Cyber and Space: Information Warfare and Joint All Domain Effects in the Youngest Domains

Joshua A. Sipper
Air Command and Staff College
Air University
Maxwell AFB, AL, United States
Email: joshua.sipper.1@us.af.mil

***Abstract*— Cyberspace and space operations are examined here as interdependent, cross-functional, and co-dependent on the electromagnetic spectrum. The research methodologies used here are survey research and comparative analysis leveraging the myriad entanglements between space, cyberspace, and electromagnetic spectrum technologies. To get a closer look at how space and interdisciplinary cyber operations can achieve these effects, cyber and space technological relationships, doctrine, operations, and cross-domain integration are analyzed and discussed. Through this analysis, it is found that these technologies have the intrinsic potential to affect deep enclaves of the electromagnetic spectrum, critical infrastructure, information infrastructure, information-related capabilities, and joint all-domain operations. These various technological and operational connections suggest various vulnerabilities and consequences if they are not properly secured and managed. However, if space and cyber can combine and interact across the full range of operations, there is a greater possibility of achieving sustained victory and peace.**

Keywords- cyber; space; infrastructure; electromagnetic; spectrum; security.

I. INTRODUCTION

The domains of space and cyber share many similarities, especially the fact that both are operationally akin to flying an aircraft that never lands, especially when referring to satellite operations. This, among other things, means that you never bring the airframe to depot for maintenance and refueling always takes place while the plane is flying. These and other similar properties were the impetus for the original assignment of Air Force Network Operations (AFNetOps), now cyber, under Air Force Space Command. Not only did the operational needs and mechanisms flow well together, the space doctrine and instructions made the most sense initially for establishing cyber guidance and procedures. Essentially, both domains follow the motto of the 26th Network Operations Squadron; Always On, Always Ready [1]. These two domains flow well together philosophically and operationally as both domains are mutually supportive, complementary, and critical enablers of Joint All-Domain Operations (JADO).

The most inherently positive correlations between space and cyber operations are their technological prowess and global empowerment of JADO. Joint All-Domain Operations require that cyber and space, from a domain perspective, focus on enabling capabilities to ensure strategic overmatch against foreign adversaries [2]. Through conjoined technological enhancements, cyber and space both push boundaries within their respective battlespaces and the kinetic, traditional domains. This fact coupled with the interlaced operational constructs of space and cyber technological capabilities brings additional power to bear in situations where networks, Global Positioning Systems (GPS), timing servers, and communications are of paramount importance to JADO. Further analysis of these technological capabilities will be examined later and special attention will be given to the specific enabling actions and effects produced using space and cyber together.

Doctrine is always at the forefront of any discussion concerning warfighting domains as it contains the best practices found in service and joint policy that guide and give weight to how wars are prosecuted. As with any highly technical subject matter, service and joint doctrine have historically found it difficult to capture the operational and tactical aura of the space and cyber domains. However, as further understanding concerning these domains and their capabilities has developed, an inclusion of their placement in JADO has begun to develop. This is vitally important as it relates to the aforementioned fact that space and cyber share a parallel function as critical enablers for all domains. Doctrine currently exists that points to joint capabilities that cross domains as this foundation is necessary for continued expansion and development of the domains and their intertwined nature [3]. Doctrine is and will continue to be an extremely important method for stating in service and joint terms how space and cyber will operate together and support JADO now and into the future.

Every domain includes specific operational capacities and limitations. However, within the space and cyber domains, these proclivities tend to reach much farther into other domains than others might into their more technical and abstract auspices. It is in these specific operational spaces that a deep exploration must take place in order to grasp how space and cyber press and change what have been considered impenetrable boundaries in the past. It is in these "technological zones" [4] that cyber and space have significant impact, spanning operational Command, Control, Communication, and Computers (C4) while saturating Intelligence, Surveillance, and Reconnaissance (ISR) and Electromagnetic Warfare (EW) as well. Operationally, space and cyber act not only as conduits for furthering operations in other domains, but also as equal partners, benefiting from one another and the air, sea, and land feedback loops, furthering the cyber and space situational awareness and ISR counterbalance. It is in this fundamentally cyclical and interdisciplinary construct that true combined JADO effects can take place.

Finally, interdisciplinary cross-domain effects are of peak concern when considering the combinatory power and effects of cyber and space within the JADO construct. As Laird put it, "A future war might first begin with attack-defense confrontation in space and network space, and seizing command of space and network dominance will become the crux to obtaining comprehensive dominance rights on the battlefield to further conquer the enemy and gain victory [5]." It is easy to sense the rhizomatic nature of space and cyber in this image of future conflicts. With the immediate battlefield advantage offered through feeding power into other domains with technological overmatch, all other domain spaces would naturally follow. Of course, this is dependent on numerous, complex factors within the space and cyber domains proper, not to mention the other domains. Some of these complexities will be underlined in later analysis.

The remainder of the paper structure is organized as follows. In section 2, space and cyberspace technical relationships are discussed to add context concerning the various linkages and dependencies across these domains. Section 3 presents an analysis of cyberspace and space doctrinal connections and overlaps for appropriate interactions within joint and service doctrinal enclaves. Section 4 delves into the complex interrelationships between cyberspace and space operations to include linkages through the Electromagnetic Spectrum (EMS) and satellite communications and telemetry. Section 5 analyzes the cross-domain synthesis and operability between space and cyberspace domains. Finally, section 6 summarizes and closes the paper and gives a forward perspective as cyberspace and space operations continue to coalesce and fuse. Technology, doctrine, operations, and cross-domain integration and effects are by no means the only considerations when exploring the cyber and space domains and their growing influence within military operational and strategic constructs. Nevertheless, these are areas of great importance that set the stage for many other issues of significance and consideration. Through analyzing and understanding these areas, a firmer comprehension of the overarching methodologies and constructs can be grasped.

II. SPACE AND CYBER TECHNOLOGICAL RELATIONSHIPS

Space and cyber are two domains, intimately linked in a constant technological surge for superiority and supremacy, both in military and civilian capacities. This linkage serves to produce ever more interesting and far reaching progress technologically while simultaneously presenting entangled complexity and problems. This is characterized by the amazing, and what Mills [6] characterizes as miraculous, technological leaps innate in cyber and space technologies, but also in security concerns and concurrent adversary advancement technologically and interdisciplinarily. These areas of import will serve as the crux of the following discussion concerning space and cyber technology, but also as a running theme represented not only here, but in the real world as cyber and space professionals have noted numerous times [7].

Technology in space and cyber are, although different, irrevocably intertwined and interdependent. As Madelyn R. Creedon, former Assistant Secretary of Defense Global Strategic Affairs, states, "the different physics and technical realities of space and cyberspace result in somewhat different threats. But despite the differences in our use of space and cyberspace, there are many similarities in the challenges [2]." These technological similarities are what drive space and cyber to continue the development of new and better technical methodologies for operations to meet the strategic concerns often seen on the horizon both domestically and abroad. These concerns are generally presented through vulnerabilities in cyber and space technologies, however, the technical realities of how space and cyber systems work together and are advancing offer ways to meet these challenges and work through and around them. For instance, the increasing capability to introduce more granular and advanced cyber and onboard space network information protection measures has increased and continues to increase rapidly. "More and more information can be stored and transported at ever-smaller scales, using profoundly fewer atoms and less energy per unit [6]." The accompanying miniaturization of components that can store increasingly more information more securely and stably offers cyber and space technological applications a way to protect against and drive past many of the current strategic concerns being forewarned. Additionally, as compared with legacy computer systems, current technology consumes over 100 million times less energy per logic operation, while working in a physical space more than one million times smaller with this same trend continuing exponentially on a daily basis [6]. And this doesn't even account for nascent technologies such as artificial intelligence, machine learning, deep learning, nanotech, and quantum computing; areas showing great promise toward increasing storage, speed, and computing at a distance through entanglement of subatomic particles. The technological interleaving of the space and cyber domains strategically and operationally offer seemingly limitless opportunities going forward, however, with any great step comes potentially great opportunity to stumble as further discussion regarding security and adversary competition shall bear out.

Security is a constant concern when dealing with any technology. The overwhelming desire of nation-state, terrorist, criminal, and corporate actors to gain access to information about and within bleeding edge cyber and space technologies presents a constant barrage of attacks and probes attempting to gain access and insight. But, even more sinister is the parallel desire to deny, degrade, deceive and destroy cyber and space assets. Adversaries across the spectrum from individuals and small groups to state and state sponsored cyber attackers, if not already, will soon have tools at their disposal to enact anti-satellite cyberattacks [8]. The consistent prodding and pushing to develop ways into cyber and space technological systems presents a growing risk to all domains of warfare, not just space and cyber. The continuing dependence of air, land, and sea operations for cyber and space situational awareness, navigation, and C4ISR carries with it myriad opportunities for mission failure. GPS is one of several examples of cyber enable satellite technology that could bring a rapid breakdown in operational capability if degraded. “These troubling trends are driving defense spending increases in resiliency and redundancy, including considerations of how best to achieve GPS-dependent Position, Navigation, and Timing (PNT) assurance [8].” It is only in protecting cyber and space technologies through mission assurance that operations can be continued, even in the most contested and congested of operational and information environments.

Peer and near-peer adversaries present several risks strategically and operationally to both cyber and space in the technological sphere. As has been reported and confirmed on numerous occasions, peer adversaries China and Russia engage constantly in industrial espionage, working vociferously to catch and surpass the United States technological aptitude and advances. “Washington views Russia’s and China’s pursuit of Anti-Satellite weapons (ASAT), including laser-armed, satellite-hunting aircraft, as an attempt ‘to reduce U.S. and allied military effectiveness’ and ‘to offset any perceived US military advantage derived from military, civil, or commercial space systems [8].” With increasing regularity and persistence, China especially has sought to maintain a foothold in United States cyber and space systems, adding to the threat of espionage and sabotage on a massive scale. This can be seen in China’s strategic move to establish its Strategic Support Force (SSF) which, among other things, consolidates space and cyber power to advance China’s strategic interests in economic growth and technological development [9]. These advancements strategically undergird China’s dream to further their space program and pass that of the United States, reaching farther into space than has been previously imagined. With this enhanced reach and power, China could set itself up for economic and technological power projection launching the country far ahead of all other competition. “China aims to establish a manned space station by 2020–22 and a space-based solar power station by 2050 to meet its burgeoning economic and energy needs, develop space science and technology, explore outer space, and land on Mars [7].” With strategic aims such as these, China stands a great chance of surpassing US technological capabilities and reaching the potentially vast resources contained in the inner solar system and belt.

Technological reach, while only one area of interest and concern within the cyber and space operational domains, is nevertheless extremely important, probabilistically affecting every other domain and area of strategic interest including doctrine, operations, and cross-domain integration. With the technological piece firmly planted in the consciousness of military and government psyches, further considerations must be made to advance cyber and space technological growth and integration, security protections and mission assurance, and peer competition. Only through continued technological advancement in these arenas will the US be able to continue to lead the way in every area of global and space power insertion.

III. CYBER AND SPACE DOCTRINE

The interlacing of doctrine concerning disparate domains has always been an area of difficulty and potential breakdown, especially when it comes to highly technical and complex domain infrastructures such as space and cyber. The level of competency and understanding the technical and architectural requirements related to operations and strategic concerns, not to mention the deep tactical intricacies, in the cyber and space domains often makes tying these areas into other operations difficult. This is true not only for the traditional domains, but even more so between space and cyber since the technologies are always growing and advancing in capability and complexity. Doctrinally, the areas cogent to this discussion are space and cyber operational entanglement, operational thresholds regarding war and potential escalation, and the operational systems associated with these domains across the spectrum of conflict.

As technologically diverse and discrete fields often are, space and cyber tie closely together due to their technological dependence for operations while simultaneously holding their own entrenched technical specificities. Regardless of any disparities, however, the space and cyber domains experience what can best be described as entanglement; the quality of a technological cause and effect relationship. This can be seen across the operational spectrum within space and cyber as certain areas of networking for cyber operations are space dependent and many areas of space operations from a networking and C4ISR perspective are supported, enabled, and driven by cyber operations. Cybersecurity supports and defends space assets, provides authentication and encryption to space assets, and uses filtering shielding, and spread-spectrum techniques to guard against electromagnetic interference, jamming, and other attack [10]. The transverse is true as space assets provide over-the-horizon communications, data linkages and network capability, network command and control, and ISR data for cyber operations, creating a continuous, complementary feedback loop. As doctrine concerning these cross-domain interactions is developed and specified, these relationships will become clearer and more defined.

Both cyber and space domains share a similar kinetic/non-kinetic threshold as well. When it comes to the level of conflict that may lead to escalation and potential acts of war, both space and cyber present advantages and complexities. For instance, both space and cyber may be used consistently to degrade, deny, and deceive adversaries, leading to conflict below the threshold of kinetic operations that may extend into potential kinetic conflict leading to war. It is important from a doctrinal perspective to draw these lines and intimate the contrasts involved in these conflict situations. Questions such as what level of operations define the level of Anti-Satellite (ASAT) weapons, whether lasing or jamming are considered ASAT, for example, persist [11]. Differentiation must also be expressed regarding the various actions potential during wartime and peacetime. "Possibly only probing and reversible cyber-type attacks would be allowed in peacetime, but more permanent, damaging attacks could be executed in general wartime situations [12]." These issues must be discussed within space and cyber doctrine in order to help operators and strategists in both disciplines create opportunities and battlefield effects across the spectrum of conflict.

The operational systems used to drive those operations are integral to the success of space and cyber operational integration. While it is usually not wise from a doctrinal standpoint to specify systems, it is nevertheless important to note that systems do exist and interleave. This is true for many domains and will only become more important as JADO continues to grow and ramify. However, space and cyber operational systems are often interdependent, leading to even more need to understand these entanglements and ensure they are spelled out in doctrine. For instance, "The term space systems refers to the equipment required for space operations, which is comprised of nodes and links. This includes all the devices and organizations forming the space network, which consists of spacecraft; ground and airborne stations; and data links among spacecraft, mission, and user terminals [13]." All of the data links, nodes, and other network linkages mentioned here are cyber driven and controlled. Unfortunately, this is not always specifically, explicitly stated in doctrinal sources. While some might cite the implicit understanding, it may not always come through to operators trying to ensure space and cyber assets and operational systems are integrated and working together.

As doctrine inevitably shifts and changes with the stand-up of the new United States Space Force (USSF), it will be increasingly important to ensure that space and cyber are linked and operationally related in every way possible. With the JADO concept of operations continuing to gain strength and significance, this will become even more important to ensure all-domain operation and superiority. As cyber and space entanglement grow continuously, the operational dependencies naturally present will need to be noted and explained in doctrine. The operational thresholds also must be framed and dictated to ensure the appropriate measures are prescribed across the spectrum of conflict. Also, operational systems related to both space and cyber domains must be interlocked and explicitly discussed in doctrine to ensure clear and concise operational understanding and future integration.

IV. CYBER AND SPACE OPERATIONS

As relatively new warfare domains, space and cyber both operate in distinct ways compared to the traditional air, land, and sea battlespaces. This can be seen primarily in the technological emphasis inherent in space and cyber, but also in several other operationally vital areas. Many of the operational support, training, and auxiliary elements associated with space and cyber are uniquely attuned to the specialized technical and navigability requirements for these domains. Without the proper equipment and operational understanding of that equipment, for instance, the space and cyber missions are intractable. Both space and cyber also contain imbedded operational vulnerabilities special to their battlespace environs. While space suffers the tyranny of distance, cyber suffers a tyranny of locality, both of which present different and convoluted vulnerabilities. Space and cyber, while young domains, also have grown and matured rapidly over the last decade, bringing with them amazing and powerful capabilities that have revolutionized warfare, making JADO and Information Warfare (IW) realities. The following areas of space and cyber operational elements, operational vulnerabilities, and operational maturity serve as major topics of understanding going forward.

The operational elements associated with cyber and space are integral to the domains' ability to interleave and prosecute missions. While some areas such as intelligence, education, and training are definitively carried over into these domains operationally [14] others such as land- and sea-based nuclear operations, cyberspace operations, and the overall missile defense mission have been suggested to be set aside as tangential [15]. While it could be understood how some of these areas might be considered tangential and need to be somewhat decentralized within their own domain structures, it is imperative that some (cyber especially) be closely held and integrate into space operations from launch to landing. This is not to say that USSF needs to hold operational control of US Cyber Command, but that the elements should work closely to ensure space and cyber operations carry forward for JADO, IW, and cross-domain support. Without this solid operations linkage, mission assurance could disintegrate rapidly.

The potential disintegration relates directly to the various, specialized vulnerabilities present within the space and cyber operational constructs. As these domains continue operating together, they tend to rub off on one another to some extent as they both are highly dependent on their respective and combined technological scaffolds. "Technology can be lost in microseconds through cyber espionage, giving rogue nations the ability to catch up without the time or investment devoted by first movers [11]." The technical, strategic, and economic vulnerabilities to space and cyber are often related to what has become an increasingly lower level of entry into these spheres; one that will continue to present risks. Integration of C2 and other systems also introduces potential problems into operations as bugs and zero day vulnerabilities may lie unpatched [16]. These issues are various and plentiful and must be considered as space and cyber integration proceeds.

Conversely, as the youthful domains of space and cyber have grown preternaturally over the last decade, they have taken on many, extremely complex operational responsibilities, leading to the development of JADO and IW strategic and operational concepts. As enabling and singularly capable operation domains, space and cyber have both found purchase in every area of warfare, leading to combinations and effects heretofore unheard of. For instance, both domains offer power and stability to information related capabilities such as Information Operations (IO), Electromagnetic Warfare (EW), and ISR that have allowed the integration and cross-disciplinary operation of all of these elements to produce IW effects. Consequently, “space and cyberspace have… grown from their original manifestations as supporting capabilities into warfighting arenas in their own right [17].” As space and cyber continue to develop and mature, the capabilities and technologies associated with and shared by both domains will doubtless continue to take new and conjoined shapes.

Operationally, space and cyber are distinct, yet linked in numerous ways. Both share elements that can be integrated and moved fluidly through both domains while still being irrevocably linked to their own operational area. Training, education, and ISR are a good example as these can easily overlap operationally, feeding necessary information between all domains, further enhancing the JADO and IW concepts. Space and cyber also share similar vulnerabilities. While space vulnerabilities are ones associated with distance such as communications and networks, they also relate with the cyber domain vulnerabilities of the same ilk which are most often made difficult in the local, global ability of adversaries to affect devices at light speed instantaneously from a distance. Ultimately, the maturity of both domains have lent them the ability to operate together, exponentially increasing each other’s potential and effectiveness while also enhancing JADO and IW battlespace efficacy.

V. CYBER AND SPACE CROSS-DOMAIN CONSIDERATIONS

As IW and JADO strategic scaffolds proliferate throughout joint and service philosophy, space and cyber cross-domain effects and concepts will continue to pervade every domain. This fact makes understanding and performing space and cyber cross-domain effects all the more important and integral to operations at every level. While there are potentially copious ways to ensure cross-domain considerations are attended to, the most vital components for discussion are cross-domain platforms, hardening across technologies, and IW and JADO superiority. Platforms within any domain are the bedrock, tangible resources upon which most operations rest. If platforms are not well designed and integrated, mission success is constantly in question. Hardening of these platforms and systems directly affects whether or not they can function since the protective measures from hardening often spell the difference between operational success and failure. If space and cyber missions are active, assured, and ready, IW and JADO can be mission assured, leading to victory across all domains, disciplines, and battle spaces.

Cross-domain operations are, more often than not, supported and assured through platform integration and interoperability. This can be seen in the more traditional domains through close air support, ground support to naval activities, and other integral platform-dependent undertakings. The same types of integration can be seen in network support to space operations and space platform network support to cyber operations and numerous other examples of platform interlocking. Position, Navigation, and Timing (PNT) is one critical area associated with cross-platform integration. “PNT information is a critical enabler for the delivery of numerous types of Precision-Guided Munitions (PGMs) including aircraft missiles, naval gunnery and land-based artillery shells. Synchronous timing provided by space-based PNT services is also a vital element of many military communication and information systems [18].” Another cross-platform solution deeply related to PNT is GPS through which coordination of cross-domain, JADO, and IW activities can be coordinated globally. These and other cross-platform necessities must be considered heavily in order to ensure operational stability.

To ensure cross-platform permanency, vulnerabilities must be identified, addressed, and continuously reevaluated as new threats arise. While threats to space and cyber sometimes differ, they tend to overlap often as the technological vulnerabilities associated with electronic traffic through the EMS pervade every corner of space and cyber operations. Various attacks across the EMS and networks are possible including jamming, spoofing and hacking attacks on communication networks via space infrastructure, attacks on satellites, targeting their control systems or mission packages, perhaps taking control of a satellite to exploit its capabilities, shut it down, alter its orbit, or “cook” or “grill” its solar cells through deliberate exposure to damaging levels of radiation attacks on ground infrastructure, such as satellite control centers, associated networks and data centers, leading to potential global cascading effects on critical information infrastructure and networks [18]. With this level of destruction at adversaries’ fingertips, it is vitally important to consider ways in which to harden and protect the cross-platform infrastructures and information transmission dependencies necessary for mission completion. “Debilitating loss of space capabilities from a surprise attack; direct assaults with ballistic and cruise missiles; cyber strikes; or, in the near future, space-based weaponry could be anticipated within minutes [15].” Thus, hardening must reach outside of the kinetic norms while continuing to consider the wide array of possible adversary attack options. Several options exist for hardening including air gapping, strong encryption, and layer authentication protocols, many of which are already in use. However, space and cyber operators must always be vigilant as new attacks, vulnerabilities, and weak spots in human diligence are always present.

Although cross-domain dependencies specifically between space and cyber are extremely important, the strategic and operational landscapes of IW and JADO must also be given full attention as these nascent concepts are growing in power and profusion. IW is currently defined as the interdisciplinary combination of information related capabilities (Cyber, ISR, EW, and IO) to produce effects. This is an extremely powerful panoply and lends its strength potentially to JADO as IW operational effects have the potential to create major weaknesses in adversary defensive and operational constructs. A prime example of this is the Israeli Air Force operation carried out in September of 2007 against the joint Syrian/North Korean nuclear operations in Syria where Israel used a combination of cyber, ISR, EW, and IO along with its kinetic air capabilities to destroy the Syrian reactor. [20] This lethal combination is just one instance where the use of IW and JADO/MDO was an unparalleled success. Space factors well into these types of operations as well as the space-eye view enables ISR, cyber, and numerous other domain and information areas close access to battlespaces. "A state may, over time, create a resilient constellation of hundreds of networked satellites (national, commercial, and allied) that may be able to convince an adversary that its forces will not be able to accomplish their objective of denying space-derived information [19]." The same can be seen in the IW sphere as combinations of information related capabilities produce a united front during conflict by leveraging space, cyberspace, and electronic warfare assets [3] as well as ISR through imagery and other intelligence disciplines [17]. The decisive victory to be gained through JADO and IW interactions and integration with space and cyber cannot be overstated. Through a full-spectrum junction of this cornucopia of capabilities, space and cyber power can create and sustain effects profoundly into every space of engagement.

VI. CONCLUSION

Cyber and space, while the youngest of the warfighting domains, have risen rapidly in prominence, capability, and maturity to become the key JADO and IW critical enablers. This can be seen in the constant operation constructs of space and cyber as ongoing missions; planes that never land. Additionally, the technical prowess and capabilities of space and cyber make them integral parts of every mission area within every domain. Through the C4ISR and cross-domain enablement found in these young domains, information flows and operations succeed. Doctrine is an area constantly striving to maintain pace with technologically agile areas and must continue to shape and expand to fill gaps and tie together warfighting concepts as they evolve. From and operational standpoint, space and cyber represent the Gemini in warfighting constructs, complementing and completing each other while offering their superior operational technological scaffold for use in IW and JADO. The possibilities are seemingly limitless as are the challenges, but if space and cyber can combine and interact across the full range of operations, there is a much greater possibility of achieving sustained victory and peace.

REFERENCES

[1] 26th NOS motto, retrieved 9 July 2020: https://www.afhra.af.mil/About-Us/Fact-Sheets/Display/Article/432510/26-network-operations-squadron-afspc/

[2] M. Creedon, "Space and Cyber: Shared Challenges, Shared Opportunities", Strategic Studies Quarterly, Vol. 6, No. 1, SPRING 2012, pp. 3-8.

[3] J. Caton, "The Land, Space, and Cyberspace Nexus: Evolution of the Oldest Military Operations in The Newest Military Domains", Strategic Studies Institute, US Army War College, 2018.

[4] J. Hay, "The Invention of Air Space, Outer Space, and Cyberspace," Rutgers University Press, 2019.

[5] B. Laird, "Space and Cyberspace Operations," Center for a New American Security, 2017.

[6] M. Mills, "Making Technological Miracles", The New Atlantis, Spring 2017, No. 52, pp. 37-55.

[7] N. Gowswami, "China in Space: Ambitions and Possible Conflict", Strategic Studies Quarterly, Vol. 12, No. 1, SPRING 2018, pp. 74-97.

[8] C. Kavanagh, "New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?" Carnegie Endowment for International Peace, 2019.

[9] A. Ni, "Dreams in Space" ANU Press, 2020.

[10] Annex 3-14 - Counterspace Operations, retrieved 7/16/2020 from https://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-14-Counterspace-Ops/

[11] T. Harrison, "Defining Space Warfare and Space Weapons," Center for Strategic and International Studies (CSIS), 2020.

[12] P. Szymanski, "Techniques for Great Power Space War" Strategic Studies Quarterly, Vol. 13, No. 4, WINTER 2019, pp. 78-104.

[13] C. King, D. Young, E. Byrne, and P. Konyha, "AU-18 Space Primer," Air Command and Staff College and Space Research Electives Seminars Air University Press, 2009.

[14] RAND Corporation, "Creating a Separate Space Force: Challenges and Opportunities for an Effective, Efficient, Independent Space Service," RAND Corporation, 2020.

[15] E. Dolman, "Space Force Déjà Vu," Strategic Studies Quarterly, Vol. 13, No. 2, SUMMER 2019, pp. 16-22.

[16] G. McCleod, G. Nacouzi, P. Dreyer, M. Eisman, M. Hura, K. Langeland, D. Manheim, and G. Torrington, "Resilience and Air Force Space Operations," RAND Corporation, 2016.

[17] D. Grant, and M. Neil, "The Case for Space: A Legislative Framework for an Independent United States Space Force," Air University Press, 2020.

[18] M. Davis, "Why maintaining space access matters," Australian Strategic Policy Institute, 2019.

[19] J. Moltz, "The Changing Dynamics of Twenty-First-Century Space Power," Strategic Studies Quarterly, Vol. 13, No. 1, SPRING 2019, pp. 66-94.

[20] V. Holath and H. Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," Der Spiegel, retrived 13 August 2023: https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

DISCLAIMERS:

The views expressed are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. Government.

DoD School Policy. DoD gives its personnel in its school environments the widest latitude to express their views. To ensure a climate of academic freedom and to encourage intellectual expression, students and faculty members of an academy, college, university, or DoD school are not required to submit papers or material that are prepared in response to academic requirements and not intended for release outside the academic institution. Information proposed for public release or made available in libraries or databases or on web sites to which the public has access shall be submitted for review.