High-Value Space Asset Defense and Threat Mitigation

Date Submitted: 06 May 2022

Word Count: 3599 words

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-May-2022	FINAL	N/A

4. TITLE AND SUBTITLE

High-Value Space Asset Defense and Threat Mitigation

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

LCDR Victor Schaefer

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Network-Centric warfare is a critical component of modern combat operations and allows the United States to retain an advantage in the Pacific Theatre. As these networks have evolved in complexity over time, a growing number have relied on space-based satellite architecture. Since its first successful Direct-Ascent Anti-Satellite (DA-ASAT) missile test in 2007, China has emerged as a challenger to U.S. superiority in space and has developed a robust anti-satellite capability. In preparation for future conflict, INDOPACOM must develop a Joint Space Defense Initiative (JSDI) to identify and defend the critical communication paths and datalinks that will enable U.S. network-centric warfare in the Pacific Theatre. To support this development, INDOPACOM must systematically:

1. Identify critical satellite links and designate high-value space assets (HVSA).
2. Develop methods to defend these space assets.
3. Develop tactics and procedures to mitigate the loss of an HVSA.

15. SUBJECT TERMS (Key words)
Satellite Defense, High-Value Space Asset, Joint Space Defense Initiative

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A		**19b. TELEPHONE NUMBER** *(include area code)* 401-841-6499

Standard Form 298 (Rev. 8-98)

Introduction

Given the critical nature of Network-Centric Warfare in modern combat operations and China's emergence as a near-peer military competitor, the United States Indo-Pacific Command (INDOPACOM) must be prepared to safeguard critical U.S. networks in a conflict where space is a contested domain. China's growing capabilities in the counter-space realm and Chinese doctrine that is increasingly bellicose when discussing space operations highlight the reality that a future conflict with China will have a significant orbital component.

In preparation for future conflict, INDOPACOM must develop a Joint Space Defense Initiative (JSDI) to identify and defend the critical communication paths and datalinks that will enable U.S. network-centric warfare in the Pacific Theatre. The JSDI must leverage current capabilities and be flexible enough to incorporate emerging technologies. To support this development, the INDOPACOM combatant commander must systematically:

1. Identify critical satellite links and designate high-value space assets (HVSA).
2. Develop methods to defend these space assets using current technology and identify future requirements if current capabilities are insufficient.
3. Develop tactics and procedures to mitigate the loss of an HVSA using current technologies and identify future requirements.

Background

The U.S. Armed Forces introduced Network-Centric Warfare in the 1990s to improve the precision of offensive and defensive firepower, decrease the time from identification to engagement, facilitate the massing of firepower at the correct time from dispersed units, and increase battlefield situational awareness.[1] As these concepts matured, the technology that

[1] U.S. Navy, *Copernicus . . . Forward C41 for the 21st Century*, U.S. Navy Brochure (Falls Church, Va: Information Assurance Technology Analysis Center, September 1995), 9, Accessed 26 April 2022, https://apps.dtic.mil/sti/pdfs/ADA390355.pdf

facilitated the networks became increasingly space-based, with satellite communication technology underlying the architecture of various data networks used by joint forces. The space basing of networks allows for the employment of weapon systems far beyond the visual horizon without the risk of flying manned aircraft close to the enemy.

Modern weaponry requires interconnected systems to function at maximum potential. Network-centric warfare is a prerequisite for overcoming the limitations of the curvature of the Earth and the dangers of emitting radars within enemy detection range. Most modern weapon systems do not operate primarily on visual cueing as gunnery did in the distant past. Weapons are increasingly launched using computer screens that integrate data from a connected radar system, satellites, aircraft, or sea-based sensors. The control systems for weapons today require target quality data to launch. An example of this process is the Naval Integrated Fires Element (NIFE), located at Buckley Space Force Base, CO. The joint NIFE team analyzes overhead data and provides location and identification information on adversary vessels to U.S. warships operating at sea.[2] The shipboard combat system processes this information, allowing the captain to decide how to best engage the target. Current conventional missile systems can strike sea-based targets at ranges up to 200 nautical miles (nm) and land-based targets at 1400nm.[3] [4] These missile ranges are well beyond a single ship or land station's visual or radar range and require targeting assistance from other sources. The networks that collect and transmit this target quality data are critical to enabling the operation of U.S. combat systems. As the U.S. joint force develops longer-range weapons and unmanned aerial systems (UAS), over the horizon targeting,

---

[2] Mimi Geerges, *Conversations from Surface Navy Association's 34th National Symposium*, video interview (Government Matters, 2022). Accessed 26 April 2022, https://govmatters.tv/conversations-from-surface-navy-associations-34th-national-symposium/.

[3] "Standard Missile-6 (SM-6)," Missile Defense Project (Center for Strategic and International Studies, 24 June 2021). Accessed 26 April 2022, https://missilethreat.csis.org/defsys/sm-6/.

[4] Antonio T Jones, "Long-Range Precision-Strike Cruise Missiles in Nato Operations," March 2014, 14. Accessed 26 April 2022, https://apps.dtic.mil/sti/citations/ADA607869.

identification and communication will become critical to retaining the advantage in any future conflict with the Peoples Republic of China (PRC).

Growing PRC Space Capabilities

The concept of Network-Centric warfare is not a well-kept secret, and United States' superiority in space is being challenged by the PRC. In 2007 China successfully tested a Direct Ascent Anti-Satellite (DA-ASAT) missile against a weather satellite in Low Earth Orbit (LEO).[5] Since then, China has rapidly expanded its counterspace proficiency and is assessed to have a "robust arsenal of space and counter-space capabilities."[6] The PRC's counterspace assets include DA-SAT missiles able to intercept satellites in LEO and are likely capable of Geosynchronous Orbit (GEO) and Medium Earth Orbit (MEO) intercepts.[7] Perhaps more concerning are co-orbital capabilities presented by the PRC, such as the SJ-17, an "inspector satellite" that maneuvers within the Geosynchronous Orbit (GEO) belt and can rendezvous with other satellites. While not an explicit ASAT weapon, it could be modified for the task. Other Chinese co-orbital assets have been observed with maneuvering capability that could also threaten LEO satellites. Co-orbital weapons are particularly menacing since they already operate in the space environment, can be represented as benign, and are prepositioned before the conflict begins. [8]

While kinetic threats to satellites are concerning and potentially disruptive, non-kinetic and indirect attacks on space-based networks can be equally disruptive. "Non-kinetic" counterspace weapons, such as lasing or high-powered microwaves, remain either classified or

---

[5] Mathias Kolleck, "Aircraft Survivability: Space Survivability - Time to Get Serious, Summer 2008," January 2008, 7. Accessed 26 Apr, 2022, https://apps.dtic.mil/sti/citations/ADA527998.

[6] Todd Harrison et al., "Space Threat Assessment 2022" (Center for Strategic and International Studies, April 2022), 10. Accessed 26 April 2022, https://www.csis.org/analysis/space-threat-assessment-2022.

[7] Todd Harrison et al., "Space Threat Assessment 2021," Policy File (Center for Strategic and International Studies, March 31, 2021), 10. Accessed 25 April 2022, ProQuest.

[8] Brian Weeden and Victoria Samson, "Global Counterspace Capabilities: An Open Source Assessment" (Secure World Foundation, April 2021), 1-10. Accessed 26 April 2022, https://swfound.org/media/207162/swf_global_counterspace_capabilities_2021.pdf.

have not been tested. However, China has proven it has a growing suite of jamming and spoofing electronic warfare capabilities to be used against space and non-space signals alike."[9] Russia, a close Chinese partner, has demonstrated intricate non-kinetic counter-space capabilities in recent years. "There are multiple, credible reports of Russia using jamming and other electronic warfare measures in the conflict in eastern Ukraine, and indications that these capabilities are tightly integrated into their military operations."[10]

Chinese cyber warfare capabilities must also be considered in any counter-space threat assessment. Electronic attack interferes with the transmission of RF signals using jamming or spoofing, while cyberattacks target the data itself through computer viruses or worms.[11] Chinese counterspace cyber capability is difficult to assess since open-source information on cyber warfare is opaque. However, China has successfully demonstrated cyber-attack ability against financial or defense-related targets and has a solid foundation to build counterspace cyber capability.[12]

Chinese warfare doctrine is highly space-focused and embraces space as the most important domain of conflict. Chinese military strategists routinely proclaim that " 'whoever controls space will control the Earth' and that outer space is the new high ground of military operations. They assert that the center of gravity in military operations has transitioned from the sea to the air and is now transitioning to space."[13] Chinese analysts assess that the U.S. Joint force relies on space for 80 percent of its communications and 70-90 percent of its intelligence.[14] Therefore, China views space infrastructure as a critical U.S. vulnerability that should be

---

[9] Harrison et al., "Space Threat Assessment 2022." 10
[10] Weeden and Samson, "Global Counterspace Capabilities: An Open Source Assessment." 2021, 2-1
[11] Harrison et al., "Space Threat Assessment 2022." 4
[12] Harrison et al., "Space Threat Assessment 2021." 11
[13] Weeden and Samson, "Global Counterspace Capabilities: An Open Source Assessment." 2021, 1-30
[14] Weeden and Samson, "Global Counterspace Capabilities: An Open Source Assessment." 2021, 1-29

targeted in a conflict. Considering Chinese doctrine and capabilities, the U.S. must anticipate that space superiority will be contested in future conflicts with the PRC.

Identifying High-Value Space Assets

The first task for INDOPACOM in countering this formidable threat must be identifying high-value U.S. space networks and assets. The U.S. has 2,944 satellites in orbit as of 31 December 2021.[15] Not all of these are critical to U.S. military interests. There are also a number of satellite ground stations that may be essential mission control links. These would require protection if inside the Chinese weapon release range. Developing the High-Value Space Asset (HVSA) list could be mission-specific: identify a critical capability and, working backward, identify the networks, satellites, and ground stations required.

One example of a critical capability could be a land attack mission using the Tomahawk Weapon System. The Tomahawk is a sea-launched land-attack missile with a range of 1400 nm. [16] Inherent requirements for a tactical tomahawk strike could be identified as: a Tomahawk Strike Network (TSN) requiring an ultra high frequency (UHF) satellite for in-flight mission updates, a planning and coordination communications network on an extremely high frequency (EHF) satellite, and Global Positioning System (GPS) satellite support (if required for targeting).[17] Once planners identify these components, the high-value assets for a Tomahawk mission can be codified.

The critical component of this planning is to identify what is absolutely necessary to accomplish the Tomahawk mission. Satellite assets are used for many supporting roles, ranging

---

[15] "UCS Satellite Database," Union of Concerned Scientists, January 1, 2022. Accessed 26 April 2022 https://www.ucsusa.org/resources/satellite-database.

[16] Jones, "Long-Range Precision-Strike Cruise Missiles in Nato Operations." 26

[17] Jeffrey S Mayer, "Tactical Tomahawk Weapon System Developmental/Operational Testing: Testing a System of Systems," December 13, 2005, 6. Accessed 26 April 2022, https://apps.dtic.mil/sti/citations/ADA497507.

from service-member internet access to television reception at sea. Eliminating these networks and other unnecessary and frivolous communication requirements is critical in the final HVSA list. Following this same tactic for other missions such as sea strike, air and missile defense (AMD), manned and unmanned aircraft strike operations, and other anticipated needs would narrow the field of defended assets. The development of HVSA lists should be a joint project and include elements from U.S. Space Command (USSPACECOM), U.S. Cyber Command (USCYBERCOM), U.S. Transportation Command (U.S. TRANSCOM), and the Department of Homeland Defense. Including all stakeholders will ensure the list covers all anticipated mission sets and critical infrastructure. Once this list is populated, defense and mitigation planning can begin.

Defending High-Value Space Assets

Once the HVSA list is complete, the joint force must develop a plan for the defense of the assets. The defense strategy must be comprehensive and include kinetic and non-kinetic means of protection. Defense strategies would vary based on the type of asset and can be broken down into defense of satellites themselves and defense of ground stations. Protection of satellites could be accomplished using movement-and-maneuver, deception, electronic or cyber warfare, and kinetic techniques. Ground stations could be defended using kinetic missile defense systems, mobility, cyber security, and electromagnetic hardening.

Satellite Defense

Maneuver warfare is one potential defense tactic for high-value satellite assets. Current satellite maneuverability is limited by power consumption and fuel. Electric and chemical propulsion systems onboard allow for small maneuvers like "adjusting their position to perform a

specific tasking."[18] The Defense Advanced Research Projects Agency (DARPA) is working to correct this deficiency by developing nuclear-powered satellites that would benefit from increased thrust and maneuverability.[19] However, even with current technology, "Academic research has shown that routine spacecraft maneuvers can be optimized to avoid detection by known sensors."[20] USSPACECOM and Space Force could develop apparently random maneuvering patterns applicable to current and near-future satellite capabilities. INDOPACOM would then have tactical doctrine and could direct satellites to "Constantly or intermittently conduct small maneuvers to frustrate an adversary's ability to calculate precise orbital parameters to target allied satellites and prevent it from understanding [U.S.] space plans, doctrine, strategies, and tactics."[21] This concept is similar to zigzag maneuvers used by ships to defeat submarine attacks during World War Two.[22] Ships would execute a (seemingly) spontaneous and random series of course changes to neutralize the threat of an attack by an enemy. Continuous or erratic maneuvers could deter ASAT or directed energy attacks by making the satellite's orbital pattern challenging to predict.

Deception is another option available to joint planners when developing satellite defense strategies. INDOPACOM could repurpose other satellites of minimal importance and mimic the orbital patterns of high-value assets. Combining this deception with the addition of electromagnetic decoys to emulate the high-value asset's radio frequency (RF) signature would

---

[18] Christopher Stone, "Maneuver Warfare in Space: The Strategic Mandate for Nuclear Propulsion," (Mitchell Institute, January 2022), vol. 33, 5. Accessed 26 April 2022, https://mitchellaerospacepower.org/wp-content/uploads/2022/01/Maneuver_Warfare_in_Space_Policy_Paper_33.pdf.

[19] "Faster, Higher, Stronger; Heavenly Power," The Economist (London), February 5, 2022, 70.

[20] Todd Harrison, Kaitlyn Johnson, and Makena Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons," Policy File (Center for Strategic and International Studies, February 25, 2021), 17. Accessed 26 April 2022, ProQuest.

[21] Paul Szymanski, "Techniques for Great Power Space War," Strategic Studies Quarterly 13, no. 4 (December 1, 2019): 81. Accessed 26 April 2022, JSTOR.

[22] Brian McCue, "An Exploration of Zigzagging," Phalanx (Alexandria) 37, no. 2 (June 1, 2004): 14 Accessed 26 April 2022, JSTOR.

confuse the enemy sensors. If the satellite comes under attack, A tactical decoy could be employed, such as the Air Force's ADM-160 Miniature Air-Launched Decoy, to misdirect the weapon's radar system.[23] These tactics would likely require modifying current satellites to equip them with RF decoy technology pre-conflict. Satellite servicing while in orbit is a complex task, but technology is progressing rapidly to simplify the process. Deception in concert with maneuver could effectively defeat or deter an attack by the PRC ASAT arsenal.

Offensive electronic or cyber warfare that disrupts the adversary's ability to track high-value satellite assets could also be a tactic for satellite defense. "China is developing a sophisticated network of ground-based optical telescopes and radars for detecting, tracking, and characterizing space objects."[24] It also has a "fleet of tracking ships and is developing relationships with countries that may host future sensors."[25] Jamming these radar systems would prevent the PRC's capability to track and target U.S. satellites. The ALQ-99 jamming pod mounted on the EA-18 Growler aircraft could be utilized to disrupt these radar systems. The pod's "jammer system facilitates optimization of transmitters and antennas for a given frequency range and can be tailored to meet mission requirements."[26] Cyber-attacks led by USCYBERCOM against Chinese radar and targeting systems can also be an option to protect U.S. space assets. "While electronic forms of attack attempt to interfere with the transmission of RF signals, cyberattacks target the data itself and the systems that use, transmit, and control the flow of data."[27] Seizure of command and control capabilities, sabotage, denial of service, and

---

[23] Harrison, Johnson, and Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons." 18

[24] Weeden Brian and Victoria Samson, "Global Counterspace Capabilities: An Open Source Assessment" (Secure World Foundation, April 2022), 03-19. Accessed 26 April 2022 https://swfound.org/media/207344/swf_global_counterspace_capabilities_2022.pdf.

[25] Weeden and Samson, "Global Counterspace Capabilities: An Open Source Assessment." 2022, 03-19

[26] "ALQ-99 Tactical Jamming System," Navy.Mil, September 16, 2021. Accessed 26 April 2022, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2395340/alq-99-tactical-jamming-system/.

[27] Harrison, Johnson, and Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons." 9

infiltration of systems could be leveraged to prevent the use of counter-space systems against U.S. assets. These tactics could be highly effective but also present a risk. Offensive electronic and cyber operations could be considered escalatory if executed pre-conflict. Additionally, once used, the enemy would become aware of the cyber and electronic capabilities and develop mitigation tactics.

The final defensive strategy for high-value satellite assets is a kinetic defense against DA-ASAT weapons. China's direct-ascent ASAT launch vehicle appears to be a mobile variant of the DF-21 medium-range ballistic missile (MRBM).[28] The AEGIS Ballistic Missile System using SM-3 Block IIA Missiles could defeat this type of missile. The AEGIS system is deployed on U.S. Navy destroyers and cruisers. The SM-3 Block IIA missiles are the latest and most capable variant designed to target ballistic missiles in the midcourse phase of flight above the atmosphere (AEGIS BMD 4).[29] Analysts estimate that "20 direct-ascent ASATs would be needed to guarantee the destruction of the six or seven EO/SAR satellites that are thought to currently constitute the bulk of classified U.S. national security space imaging."[30] Several AEGIS capable ships could be assigned to high-value space asset protection duty and destroy the DA-ASATs in flight. SM-3 missiles could potentially also be repurposed to destroy co-orbital ASATs that begin to exhibit suspicious or aggressive behavior. However, this tactic would have to be weighed against the potential creation of destructive space debris and the escalatory nature of a kinetic preemptive strike.

---

[28] Ian Easton, "The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy" (Project 2049 Institute), 2. Accessed 26 April 2022, https://project2049.net/2009/06/24/the-great-game-in-space-chinas-evolving-asat-weapons-programs-and-their-implications-for-future-u-s-strategy/.

[29] Ronald O'Rourke, "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress" (Congressional Research Service, 1 April 2022), 4. Accessed 26 April 2022, https://sgp.fas.org/crs/weapons/RL33745.pdf.

[30] Easton, "The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy." 4

Ground Station Defense

Defense of the satellite ground control segment is also critical to maintaining the networks required for network-centric warfare. The ground segment "handles satellites in orbit, monitors satellite health and provides monitoring and planning of operations."[31] One method of making these segments more survivable is mobility. The new Advanced Extremely High Frequency Satellite System employed by the Space Force is supported by a number of fixed and mobile stations to ensure the system's survivability in an enemy attack.[32] Some critical space infrastructure cannot be made mobile. An example is the Space Fence Radar located at Kwajalein Atoll in the Republic of the Marshall Islands. The radar system is the most advanced space radar system in the world and "provides information that Space Force needs to make informed decisions and take actions to protect key assets in orbit."[33] If Space Fence were determined to be an HVSA, it would need to be protected from kinetic attack. Theatre High Altitude Area Defense (THAAD) and the Patriot Missile System are two mobile missile defense systems operated by the U.S. Army that could be used to protect against ship-based land-attack cruise missiles and ballistic missiles.[34][35]

Cyber and Electromagnetic spectrum attacks against ground systems are also a concern that must be addressed in the defense plan. INDOPACOM, with support from USCYBERCOM, could dispatch cyber defense teams to ensure that satellite ground stations are properly air

---

[31] "Advanced Extremely High Frequency (AEHF) Satellite System," Airforce Technology, March 19, 2021. Accessed 26 April 2022, https://www.airforce-technology.com/projects/advanced-extremely-high-frequency-aehf/.
[32] "Advanced Extremely High Frequency (AEHF) Satellite System."
[33] "Space Fence," Lockheed Martin, 2022. Accessed 26 April 2022, https://www.lockheedmartin.com/en-us/products/space-fence.html.
[34] "THAAD Theatre High Altitude Area Defense – Missile System," Army Technology, July 27, 2020 Accessed 26 April 2022, https://www.army-technology.com/projects/thaad/#:~:text=The%20THAAD%20missile%20uses%20kinetic,hit%2Dto%2Dkill%20technology.
[35] "Patriot Missile Long-Range Air-Defence System," Army Technology, March 14, 2022, Accessed 26 April 2022, https://www.army-technology.com/projects/patriot/.

gapped from the public internet. "Air-gapped systems that are physically separated from the public internet can make attempts to infiltrate a system much more difficult for an adversary without insider help."[36] Systems that communicate with satellites must use the latest encryption technology, and all new communication paths should be designed with jam-resistant waveforms and frequency hopping spread spectrum technology (FHSS). "FHSS involves rapidly changing the transmission frequency using a pseudorandom pattern."[37] Frequency hopping makes jamming difficult since the jammer cannot easily match the transmitter's frequency. Some of these techniques will require hardware and software upgrades beyond the capability of the combatant commander. However, operational requirements often drive procurement. Vulnerabilities identified in the high-value asset defense planning process can drive demand for new technology development.

Mitigating the Loss of an HVSA

To guard against the loss of an HVSA, INDOPACOM planners must develop mitigation strategies to maintain the lost network capability. These mitigation strategies could involve the employment of a backup satellite or a non-satellite asset that can temporarily provide network access. USSPACECOM could allocate a predesignated backup satellite to restore the network. If no backup is available, INDOPACOM should have designated non-space assets allocated to the task. For example, if a satellite Link-16 Network is required to maintain targeting data on a threat ship or aircraft, but the satellite or controlling station is lost, a collection of unmanned aerial systems (UAS) and manned aircraft could replace the satellite and enable connectivity. MQ-4

[36] Harrison, Johnson, and Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons." 16

[37] Harrison, Johnson, and Young, "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons." 15

Triton UAS, E2-D Hawkeye aircraft, and E-3 Sentry aircraft are all examples of Link-16 capable units.[38] Each could maintain the link over an area of 400-500NM and provide overlapping network continuity.[39]

Shifting satellites and launching aircraft to cover network losses will require significant joint force and interagency coordination. INDOPACOM must execute theatre-wide exercises to test the feasibility of coordinated communications shifts in realistic combat scenarios. Some networks may only have a satellite architecture, and mitigation may be difficult or impossible due to a lack of redundancy. Identification of these vulnerabilities can drive technical and tactical solutions. An example of a mitigation solution to known network vulnerability is The Air Force Research Lab (AFRL) experimenting with installing Link-16 transponders on LEO satellites rather than traditional GEO communications satellites. While the LEO may be easier to target, they are more dispersed, orbit the Earth faster, and are more numerous. According to a project representative, "We have a proliferated LEO constellation… what we could do is put one of these Link 16 transponders onto each of these LEO satellites and you would...have a Link 16 capability... all the time, all over the world."[40] This capability could be applied to other networks but only if these are identified as critical, and the demand is clear to drive new tactics and technologies.

---

[38] "MQ-4C Triton Broad Area Maritime Surveillance (BAMS) UAS," Naval Technology, September 18, 2020. Accessed 26 Aug 2022, https://www.naval-technology.com/projects/mq-4c-triton-bams-uas-us/.

[39] Tom Schlosser, "Potentials for Navy Use of Microwave and Millimeter Line-of-Sight Communications (Final Report)," Potentials for Navy Use of Microwave and Millimeter Line-of-Sight Communications (Final Report), February 1, 1996, 2. Accessed 26 April 2022, https://apps.dtic.mil/sti/pdfs/ADA318338.pdf . Equations are utilized to calculate the potential range of Link-16 coverage based on nominal aircraft and UAS altitudes.

[40] Courtney Albon, "AFRL Aiming To Fly LINK 16 Transponder On Satellite Next March," Inside the Pentagon's Inside the Air Force 31 (Arlington: Inside Washington Publishers, June 12, 2020), no. 24, Accessed 26 April 2022, ProQuest

Counterargument

Opponents of network-centric warfare have argued that U.S. forces should be actively working to reduce reliance on networks rather than fighting to maintain them in combat. Admiral Scott Swift in his article Master the Art of Command and Control, asserts, "In the increasingly hyper-technological age in which the U.S. military may be called on to fight, too much time, attention, and resources are being devoted to the science of warfare, rather than the art of it."[41] He asserts that the U.S. should be reducing our reliance on elaborate technology and finding ways to reduce dependence on networks. Admiral Swift stresses, "we must not become reliant on systems that can be disrupted easily in battle. Instead, we should…enable "mission command" by providing clear and widely understandable commander's guidance and intent before communications and networks are put at risk."[42] The central root of this argument is that clear and coherent guidance issued to commanders can overcome the loss of networks in combat by leveraging leaders' initiative in battle.

Another argument is that kinetic space warfare is unlikely since the debris fields created by widespread satellite destruction will destroy all satellite activity in space, rendering Earth's orbit closed to all. Analysts have asserted that the "Creation of too much space debris during space conflicts may make losers out of all sides."[43] Large amounts of orbiting debris would be the 21st-century equivalent of deterrence based on mutually assured destruction. The inability to operate in orbit would set humanity back to a pre-space age lifestyle. A recent Russian DA-ASAT test supported this assertion. On November 15th, 2021, a Russian missile destroyed a Soviet-era weather satellite in low earth orbit. The destruction created 1500 trackable pieces of

---

[41] Scott Swift, "Master the Art of Command and Control," United States Naval Institute. Proceedings 144 (Annapolis: United States Naval Institute, February 1, 2018), no. 2, 30.
[42] Swift, "Master the Art of Command and Control," no. 2, 31
[43] Szymanski, "Techniques for Great Power Space War," 89.

debris and threatened to damage the international space station.[44] When a satellite is destroyed, "the debris starts off close to the satellite's previous position and orbit…Over weeks, the debris (will) spread out...into a shell" around Earth.[45] Multiple satellites destroyed in orbit could create a thick shell of debris moving at orbital speeds around the globe, threatening anything in orbit. For this reason, the United States has announced an end to all DA-ASAT testing in a move to reduce the risk of debris in the current space environment.[46] As more countries become aware of the risk associated with orbital debris, universal access denial of Earth's orbit could deter kinetic satellite attacks in a future conflict.

Conclusions

Network-Centric warfare is a critical component of modern combat operations and allows the United States to retain an advantage in the Pacific Theatre. The capability to communicate and accurately employ ammunition over the horizon with tremendous accuracy and lethality can overcome the growing advantage in total force size that the PRC can field in combat. Modern combat systems increasingly require target quality data from non-organic sensors. Although space-based assets and networks are vulnerable to attack, the argument for transitioning away from an interconnected joint force would advocate that the U.S. cede a significant advantage. Networks are more than just communication tools, and no amount of commander initiative can produce target quality data hundreds of miles beyond human sight. The argument that kinetic strike capability is unlikely due to debris risk ignores the fact that the United States has six times as many satellites in orbit than the PRC and would therefore bear the more extensive loss in operational capability.

---

[44] "Fragmentation Grenade; ASATs and the ISS," The Economist (London), November 20, 2021, 77.
[45] "Fragmentation Grenade; ASATs and the ISS," 77.
[46] "Launch Break; Space War," The Economist (London), April 23, 2022, 72.

Near peer and peer competitors have threatened U.S. forces in the past. Adversary development of anti-ship cruise missiles has resulted in hardened ships with missile defense systems and tactics. Anti-aircraft weapons have led to the development of superior stealth airframes and countermeasures. The threat of attack on networks requires yet another generation of improvement to the United States' combat systems. While the problem of network defense is complex, it is inherently a joint service problem as all U.S. Services have capabilities to contribute to the solution. Network-centric warfare is too critical to abandon or lose due to a lack of coherent planning. A future conflict with the PRC will involve conflict in the space domain. INDOPACOM must systematically identify critical networks and develop a Joint Space Defense Initiative to maintain these systems in a real-world combat environment.

Glossary

ASAT: Any type of Anti-Satellite Weapon system

Co-Orbital ASAT: An attacking satellite that is first placed into orbit, and then later maneuvered into an intercepting orbit. [47]

Direct Ascent Anti-Satellite (DA-ASAT): A direct-ascent ASAT typically involves a medium- or long-range missile launching from the Earth to damage or destroy a satellite in orbit.[48]

Geosynchronous Earth Orbit (GEO): Satellites orbiting at 35,786 km (22236 miles) and have an orbital period precisely equal to one day.[49] These satellites observe the Earth as if it were not rotating since the speed is equal to that of the Earth's rotation. Satellites in GEO are constantly in the field of view for approximately one-third of the planet's surface. [50]

Low Earth Orbit (LEO): An orbital regime at altitudes between 160 km (100 miles) and 2,000 km (1242 miles).[51] Due to the satellites' relative closeness to the Earth, satellites in LEO typically take between 90 minutes and 2 hours to complete one full orbit around the Earth.[52]

Medium Earth Orbit (MEO): The orbital zone between LEO and GEO.[53]

Joint Space Defense Initiative (JSDI): A proposed Joint Force initiative to identify and defend High-Value Space Assets, and mitigate the loss of critical space based networks.

High-Value Space Asset (HVSA): A satellite or satellite linked ground station designated under the JSDI as high-value. These assets should have a defense and/or mitigation plan assigned.

---

[47] "Counterspace Weapons 101," Aerospace Security, July 23, 2020. Accessed 2 May 2022, https://aerospace.csis.org/aerospace101/counterspace-weapons-101/.
[48] "Counterspace Weapons 101."
[49] "Popular Orbits 101," Aerospace Security, October 26, 2020. Accessed 2 May 2022, https://aerospace.csis.org/aerospace101/popular-orbits-101/.
[50] "Popular Orbits 101."
[51] "Popular Orbits 101."
[52] "Popular Orbits 101."
[53] "Popular Orbits 101."

BIBLIOGRAPHY

"Advanced Extremely High Frequency (AEHF) Satellite System." Air Force Technology, March 19, 2021. https://www.airforce-technology.com/projects/advanced-extremely-high-frequency-aehf/.

Albon, Courtney. "AFRL Aiming to Fly Link 16 Transponder on Satellite Next March." Inside the Pentagon's Inside the Air Force 31. Arlington: Inside Washington Publishers, June 12, 2020. ProQuest.

"ALQ-99 Tactical Jamming System." Navy.Mil, September 16, 2021. https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2395340/alq-99-tactical-jamming-system/.

Barnett, John. *Mission Command Will Not Save the Navy*. Newport, RI: NWC, 2020.

Brian, Weeden, and Victoria Samson. "Global Counterspace Capabilities: An Open Source Assessment." Secure World Foundation, April 2022. https://swfound.org/media/207344/swf_global_counterspace_capabilities_2022.pdf.

"Counterspace Weapons 101." Aerospace Security, July 23, 2020. https://aerospace.csis.org/aerospace101/counterspace-weapons-101/.

Easton, Ian. "The Great Game in Space: China's Evolving ASAT Weapons Programs and Their for Future U.S. Strategy." Project 2049 Institute. June, 24 2009. https://project2049.net/2009/06/24/the-great-game-in-space-chinas-evolving-asat-weapons-programs-and-their-implications-for-future-u-s-strategy/.

"Faster, Higher, Stronger; Heavenly Power," The Economist (London), February 5, 2022, 70.

"Fragmentation Grenade; ASATs and the ISS," The Economist (London), November 20, 2021, 77.

Garretson, Joshua J. "Satellite Servicing: A History, the Impact to the Space Force, and the Logistics Behind It ," Wild Blue Yonder, 2021. https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/2538269/satellite-servicing-a-history-the-impact-to-the-space-force-and-the-logistics-b/

Geerges, Mimi. *Conversations from Surface Navy Association's 34th National Symposium*. Video Interview. Government Matters, 2022, 5:22. https://govmatters.tv/conversations-from-surface-navy-associations-34th-national-symposium/.

Harrison, Todd, Kaitlyn Johnson, Joe Moye, and Makena Young. "Space Threat Assessment 2021." Policy File. Center for Strategic and International Studies, March 31, 2021. ProQuest.

Harrison, Todd, Kaitlyn Johnson, and Makena Young. "Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons." Policy File. Center for Strategic and International Studies, February 25, 2021. ProQuest.

Harrison, Todd, Kaitlyn Johnson, Makena Young, Nicholas Wood, Alyssa Goessler, and Susan M Gordon. "Space Threat Assessment 2022." Center for Strategic and International Studies, 2022. https://www.csis.org/analysis/space-threat-assessment-2022.

Jones, Antonio T. "Long-Range Precision-Strike Cruise Missiles in Nato Operations," March 2014. https://apps.dtic.mil/sti/citations/ADA607869.

Kolleck, Mathias. "Aircraft Survivability: Space Survivability - Time to Get Serious, Summer 2008," January 2008. https://apps.dtic.mil/sti/citations/ADA527998.

"Launch Break; Space War," The Economist (London), April 23, 2022, 72.

Mayer, Jeffrey S. "Tactical Tomahawk Weapon System Developmental/Operational Testing: Testing a System of Systems," December 13, 2005. https://apps.dtic.mil/sti/citations/ADA497507.

McCue, Brian. "An Exploration of Zigzagging," Phalanx (Alexandria) 37, 37, no. 2 (June 1, 2004): 14–29. JSTOR

"MQ-4C Triton Broad Area Maritime Surveillance (BAMS) UAS." Naval Technology, September 18, 2020. https://www.naval-technology.com/projects/mq-4c-triton-bams-uas-us/.

O'Rourke, Ronald. "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress. CRS Report." Congressional Research Service, 2022. https://sgp.fas.org/crs/weapons/RL33745.pdf.

"Patriot Missile Long-Range Air-Defence System." Army Technology, March 14, 2022. https://www.army-technology.com/projects/patriot/.

"Popular Orbits 101." Aerospace Security, October 26, 2020. https://aerospace.csis.org/aerospace101/popular-orbits-101/.

Schlosser, Tom. "Potentials for Navy Use of Microwave and Millimeter Line-of-Sight Communications (Final Report)." Naval Command Control and Ocean Surveillance Center RDT&E Division, February 1, 1996. https://apps.dtic.mil/sti/pdfs/ADA318338.pdf.

Singleton, Andrew. Threatening Celestial Lines of Communication: A Naval Counterspace Concept for Deterring China's Preemptive Space Strike. Newport, RI: NWC, 2021.

"Space Fence." Lockheed Martin, 2022. https://www.lockheedmartin.com/en-us/products/space-fence.html.

"Standard Missile-6 (SM-6)." Missile Defense Project. Center for Strategic and International Studies, June 24, 2021. https://missilethreat.csis.org/defsys/sm-6/.

Stone, Christopher. "Maneuver Warfare in Space: The Strategic Mandate for Nuclear Propulsion." Vol. 33. 33. Mitchell Institute, January 2022. https://mitchellaerospacepower.org/wp-content/uploads/2022/01/Maneuver_Warfare_in_Space_Policy_Paper_33.pdf.

Swift, Scott. “Master the Art of Command and Control.” United States Naval Institute. Proceedings 144. 28-33, Annapolis: United States Naval Institute, February 1, 2018.

Szymanski, Paul. “Techniques for Great Power Space War,” Strategic Studies Quarterly 13, 13, no. 4 (December 1, 2019): 78–104. JSTOR.

“THAAD Theatre High Altitude Area Defense – Missile System.” Army Technology, July 27, 2020. https://www.army-technology.com/projects/thaad/#:~:text=The%20THAAD%20missile%20uses%20kinetic,hit%2Dto%2Dkill%20technology.

“UCS Satellite Database.” Union of Concerned Scientists, January 1, 2022. https://www.ucsusa.org/resources/satellite-database.

U.S. Navy. Copernicus . . . Forward C41 for the 21st Century. U.S. Navy Brochure. Falls Church, VA: Information Assurance Technology Analysis Center, September 1995. https://apps.dtic.mil/sti/pdfs/ADA390355.pdf.

Weeden, Brian, and Victoria Samson. “Global Counterspace Capabilities: An Open Source Assessment.” Secure World Foundation, April 2021. https://swfound.org/media/207162/swf_global_counterspace_capabilities_2021.pdf.