Reframing the Special Operations Forces-Cyber-Space Triad

Special Operations' Contributions to Space Warfare

Maj. Brian Hamel, U.S. Army

SOF has a culture of decentralized combat operations with a focus in the human domain.

—Col. Mark Orwat

Humans are always in the loop of spacepower.

—Dr. Bleddyn Bowen

In November 2021, the commander of the U.S. Army Special Operations Command, Lt. Gen. Jonathan Braga, articulated a new deterrence framework to his staff.[1] This emergent framework included the space, cyberspace, and special operations communities having symbiotic relationships to converge effects throughout the competition continuum. As a homage to the nuclear Triad (intercontinental ballistic missiles, submarine-launched ballistic missiles, and strategic bombers), this "special operations forces (SOF)-cyberspace-space Triad" provides policymakers additional options to campaign against our adversaries. While the Triad has made substantial headway, no existing literature delineates the nexus of the SOF-space relationship. Joint Publication 3-14, *Space Operations*, and Field Manual 3-14, *Army Space Operations*, are both quick to point out that SOF receives effects from space, but only a few student theses and authors tangentially describe how SOF can create effects in the space domain.[2] In this study, the author elucidates the SOF-space segment of the Triad and recommends that the joint SOF enterprise conduct preparation of the environment, special reconnaissance, and military information support operations to set the conditions to influence, deceive, or degrade adversarial terrestrial-based, space-enabling infrastructure.

Unfortunately, SOF has not clearly defined how it can generate effects in the space domain. Failure to prescriptively delineate effects ensures that our adversaries will continue to hold positions of relative advantage and predisposes any efforts to failure due to their inability to be accurately measured and war-gamed prior to execution. This sharply increases risk to force and risk to mission. Current unclassified literature explains that SOF receives effects from the space domain through services such as satellite communications; positioning, navigation, and timing; and intelligence, surveillance, and reconnaissance. This article expounds on how SOF core activities, normally conducted during irregular warfare (IW), can create effects in the space domain to advance concepts within the Triad and provide flexible response options to counter the People's Liberation Army Strategic Support Force, which was created in 2015.[3]

How Can SOF Contribute?

Space warfare should not be synonymous with orbital warfare, or warfare that only takes place in the space segment (see the figure). The preponderance of space warfare relies on terrestrial infrastructure (ground segment), and more importantly, the human beings making decisions on how to manipulate that infrastructure and employ those capabilities. In that vein, the decision-making calculus, biases, and heuristics of our adversaries are as important as the on-orbit capability that they control. While U.S. Space Command manages the space segment portfolio against adversaries of the United States, there is ample opportunity for the joint SOF enterprise to examine how they can contribute to degrading the terrestrial-based, space-enabling infrastructure (SEI) of our adversaries.

U.S. Army Special Operations Command distinctive unit insignia (Image courtesy of the U.S. Army via Wikimedia Commons)

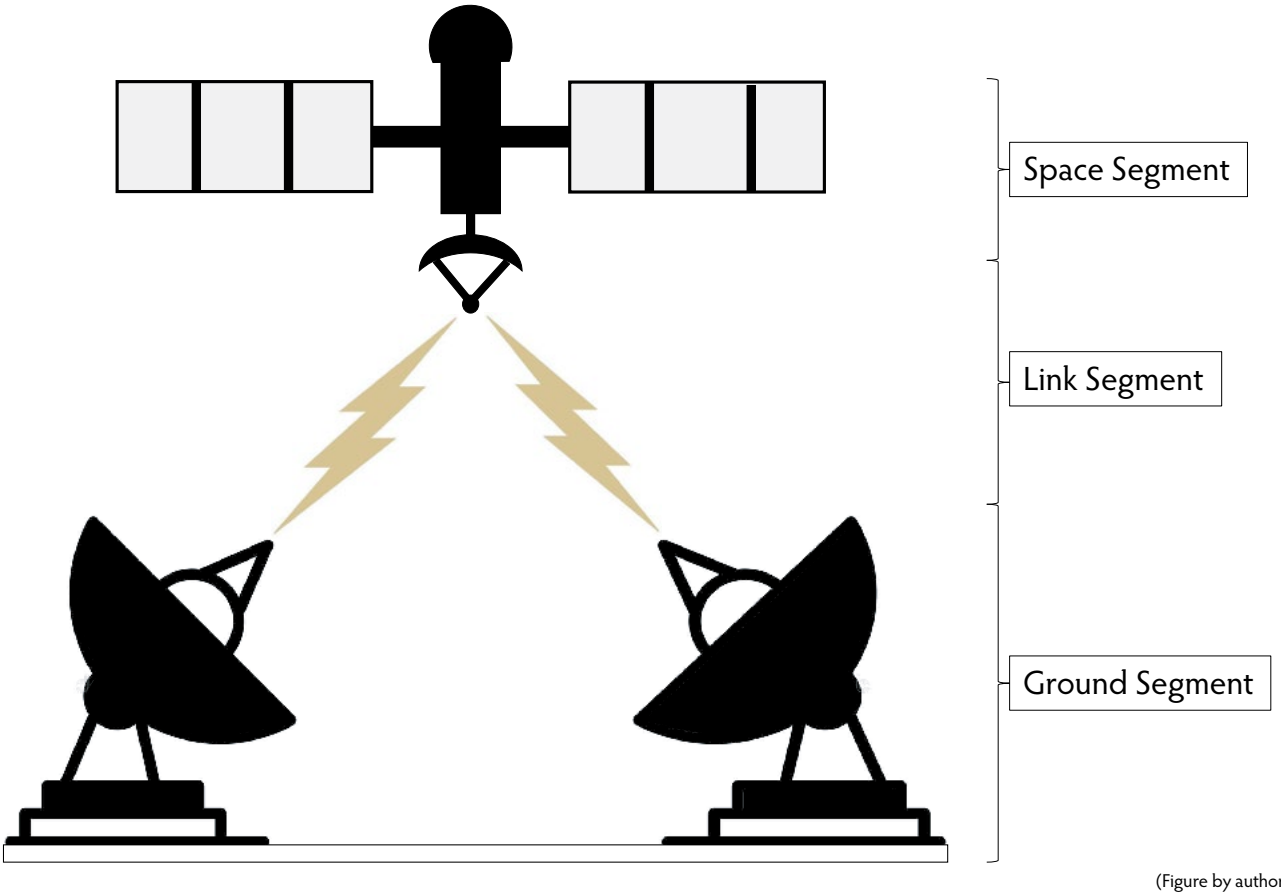
What does SEI encompass? The closest related term is critical infrastructure, but that definition varies throughout publications within the Department of Defense and the civilian community, neither of which come close to accurately explaining the intricacies of SEI. In lieu of no practical definition for SEI, the author proposes an amalgamation of tangentially related definitions to encapsulate the changes of the contemporary operational environment. Therefore, SEI is the

> systems, physical facilities, services, support personnel, staff, and essential services necessary to support operations, activities, and investments, to, from, and through space. This includes but is not limited to the activities conducted on the electromagnetic spectrum, launch facilities, ground control stations, celestial lines of communication, spaceports, computer hardware, software, and the cyber infrastructure that enables these operations, activities and investments. At an operational and strategic level, SEI encompasses legal infrastructure to include regulations, resources, and policies that govern a country's commercial, civil, and military space program and its interoperability with other state-owned and civilian-owned SEI.[4]

While a broad definition could dissuade some, the intent is to showcase as many vulnerabilities as possible as the adversary and type of the terrestrial infrastructure will change based off the geographic area of responsibility. As an example, a People's Republic of China space situational awareness site in South America may not have the same vulnerabilities as a Russian electronic warfare platform in Ukraine.

Modified Methodology and Results

This article uses the same case study as the thesis from which it was derived. The thesis describes the Espacio Lejano ground station in Neuquén, Argentina, one of several ground stations that the People's Republic of China uses to transmit information for assets over the Southern Hemisphere. Understanding that the Chinese Communist Party is responsible for all national-level operations, activities, and investments (OAI) has led many in the region, and in Washington, D.C., to suspect that this ground station is dual use.[5] Espacio Lejano is run by China Satellite Launch and Tracking Control, a subentity of the People's Liberation Army Strategic Support Force, and currently boasts a primary antenna of 35 m and a secondary antenna of 13.5 m.[6] Recent assessments indicate that the larger antenna has been broadcasting data in the S and X band for sending data, and in the Ka band for receiving data.[7] Transmission of classified information typically occurs on the X and Ka bands, which is why there is



(Figure by author)

Figure. Different Segments of the Space Domain

scrutiny regarding the site's dual use. Scholars assess that the site at Espacio Lejano contributes to China's space situational awareness network and supports interplanetary spacecraft missions as part of China's Deep Space Network.[8] As is the case at other regional ground stations, China has also come under criticism for spying on other governments while it conducts its own space operations.[9] The repercussions of this could potentially back China into a corner and may force it to engage with one of the few sympathetic regional partners it has left, Venezuela.[10] This could limit the efficacy of China's OAIs by geographically constraining operations that typically require broad geographic dispersion to be effective.

Using this case study as a backdrop for the analysis, the author also standardized definitions for degradation measures. In this article, the word "degrade" is a sliding scale of potential effects as noted in table 1.[11]

With degrade now understood and SEI defined, the case study offers an opportunity to examine the realm of the possible SOF core activities that could be conducted against this ground site. It does not evaluate the efficacy of the actions, the risk, attribution, or second- and third-order effects. Through the lens of analytic generalization, table 2 was compiled to evaluate the outcome of SOF core activities juxtaposed against an adversary's SEI with an annotation of D, I, or N, for whether that core activity could directly (D), indirectly (I), or not degrade (N) the adversary's SEI. For the sake of brevity, not every core task will be explained. Please note that the definition for each SOF core activity as it is used in this article can be found in Joint Publication (JP) 3-05, *Special Operations*.

SOF Direct Effects against the Ground Segment

Direct action. Direct action (DA) would primarily be aimed at disrupting, denying, degrading, or destroying adversarial SEI. This could be conducted through raids, electronic warfare, sabotage from human

Table 1. Space Negation Measures

Deceive	Measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence or information into a system, to induce the adversary to react in a manner prejudicial to their interests.
Disrupt	Measures designed to temporarily impair an adversary's use or access of a system for a period, usually without physical damage to the affected system.
Deny	Measures designed to temporarily eliminate and adversary's use, access, or operation of a system for a period, usually without physical damage to the affected system.
Degrade	Measures designed to permanently impair (either partially or totally) the adversary's use of a system, usually with some physical damage to the affected system.
Destroy	Measures designed to permanently eliminate the adversary's use of a system, usually with physical damage to the affected system.

(Table from Joint Publication 3-14, *Space Operations*)

intelligence-enabled operations on site, or against the domiciles of the employees. Furthermore, DA could also be targeted to disrupt the essential services at the ground site or the essential services in proximity to the ground site that enable it (electricity, sewage, water). Prominent authors such as Dr. Bleddyn Bowen have called for killing the scientists or nefarious experts of a particular initiative (e.g., a small team of scientists working on a chemical weapons program).[12] This line of thinking could extend to the families of these experts to create an effect so that an operator does not arrive to work on time, or a situation so undesirable is created that the services provided by this ground station are disrupted.[13] A parallel concept taken from the Air War Plans Division 1 paper, DA could also be taken against economic nodes that are enabling this ground station or against the supply lines that facilitate its services.[14] Finally, all these DA-related actions could be done unilaterally, through a proxy force, or with a unified action partner.

Military information support operations. Military information support operations (MISO) would be conducted by the psychological operations (PSYOP) community to influence two primary groups, nested under the space negation effect of deceiving.[15] The first target audience is people who can directly impact operations because they work onsite. Examples include supply or support personnel, satellite operators, or those filling a leadership role. The second target audience is family members of the employees or operators who live in the surrounding area and can indirectly impact the ground site. A complementary activity that MISO personnel could conduct includes a targeted military deception (MILDEC) campaign, to include tactical deception. While MILDEC is not an activity exclusive to the MISO community, the principles of deception best align with the MISO community. Effects from MISO and MILDEC could affect the ground, link, or space segment (see the figure).

Related to the ground segment, MISO or MILDEC could foment enough discord within target audiences or select individuals that desired effects could range from employees leaving doors unlocked, conducting simple sabotage, deserting their posts, tainting fuel supplies, or adversely affecting local or regional politics, to police brutality against the families of workers. In the link segment, MISO efforts could influence either of the two

Maj. Brian Hamel, U.S. Army, is a student attending the Advanced Military Studies Program at Fort Leavenworth, Kansas. This article is a distilled version of his thesis, "Reframing the Special Operations Forces-Cyber-Space Triad: Special Operations' Contributions to Space Warfare," which he completed as part of the Information Advantage Scholars Program. He is a graduate of multiple space and cyber courses, the Special Operations Forces Military Deception Planner's Course, and the Red Team Leader Course. His monograph is focused on a logistics-centric satellite constellation in low earth orbit that could clandestinely provide blood, money, weapons, or 3D-printed parts to small units of action.

Table 2. Results of Joint SOF Core Activities against Adversarial Space-Enabling Infrastructure

SOF Core Activities	Effect on Space-Enabling Infrastructure
Civil Affairs Operations (CAO)	I
Countering Weapons of Mass Destruction (CWMD)	N
Counterinsurgency (COIN)	N
Counterterrorism (CT)	N
Direct Action (DA)	D
Foreign Humanitarian Assistance (FHA)	I
Foreign Internal Defense (FID)	I
Hostage Rescue and Recovery (HRR)	N
Military Information Support Operations (MISO)	D
Security Force Assistance (SFA)	I
Special Reconnaissance (SR)	I
Such other activities as may be specified by the President or the Secretary of Defense (OA)	N
Unconventional Warfare (UW)	D
(D – direct effect, I – indirect effect, N – no effect)	

(Table from Joint Publication 3-14, *Space Operations*)

target audiences to degrade or disrupt essential services to that ground station, or they could use electronic warfare platforms to inhibit the link segment from functioning correctly. Finally, influence efforts in the space segment could manifest as the onsite operators or employees maneuvering a satellite when there was no need to, thereby depleting the finite amount of propellant. While admittedly a very specific list of actions, these same types of effects can be created by other capabilities within the joint SOF formation, which remain outside the scope of this article. This is not an exhaustive list, and SOF operators should be encouraged to think of ways to impose cost on our adversary.

In the joint community, MISO is one of nearly a dozen information operations capabilities. Information operations capabilities integrate with the staff, and nest effects to support targeting and the maneuver formations. In the joint world, these information operations capabilities can include public affairs, MILDEC, electronic warfare, computer network operations and civil-military operations.[16] Within the Army, the PSYOP community under U.S. Army Special Operations Command best supports this role of MISO in IW and is most apt to conduct these types of OAIs.

Unconventional warfare. Noting the definition for unconventional warfare from JP 3-05, *Special Operations*, a large part of related subtasks focus on coercing or disrupting the host-nation government, not always overthrowing it.[17] Predicated on the fact that the indigenous or surrogate capabilities are developed, the PSYOP or information operations element inside of the resistance could refine their OAIs to coerce specific target audiences or decision-makers. Concurrently, the guerilla force, or the "underground," could focus on disrupting, denying, degrading, or destroying the requisite human network and physical infrastructure for the ground

station to operate. Many of the parameters discussed in direct action, military information support operations, and special reconnaissance can be applied to this core activity.

SOF Indirect Effects against the Ground Segment

Special reconnaissance. Special reconnaissance (SR), as defined by JP 3-05, *Special Operations*, is "reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces."[18] In light of that definition, SR could be conducted through signals intelligence, human intelligence, or SOF, and could be amplified by collaborating with interagency equities (e.g., National Security Agency, National Reconnaissance Office, Central Intelligence Agency) to facilitate any of the five space negation measures indirectly. SR should also include SOF-enabled cyber reconnaissance to map the digital infrastructure, find vulnerabilities, and gain access to other parts of the network. Both human intelligence and SOF-enabled cyber could be OAIs that serve two direct and indirect purposes. As an example, human intelligence can be used to conduct reconnaissance, but it can also be used in a different capacity to facilitate a direct degradation measure. This could manifest itself as a human cutout passing a mensurated grid to an operator or cutting the electricity to a building.[19] Another example of SR that transitioned to a cyberattack having direct degradation impacts was the Stuxnet attack against Iran.[20]

SR could be used to map the interior of the physical infrastructure to include doors, windows, access codes, and patterns of life for those working at this facility. As mentioned in the DA section, SR can extend beyond the employees, site operators, and leadership at the ground site, and can encompass family members and other personnel in vicinity of the ground site that could indirectly impact operations. As some of our adversary's space operations become automated through artificial intelligence and machine learning, SR can map potential vectors for data poisoning. If the data poisoning were then to occur, its effects could span from disrupt to destroy.

Civil affairs operations. Given the rise of the civil and commercial space sector, civil affairs operations can be integrated to engage and evaluate the capabilities of civilian networks that work at these adversarial terrestrial space sites. Subsequent civil affairs operations can be tailored toward civil knowledge integration and civil network development and engagement, highlighting key links and nodes in the environment. Information from these reports could enable all five of the space negation measures. Paramount to this endeavor is standardization of data collation, and quality network engagement. Network engagement is "the interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an operational area."[21] Network engagement "utilizes the three activities of supporting, influencing, and neutralizing to achieve the commander's desired end state."[22] If this paradigm of network engagement is actively managed across civil affairs formations, then the data will be more standardized, which means more holistic analysis can be conducted.

Foreign internal defense and security force assistance. Reviewing the funding streams that Gen. Richard Clarke and Gen. Bryan Fenton highlighted in their posture statements to Congress, there is an argument that building capacity with our unified action partners could indirectly disrupt or deny the service that the Espacio Lejano ground station provides.[23] While this approach would take years to come to fruition, there is a case to be made that the U.S. military would garner extra attention from host-nation senior military leaders if training and developing host-nation capabilities with SOF, security force assistance brigades, and the National Guard's State Partnership Program were overwhelmingly successful. Senior military officials in South America, much like the United States, brief and advise politicians. As such, the senior military leaders of the host-nation country may convince the diplomats not to renew the country's land contracts with the People's Republic of China due to overwhelming support for the United States as the partner of choice. Out of all the proposed OAIs, this one would require the most synchronization between the

elements of national power and is encapsulated in the strategic-level aperture of SEI.

Conclusions

Given the U.S. Special Operations Command's global disposition and concentration on an IW approach to campaigning, SOF is the most well-postured equity to provide direct and indirect effects against adversarial SEI. This emerging concentration requires an understanding of space infrastructure as critical infrastructure and would contribute to the Department of Defense maintaining a position of relative advantage against the adversaries of the United States in the space domain. While SOF will always be innovative in its approach to solving complex problems, history is replete with examples that can provide planners and operators a foundational understanding for grappling with a complex issue such as space warfare.

While DA provides the most damaging effects against adversarial SEI, this is not the recommended course of action. A nuanced approach, accounting for attribution and risk, points toward SR and MISO as preferred OAIs to conduct against our adversaries to stay below the level of armed conflict. This is imperative so our adversaries do not disproportionally retaliate. While currently not a joint SOF core activity, preparation of the environment needs to be added to the list of recommended OAIs as well. The previous version of JP 3-05, *Special Operations*, defined preparation of the environment as "an umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations."[24] Leveraging preparation of the environment efforts to conduct future OAIs against adversarial SEI will be paramount to maintaining positions of relative advantage.

SOF must execute SR in conjunction with the interagency to bring to bear national-level capabilities and to facilitate a comprehensive and enduring approach. The consolidation of collection efforts should focus on network mapping to include the physical and cyber infrastructure, dossiers on the employees at these sites, the surrounding essential services that supports the SEI site, and the essential services that support employees when they are at their domicile.

The global integration of SEI also introduces more vulnerabilities against the adversary. Much like concepts from the Air War Plans Division 1 document, niche components that allow these ground stations to function may only be produced by a select number of factories in an adversary's domestic industry or the domestic industries of their partners. Therefore, if the few factories that made these components were degraded, then repercussions may extend globally to adversely affect an adversary's SEI. Predicated on gaining access to the network, cyber forces will have a large part to play against adversarial SEI. The cyber community will need to map the digital infrastructure to find vulnerabilities and potentially cause physical repercussions. Finally, the conduct of these OAIs is predicated upon funding, appropriate authorities and permissions, requisite training infrastructure, and tailored military education. This will enable our tactical formations to articulate requirements at an intelligible level to experts and prosecute intended effects. The capacity to hold adversarial SEI at risk will be a key marker in how irregular warfare contributes to integrated deterrence. Effectively implementing the Triad gives policymakers offensive options across the competition continuum and ensures that the United States remains in a position of relative advantage in the space domain.

Recommendations

The author proposes the following recommendations by precedence to better posture the United States to compete against our adversaries:

- The Joint Staff should adopt the definition for space-enabling infrastructure proposed in this article as well as incorporate celestial lines of communication into the professional lexicon.
- Given the emphasis from senior space leaders and prominent authors on the role of the cognitive dimension in space warfare, greater collaboration is needed between SOF PSYOP and the specific space equities focused on altering adversary decision-making to create greater shared understanding regarding MILDEC and MISO operations.
- Synchronize IW campaigning efforts among the Central Intelligence Agency, National Security Agency, National Space Intelligence Center, and the SOF community to conduct space, terrestrial, and cyber preparation of the environment on adversarial SEI. As this IW campaign continues

to grow, the security force assistance brigades and National Guard's State Partnership Programs should be brought into the fold to augment OAIs surrounding building partner-nation capacity.

Areas for Future Research

Given the limitations on this research and the ever-changing nature of the operational environment, there are several areas that warrant additional scrutiny:

- What are the appropriate command and control relationships for employing SOF elements in support of targeting SEI? Is it the respective theater special operation commands at the geographic combatant commands, a SOF cell in the operations section at U.S. Space Command; or as a geographic combatant command, does U.S. Space Command warrant its own theater special operation commands, granting access to major force program eleven funding? Furthermore, who is augmenting U.S. Space Command's staff with planning irregular warfare OAIs?
- Through the lens of orbital warfare, what are the SOF-facilitated effects in the space segment itself? What does maneuver warfare look like on orbit? While the physics and energy requirements do not currently support a robust answer to this question, what might it look like ninety years from now? As SOF cannot be mass-produced, this capability would take time to generate, and it may be a mission most suited for a future SOF component within the U.S. Space Force.
- In the same vein that the Department of Defense has aerial and sea points of departure, how do the Department of Defense and its civil and commercial partners exploit on-orbit capabilities, and how might we operationalize the Lagrange points (points of gravitational parity between two celestial bodies) into celestial points of debarkation to enable space logistics that support IW?
- Given the amount of specialized training that SOF service members receive, how does the SOF community grow a cadre of SOF space experts amongst the officers, warrant officers, and senior noncommissioned officers? ■

Notes

Epigraph. Mark Orwat, *Touch Points in Emerging Capabilities: Cyber, Space, and Special Operations* (Carlisle, PA: U.S. Army War College, 15 April 2014), 20.

Epigraph. Bleddyn Bowen, *War in Space: Strategy, Spacepower, Geopolitics* (Edinburgh, UK: Edinburgh University Press, 2020), 160.

1. Todd Lopez, "Parent Services Integration a Top Priority for Special Operations Components," U.S. Department of Defense News, 2 May 2022, https://www.defense.gov/News/News-Stories/Article/Article/3016652/parent-services-integration-a-top-priority-for-special-operations-components/.

2. Joint Publication (JP) 3-14, *Space Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2020 [CAC required]), II-6; Field Manual 3-14, *Army Space Operations* (Washington, DC: U.S. GPO, 2019), 3-8.

3. Defense Intelligence Agency, *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion* (Washington, DC: Defense Intelligence Agency, 2022), https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf. The creation of the Strategic Support Force allowed for the integration of cyberspace, space, and electronic warfare capabilities into joint military operations for the People's Republic of China.

4. Developed by the author with the concept of "celestial lines of communication" integrated from John J. Kline.

5. Matthew Funaiole et al., "Eyes on the Skies: China's Growing Space Footprint in South America," Hidden Reach, no. 1 (4 October 2022), https://features.csis.org/hiddenreach/china-ground-stations-space/.

6. Ibid.

7. Ibid.

8. Ibid.

9. Ibid.

10. Ibid.

11. Table from JP 3-14, *Space Operations*, II-2.

12. Bowen, *War in Space*, 73.

13. "United States Intelligence Activities," Exec. Order No. 12333, 46 Fed. Reg. 59941 (4 December 1981), https://www.archives.gov/federal-register/codification/executive-order/12333.html. This article focuses on theoretical generalization but acknowledges that Executive Order 12333 bans assassination by persons employed, or acting on behalf, of the United States.

14. Peter R. Faber, "Interwar U.S. Army Aviation and the Air Corps Tactical School: Incubators of American Airpower," in *The Paths of Heaven: Evolution of Air Power Theory*, ed. Phillip S. Meilinger (Maxwell Air Force Base, AL: Air University Press, 1997), 183–238.

15. During the editing process, JP 3-14, *Joint Space Operations*, rescinded the term "space negation." As the author's accompanying thesis was published before the publication of the new joint doctrine, the author chose to keep the article in line with the original thesis for the sake of continuity.

16. JP 3-13, *Information Operations* (Washington, DC: U.S. GPO, 2014).

17. JP 3-05, *Joint Doctrine for Special Operations* (Washington, DC: U.S. GPO, 2020 [CAC required]), GL-10.

18. Ibid.

19. A cutout is typically an unwitting individual meant to conduct an action as an obfuscation measure meant to protect the identity of the originator of that action.

20. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

21. Army Technical Publication 5-0.6, *Network Engagement* (Washington, DC: U.S. GPO, June 2017), 1-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3696_ATP%205-0x6%20FINAL%20WEB.pdf.

22. Ibid.

23. *A Statement on the Posture of the United States Army before the Comm. on Armed Services, United States Senate*, 117th Cong., 2nd sess. (5 April 2022) (statement of Gen. Richard D. Clake, Commander, United States Special Operations Command); *A Statement on the Posture of the United States Army before the Comm. on Armed Services, United States Senate*, 118th Cong. (7 March 2023) (statement of Gen. Bryan P. Fenton, Commander, United States Special Operations Command).

24. JP 3-05, *Special Operations* (Washington, DC: U.S. GPO, 2014 [obsolete]), GL-9.

Military Review

WE RECOMMEND

Your attention is invited to a legacy edition of *Military Review* with a special section on exploitation of space technology. See pages 12–51 of the March 1988 edition at https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/515/rec/9.