Designer Satellite Collisions from Covert Cyber War

Jan Kallberg

Outer space has enjoyed two decades of fairly peaceful development since the Cold War, but once again it is becoming more competitive and contested, with increased militarization. Therefore, it is important the United States maintain its space superiority to ensure it has the capabilities required by modern warfare for successful operations. Today is different from earlier periods of space development,[1] because there is not a blatantly overt arms race in space,[2] but instead a covert challenge to US interests in maintaining superiority, resilience, and capability. A finite number of states consider themselves geopolitical actors; however, as long as the United States maintains space superiority, they must play according to a set of rules written without their consent and forced upon them. US space assets monitor the actions of authoritarian regimes and their pursuit of regional influence—a practice these regimes find quite disturbing. Therefore, any degradation or limitation of US space-borne capabilities would be seen as a successful outcome for such regimes. Cyber warfare offers these adversarial actors the opportunity to directly or indirectly destroy US space assets with minimal risk due to limited attribution and traceability. This article addresses how they might accomplish this objective. We must begin by examining US reliance on space before focusing on space clutter and the means an adversary might use to exploit it. While satellite protection is a challenge, there are several solutions the United States should consider in the years ahead.

US Reliance on Space

Network-centric warfare is dependent on the global information grid for joint war-fighting capabilities.[3] The pivotal layer creating global war-fighting

Jan Kallberg, PhD, is a Swedish-American lawyer, political scientist, and opinion writer. He received his doctorate in public affairs and MA in political science from the University of Texas at Dallas and holds a law degree from Stockholm University. His research interests include national security issues such as strategic deterrence and the Internet battlefield.

capability is the space backbone of the information grid where space assets are the decisive element. The United States depends on space-borne capabilities for success, and US national security relies today on a limited number of heavily used satellites. These satellites are crucial for strategic deterrence, surveillance, intelligence gathering, and military communications. If strategic deterrence fails, the satellites become an integral part of offensive and defensive ballistic missile defense. Satellites are pivotal not only for American space superiority but also for information superiority—the engine in the multichannel joint war-fighting machinery that has proven to be successful in recent conflicts. American forces can fight globally because of access to satellite-supported C4ISR. Potential adversaries of all sizes and intentions understand that American military might is closely linked to the capabilities of US space assets. James Finch and Shawn Steene of the Office of the Undersecretary of Defense for Policy express this unique link between space assets and national security well:

> Although other states increasingly utilize space for economic and military purposes, the United States is by far the most reliant on space systems due to its global responsibilities and high-technology approach to warfare that heavily leverages space systems for communication, navigation, and intelligence, surveillance, and reconnaissance. This asymmetry creates an imbalance; the more a nation relies on space systems, the more tempted a potential adversary is to target those systems.[4]

Since the fall of the Soviet Union, US space superiority has not been extensively challenged, and we have seen two decades of US space supremacy. Attacks against US satellites have been a concern since the 1970s,[5] with a focus on signal jamming, laser beams from the earth,[6] and direct kinetic antisatellite (ASAT) missile attacks. William J. Lynn III, former US deputy secretary of defense, stated in the summer of 2011, "The willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our warfighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate."[7]

Lynn's comments are to a high degree drawn from the *National Security Space Strategy* of January 2011. That strategy states that space is becoming congested, contested, and competitive. It clearly outlines the importance of protecting US space-borne capabilities:

> The *National Security Space Strategy* draws upon all elements of national power and requires active US leadership in space. The United States will pursue a set of

> interrelated strategic approaches to meet our national security space objectives: Promote responsible, peaceful, and safe use of space; provide improved US space capabilities; partner with responsible nations, international organizations, and commercial firms; prevent and deter aggression against space infrastructure that supports US national security; and prepare to defeat attacks and to operate in a degraded environment.[8]

Lynn also noted the impact of the growing amount of space debris:

> The specter of jamming is not the only new concern. The February 2009 collision of an Iridium communications satellite with a defunct Soviet satellite, and the earlier, deliberate destruction of a satellite by China, produced thousands of debris fragments, each of which poses a potentially catastrophic threat to operational spacecraft. In an instant, these events—one accidental, the other purposeful—doubled the amount of space debris, making space operations more complicated and dangerous.[9]

The deliberate kinetic attack and destruction of an outdated satellite by the Chinese themselves using an ASAT missile drew attention not only to the fact that the Chinese tested the missile and its policy impact[10] but also to the debris cloud the explosion created.

A Very Cluttered Space

The question of space debris is complicated by a myriad of issues involving not only the physical hurdles encountered in removing it but also legal and international issues.[11] As a result, space is becoming more congested, with around 1,100 active and 2,000 inactive satellites in orbit.[12] The amount of space debris has steadily increased over time,[13] with the total amount of debris currently tracked at 22,000 objects. The first steps to create a debris mitigation strategy were taken in the late 1970s.[14] Since then, thousands of satellites have been launched into space, and the majority of these are now either inactive or of an older technology generation and at the end of their life spans. The United States has led the debris reduction effort to mitigate risks by actively designing space vehicles that can be disposed of safely or removed by orbital decay.[15] The overriding concern regarding space debris is the mutual interest in limiting its effects and in creating a joint effort to decrease the amount of debris so that, eventually, orbital decay and gravity would prevail.

To understand the destructive power of space debris, one must consider velocity. A standard military-issue 5.56-mm round is traveling at 940 meters per second (m/sec.) when it leaves the barrel and can easily penetrate a

human being. The US Army's 120-mm tank round has a muzzle velocity of 1,740 m/sec. and can pass through a medium-sized battle tank.[16] Space debris and space junk traveling at circular orbital speed will hit a satellite at speeds of from 3,000 m/sec. up to 7,600 m/sec., depending on altitude. Debris traveling up to eight times faster than a high-velocity rifle round—whether a long-lost monkey wrench from the 1970s stamped "CCCP," small fragments, or an intentionally dispersed steel ball—creates an unprecedented impact. Deliberately creating space debris in specific orbits can radically change the probabilities of impact, even if the majority of that debris were dispersed in various directions or removed by physical effects. A targeted collision or a large debris cloud in identical orbit would nullify the option to move the target out of the targeted area. Satellites are fragile masterpieces of electronics, cables, connectors, solar panels, integrated circuits, and high-frequency antennas. Every inch has a dedicated function. Any object traveling at 7,600 m/sec. is a real threat to a satellite.

The Kessler Syndrome

Former NASA expert on space debris, Donald J. Kessler, predicted the probability for collisions in space and the risk of a high amount of space debris being generated by the impact of a high-velocity collision.[17] A chain reaction, called the Kessler Syndrome, could result. The Kessler Syndrome occurs when debris or another satellite hits a satellite or space junk with hypervelocity, creating a burst of more debris by the hypervelocity impact. If the satellite (or space junk) density is high enough, it can have a cascading effect through space. Kessler identified this problem but also clearly stated in the 1970s that the amount of space junk and satellites was too low to trigger such cascading effects and later reconfirmed that position. His contribution was to identify the potential problem and explain it. Since Kessler wrote about this phenomenon in 1978, he has returned to the topic to clarify, extend the question, or present his calculations.[18] Kessler's work is focused on unintended, random, and uncontrolled collisions. Similarly, the debate about space debris is focused on the unintentional creation of space debris by littering from space stations, exploding space boosters, and colliding objects.[19] In real terms—due to the limited probability for a random collision—the highest risk occurs with intended and premeditated creation of debris clouds that are concentrated around US mission-critical satellite orbits. If the collisions are intended, planned, and controlled, the risks are multiplied, presenting an adversary the

opportunity to destroy pivotal US satellite hardware. To reach a cascading threshold, an adversary can add space debris through controlled and intentional actions. The fastest way to add space debris to an orbit is to collide the existing mass of satellites and space junk that orbits Earth. If the mass already in space can be hijacked through cyber attacks, the attacker minimizes its exposure to traceability and attribution.

Types and Means of Attack

Satellites are a major concern for any state or nonstate actor who intends to conduct operations in secrecy. Satellites gather intelligence, provide surveillance, and perform reconnaissance. This can be extremely annoying to states that seek to avoid transparency between their international commitments, their public posture, and their actions behind the scenes. Several options are available to those actors who seek to diminish this satellite threat.

Kinetic Attacks. Essentially, an adversary can choose between two types of noncyber antisatellite attacks: direct kinetic and indirect kinetic. While a direct kinetic antisatellite missile attack on a US satellite is possible, it would provide direct attribution to the attacker, thus leading to repercussions. The thruster and the heat from the missile would be identified and attributed to the country or vessel that launched the attack. A direct kinetic attack might be inviting, but the political price is high. Even though it would be inviting to attack satellites, an adversary would not be able to attack without leaving a trace of tangible evidence. Using an ASAT missile is a grave act of war and can only reasonably be used if the perpetrator anticipates and accepts a wartime response.

For a potential adversary, it can be far more advantageous to increase the amount of debris that clutters specific orbits, thus epitomizing the indirect attack. Increasing debris can be accomplished through actively adding debris to specific well-targeted orbits, systematic designer accidents, or collisions in space.

During the eighteenth century and until the Second World War, artillery units had a special round to be used if enemy infantry came uncomfortably close to the battery position—the case shot. The battery aimed toward the closing infantry and fired the case shots, which dispersed thousands of steel balls that created massive losses in the infantry ranks. Whether those steel balls hit an arm, a leg, the torso, or a hand did not matter; the infantry assault against the battery position lost momentum

and ended. By applying the case shot idea to space, we can see an unsophisticated way to radically increase debris by using space boosters to reach lower Earth orbit (LEO) and then using kinetic energy to disperse hundreds of thousands of steel balls into a segment of space. Any obsolete or crude missile—exemplified by the Iranian Shahab or the North Korean Taepodong—could act as a space booster to take the payload to space. A salvo of 20 such crude space boosters delivering a significant amount of prefragmented shrapnel or steel balls could radically increase the amount of hypervelocity debris.

The probability for collision in space between a functional satellite and debris is a numbers game. Reduced to a simplified example, if the presence of 5,000 debris pieces at a specific altitude generates a risk of one satellite hit every 10 years—not taking into account additional debris generated from the impact—an additional 100,000 debris pieces would increase that risk drastically. To illustrate the principle, 20 space boosters can lift 30 metric tons of payload to LEO—roughly 400,000 steel balls—that would be spread at hypervelocity into the satellite orbits. The attack is kinetic but indirect, as the target satellites are not individually targeted but are instead approached by a swarm of hypervelocity debris that impacts the target satellites either by penetration or by destroying antennas, solar panels, or other equipment. This impact would initially generate more debris, although orbital decay would counterbalance some of it by moving it to a lower altitude; eventually it would disappear from space.

Either a direct or indirect kinetic attack would be an act of war and provide the necessary attribution to give the United States casus belli approved by at least a part of the international community. First, both the direct and indirect kinetic attack would be attributable to the nation that launched the attack, and observations from space-borne monitoring satellites would be accurate enough to give the United States a solid case. Second, creating unprecedented amounts of space debris would not only be hazardous to US satellites but also to those of other major powers. If rogue nation X launches an indirect kinetic attack, it would affect Russia's, Europe's, China's, India's, Pakistan's, and other nations' satellites. Depending on the dispersement of these debris objects, damage could be limited to small areas of space, but it would still be a space territory not used solely by the United States. Rogue nation X traditionally has avoided United Nations–supported repercussions from the international community when US interests have been damaged. Russia and/or China, in particular, are likely to veto any

punitive actions proposed by the United States in the UN Security Council.[20] In this scenario, rogue nation X cannot afford to lose that support by damaging Russian or Chinese space assets as collateral damage from its attack on US satellites. Chinese space assets are quite limited compared to Russian or US inventories; therefore, an indirect kinetic attack against US assets could result in severe damage to Chinese interests, as the Chinese lack space resilience. Neither direct nor indirect kinetic attacks are suitable or viable options for a rogue nation that intends to harm US satellites.

Cyber Attacks in Space. The life span of a satellite is between five and 30 years, and even afterward it can still be orbiting with enough propellant to move through space and with functional communications which could be reactivated. Space contains thousands of satellites, both active and inactive, launched by numerous organizations and countries, hosting 5,000 space-borne transponders communicating with Earth. Every transmission is a potential inlet for a cyber attack. Older satellites share technological similarities, providing opportunities to cyber-exploit industrial systems for control and processing. Supervisory control and data acquisition (SCADA) systems within our municipalities, facilities, infrastructure, and factories are designed and built on older technology and hardware, sometimes designed decades ago, and the software is seldom updated. These SCADA systems are considered a strategic vulnerability and have drawn growing attention from the US cyber-defense community in recent years. Satellites may be based on hardware and technology from the 1980s for one very simple reason—they are unlikely to be upgraded after they have been launched into space.

Terrestrial cyber attacks are a single exploit on thousands, if not millions, of identical systems, and the exploit will be eliminated afterward by updates or upgrades. The difference between satellites and terrestrial cyber exploits is that a satellite is in many cases custom made, whereas the computing design is proprietary. Cyber attacks in space exploit a single system, or limited group of systems, within a larger group of satellites. These space-borne assets have a variety of operating systems, embedded software, and designs from disparate technological legacies. As more nations engage in launching satellites with a variety of technical sophistication, the risk for hijacking and manipulation through covert activity increases. A satellite's onboard computer (OBC) can allow reconfiguration and software updates, which increase its vulnerability to cyber attacks. A vulnerable

satellite that will be orbiting for the next 10 years can be preset by a cyber perpetrator for unauthorized usage when needed.

Even with the most-advanced digital forensics tools, tracing a cyber attack is complicated on terrestrial computer systems, which are physically accessible. Space-borne systems do not allow physical access, thus, lack of access to the computer system nullifies several options for forensic evidence gathering. The only trace from the perpetrator is the actual transmissions and wireless attempts to penetrate the system. If these transmissions are not captured, the trace is lost.

If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Attribution can be graduated, and the level varies as to what would be accepted as an "attributed" attack. The national leadership can accept a lower level of tangible attribution, based on earlier intelligence reports and adversarial modus operandi, than the international community might demand, but it is restrained in taking action. China has had a growing interest in building cyber warfare capabilities[21] and is one of several nations that would have a sincere interest in degrading US space assets. Currently, nation-states are restrained by the political and economic repercussions of an attributed attack, but covert cyber war targeting US space assets removes the restraint of attribution.

A cyber attack resulting in a space collision would lack attribution and thus would be attractive to our covert adversaries. A collision between a suddenly moving foreign satellite and a mission-critical US satellite is neither a coincidence nor an accident. But without attribution, it does not matter that this is so obvious. Other forms of direct and indirect attack would be traceable to an attacker, which could result in military, economic, and political repercussions. In criminology we know that the major consideration of a perpetrator for premeditated acts is the risk of getting caught. The size of any repercussions if caught is secondary. If a cyber attack can destroy or disable US satellites with no attribution or traceability, it is likely to be considered by those who are openly adversaries and certainly by those who are covert. From a cyber warfare perspective, this creates an opportunity for a third party to hack and hijack a satellite with the express purpose of colliding with a mission-critical US satellite.

The attack could be either a direct collision or an indirect attack using the debris cloud from another collision. The ramming satellite can come from any country or international organization. The easiest way to perpetuate this attack would be to hijack satellites from countries less technically advanced or from less-protected or outdated systems.

The Hypervelocity Eight Ball. The term *hypervelocity eight ball* refers to the hitting of targeted satellites, directly or indirectly, with the intent to destroy the target by collision with hypervelocity objects. As previously discussed, the adversary can create a direct attack by ramming targeted US satellites with space vehicles through unauthorized cyber commands. The target for the initial step in an indirect attack may well be another satellite, part of a delivery vehicle, or space junk that will create significant debris upon impact. The collision creates hundreds or thousands of debris pieces that continue in space at high velocity. The debris cloud will affect other satellites in the collision orbit and may even initiate the Kessler Syndrome, causing proliferating damages if the threshold is reached.

Resolving the Space Challenge

While the problems and vulnerabilities in space and the means to attack space assets are significant, the United States does have options to mitigate these risks. The hypervelocity eight ball is more likely to occur if there are obsolete and inactive satellites abandoned in space that can be exploited for targeting and collision. Post-mission disposal (PMD),[22] the UN-initiated international effort to remove satellites after their productive life spans, would require satellites to be removed from space within 25 years[23] after their mission ends.[24] Naturally, it could happen earlier than 25 years, but it can also be a drawn-out process, as there are currently no tangible sanctions for noncompliance. If a satellite has a life span of 10–20 years, the additional 25-year allowance would increase the total number of years when the satellite can be remotely commanded to 35–45 years. Satellites launched in 1977, 1987, and 1997 are already technically outdated and several technology generations behind. The time between launch and end of operation for a satellite is the foundation for its cyber vulnerability. It is a sound financial decision to use a satellite to the full extent of its life span. But the question becomes Is it worth the risks? We must keep in mind technical leaps made since early space launches and what vulnerabilities could be embedded when space is populated by 25- to 45-year-old assets

that can still navigate. Since technology today develops so quickly, PMD in reality increases the risk of cyber attack by hijacked satellites because it prolongs the time a satellite can be remotely commanded by radio signals exploiting obsolete and outdated communication equipment. The United States should propose shortening the PMD removal period and insist on communications updates to create secure control for all space assets.

If the peaceful and safe use of space is threatened, the United States will seek to deter and defeat aggression against space infrastructure. Preparedness to defeat attacks and operate in a degraded environment requires resilience—the ability to absorb loss of capacity while remaining operational. A single satellite can be used for intelligence gathering, all levels of military communications, and as a platform for different sensors. A specific type or design of satellite can be of critical importance and, therefore, a high-value target for adversaries to destroy. If a budget shortfall forces the United States to overutilize its satellites, it also increases the reliance on each individual satellite for war fighting and intelligence.[25] The obvious risk in an era of austerity is that budget cuts will prevail over resilience in pivotal space systems.

The 2010 *National Space Policy* requires us to "increase assurance and resilience of mission-essential functions enabled by commercial, civil, scientific, and national security spacecraft and supporting infrastructure against disruption, degradation, and destruction, whether from environmental, mechanical, electronic, or hostile causes."[26] Even in an era of federal austerity, it will be necessary to replace an aging fleet of US space assets because these assets are crucial for both commercial and national security functions. That would mean an increased number of satellites, even if the investment would create significant redundancy. This redundancy is a safeguard against the ability to operate in a degraded environment and provides vital resiliency.

Finally, the United States must adopt an active defense and probe the boundaries of cyber war in space. A limiting factor for success in defending space assets against cyber attack is regulatory constraints on information operations conducted by the DoD and related agencies. It is a policy decision that requires policy makers to understand the unique tenets of cyberspace. The unique character of cyber war will require easing restrictions on preemptive cyber warfare. If the United States can determine which satellites—active or inactive—can be used for designer collisions as a result of communication or navigational weaknesses, it can secure the

disposal or safe removal of these vulnerabilities. By using active defenses, the United States increases its likelihood of detecting foreign countries trying to command satellite attacks.

The best way we can determine if the threat is real and if foreign space assets can be hijacked is to go out and try it ourselves—if only to determine possibilities. Assurance is not created by waiting for adversaries to execute their options and relying only on reactive incident response; instead, assurance requires mitigating the risks and determining the vulnerabilities. The only way to establish knowledge about foreign assets' vulnerabilities is to digitally probe their defenses. Taking an active defensive stand increases the opportunity to attribute and trace cyber attacks, which builds uncertainty among potential adversaries.

Conclusion

Attacking US satellites may well be a top priority for any potential or covert adversary, and the geopolitical benefit for successful covert attacks on US space assets is high. At the same time, the cost of entry into cyber warfare is low, which enables nation-states and nonstate actors that are unable to challenge US regional presence by conventional means to adapt and pursue unattributed cyber attacks against space assets to degrade US war-fighting ability.

Space assets are critical to the way the United States fights today, and it is likely the United States will be even more reliant on the use of space assets to maintain and defend information superiority in the foreseeable future. The fact that adversaries have not attacked, tampered with, or destroyed US satellites does not affirm their intent not to.

Cyber attacks are traditionally one shot, because they exploit a vulnerability that can be eliminated afterward or corrected by newer technology. In reality, with 3,000 satellites—active and inactive—on-orbit, it is likely some are already staged to be hijacked if needed. Any adversary might exploit the opportunity provided by a vulnerable satellite that will be orbiting for the next 10 years. Cyber attack also offers the option for an adversary not already at war with the United States to damage US satellites covertly.

The best solution is active defense: gather information and probe the vulnerabilities of US and foreign satellites, build new satellites to replace aging US space assets, maintain the full military radio spectrum to ensure

secure communications, and increase the number of satellites to ensure resilience in a degraded environment. Renewal and expansion of US space assets is critical for national security over the coming decades. SSQ

Notes

1. John Renaker, *Dr. Strangelove and the Hideous Epoch: Deterrence in the Nuclear Age* (Claremont, CA: Regina Books, 2000).

2. James Clay Moltz, *The Politics of Space Security*, 2nd ed. (Stanford, CA: Stanford University Press, 2011).

3. David S. Alberts, John J. Garstka, Richard E. Hayes, and David T. Signori, *Understanding Information-Age Warfare* (Washington: Command and Control Research Program Publication Series, 2001).

4. James P. Finch and Shawn Steene, "Finding Space in Deterrence: Toward a General Framework for 'Space Deterrence,' " *Strategic Studies Quarterly* 5, no. 4, (Winter 2011): 10–17. Finch and Steene are director and deputy director, respectively, of space policy and strategic development in the OSD-Policy.

5. "Soviet Arms Could Destroy U.S. Satellites, Brown Says," *Baltimore Sun*, 5 October 1977.

6. "Russian Laser 'Blinds' U.S. 'Spy Satellite', " *Chicago Tribune*, 22 November 1976.

7. William J. Lynn III, "A Military Strategy for the New Space Environment," *Washington Quarterly* 34, no. 3 (Summer 2011): 7–16.

8. Department of Defense, *National Security Space Strategy, Unclassified Summary* (Washington: DoD, January 2011), http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

9. Ibid.

10. Stefan A. Kaiser, "Viewpoint: Chinese Anti-Satellite Weapons: New Power Geometry and New Legal Policy," *Astropolitics* 6, no. 3 (Fall 2008): 313–23.

11. Andrew Brearley, "Faster than a Speeding Bullet: Orbital Debris," *Astropolitics* 3, no. 1 (Spring 2005): 1–34.

12. NASA, *Orbital Debris Quarterly News* 15, no. 4 (October 2011).

13. J. C. Liou and N. L. Johnson, "Risks in Space from Orbiting Debris," *Science* 311 (20 January 2006): 340–41.

14. Donald J. Kessler, "Sources of Orbital Debris and the Projected Environment for Future Spacecraft," AIAA International Meeting and Technology Display, AIAA-80-0855 (1980).

15. N. L. Johnson, "The Historical Effectiveness of Space Debris Mitigation Measures," *International Space Review* 11 (December 2005): 6–9.

16. American Ordinance, *KEW/KEWA1/KEWA2 Sales Brochure*, http://www.aollc.biz/pdf/120mmTankKEW.pdf.

17. Donald J. Kessler and Burton G. Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research* 83 (1978): 63.

18. Donald J. Kessler, Nicholas L. Johnson, J. C. Liou, and Mark Matney, "The Kessler Syndrome: Implications to Future Space Operations," presentation to 33rd Annual AAS Guidance and Control Conference, 6–10 February 2010, Breckenridge, CO.

19. United Nations Office for Outer Space Affairs, *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space*, http://orbitaldebris.jsc.nasa.gov/library/Space%20Debris%20Mitigation%20Guidelines_COPUOS.pdf.

20. "Russia and China Veto Draft Security Council Resolution on Syria, UN News Service," 4 October 2011, http://www.un.org/apps/news/story.asp?NewsID=39935&Cr=syria&Cr1=.

21. Kim Zetter, "Hackers Targeted U.S. Government Satellites," *Wired*, 27 October 2011, http://www.wired.com/threatlevel/2011/10/hackers-attack-satellites/.

22. P. H. Krisko, N. L. Johnson, and J. N. Opiela, "EVOLVE 4.0 Orbital Debris Mitigation Studies," *Advances in Space Research* 28, no. 9 (2001): 1385–90.

23. Nicholas L. Johnson, *The Disposal of Spacecraft and Launch Vehicle Stages in Low Earth Orbit* (Houston: NASA, 2007), http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20070021588_2007019149.pdf.

24. National Research Council Committee for the Assessment of NASA's Orbital Debris Programs, *Limiting Future Collision Risk to Spacecraft: An Assessment of NASA's Meteoroid and Orbital Debris Programs* (Washington: National Academies Press, 2011).

25. Office of the Undersecretary of Defense, *National Defense Budget Estimates for FY 2012*, http://comptroller.defense.gov/defbudget/fy2012/FY12_Green_Book.pdf.

26. *National Space Policy of the United States of America* (Washington: The White House, 2010), http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf.