

SPACE-BASED DATA CENTERS ROADMAP: THE CASE FOR CAUTION

November 2026

CHAPTER 1.6:

Vulnerability to Attack

Kathleen Curlee



Innovation for Cool Earth Forum

WORKING PAPER

TABLE OF CONTENTS

CHAPTER 1.6: 1.6-1
VULNERABILITY TO ATTACK – *Kathleen Curlee*

A. Threats to Space-Based Data Centers 1.6-1
i. Kinetic Threats 1.6-2
ii. Non-Kinetic Counterspace Capabilities 1.6-3
B. Defense of Space-Based Data Centers 1.6-3
C. Attack Scenarios 1.6-5
i. Military Conflicts 1.6-5
ii. Economic Competition 1.6-6
iii. Dual-Use Implications 1.6-6
D. Policy Considerations 1.6-7
E. Recommendations 1.6-8
F. References 1.6-9

CHAPTER 1.6:

VULNERABILITY TO ATTACK

Kathleen Curlee

MAIN MESSAGES

- Space-based data centers (SBDCs) would be vulnerable to multiple forms of attack including jamming, cyber attacks and kinetic threats.
- Defenses for SBDCs include resilient and redundant constellations, systems hardened against electronic warfare, and secure ground infrastructure.
- SBDCs could be targets in conflicts if they become significant portions of a country's economy or support military operations.
- Current technologies and legal oversight are insufficient to protect commercial or civil SBDCs from any form of attack, in large part due to the isolated nature of space and lack of enforcement of international law.

Space-based data centers (SBDCs) are not inherently safe because they are in space. They would be vulnerable to attack from hostile actors: several nation states and non-state actors have the demonstrated capability to disrupt SBDCs. Defense of SBDCs could be difficult because of technological limitations. Moreover, SBDCs that support military missions could become targets during conflict. Commercial SBDCs could also attract hostile attention if their disruption would create economic or political damage.

On top of this, escalation dynamics in space are poorly understood.[1] Measures intended to protect SBDCs could be misread during a crisis. For example, a spacecraft sent to inspect or repair another spacecraft could be viewed as a threat to surrounding satellites. Intentional jamming, cyber intrusion or close approaches of SBDCs often have ambiguous attribution which can lead to governments responding to threats in space before full understanding of the situation is known.

This chapter examines how hostile actors might target SBDCs, the limits of current defenses, attack scenarios and policy considerations. The chapter closes with recommendations.

A. Threats to Space-Based Data Centers

SBDCs face several forms of hostile interference in space. Some threats can go as far as damaging or destroying an individual or group of SBDCs. Other threats can interrupt service without causing permanent harm to the spacecraft. An attacker can also target the communications links and ground



F-15 launching the ASM-135 anti-satellite missile. Source: U.S. Air Force Research Laboratory / Michael Weber (Disclaimer: The appearance of U.S. Department of War (DoW) visual information does not imply or constitute DoW endorsement.)

systems on Earth needed to operate SBDCs. The most significant threats include kinetic attacks, co-orbital interference, electronic warfare, cyber operations and directed-energy systems.[2]

i. Kinetic Threats

Direct-ascent anti-satellite (ASAT) weapons are missiles launched from the ground or air that target objects in space. The United States, China, India and Russia have demonstrated destructive direct-ascent ASAT capabilities. These attacks can destroy spacecraft. On top of this, they can make debris that remains in orbit, creating persistent risks for other satellites. For example, China's 2007 test accounts for 19% of all debris in orbit today.[3] These fragments increase risks for other spacecraft, as an object as small as ten centimeters can hit with the force of several kilograms of TNT.[4]

Co-orbital systems present another form of physical threat. These systems rendezvous with satellites, interfering with them at close range. Potential hostile actions include physical manipulation or deliberate collision. Some rendezvous and proximity operations support benign missions such as inspection. However, these same capabilities could also support hostile activity or could be perceived as such.[5]

Rendezvous and proximity operations allow one spacecraft to closely approach and maneuver around another.

ii. Non-Kinetic Counterspace Capabilities

Other counterspace operations can create reversible effects. An attacker may seek to deny service during a crisis without destroying the system. Temporary disruption may be harder to attribute than a kinetic strike. It would also avoid the debris created by a physical attack.



U.S. Space Force Guardians train on a system detecting satellite electromagnetic interference, 2026. Credit: U.S. Space Force/David Grim

Electronic warfare could disrupt an orbital data center without damaging the spacecraft:

- Jamming can prevent a satellite from receiving or transmitting signals
- Spoofing can introduce false information into a system or mislead users about the source and accuracy of a signal
- Cyber operations could target onboard software or command systems, as well as ground stations and terrestrial networks

This means an attacker may be able to disrupt an orbital service without directly reaching the spacecraft. Directed-energy weapons can also temporarily disrupt an asset or cause permanent damage by using lasers or high-powered radiofrequency energy to interfere with spacecraft systems.[6]

B. Defense of Space-Based Data Centers

Defending SBDCs and other space infrastructure will require a layered approach that combines prevention, protection, resilience and recovery.[2] The challenge is that few active protection mechanisms currently exist for satellites once they are deployed. Satellites operate in a remote environment, move at orbital velocity and have limited fuel without the ability to refuel.[7] This makes repair and active defense more difficult than comparable efforts for terrestrial data centers. This is one reason national space security plans emphasize resilience across the full space system as a means of defense against threats.

On-orbit servicing technologies are promising emerging capabilities but not yet usable at scale. Northrop Grumman's Mission Extension Vehicles have demonstrated commercial life-extension services for geostationary satellites, and the US Defense Advanced Research Projects Agency's (DARPA's) Robotic Servicing of Geosynchronous Satellites program is working toward cooperative inspection and servicing in Geostationary Equatorial Orbit (GEO).[8] At the same time, NASA cancelled OSAM-1 after cost growth and schedule delays. These development challenges illustrates the technical and programmatic difficulty of servicing satellites that were not designed for repair.[9]

The most practical defense for many space systems is architectural resilience. One approach is to distribute capabilities across many satellites so that the loss or degradation of one part of a constellation or ground segment does not ruin the spacecraft. This approach already appears in several national and allied space strategies. The US Space Development Agency's Proliferated Warfighter Space Architecture is built around a layered, proliferated Low Earth Orbit (LEO) architecture and mesh networking.[10] Japan's Space Security Initiative similarly emphasizes retaining large numbers of satellites with similar functions, diversifying architectures, protecting ground stations and improving cyber resilience.[11] The United Kingdom's Space Command has also described a "system of systems" approach that connects space capabilities, ground infrastructure and multiple users to improve resilience and redundancy.[12] For orbital data centers, this means avoiding excessive concentration of critical workloads on a single large platform. A more resilient architecture would distribute processing and communications across multiple nodes.



Mission Shakti launch of interceptor missile for ASAT test, March 2019. Source: Press Information Bureau on behalf of Ministry of Defence, Government of India

Redundancy and rapid replacement are central to defense. The US Space Force Commercial Space Strategy states that commercial integration can strengthen resilience by increasing the number of providers and diversifying supply chains.[13] The North Atlantic Treaty Organization's (NATO's) Commercial Space Strategy similarly focuses on cooperation with the commercial sector to improve complementary capabilities, capacity and resilience across the Alliance.[14]

Ground infrastructure is another major defense priority. Space systems depend on command centers, antennas, cloud interfaces, user terminals, fiber links, power supplies, terrestrial software systems and more.[15] An adversary may attack these supporting systems as they are more accessible than the spacecraft themselves, although this is a high-risk approach as kinetic attacks can be viewed as an act of war. Defensive planning should include geographically distributed ground stations, hardened command-and-control links, secure power supplies and procedures for operating through degraded conditions. The EU Space Strategy for Security and Defence already recognizes the need to improve the resilience and protection of space systems and related services.[16]

Cybersecurity and network resilience will be especially important for orbital data centers. Proposed security measures include encryption, authentication, frequent software updates, zero-trust access controls, intrusion detection, segmented workloads, trusted execution environments, backup data paths and isolation of compromised nodes.[17] The US National Institute for Standards and

Technology's (NIST's) hybrid satellite network cybersecurity profile is an example of addressing systems in which multiple participants can own or operate different portions of the network.[18]

Defenses should also include electronic warfare resilience. Jamming, spoofing and interference are among the most accessible counterspace threats and are already used in conflicts.[19] Operators can mitigate risks through protected waveforms, interference monitoring, or rerouting traffic through multiple satellites and ground stations.[20,21] For allied users, this also means planning for cross-support between national and commercial networks so that loss of one communications path does not sever access to essential services. Across these defense areas, allied governments need shared expectations for continuity of services and crisis coordination with commercial providers.[18]

C. Attack Scenarios

i. Military Conflicts

SBDCs could support a range of military and national security functions. For example, they may process satellite imagery or support secure communications.[22] They could also host artificial intelligence (AI) models used for detection or decision support.[23] Existing defense strategies already identify satellite communications, intelligence, surveillance, reconnaissance, cyberspace operations and spacecraft operations as areas where commercial space systems can contribute to national security missions.[24] SBDCs might have the ability to enhance these functions.

These applications make SBDCs a potential target during conflicts. An adversary may view SBDCs as a military target if disrupting them can weaken national command networks or reduce access to critical information for security operations. The risk would be highest for systems that support time-sensitive missions or serve several military users at once. SBDCs could accelerate space-based decision-making and improve the responsiveness of military space operations making them attractive for countries to pursue.[23]

Commercial ownership would not mitigate this risk. Governments purchase communications and other space capabilities from private companies. SBDCs could operate under similar agreements. Defense agencies are also seeking deeper integration of commercial systems into military architectures to support resilience. As a result, a privately operated SBDC could support civilian customers and defense users through the same infrastructure. Its role could expand during a crisis if governments purchase additional capacity or redirect existing services toward military needs.

This pushes SBDCs into the uncertainty that already exists around dual-use infrastructure. It may be difficult for an adversary to determine which spacecraft are exclusively for military purposes and which are commercial. Policymakers will need to consider how military use affects the status of commercial orbital systems and what responsibilities follow from that integration. Moreover, policymakers must contend with the fact that valuable commercial assets in space are highly vulnerable to interference and make attractive targets if a total-war strategy is used.

ii. Economic Competition

SBDCs may be economically important even if they have no direct military role. Businesses may come to depend on them, and their loss of SBDCs could disrupt services on Earth and impose costs across several industries. The economic value of SBDCs make them attractive targets. A hostile actor may seek to damage a competitor's technology sector or undermine confidence in space-based services. An attack could also interrupt markets or create pressure on governments whose economies depend on the affected systems.



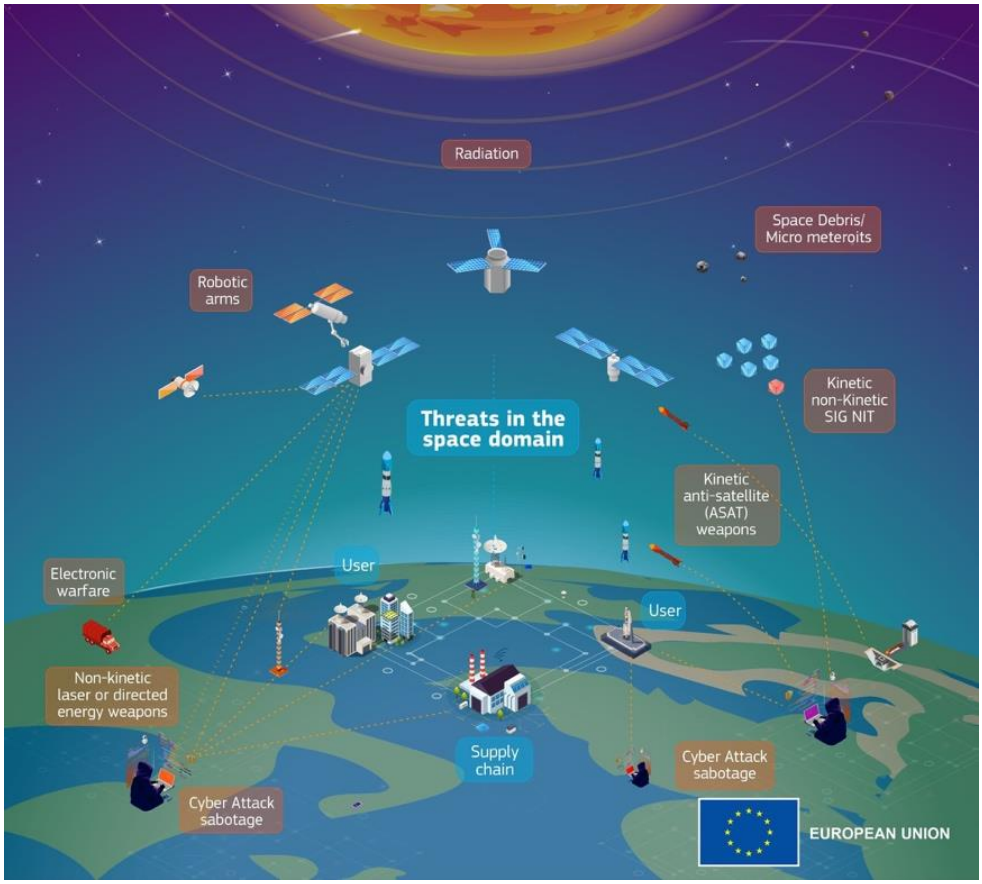
Early Warning Radar facility for missile warning and space surveillance missions, 2024. Source: U.S. Space Force/David Grim

Terrestrial critical infrastructure already experiences disruptions during conflicts. Hostile actors have targeted systems like energy grids and financial institutions to create economic disruption without engaging military forces directly.[25] SBDCs offer another means of applying pressure to civilian life. SBDCs' location in space also creates uncertainty around attribution and response. The risk would increase if customers depend on a small number of SBDC providers.[26] A disruption could have effects far beyond the operator that owns the asset. Policymakers must assess what level of protection or resilience SBDCs should require, especially if they become critical components of their economies.

iii. Dual-Use Implications

Distinguishing civilian and military infrastructure is difficult in space, where many systems are inherently dual use.[27] Satellites that provide communications, navigation, remote sensing, weather monitoring or data-relay services support everyday civilian activity while also enabling military operations. Commercial systems further complicate this distinction as they serve a mix of private and military customers through the same infrastructure. Even if an SBDC is privately owned and primarily commercial, an adversary may view its wartime function, customer base or integration with military networks as more important than its ownership structure and thus a valid and strategically important target for interference.

This overlap could create legal and strategic ambiguity. Policymakers need to clarify expectations for disclosure, workload separation, service continuity and government support for these data centers.[28] They also need to consider how civilian and military applications can be distinguished in practice, whether certain uses would increase the risk that a commercial system is treated as a military objective and what protections remain for civilian users whose data or services rely on the same infrastructure. These questions are not unique to SBDCs but reflect a broader emerging challenge in space in which commercial infrastructure is central to national security but remains deeply intertwined with civilian economies and global services.



Threats in the space domain (2023). Source: European Commission

D. Policy Considerations

Policymakers must plan for a space environment that is contested and likely to become more crowded with critical commercial infrastructure should SBDC proposals be realized. Satellites already support communications, navigation, remote sensing, financial systems, military operations and disaster response. SBDCs would add another layer of economically and strategically important infrastructure to orbit.

Several issues should be addressed before these systems reach large-scale deployment:

- Governments will need to decide whether some commercial space assets should be treated as orbital critical infrastructure
- Governments will need criteria for identifying which systems are critical to national security or economic stability
- Policymakers should clarify public-private security responsibilities

Operators may be responsible for cybersecurity, redundancy, service continuity and protection of ground infrastructure. Similarly, governments may also need to provide support to allies during attacks or major disruptions.

Governments should also think through deterrence and response. Attacks on commercial orbital infrastructure would impact private and government domains. Defensive measures may also carry escalation risks if an adversary interprets them as preparation for offensive action. Policymakers should clarify how they would assess attacks on SBDCs, when they would support commercial operators, which responses could increase escalation risks and what role alliances would play in a crisis.

E. Recommendations

1. Define orbital critical infrastructure: Governments should identify which commercial space assets are critical to national security, economic stability or public safety.
2. Set baseline security and resilience requirements: Policymakers should establish expectations for cybersecurity, redundancy, service continuity and protection of ground infrastructure before SBDCs reach large-scale deployment.
3. Clarify public-private responsibilities: Governments should assign clear roles for threat monitoring, incident reporting, crisis response and service restoration before a disruption occurs.
4. Plan for attacks on ground infrastructure: Security planning should cover ground stations, cloud interfaces, user terminals, power supplies and terrestrial networks that support orbital systems.
5. Develop crisis coordination mechanisms: Governments should establish standing channels with operators and allied partners for sharing threat information and coordinating responses during jamming, cyber incidents or physical attacks.
6. Address deterrence, response and escalation risks: Policymakers should clarify how attacks on commercial orbital infrastructure would be assessed, what responses could raise escalation risks and how allies would coordinate in a crisis.

F. References

1 Nivedita Raju. Parameters to Assess Escalation Risks in Space (SIPRI Research Policy Paper); Stockholm International Peace Research Institute (SIPRI), Solna, Sweden, https://www.sipri.org/sites/default/files/2025-02/parameters_to_assess_escalation_risks_in_space_0.pdf (2025).

2 Victoria Samson & Kathleen Brett. 2026 Global Counterspace Capabilities Report; Secure World Foundation, Broomfield, CO, https://www.swfound.org/publications-and-reports/2026-global-counterspace-capabilities-report (2026).

3 Kathleen Curlee & Lauren Kahn. Mapping Space Debris: An Interactive Data Visualization of Orbital Debris and Its Origins (Data Snapshot); Center for Security and Emerging Technology (CSET), Walsh School of Foreign Service, Georgetown University, Washington, D.C., https://cset.georgetown.edu/publication/mapping-space-debris/ (2025).

4 Heather F. Riley. Micrometeoroids and Orbital Debris (MMOD); National Aeronautics and Space Administration (NASA), Washington, D.C., https://www.nasa.gov/centers-and-facilities/white-sands/micrometeoroids-and-orbital-debris-mmod/ (2016).

5 Kathleen Brett. US Co-Orbital Anti-satellite Testing Fact Sheet; Secure World Foundation, Broomfield, CO, https://www.swfound.org/publications-and-reports/u-s-co-orbital-anti-satellite-testing-fact-sheet (2026).

6 Lisa Sodders & Brad Smith. Focused on the Threat: Directed Energy Weapons (Part 3 of 6); US Space Force (USSF), Space Systems Command (SSC) Public Affairs Office, Department of the Air Force, Los Angeles Air Force Base (LAFB), CA, https://www.ssc.spaceforce.mil/Newsroom/Article/3913339/focused-on-the-threat-directed-energy-weapons-part-3-of-6 (2024).

7 Clayton Swope, Kari A. Bingen, Makena Young & Kendra LaFave. Space Threat Assessment 2025; Center for Strategic and International Studies (CSIS), Washington, D.C., https://www.csis.org/analysis/space-threat-assessment-2025 (2025).

8 Northrop Grumman Corporation. SpaceLogistics: Making satellite servicing routine; Northrop Grumman Corporation, Falls Church, VA, https://www.northropgrumman.com/what-we-do/space/space-logistics-services (Accessed August 2026).

9 Jeff Foust. NASA reaffirms decision to cancel OSAM-1; SpaceNews, Denver, CO, https://spacenews.com/nasa-reaffirms-decision-to-cancel-osam-1/ (2024).

10 Space Development Agency (SDA). Proliferated Warfighter Space Architecture (PWSA); SDA, The Pentagon, Arlington County, VA, https://www.sda.mil/wp-content/uploads/2024/05/Transport-Layer_distro-A_FINAL.pdf (2024).

11 Strategic Headquarters for Space Development. Space Security Initiative; Strategic Headquarters for Space Development, Tokyo, Japan, https://www8.cao.go.jp/space/anpo/kaitei_fy05/enganpo_fy05.pdf (2023).

12 UK Space Agency. Guidance: Cross-government Space Domain Awareness (SDA) requirements; UK Space Agency, Ministry of Defence, Oxfordshire, England, https://www.gov.uk/government/publications/space-domain-awareness-requirements/cross-government-space-domain-awareness-sda-requirements (2026).

13 U.S. Space Force (USSF). U.S. Space Force Commercial Space Stragegy; USSF, Department of the Air Force, The Pentagon, Arlington County, VA, https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf (

14 North Atlantic Treaty Organization (NATO). NATO Commercial Space Strategy; NATO, Brussels, Belgium, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-commercial-space-strategy (2025).

15 National Aeronautics and Space Administration (NASA). State-of-the-Art of Small Spacecraft Technology: 11.0 Ground Data Systems and Mission Operations; NASA, Washington, D.C., https://www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations/ (2026).

16 European Commission Directorate-General for Defence Industry and Space (DG DEFIS). EU Space Strategy for Security and Defence; DG DEFIS, Brussels, Belgium, https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en (Accessed August 2026).

17 Brandon Bailey. Cybersecurity Protections for Spacecraft: A Threat Based Approach; Aerospace Corporation, Chantilly, VA, https://aerospace.org/paper/cybersecurity-protections-spacecraft-threat-based-approach (2021).

18 James McCarthy, Dan Mamula, Joseph Brule, Karri Meldorf, Rory Jennings, John Wiltberger, Chris Thorpe, John Dombrowski, O'Ryan Lattin & Sam Sepassi. Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) (NIST Interagency Report NIST IR 8441); National Institute of Standards and Technology (NIST); US Department of Commerce, Gaithersburg, MD; Washington, D.C., https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8441.pdf (2023).

19 Clayton Swope, Kari A. Bingen, Makena Young & Kendra LaFave. Space Threat Assessment 2025 (A Report of the CSIS Aerospace Security Project); Center for Strategic and International Studies (CSIS, Washington, D.C., https://www.csis.org/analysis/space-threat-assessment-2025 (2025).

20 Travis J. Kneen. Technologies and Strategies to Protect Satellites From Cyber and Electronic Warfare: What technologies and strategies are being assessed to mitigate electronic and cyber warfare threats to GPS and communication satellites in space?; Defense Systems Information Analysis Center (DSIAC), Belcamp, MD, https://dsiac.dtic.mil/technical-inquiries/notable/technologies-and-strategies-to-protect-satellites-from-cyber-and-electronic-warfare/ (2019).

21 Lisa Sodders & Brad Smith. Focused on the Threat: Electronic Warfare (Part 2 of 6); US Space Force (USSF) Space Systems Command (SSC) Public Affairs Office, Department of the Air Force, Los Angeles Air Force Base (LAFB), CA, https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/3907877/focused-on-the-threat-electronic-warfare-part-2-of-6 (2024).

22 Tabitha Reeves. JUST IN: Data Centers on Orbit Could Boost Space Operations, Experts Say; National Defense Industrial Association (NDIA), Arlington, VA, https://www.nationaldefensemagazine.org/articles/2026/3/25/data-centers-in-space (2026).

23 Christopher Huynh. AI on the Edge of Space; Center for Security and Emerging Technology (CSET), Walsh School of Foreign Service, Georgetown University, Washington, D.C., https://cset.georgetown.edu/wp-content/uploads/CSET-AI-on-the-Edge-of-Space.pdf (2025).

24 US Department of Defense (DOD). Commercial Space Integration Strategy; US DOD, The Pentagon, Arlington County, Virginia, https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF (2024).

25 North Atlantic Treaty Organization (NATO). Countering hybrid threats; NATO, Brussels, Belgium, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats (2026).

26 Kathleen Curlee. Sustaining the U.S. Edge in Remote Sensing, Launch, and Advanced Technologies for National Security; Center for Security and Emerging Technology (CSET), Walsh School of Foreign Service, Georgetown University, Washington, D.C., https://cset.georgetown.edu/wp-content/uploads/CSET-Sustaining-the-U.S.-Edge-in-Remote-Sensing-Launch-and-Advanced-Technologies-for-National-Security.pdf (2025).

27 Bruce McClintock, David Glickstein, Krista Langeland, Anca Agachi, Mélusine Lebret & Karen Schwindt. Establishing a Foundational Understanding of Dual-Use Space Activities; RAND, Santa Monica, CA, https://www.rand.org/pubs/research_reports/RRA4003-3.html (2026).

28 International Committee of the Red Cross (ICRC). The Principle of Distinction; ICRC, Geneva, Switzerland, https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf (2023).