location
    i. Examples: Command-and-control assets, global sensor management, missile warning, Military Satellite Communications Directorate, and intelligence, surveillance, and reconnaissance
    ii. Result: PCAL based on criticality
2. Priorities and criticality analyzed for specific threat environment
    i. Examples: Ground attack, cyberattack, ASAT weapons, and space object surveillance and identification
    ii. Result: PCAL based on criticality, vulnerability, and threat
3. Vulnerability analysis
    i. Example: Susceptibility to attack, resiliency to recover, and redundancy
    ii. Result: PCAL based on criticality, vulnerability, and threat
4. Joint mission thread analysis
    i. Example: Warfighter space dependency model and space interactive blueprints
    ii. Result: Initial PCAL
5. Combatant commander supplies guidance
    i. Example: Human analysis
    ii. Result: Commander's guidance
6. Combine initial PCAL with commander guidance
    i. Result: Joint/combined PCAL

Interagency partners assess criticality, threat, and vulnerabilities by assigning analysis responsibilities to an agency or department's area of responsibility. Critical priorities are space warfare, space service support, space support operations, space domain awareness, and Office of the Director of National Intelligence objectives. Each priority encompasses specific capabilities in an area of responsibility scored on a scale of one to five, with five as the highest threat. Threats like cyberattacks or ASAT weapons are scored as well, using the same scale and categorized by actors that have that capability. Lastly, vulnerabilities are categorized by type and scored using the same scale under orbital or terrestrial domains.[28] These PCAL scores along with the US Space Command commander's guidance allow for the annual interagency development of a Joint PCAL that identifies the most critical assets to protect.

27. US Space Command (USSPACECOM), "Prioritized Critical Asset List (PCAL)" overview brief (Colorado Springs, CO: USSPACECOM, undated)

28. USSPACECOM, "PCAL" overview brief.

Automating this process with an AI/ML decision support system will not only streamline the process but also uncover dependencies and deficiencies in the analysis process. To narrow the research, this article will analyze how AI/ML can use statistical models to streamline the assessment of space debris, ASAT, and cyberattack threats to orbital assets.

Bayesian Networks for Criticality/Risk Assessments

The use case for Bayesian networks to determine criticality and risk assessments in the PCAL process lies in probability theory, using mathematical formulas to determine conditional probability, or the predicted likelihood of the next output based on a past event's experiences.[29] Bayesian networks incorporate common knowledge to train models that predict the most likely next occurrence of an event.

The use of Bayes' rule for conditional probability underpins this method and states

$$P(Y_i|X)=P(X|Y_i)P(Y_i)/(\Sigma^{n}\ (P(X|Y_i)P(Y_i)))$$

where *X* and *Y* are random variables, *Yi* denotes a specific variable (among *n*), and *P* is a probability distribution function that maps values between zero and one. Initial research from the Massachusetts Institute of Technology–Lincoln Laboratories identifies the chain below in determining nodes in the decision support system:

Actor > Threat > Vulnerability > Domain > Asset Class > Asset > System > Mission

In response to the issue of exponential growth ~~in~~ conditional probability tables, the lab plans to use noisy-Boolean constructs to reduce the complexity of the system, thereby speeding up calculations as the number of inputs increase within the network.[30] Using this methodology, the authors explored AI/ML DSS techniques to understand how these models could determine criticality in three areas: space debris, ASAT, and electronic warfare/cyberattacks.

Space Debris

On average, 21 potential space-collision warnings are issued by the military each day. Researchers are looking into innovative ways to minimize space debris. Initiatives range from developing nets to pushing debris into medium Earth orbit for satellites to hit gravitational resonance over time and burn up in the atmosphere.[31] There are around 55,338 trackable objects consisting of 62 percent debris, 26 percent payloads, 12 percent rocket bodies, and <1 percent unknown. The dataset used to feed the DSS includes the apogee, perigee, inclination, and period for each object and offers to retrieve the following additional information for each:[32]

29. Hurley, Castellarin, and Hallapy, "Bayesian Network Overview."

30. Hurley, Castellarin, and Hallapy.

31. Alexandra Witze, "The Quest to Conquer Earth's Space Junk Problem," *Nature*, September 5, 2018, 6, https://www.nature.com/.

32. Duli Chand, Space Objects from All Countries (orbital objects dataset), Pacific Northwest National Laboratory, February 2023.

1. Orbit of the object
    i. Orbits of interest: low Earth orbit (LEO), highly elliptical orbit, or geostationary orbit
2. Velocities of the objects at apogee and perigee
    i. Calculating periapsis a: radius R of the Earth plus the perigee
    ii. Calculating apoapsis b: radius R of the Earth plus the apogee
    iii. Calculating the semi-major axis: $(a+b)/2$ where $a < b$
    iv. Vis-viva equation: $v^2=2GM(1/r - 1/(a+b))$ (here r is the distance of the satellite from the center of the earth to any point in the orbit)
    v. Velocity at perigee: $(r = a)$: $v_a = \sqrt{(2GMb/(a(a + b)))}$
    vi. Velocity at apogee: $(r = b)$: $v_b = \sqrt{(2GMa/(b(a + b)))}$
3. Spatial and temporal proximity of the orbital objects

As government, commercial, and science organizations launch more assets into space, space debris will inevitably increase in LEO, causing launch missions with the final destination of geosynchronous orbit to become increasingly more difficult. If using Bayesian networks in the DSS, space debris would be one of the threat nodes at the beginning of the decision tree that affects mission success.

By harnessing existing information from space object surveillance and identification programs and open-source space tracking sites like Space-Track.org, a DSS can ingest orbital trajectory data and combine it with data from other warfighting domains. Normally, combining datasets and results from multisourced intelligence sectors is the responsibility of the analysts; however, if a DSS can automate this process it allows the analyst to strategically forecast not only one decision, but also how that decision may affect other constellations or resources in another domain.

Space debris datasets include country designations which assist in identifying assets and debris from other countries. For example, the United States has the following breakdown of tracked objects in space: 9,430 debris; 7,267 payloads; and 1,490 rocket bodies. In comparison, Russia tracks 17,039 debris; 3,656 payloads; and 3,955 rocket bodies. Lastly, the PRC tracks 5,451 debris; 704 payloads; and 451 rocket bodies.

The United States, Russia, and China are responsible for most assets and debris in space. As competition increases, more assets in space will only create additional debris, especially as the Artemis I program and other cislunar projects commence in the next 5 to 10 years. Orbital debris is not the only threat; however, it affects all satellites and has implications for government, private, and other assets in space.

Antisatellite

In 2007, the PRC's first successful test of a kinetic physical ASAT destroyed an old PRC satellite system with a direct-ascent SC-19 missile system and created over 3,000 pieces of debris, of which roughly 2,800 are still in LEO around the earth.[33] Other examples of China's ASAT technologies include BX-1, which jettisoned as a small

33. Chand.

imaging satellite from Shenzhou; SJ-12, conducting rendezvous and proximity operations (RPOs) to test possible jamming/counterspace capabilities; and Aolong-1, which included a robotic arm.[34] One case of particular interest is SJ-17, a PRC communications satellite. SJ-17 launched in November 2016 and performed RPOs around communications satellite Chinasat 6A from June to July 2017. On July 1, 2017, SJ-17 came within 1.67 kilometers of Chinasat 6A and stayed within 15 kilometers until normalizing proximity on July 6, 2017.[35]

Satellites in geostationary orbit require authorization and reservation of orbital slots from the International Telecommunications Union (ITU), a specialized UN agency that assigns global radio frequencies to satellites to minimize interference with other satellites. A satellite operating outside its official ITU position could pose a threat to other satellites transiting that area.[36] Even though SJ-17 and Chinasat 6A are both PRC satellites, the signatures of two satellites moving close together and performing very close RPO maneuvers is of interest. Pushing proximity space norms may cause accidental collisions and unnecessary space debris, which will affect all satellites in the space domain.

In an effort to characterize how a DSS could model the threat of close RPO maneuvers, the National Intelligence University and Pacific Northwest National Laboratory pulled satellite telemetry data from Space-Track.org and built a model to characterize the orbital trajectories of SJ-17 and Chinasat 6A from May 2017 to December 2018.[37] After combining SJ-17 and Chinasat 6A's datasets, the team developed a Python program to create the upper limits and lower limits on each satellite's apoapsis and periapsis. Limits on the apoapsis and periapsis created zones for each satellite depending on the location in relation to the other satellite to identify aggressive orbital movements.

Since the ITU reserves orbital slots for each geostationary orbit satellite, there is a general location in the specified space within which the satellite should remain. Due to numerous factors, satellites usually have a "wobble" within their original ITU designation; however, that usually does not interfere with other satellites. When comparing both orbits of the satellite during the May to December 2017 time frame, the orbital data shows SJ-17 moving from its original ITU designation toward the Chinasat 6A satellite.

34. Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Broomfield, CO: Secure World Foundation, April 2022), 113, https://swfound.org/.

35. Kaitlyn Johnson, "GEO Close Approach: SJ-17/Chinasat 6A," Satellite Dashboard, last updated January 28, 2022, https://satellitedashboard.org/.

36. "Regulation of Satellite Systems," ITU [International Telecommunications Union], last updated February 2022, https://www.itu.int/.

37. Chinasat 6A / SJ-17 datasets, Space-Track.org, March 2023, https://www.space-track.org.

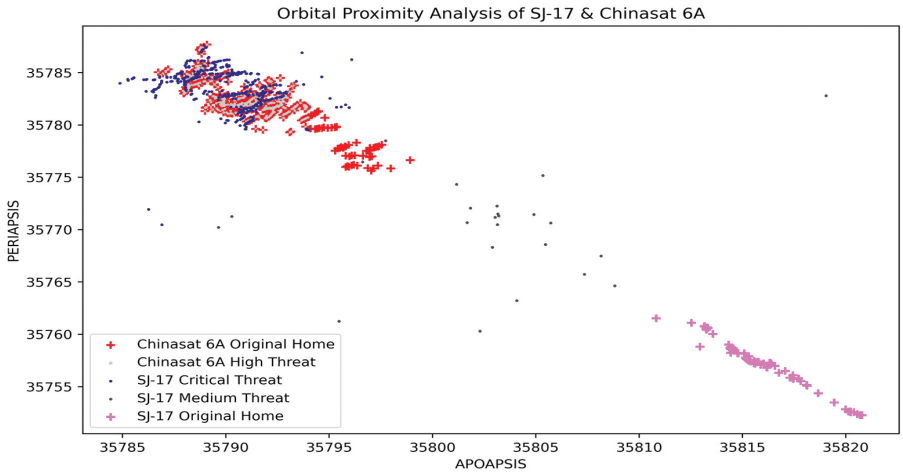

Figure 1. Orbital proximity analysis of SJ-17 and Chinasat 6A[38]

Additional data (2011 to present) with multiple space variables available from SJ-17 and Chinasat 6A will be used to further assess and test criticality and threats. The goal of this model is to identify when Chinasat 6A and SJ-17 are dangerously close and assign proximity scores based on their proximity to each other using their apoapsis and periapsis.

Organizations around the world already have similar capabilities to analyze satellite behavior. Since SJ-17's launch in 2016, there have been numerous abnormalities in its orbital trajectories. Figure 2 identifies anomalous SJ-17 orbital trajectories from 2016 to 2023 by analyzing the right ascension of ascending node (RAAN), which is the angle between the vernal equinox and the ascending node of the orbit. This is the point where the satellite passes from the southern hemisphere to the northern hemisphere.

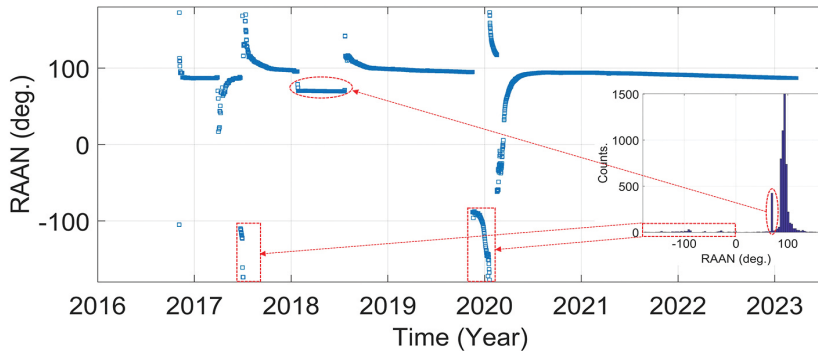

Figure 2. SJ-17 maneuvers between 2016 and 2023[39]

38. Danielle K. Ciesielski, SJ-17 & Chinasat 6A Proximity Threat Model, 2023.

39. Duli Chand, Space Objects and SJ-17 & Chinasat 6A Analysis (orbital objects dataset), Pacific Northwest National Laboratory, February 2023.

Examples such as these draw alarm and have the potential to affect mission planning if similar aggressive positioning and anomalous orbits are deployed against competitor satellites. Mission planning and satellite adjustments take many days to start due to authorizations, analysis, and priority deconfliction. In comparison, a DSS using AI/ML statistical models and necessary inputs from subsystems could rapidly recalculate probabilities based on inputs from analysts or operators. By adjusting weighted values on assets, an analyst using the model could simulate aggressive behavior and offer predictions about the battlespace in advance of any aggressive act. This in turn would allow for wargaming-like scenarios based on real-time signatures and warnings, improving the ability to identify potential threats and vulnerabilities.

Electronic Warfare and Cyberattacks

Dickinson's 2022 Senate Arms Services Committee testimony highlighted cyber integration as a way to defend space mission systems and intellectual property while Space Command is implementing zero-trust architecture and AI/ML techniques to harden current and future systems.[40] Given today's cyber threats, it is paramount for ground, air, and space domains to prepare for cyberattacks to critical infrastructure.

Adversaries use satellite jammers, spoofers, laser dazzlers, and other forms of electronic warfare (EW) to influence or disrupt operations, with attribution being difficult in the space domain. Attributable real-world examples include Russia's jamming and spoofing of satellites to degrade drone operations in Syria, its jamming of GPS and satellites to disrupt Ukraine's satellite navigation and timing for radios since 2014, Moscow's periodic jamming of GPS signals in Norway and Finland during NATO exercises, and its spoofing of GPS signals in the Black Sea causing navigation errors.[41] These are a few examples of the reported cyberattacks on orbital assets, but each had a significant negative mission impact when considering the area of coverage for each system.

While SJ-17 performed RPO maneuvers around Chinasat 6A, it can be assumed EW actions such as jamming were deployed by SJ-17 against Chinasat 6A. Using this example, a binary "on" or "off" cyber or EW variable was added to the dataset, indicating if jamming was present during the RPO maneuvers. The proximity variable calculated in the previous ASAT criticality section characterized the proximity level on a scale of one to five, with five being close to each other, and one being far apart. Using this calculation, the cyber/EW variable was set to on for proximity levels with the value four and five, and the cyber/EW variable was set to off for proximity levels three to one.

This technique shows how to connect RPO maneuvers to possible jamming tactics. The combination of orbital trajectories, proximity variables, and cyber/EW data into one dataset is an example of how applied analytic models can characterize behavior in the space domain and create signatures for specific RPO maneuvers.

40. *NDAA for FY 2023*, 13.

41. Melissa Dalton et al., *By Other Means Part II: Adapting to Compete in the Gray Zone* (Washington, DC: Center for Strategic and International Studies, August 2019), 20, https://csis-website-prod.s3.amazonaws.com/

Using these signatures, analysts can then continue to update the DSS statistical model with other threat reporting.

Conclusion

Decision support systems are essential for US space operations and during contingency planning to counter emergent threats against critical space infrastructure. The United States has an opportunity to harness existing taxonomies in information systems and address potential systemic biases by implementing a critical space infrastructure DSS. This system will assist in rapidly analyzing space threats, vulnerabilities, and capabilities for decision advantage. Implementing a DSS for space-domain threat analysis will allow operators and analysts not only to characterize threats, vulnerabilities, and capabilities of the space domain, but also to create a common body of knowledge where there is limited experience.

Implementing a DSS in the space domain will combat the lack of transparency and automation in the sector. The combination of inexperience, aggressive competitors, norms testing, and influence operations increases the likelihood of mistakes not only in the space domain, but also in the geopolitical environment. Building trust, coalitions, and common knowledge throughout the space community will enable senior-level decisionmakers throughout the US government to champion space topics at the highest levels. Through increased collaboration and research initiatives, the US government can employ the following strategy to realize a DSS that encompasses all current capabilities while increasing domain awareness. The government should:

- Deploy a national-level DSS in the space domain that ingests indicators, signals, and warnings from defense, private sector, and scientific space systems.
- Gather analyst, operator, and subject-matter-expert knowledge on characterizing space threats and incorporate this into the DSS.
- Build analytic tools to enable wargaming in the space domain. Operators and analysts should be able to set priorities, update weighted values for assets, create ad-hoc reports, and rapidly detect anomalous behaviors.

By collaborating with nation-state Allies and partners, commercial partners, and the scientific community, the US government will not only achieve decision advantage in the growing space domain, but also drive space policy and norms for the entire space community. As Artemis I and other space missions bring humanity back to the moon, the United States and its Allies and partners must harness emergent technologies for improved decision advantage. **Æ**