INSTITUTE FOR DEFENSE ANALYSES

Cyberspace and Space Similarities, Differences, and Related National Security Issues

Thomas H. Barth, Project Leader

July 2024

IDA Product 3001828

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project C5237, "Cyberspace and Space Domains," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Priscilla E. Guthrie, James H. Kurtz

For More Information

Thomas H. Barth, Project Leader
tbarth@ida.org, 703-845-6672

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

Executive Summary

Cyberspace and space are both new national security frontiers that blur traditional ideas about borders, sovereignty, and defense strategy. Both also share a history of having starting as intelligence activities rather than as warfighting domains, and both remain closely linked to their intelligence origins. Both were also originally dominated by the government but are now increasingly essential commercial activities, and the United States military is increasingly turning to the private sector for many of its cyberspace and space services. Both are accessible through the use of sophisticated technology employed by a technically capable workforce. However, although space and cyberspace are similar in many respects, there are also differences between them. Space is a naturally occurring part of our earthly surroundings, whereas cyberspace is a manmade phenomenon. Space-based systems typically require massive capital outlays, whereas cyberspace operations require much less. These similarities and differences between cyberspace and space present several national security issues for the U.S.

Three of these issues concern (a) defining the national security relationship between the government and the commercial sector in each domain; (b) the recruiting, professional development, and retention of a technically capable workforce; and (c) achieving unity of effort within each and between both, which includes determining the appropriate relationships between U.S. Cyber Command (CYBERCOM) and the National Security Agency (NSA), between U.S. Space Command (SPACECOM) and the National Reconnaissance Office (NRO), and between both CYBERCOM and SPACECOM and the geographic and functional combatant commands (CCMDs).

Addressing the national security relationship between the government and the commercial sector in both cyberspace and space will require the active participation of several government agencies, including the Department of Defense (DoD). DoD's needs will be particularly critical when discussing those national security systems that operate in or transit through cyberspace or space. Similarly, addressing the underlying shortage of technically capable uniformed and civilian workers for both cyberspace and space will require a whole-of-nation approach. However, the Department must ensure that its internal policies, procedures, and resourcing levels for recruiting, retaining and professionally developing both its uniformed and civilian cyberspace and space workforces enables it to be competitive with the rest of government and the commercial sector. Finally, the Department should conduct a series of stress tests of the current approaches for support between CYBERCOM and NSA, SPACECOM and NRO, and the command relationship

between both CYBERCOM and SPACECOM and the geographic and functional CCMDs. These tests will be critical components in the Department's efforts for achieving future joint warfighting concepts and fielding key future capabilities for the Joint Force, such as the unified ecosystem of sensors and data streams through Joint All Domain Command and Control (JADC2) and the ability to track emerging threats like hypersonic missiles, all of which will be dependent on assured access to both cyberspace and space.

Table of Contents

Figures and Tables

1. Introduction

A. Similarities, Differences, and National Security Implications of Cyberspace and Space

Cyberspace and space share several key similarities. Both are new frontiers for national security that blur traditional ideas about borders, sovereignty, and defense strategy. Both also share a history of starting as intelligence activities rather than as warfighting domains, and both remain closely linked to their intelligence origins.

Note: The term domain *was first used to describe both space and cyberspace in* Joint Publication 1, Doctrine for the Armed Forces of the United States *(2007). Change 1 to that publication (2009) incorporated "the use of the term and approved definition of 'cyberspace'." Effective with Change 1, "the capstone publication for all joint doctrine" described air, land, maritime, and space as physical domains, and defined cyberspace as "a global domain within the information environment."*[1] *The most recent iteration,* Joint Publication 1, Volume 1, Joint Warfighting *(2023) appears to have backed away from describing cyberspace as a domain and instead states "Joint warfighting requires joint force commanders to integrate forces throughout the operational environment, which includes all domains and the information environment, to create military advantage. A combatant commander's operational environment is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the commander's decisions. This environment encompasses the physical domains of air, land, maritime, and space; the information environment (which includes cyberspace); and the electromagnetic environment."*[2]

[1] Department of Defense, *Joint Publication 1, Doctrine for the Armed Forces of the United States*, May 2003 (Change 1, March 2009).

[2] Department of Defense, *Joint Publication 1, Volume 1, Joint Warfighting*, August 2023, https://jdeis.js.mil/jdeis/new_pubs/jp1_vol1.pdf.

Both were also originally dominated by the government but have become increasingly essential commercial activities, and the United States (U.S.) military is increasingly turning to the private sector for many of its cyberspace and space services. Both are accessible through the use of sophisticated technology employed by a technically capable workforce.

Although space and cyberspace are similar in many respects, there are also differences between them. Space is a naturally occurring part of our earthly surroundings, whereas

cyberspace is a manmade phenomenon. Space-based systems typically require massive capital outlays; in comparison, cyberspace operations require much smaller capital outlays.

The similarities and differences between cyberspace and space present several national security issues for the U.S. Three of these issues concern (a) defining the national security relationship between the government and the commercial sector in each domain; (b) the recruiting, professional development, and retention of a technically capable workforce; and (c) achieving unity of effort within each and between both, which includes determining the appropriate relationships between U.S. Cyber Command (CYBERCOM) and the National Security Agency (NSA), between U.S. Space Command (SPACECOM) and the National Reconnaissance Office (NRO), and between both CYBERCOM and SPACECOM and the geographic and functional CCMDs.

B. Expanding Warfare into a Global Enterprise

Prior to the introduction of networked computer technology and the militarization of space, warfare occurred on a global scale, but physical distances largely isolated geographically oriented commanders from conflicts in other theaters. Information sharing was accomplished by sending coded messages over wire, radio, or by physical delivery. Today, satellites provide data and communications to multiple theaters through ground-based, computer-operated information architectures. In addition to communications and information sharing, cyberspace and space-based systems are also critical in enabling modern warfare capabilities such as imagery intelligence and geospatial information, early warning, command-and-control systems capable of processing vast amounts of information, precision strike, positioning, navigation, and timing.[1] Key future capabilities for the Joint Force, such as building out a unified ecosystem of sensors and data streams through Joint All Domain Command and Control (JADC2) and tracking emerging threats like hypersonic missiles, will be dependent on assured access to both cyberspace and space.

[1] Matthew Mather, "How Space and Cyberspace Are Merging to Become the Primary Battlefield of the 21st Century," *Space Quarterly Magazine*, 2013, https://matthewmather.com/how-space-and-cyberspace-are-merging-to-become-the-primary-battlefield-of-the-21st-century/

2. Initially an Intelligence Activity

To understand the evolutionary links between space and cyberspace and their origins as intelligence activities, it is necessary to understand the multiple functions comprising intelligence today. The field of intelligence has always included human reconnaissance, surveillance, espionage and counterespionage, but technical collection is also a significant component of modern intelligence work.[2] Today, the Office of the Director of National Intelligence identifies six basic intelligence sources or collection disciplines: signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), human intelligence (HUMINT), open-source intelligence (OSINT), and geospatial intelligence (GEOINT).[3] Cyberspace operations can trace its origins to SIGINT.

A. Cyberspace

SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.[4] The modern era of communications began with improvements to the telegraph, which allowed quantities of messages, information and data[5] to be transferred across global distances in near-real time. Wireless telegraphy and then radio broadcasting accelerated this trend. With the development of digital communications and computer networks, SIGINT evolved to include data collection, digital transmission, and computer storage, which also offered the capability to translate data in more than one language. *Computer network exploitation* is a SIGINT technique in which computer networks are used to infiltrate a target computer's networks to extract and gather intelligence data. A cyberspace attack uses many of the same techniques as computer network exploitation to reach the target's computer networks.

---

[2] Michael Warner, "Intelligence in Cyber–and Cyber in Intelligence," in *Understanding Cyber Conflict: 14 Analogies*, eds. George Perkovich and Ariel E. Levine (Washington D.C.: Georgetown University Press, 2017), 17–30. Warner was serving as the command historian for USCYBERCOM when he wrote the chapter.

[3] Office of the Director of National Intelligence, "What Is Intelligence?", https://www.dni.gov/index.php/what-we-do/what-is-intelligence

[4] National Security Agency/Central Security Service, "Signals Intelligence (SIGINT) Overview," https://www.nsa.gov/Signals-Intelligence/Overview/

[5] *Messages*: A verbal, written or recorded communication; *Merriam-Webster*, s.v. "message (*n.*)," https://www.merriam-webster.com/dictionary/message). *Information*: Data that has been organized, processed and given context; *Data*: Raw unprocessed facts and figures; (see https://www.diffen.com/difference/Data_vs_Information).

However, whereas the objective of computer network exploitation is to gather intelligence data, the objective of a cyber-attack is to degrade, disrupt, or destroy the targeted computer network or to modify the data inside the targeted computer network to deceive the network's users. The similarities between computer network exploitation and a cyber-attack have led some to conclude that computer network exploitation and cyberspace attacks look the same from the perspective of the targeted computer networks, except for the end results.[6]

Space-based capabilities are also used in the collection of electronic signals. SIGINT spacecraft in geosynchronous orbits are used to pick up ultra-high frequency (UHF) and very high frequency (VHF) communications, while low- to medium-Earth-orbit spacecraft are used to collect signals from air defense and early warning radars.[7] Highly elliptical orbits give satellites long dwell times at high altitudes and short dwell times at low altitudes. Using both high and low altitudes maximizes signal collection over multiple regions for specific and repeating durations or frequencies.[8] Space-based assets are also used to support the U.S. intelligence community's IMINT and MASINT collection efforts.

B. Space

The U.S. intelligence community has a long history of developing and employing space-based systems to support IMINT and MASINT collection efforts. The CORONA program had its first successful satellite launch in August 1960. In September 1961, the NRO was formed to execute the national reconnaissance program.[9] The CORONA program operated as a film-return capsule system. A camera took photographs and stored them on film roll systems stored within the satellite. Film canisters were then ejected from the satellite and returned to Earth. Once the capsule penetrated Earth's atmosphere, a small parachute would open. As the capsule slowly fell to the surface, usually over an ocean, it would be plucked out of the air by a U.S. Air Force C-119 aircraft.

---

[6] The discussion of computer network exploitation and cyberspace attack was summarized from several sources: The unclassified version of Department of Defense, *Joint Publication 3-12, Cyberspace Operations*, June 8, 2018 (https://nsarchive.gwu.edu/document/16681-joint-chiefs-staff-joint-publication-3-12), and Bruce Schneier, "Computer Network Exploitation vs. Computer Network Attack," *Schneier on Security*, 2014, https://www.schneier.com/blog/archives/2014/03/computer_networ.html.

[7] Steven Lambakis, *On the Edge of the Earth: The Future of American Space Power* (Lexington, KY: University Press of Kentucky, 2001), 33.

[8] Ibid, 60.

[9] Bill Sweetman and Kimberley Ebner, eds., *Jane's Space Systems and Industry: 2007–2008* (Alexandria, VA: Jane's Information Group, 2007), 267.

Today most space-based imagery is collected by space-based camera systems and transmitted electronically to Earth and is referred to as electrical-optical imagery.[10] Other space-based imagery systems include spaced-based radar imagery, which uses synthetic aperture radar; infrared imagery, which uses sensors in the satellite to collect images in the infrared portion of the electromagnetic spectrum; and multispectral imagery, which records spectral reflectance values in different portions of the electromagnetic spectrum. Multispectral imagery supports a variety of important tasks including mission planning, thermal signature detection, and terrain analysis.[11]

[10] Brian Crothers, Jeff Lanphear, Brian Garion, Paul P. Konyha, and Edward P. Byrne, *U.S. Space-Based Intelligence, Surveillance, and Reconnaissance* (Montgomery: Air University Press, 2009), 172, https://www.jstor.org/stable/resrep13939.20.

[11] Ibid.

3. Commercialization

The commercial sector has always been involved in the development of the technology surrounding both cyberspace and spaceflight as contractors to government agencies like DoD and National Aeronautics and Space Administration (NASA). However, the creation of the Internet, a major component of the cyberspace portion of the information environment, and the operational use of both cyberspace and space were driven and resourced by the government. To track the evolution of commercial activity in cyberspace, an understanding of the Internet's origins and of the key technological developments that transformed it is necessary. The Commercial Space Act of 1998 also provides insight to the evolution of commercial activity in space.

A. Cyberspace

The Internet can trace its origins to the first computer networks dedicated to special-purpose systems such as SABRE (an airline reservation system) and AUTODIN I (a defense command and control system). In the late 1950s and early 1960s, the first host-to-host network connections were achieved by the Advanced Research Projects Agency (ARPA) with the creation of the ARPANET in 1969. In the 1970s, the Defense Advanced Research Projects Agency (DARPA — formerly ARPA) led efforts to connect various research networks in the U.S. and Europe. In 1983, ARPANET was divided into two parts: MILNET for the military and defense agencies, and a civilian version of ARPANET.

The National Science Foundation (NSF), working with DARPA, supported infrastructure efforts that expanded access to the civilian version of ARPANET for the entire scientific and academic community. This network was called the NSF Network (NSFNET). However, by 1995, the NSF determined that its support of the NSFNET infrastructure was no longer required as many commercial providers were now able to support the scientific community's networking requirements.[12] DoD, which had taken control of ARPANET in 1975, had a similar experience with MILNET. By the 1990s, commercial providers had become quite capable of providing the "long-haul"[13]

[12] *Encyclopedia Britannica*, s.v "Internet," https://www.britannica.com/technology/Internet.

[13] DISA defines long-haul transport infrastructure as the communication systems and service between the fixed environments and the deployed Joint Task Force (JTF) and/or Coalition Task Force (CTF). The deployed warfighter and associated CCMDer telecommunications infrastructure are primarily the responsibility of the individual Services. Wikiwand, s.v. "Defense Information System Network," https://www.wikiwand.com/en/Defense_Information_System_Network.

infrastructure requirements needed to support MILNET.[14,15] With the growth of commercial Internet providers and government actions like the Telecommunications Act of 1996, control of the Internet steadily shifted from government stewardship, to private-sector participation, and finally to private custody with government oversight. The rise of commercial Internet services and several technical developments fueled a rapid commercialization of the Internet.

The introduction of the personal computer, progress in integrated circuit technology, the associated decline in computer prices, and the emergence of Ethernet and other local area networks to link personal computers were key developments in the rapid commercialization of the Internet. Other developments included the success of the Corporation for National Research Initiatives' 1988 experiment linking commercial email service to the Internet, which resulted in a significant increase in Internet traffic, and the National Center for Supercomputing Applications' releasing the Mosaic browser (which ran on most types of computers). With its "point-and-click" interface, Mosaic, and browsers that followed, simplified access to and retrieval and display of files through the Internet. Later in the 21st century, what some have called "Web 2.0 Internet" began emphasizing social networking and content generated by users along with cloud computing, both of which generated even more commercialization of the Internet. Social media sites, which allow users to share their own content with friends and the wider world, have become some of the most popular sites on the Internet. With the introduction of smartphones and their ability to access the Web, the number of Internet users exploded from about one sixth of the world population in 2005 to more than half by 2020. The increased availability of wireless networking has also made applications that are compatible with user mobility, such as navigation applications, more profitable for commercial developers. Reuters estimated that the rapidly growing Internet sector accounted for $2.1 trillion of the U.S. economy in 2018 or about 10% of the nation's gross domestic product.[16] This transition from a largely paper-based world to a fully digital world is also pushing computing as close to the source of data as possible to reduce latency and bandwidth use.

---

[14] DISA is the DoD focal point for the acquisition of long-haul telecommunications and will procure commercial communications required by the Departments, agencies, offices, and other government agencies (https://depsland.csd.disa.mil/documents/procurement-guide-telecommunications-v1.pdf).

[15] MILNET was expanded and became the Defense Data Network. In September 1991, DISA established the Defense Information Systems Network (DISN) to consolidate all Service and agency transmission multiplexor infrastructure, including Service and agency Internet Protocol (IP) router networks. DISA operates two worldwide IP router networks, one for sensitive but unclassified content (NIPRNET) and one for secret content (SIPRNET).

[16] David Shepardson, "Internet Sector Contributes $2.1 Trillion to U.S. Economy: Industry Group," Reuters, September 26, 2019, https://www.reuters.com/article/idUSKBN1WB2QB/.

The "edge" today is the growing and already considerable Internet of Things (IoT). The IoT consists of a diverse set of familiar everyday technologies, like dishwashers, refrigerators, cameras, medical devices, satellites, automobiles, televisions, traffic lights, drones, baby monitors, building fire/security systems, smartphones, and tablets. The IoT also includes familiar technologies that are vital to maintaining and safeguarding the world in which we live today. These technologies include advanced military weapons systems; industrial and process control systems that support power plants and the nationwide electric grid, manufacturing plants, and water distribution plants; emergency response systems; banking and financial systems; and transportation systems.

B. Space

The Commercial Space Act of 1998 was an investment initiative to stimulate the commercial space flight industry. The Act promoted increased commercialization at all levels of the industry, including commercializing the International Space Station (ISS), creating space ports outside of NASA's Florida Kennedy Space Center, and bolstering private launch services. Similar to the way in which the government rallied behind commercial aviation decades earlier, in 2004, President George W. Bush advanced a new U.S. Space Exploration Policy that significantly redirected NASA's priorities. Bush directed NASA to support the development of commercial space flight, specifically so that private companies could service the ISS.[17] By 2022, three companies — SpaceX, Blue Origin, and Virgin Galactic — transported astronauts to the ISS, flew space enthusiasts into space, delivered cargo to low-Earth orbit, and developed reusable booster rockets.[18] Spaceflight is only one aspect of the commercialization of space; the gradual deregulation of space by the U.S. government has resulted in a tremendous growth of commercial space initiatives.[19]

According to an article published by the *Harvard Business Review* in February 2021, 95% of the estimated $366 billion in revenue earned in the space sector was from the space-for-Earth economy.[20] The *Harvard Business Review* defines the space-for-Earth economy as the goods or services produced in space for use on Earth. These goods and services included telecommunications and Internet infrastructure, Earth observation capabilities, and national security satellites, among others. Decreasing costs for launch and space

---

[17] Rachel Barton, *Technology and the History of Commercial Spaceflight* (West Lafayette: Purdue University Online, 2022), https://polytechnic.purdue.edu/purdue-online/blog/technology-and-history-of-commercial-spaceflight

[18] Svetla Ben-Itzhak, "Companies Are Commercializing Outer Space. Do Government Programs Still Matter?" *Washington Post*, January 11, 2022.

[19] Ibid.

[20] Matthew Weinzierl and Mehak Sarang, "The Commercial Space Age Is Here," *Harvard Business Review*, February 12, 2021, https://hbr.org/2021/02/the-commercial-space-age-is-here.

hardware have attracted new participants into the space-for-Earth market, and a variety of industries have already begun leveraging satellite technology and access to space to drive innovation and efficiency into the products and services they provide on Earth. The space-for-space economy, comprising goods and services produced in space for use in space, such as mining the Moon or asteroids for material to construct in-space habitats or supply refueling depots, has not had the same success as the space-for-Earth economy. However, Made In Space, Inc[21] has been at the forefront of manufacturing in space since 2014 when it 3D-printed a wrench onboard the ISS. Since 2014, Made In Space, Inc has been exploring other products produced in space, such as high-quality fiber-optic cable manufactured in zero-gravity. The company also received a $73.7 million contract from NASA in July 2019 to demonstrate the ability of a small spacecraft, called Archinaut One,[22] to manufacture and assemble spacecraft components in low-Earth orbit; it passed its Mission Critical Design Review in April 2022.[23] Another example of the U.S. government's increasing reliance on commercial space-based capabilities is the National Geospatial-Intelligence Agency's (NGA) recent announcement to gather more unclassified economic and military intelligence from commercial satellites.

The objective of NGA's initiative, called Luno A, is to acquire products, data, and services (analyses by commercial firms) produced from unclassified commercial GEOINT on unclassified networks. The expectation is the commercial products and data will enable analysts in the National System for Geospatial Intelligence (NSG) network to add context to their analytic assessments and to have unparalleled insight into the data to quantify worldwide economic and environmental activity and military capabilities. NGA sent a request for proposals (RFP) on January 10, 2024, and gave interested companies until March 29, 2024, to respond.[24]

---

[21] In June 2020, Redwire announced it had acquired Made In Space, Inc.

[22] Archinaut One is also known as the On-Orbit Servicing Assembly and Manufacturing 2 (OSAM-2) mission.

[23] Redwire, "Redwire's Trailblazing OSAM-2 Mission Passes Critical NASA Milestone," April 6, 2022, https://redwirespace.com/newsroom/redwires-trailblazing-osam-2-mission-passes-critical-nasa-milestone/.

[24] The description of NGA's Luno A initiative is from Theresa Hitchens, "NGA to Gather More Unclassified Economic, Military Intel From Commercial Sats," *Breaking Defense*, January 22, 2024, https://breakingdefense.com/2024/01/nga-to-gather-more-unclassified-economic-military-intel-from-commercial-sats/.

4. Technically Capable Workforce

While serving as the ranking member of the House Armed Service Subcommittee on Emerging Threats and Capabilities, Representative Jim Langevin (D-RI) said. "Perhaps the greatest challenge faced by the Department of Defense — and the entire government enterprise — is human resources. Technological dominance is meaningless without a skilled workforce capable of operating at the highest levels of their field."[25] According to a Center for Strategic and International Studies (CSIS) November 2020 briefing, "Geopolitical competition and the nature of modern warfare are increasingly shaped by technology."[26]

The CSIS brief details the DoD's recent efforts to create technical centers of excellence within DoD and build stronger relationships with Silicon Valley and other tech hubs. Additionally, DoD's largest investment in research and development in the last 70 years focuses on geopolitical competition and the nature of modern warfare. However, according to the CSIS brief, to fully modernize and compete effectively, the U.S. defense enterprise must also invest in the uniformed and civilian workers directly employed by the federal government.[27] The cyberspace and space workforces are two of the critical workforces the DoD must invest in.

A. Two Critical Workforces

1) Cyberspace Workforce

The DoD Cyber Workforce Framework (DCWF) lists seven workforce elements. Two of these elements, software engineer and AI/data, have been added as part of an ongoing initiative to transition the framework from a cyber focus to a broader digital workforce framework.[28] The five cyberspace-focused workforce elements are (1)

[25] Robert W. Turk, *Preparing a Cyber Security Workforce for the 21st Century* (Carlisle: U.S. Army War College, 2013), https://apps.dtic.mil/sti/pdfs/ADA590251.pdf.

[26] Morgan Dwyer, Lindsey Sheppard, Angelina Hidalgo, and Melissa Dalton, "To Compete, Invest in People: Retaining the U.S. Defense Enterprise's Technical Workforce," Center for Strategic & International Studies, November 23, 2020, https://www.csis.org/analysis/compete-invest-people-retaining-us-defense-enterprises-technical-workforce .

[27] Ibid.

[28] The DoD Cyber Exchange website (https://public.cyber.mil/wid/dcwf/) lists seven workforce elements for the DCWF. Department of Defense, *DoDI 8140.02, Identification, Tracking, and Reporting on Cyberspace Workforce Requirements*, December 21, 2021, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/814002p.PDF?ver=XEaIhBYPP_Ib2wnHOnA7xw%3d%3d, lists the five workforce elements listed above.

information technology – cyberspace, (2) cybersecurity, (3) cyberspace effects, (4) intelligence – cyberspace, and (5) cyberspace enablers. Information technology – cyberspace personnel design, build, configure, operate, and maintain information technology networks and capabilities. Cybersecurity personnel secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place and by taking internal defense actions. The cyberspace effects element of the workforce plans, supports, and executes cyberspace capabilities that externally defend or conduct force projection in or through cyberspace. Intelligence – cyberspace personnel collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operations. Finally, cyberspace enablers perform work roles to support or facilitate the functions of the other workforce elements.[29] These workforce elements require personnel with skills in a wide range of technical subjects including computer architecture, programming, data structures, networks, the Internet, database systems, information assurance, cryptography, and forensics.[30]

2) Space Workforce

The requirement for a technically capable Space Force is detailed in the "Guardian Ideal" published by the Space Force in September 2021.

> [The Space Force] will deploy force-multiplying technology and tools to enable Guardians to focus their talents on understanding, anticipating, and out-pacing our potential adversaries. Over time, we will increasingly free our Guardians from routine and repetitive tasks using process automation and artificial intelligence so they can accelerate innovation efforts and devise new ways to keep our potential adversaries on the horns of a dilemma. In so doing, we will create the military's first truly digital service.[31]

During the unveiling of the Guardian Ideal, then Chief of Space Operations General John Raymond stated as follows,

> While all Guardians will require a level of digital fluency to be successful, the Space Force also requires a cadre with mastery of digital competencies to include agile software development, software product management,

---

[29] https://public.cyber.mil/wid/dcwf/

[30] U.S. Naval Academy, "Cyber Operations: The Discipline and the Major," https://www.usna.edu/Academics/Majors-and-Courses/Majors/Cyber-Operations.php

[31] U.S. Space Force, "The Guardian Ideal," September 17, 2021, https://media.defense.gov/2021/Sep/21/2002858512/-1/-1/1/GUARDIAN%20IDEAL%20-%20FINAL.PDF

product lifecycle management, data architecture, data analytics, cyber security, cyber defense, and information technology infrastructure.[32]

General Raymond also acknowledged during the same press conference that these same skills are also in high demand in the private sector and that the Space Force will need a strategy to compete for this talent.

B. Realizing a Technically Capable Workforce

1) Cyberspace Workforce

Federal government workforce studies have noted that government agencies continue to experience a steady increase in cybersecurity workforce turnover rates — a trend that has spanned several decades. These same studies recommend the federal government seek to better understand employee shortages, recruitment roadblocks, and what motivates an employee to leave the federal workforce.[33] DoD has had a similar experience with its cyberspace workforce. According to John Sherman, DoD Chief Information Officer, there are gaps in the current cyber workforce, as well as a need to expand it. Mr. Sherman added that the Department must continue efforts to develop a talented cyber workforce that can securely build, operate, and maintain the Department's digital and critical infrastructures while also protecting and defending the Department's data against cyber adversaries.[34]

The U.S. Congress has also expressed concerns about whether adequate resources, policies, and programs are in place to support a cyber-capable workforce. The Fiscal Year 2023 National Defense Authorization Act (NDAA) included several provisions that relate to recruiting, retention, and career management of DoD military and civilian personnel in cyber career fields.[35]

- Section 1502 requires DoD to provide annual reports with the President's Budget on Cyber Mission Force (CMF) readiness; the adequacy of policies, plans, and procedures; and the execution of manning, training, and equipping the CMF, starting in Fiscal Year 2024.

---

[32] Ibid.

[33] Michael Ugarte. *Challenges and Way Ahead for Cybersecurity Workforce in Today's Federal Government* (Washington, DC: Defense Information Systems Agency, 2022), https://www.disa.mil/en/NewsandEvents/2022/Cybersecurity-Workforce.

[34] Written statement by John B Sherman, Department of Defense Chief Information Officer, before the House Armed Services Committee subcommittee on Cyber, Innovative Technologies, and Information Systems, March 9, 2023, https://docs.house.gov/meetings/AS/AS35/20230309/115478/HHRG-118-AS35-Wstate-ShermanJ-20230309.pdf.

[35] Kristy N. Kamarck and Catherine A. Theohary, *FY2023 NDAA: Cyber Personnel Policies* (Washington, DC: Congressional Research Service, March 6, 2023), https://crsreports.congress.gov/product/details?prodcode=R47270.

- Section 1532 directs the Secretary of the Navy to establish and sustain certain Cyber Warfare career designators, a training pipeline, and an implementation plan.
- Section 1533 requires a DoD study on the responsibilities of the military services for organizing, training, and presenting the total force to U.S. Cyber Command.
- Section 1534 requires the Secretary of Defense and the Chairman of the Joint Chiefs of Staff to develop a plan and recommendations to address CMF personnel readiness shortfalls.
- Section 1535 directs the Secretary of Defense to establish a program that provides financial support for the pursuit of programs that are critically needed and related to cyber or digital technology.
- Section 1540 requires DoD to engage with a federally funded research and development center or other non-profit to assess the feasibility and advisability of creating a civilian cybersecurity reserve corps.
- Section 1541 requires DoD to conduct a comprehensive review of Cyber Excepted Service (CES) policies, including personnel compensation and advancement, and to report annually on CES positions through 2028.

The private sector is also struggling to hire the cyberspace professionals it needs. According to the results of a survey by ManpowerGroup, a workforce solutions company, there is a 78% talent shortage in the information technology and tech sectors globally. Projections by the U.S. Bureau of Labor Statistics show that information technology jobs are expected to grow 15% by 2031 and will result in nearly 700,000 new jobs in the U.S. Additionally, the 7% replacement rate for existing tech jobs will require roughly 400,000 new workers a year, or about 4 million by 2033, according to CompTIA's State of the Tech Workforce report. Overcoming the shortage of cyberspace professionals will likely require a whole-of-nation approach that draws on the efforts of government, academia, and industry.[36]

DoD will have a role in this whole-of-nation approach in overcoming the shortage of cyberspace professionals, but there are unconventional approaches the Department should consider now to overcome some of the challenges it faces with recruiting a talented

[36] Tim Starks and David DiMolfetta. "Inside the White House Blueprint for Filling U.S. Cyber Jobs," *The Washington Post*, August 1, 2023, https://www.washingtonpost.com/politics/2023/08/01/inside-white-house-blueprint-filling-us-cyber-jobs/.

cyberspace workforce. Some of the unconventional recruiting approaches the Department should examine include the following:[37]

- Accepting candidates with different education experiences. Specifying a degree requirement or required knowledge in a job announcement can restrict the number of candidates that apply. Considering candidates who have taken boot-camp-style courses, obtained certifications, or attended a technical school could expand the pool of applicants. When looking for new talent, determining whether someone has the aptitude for learning a skill is more important than finding someone who already has the skill.
- Training new employees is a way to tailor the employee's development to the organization's needs while also providing opportunities for growth. Additionally, investments in employee professional development often lead to higher levels of employee retention.
- Apprenticeship programs can open career opportunities for talented individuals. Instead of buying experience, apprenticeships allow the organization to train entry-level talent.
- Developing talent pipelines through partnerships with local schools and nonprofit organizations would provide learning opportunities for students from elementary school through college and encourage them to consider professions in the fields they were exposed to. Teaching and mentoring the next generation of cyberspace professionals will be crucial for growing the size of the future talent pool.
- Bench positions are another approach for expanding entry-level talent pools. Bench positions are designed to get talented individuals into an organization with the idea that they will move into more permanent roles as the right fits become available. While they are waiting for the right position, they are rotated through different assignments or disciplines to expand their strengths and work experience.

To meet the demands of the changing nature of the cyberspace domain, the Department recently published a DoD Cyber Workforce Strategy Implementation Plan

[37] Tracy Kemp, "Unconventional Recruiting Methods That Can Help Fill The Tech Talent Gap," *Forbes*, July 14, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/07/14/unconventional-recruiting-methods-that-can-help-fill-the-tech-talent-gap/?sh=fcd8b7d75be7.

with two out of the four goals containing objectives focused on workforce professional development.[38]

Three of the objectives for goal number two, "Establish an Enterprise-wide Talent Management Program to Better Align Force Capabilities with Current and Future Requirements," focus on workforce development:

- Drive continuous development to foster capability advancement across all proficiency and experience levels.
- Improve and expand new employee development programs as part of talent management.
- Include changing mission requirements in development pipelines to match talent management to mission.

Two of the objectives for goal number four, "Foster Collaboration and Partnership to Enhance Capability Development, Operational Effectiveness and Career Broadening Experiences," focus on the development of the workforce.

- Strengthen partnerships with federal agencies, specifically partnerships focused on career-broadening opportunities, cross-training, and information-sharing.
- Leverage partnerships with allies and partner nations to strengthen force development capabilities.

One of the challenges the Department will face when implementing these workforce development initiatives is resources. Not only will the development programs require funding, the cyber workforce at the organization level will also need to be large enough to retain sufficient manpower for its operational missions while individual employees participate in the development programs. Similarly, the partnership programs will likely require the participating government agency to provide a capable employee in the exchange so the DoD organization can still accomplish its mission.

2) Space Workforce

The Space Force has not been in existence long enough to generate useful data on its ability to recruit, professionally develop, and retain talented uniformed and civilian members of the U.S. Space Force. Current reporting indicates the Space Force has met its recruiting goals the first two years of its existence.[39] What has been more interesting is the Space Force's efforts to embrace innovative recruiting practices. One of these innovative

---

[38] Department of Defense, *DOD Cyber Workforce Strategy Implementation Plan 2023–2027* (Washington, DC: Department of Defense, 2023), https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf.

[39] Adrian Boneberger, "Space Force: Surprisingly Good at Recruiting," *Military Media*, August 28, 2023, https://www.militarymedia.org/p/recruiting-space-force-success.

approaches is the "constructive service credit program." The program, introduced in 2022, allows experienced professionals in the fields of cybersecurity and intelligence to be directly commissioned into the Space Force at ranks appropriate to their years of experience. Another, more unconventional initiative recently approved by Congress[40] allows full-time Guardians to serve part-time to avoid the need for a dedicated reserve force. The idea is to have an active-duty force with full-time and part-time members. This system will allow Guardians to transfer out of full-time duty status to pursue opportunities outside military service and to subsequently return to full-time duty without barriers to reentry or detriment to their careers. The Space Force believes this approach will strengthen their recruiting and retention efforts by providing unique and flexible career paths.[41]

[40] Jonathan Lehrfeld and Rachel S. Cohen, "Congress Approves Space Force Part-Timers, but Still No Space Guard," *Air Force Times*, January 16, 2023, https://www.airforcetimes.com/news/your-military/2024/01/16/congress-approves-space-force-part-timers-but-still-no-space-guard/.

[41] Sandra Erwin, "Space Force Embraces Unconventional Ways to Attract and Retain Talent," *SpaceNews*, April 5, 2023, https://spacenews.com/space-force-embraces-unconventional-ways-to-attract-and-retain-talent/.

5. Defining the National Security Relationship Between the Government and the Commercial Sector

A. Cyberspace

The transition to a digital world has not been without challenges. One critical challenge that requires government and private sector coordination is network security. At the August 25, 2021, White House Cybersecurity Summit, President Biden described cybersecurity as a "core national security challenge." The President went on to say, "the reality is, most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone."[42] Industry participants at the summit discussed how they could reshape their industries to enhance user security, likening it to the effort to standardize automobile seat belts and airbags. Insurance providers suggested they could use incentives and mandatory requirements to nudge customers in the right directions, and others suggested tougher application of financial regulation on cryptocurrencies to limit the rewards associated with launching ransomware attacks. The National Institute for Standards and Technology (NIST) said it would work with Microsoft and Google, as well as the insurance industry companies Travelers and Coalition to design a new framework to guide the creation of more secure technology products and to audit the security of technology products.

Two recent significant cyberattacks highlight the ongoing cybersecurity challenge in the U.S. They are the SolarWinds supply chain and the Colonial Pipeline ransomware attacks. The SolarWinds attack highlighted the vulnerabilities in the global software supply chains that affect both government and private sector computer systems. The Colonial Pipeline ransomware attack highlighted the challenges the U.S. faces providing cybersecurity to critical infrastructure.

Another significant challenge is combating cybercrime. A *Forbes* article, "Cybersecurity Trends and Statistics for 2023; What You Need to Know," cited research by Cybersecurity Ventures in declaring that cybercrime is "growing exponentially." According to the article, the cost of cybercrime was predicted to reach $8 trillion in 2023

[42] White House, "Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/, and Cat Zakrzewski, Joseph Marks, and Jay Greene, "Biden Tells Top CEOs at White House Summit to Step Up on Cybersecurity," *The Washington Post*, August 25, 2021, https://www.washingtonpost.com/technology/2021/08/25/white-house-cybersecurity-summit-apple-amazon/.

and grow to $10.5 trillion by 2025. The *Forbes* article identified two contributing factors: (1) at least one open-source vulnerability was found in 84% of code bases, indicating that software applications' reliance on open-source code is still a significant cybersecurity issue; and (2) phishing continued to be successful for hackers in 2023. Unfortunately, many of the obvious signs of phishbait, such as misspelled words and poor grammar, are no longer present in phishing emails, which necessitates changes to employee cybersecurity training to keep pace with the evolving phishing threat.[43] On top of those trends, the effects of artificial intelligence (AI) on the vulnerability and adequacy of security measures has not yet been explored.

The Government Accountability Office (GAO) High-Risk Series states that the nation's cybersecurity has regressed since it was first evaluated in 2019.[44] Figure 5-1 summarizes what the GAO described in March 2021 as the four major cybersecurity challenges and the 10 associated critical actions.

[43] Chuck Brooks, "Cybersecurity Trends and Statistics for 2023: What You Need to Know," *Forbes*, March 5, 2023, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=4c3f91f519db.

[44] U.S. Government Accounting Office, "High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas," March 2, 2021, https://www.gao.gov/products/gao-21-119sp#:~:text=GAO%27s%20High-Risk%20Series%20identifies%20government%20operations%20with%20vulnerabilities,transformation%20to%20address%20economy%2C%20efficiency%2C%20or%20effectiveness%20challenges.

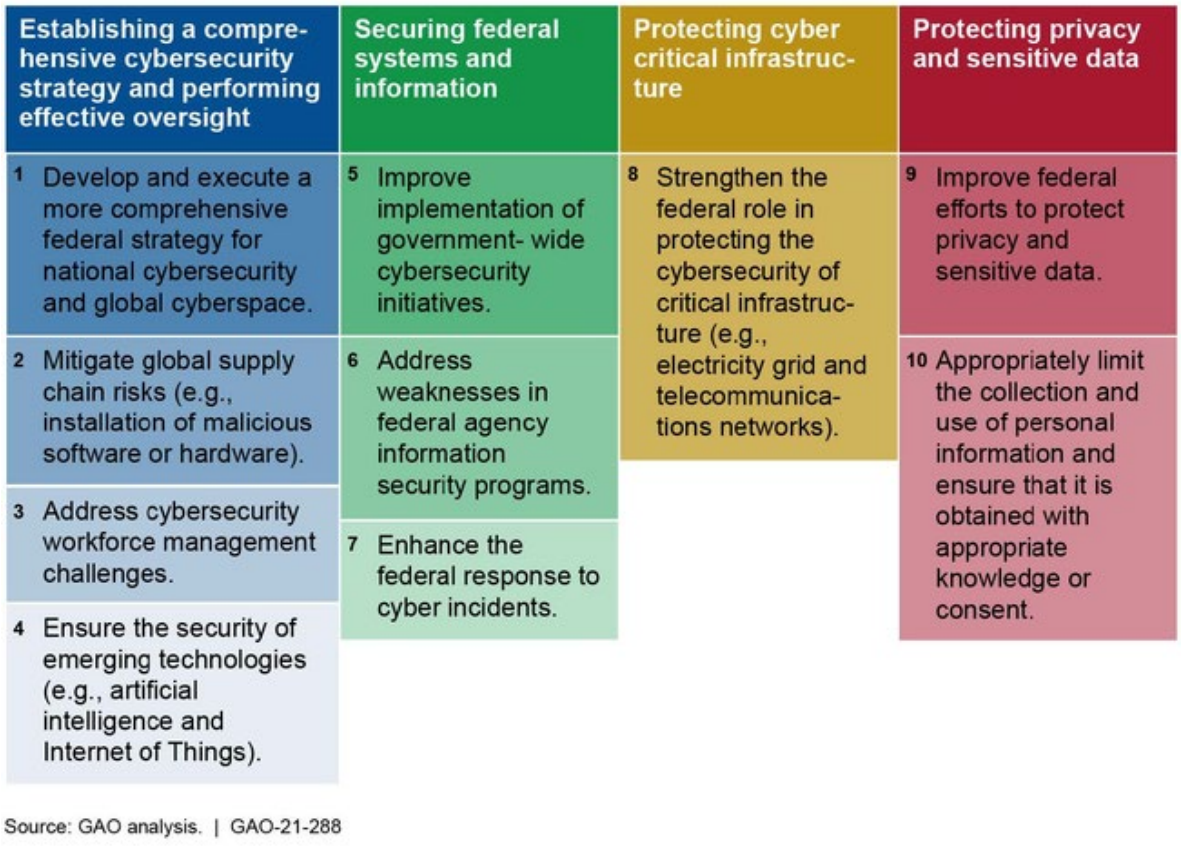

Figure 5-1. Four Major Cybersecurity Challenges and 10 Associated Critical Actions

Recommendations by the GAO and other government and private sector organizations for meeting the challenges cybersecurity presents to national security may not be successful until the government and private sector answer key questions posed in Michael Daniel's 2017 *Harvard Business Review* article, "Why Is Cybersecurity So Hard?"

Daniel argued that "if you look at cybersecurity challenge more broadly, even if we resolved the technical issues, cybersecurity would remain a hard problem for three reasons: It's not just a technical problem; the rules of cyberspace are different from the physical world's; and cybersecurity law, policy, and practice are not yet fully developed."[45] The immaturity of legal and policy frameworks for cyberspace still presents a significant challenge today. As Daniel suggested in 2017, we do not yet have clear answers to the following key questions:

[45] Michael Daniel, "Why Is Cybersecurity So Hard?", *Harvard Business Review*, May 22, 2017, https://hbr.org/2017/05/why-is-cybersecurity-so-hard#:~:text=But%20if%20you%20look%20at%20the%20challenge%20more,policy%2C%20and%20practice%20are%20not%20yet%20fully%20developed.

- What is the right division of responsibility between governments and the private sector in terms of defense?
- What standard of care should we expect companies to exercise in handling our data?
- How should regulators approach cybersecurity in their industries?
- What actions are acceptable for governments, companies, and individuals to take and which actions are not?
- Who is responsible for software flaws?
- How do we hold individuals and organizations accountable across international boundaries?[46]

Although there has been progress in all of these areas, the absence of fully developed answers will hinder the development approaches to the challenges and critical actions depicted in Figure 5-1.

B. Space

U.S. companies have always been involved in space flight as contractors to government agencies; however, activities in space are increasingly being led by private sector companies. A majority of U.S. satellites are now commercially owned, and the government no longer has a monopoly on space launches.[47] SpaceX's achievements (in cooperation with NASA) and the efforts by Boeing, Blue Origin, and Virgin Galactic to put people in space sustainably and at scale could signal the start of the space-for-space economy.[48] The commercialization of space raises two issues for the U.S. government: how will the federal government regulate, oversee, and promote the commercial space sector, and how will the federal government itself use commercial space capabilities?[49] These two issues raise additional questions:[50]

- Should the federal regulatory framework for commercial space activities be consolidated?

---

[46] Ibid.

[47] Daniel Morgan, *Commercial Space: Federal Regulation, Oversight, and Utilization* (Washington, DC: Congressional Research Service: November 29, 2018) https://crsreports.congress.gov/product/pdf/R/R45416.

[48] Weinzierl and Sarang, "The Commercial Space Age Is Here."

[49] Morgan, *Commercial Space: Federal Regulation, Oversight, and Utilization*.

[50] Ibid.

- Can the commercial space licensing process balance industry's need for timeliness and transparency with the government's need to meet national security and foreign policy objectives?
- How should federal regulatory policies be adjusted as the commercial space industry develops new capabilities and applications?
- What government space activities can or should be conducted by commercial entities?
- How can government and industry best work together?

Space's transition from an area of scientific exploration and discovery dominated by the government to an area of significant commerce and commercial activity will also require new international agreements to normalize space activity and security operations to safeguard access and maneuverability and prevent malign actions from disrupting space activity.[51] The Internet (the logic layer of cyberspace)[52] has also evolved from government dominance to one of significant commercial activity.

[51] Clementine G. Starling, Mark J. Massa, Christopher P. Mulder, and Julia T. Siegel, *The Future of Security in Space: A Thirty-Year U.S. Strategy*, Atlantic Council, April 2021, https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/the-future-of-security-in-space/.

[52] Cyberspace is defined by the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 as "The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." Cyberspace consists of four different layers: (1) the physical layer, (2) the logic layer, (3) the information layer, and (4) the personal layer. The physical layer consists of physical devices such as PCs, networks, wires, grids, and routers. The logic layer is where the Internet platform is defined and created. Cyberspace depends on the design of the Internet. It is built out of components that provide services for users, such as social media, content, shopping, etc. The information layer includes the creation and distribution of information and interaction between users. The personal layer consists of people who create websites, tweet, blog, and purchase goods online. Electrical Academia, "What Distinguishes Cyberspace, the Internet, and the World Wide Web?", https://electricalacademia.com/tech-articles/distinguishes-cyberspace-internet-world-wide-web/.

6. Achieving Unity of Effort in Cyberspace and Space Operations

A. Space Command and Cyber Command Are Inseparable

General James H. Dickinson, commander of U.S. Space Command, said his work is "inseparable from that of U.S. Cyber Command but that policy must change to keep up with evolving threats in the cyber domain." General Dickinson went on to say, "Given our unique operating environment, there is a special synergy between U.S. Space Command and U.S. Cyber Command. Securing one means securing the other. Operating in one requires operating in the other." General Dickerson also pointed out that his Navy (Space) component command has the same leader as that Service's component command for U.S. Cyber Command. This leads one to believe that there is great synchronization between the two domains.[53] General Dickinson was not the first to describe the connection between space and cyber. Lieutenant General DeAnna Burt, Space Force's Deputy Chief of Space Operations for Operations, Cyber and Nuclear, recently spoke at a Mitchell Institute for Aerospace Studies and called cyber "critical to us," adding that "on order of gas to the Air Force, cyber is to the Space Force." She noted that the Space Force has "developed tools that we've put onto our weapons systems to be able to detect cyber intrusions." She also said CYBERCOM has been "an incredible partner" and is working to "build this cybersecurity mindset into the acquisition process."[54]

While serving as the Assistant Secretary of Defense for Global Strategic Affairs, Madelyn Creedon commented at the 2011 U.S. Strategic Command Cyber and Space Symposium that cyber and space capabilities are connected operationally. "A bit of data from an analyst sitting at a computer may be directed through a local network, transmitted by satellite, and then received by troops in the field halfway around the world. Space capabilities supplement and enhance cyber capabilities and vice versa." Creedon also described how cyber and space are connected by common threats. "Each of these depends on the electromagnetic spectrum and IT infrastructure that affords us great capabilities but also creates cross-domain vulnerabilities and challenges."[55] Others have made these same

[53] Abraham Mahsie, "Dickinson: Space Command and Cyber Command 'Inseparable,'" *Air & Space Forces Magazine,* July 27, 2021, https://www.airandspaceforces.com/dickinson-space-command-cyber-command-inseparable/.

[54] Edward Graham, "How Space Force Is Raising Its Cyber Defenses," *Defense One*, January 9, 2024, https://www.defenseone.com/policy/2024/01/how-space-force-raising-its-cyber-defenses/393197/

[55] Madelyn R. Creedon, "Space and Cyber: Shared Challenges, Shared Opportunities. Edited Remarks to the USSTRATCOM Cyber and Space Symposium," *Strategic Studies Quarterly* 6, no. 1, (Spring 2012): 3–8. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/creedon.pdf.

observations and have argued for changes in the way DoD mans, trains, and equips space and cyber forces to better integrate with the rest of the joint force.

Ethan Brown, a Senior Fellow at the Mike Rogers Center for Intelligence and Global Affairs at the Center for the Study of the Presidency and Congress, argued four years ago that "cyber warfare has outgrown its place as a unified combatant command and now demands the full weight of a service component as its vehicle of execution." Brown declared "it is time to transition the national security cyber domain architecture from a combatant command into the operational mechanism of space warfighting."[56] However, others are more cautious about making cyber a separate armed service or combining it with space under the Space Force.

The Deputy Assistant Secretary of Defense for Cyber Policy, Mieke Eoyang, warned that standing up an independent cyber military service similar to Space Force could potentially pose new challenges for the DoD when it comes to understanding warfighting needs within the military services. Eoyang added that a cyber service might have some benefits in ease of administrative management, but added that the Department has a variety of military services who perform many different types of missions and those missions are enabled by technologies that are particular to those mission sets. A cyber service divorced from these mission sets may pose challenges in understanding the cyber warfighting needs of the other services that enables an effective joint fight.[57] Although Eoyang did not address the possibility of combining cyber and space forces under a single service, it appears she would have a similar concern with a combined cyber–space force because it too could find itself separated from the mission sets of the other military services. These claims of synergy between cyber and space, their common threats, their dependency on the electromagnetic spectrum and IT infrastructure, and their requirement to understand the warfighting needs of the military Services suggest several issues that warrant an examination by DoD. One of these issues involves of the need for a unified effort in cyberspace and space to accomplish a combatant commander's operational objectives. Understanding the potential challenges to achieving unity of effort in cyberspace and space requires an examination of the planning, coordination, and execution of cyberspace and space operations in support of geographic combatant commanders.

---

[56] Ethan Brown, "A Combat Role for The Space Force: Why the Newest Armed Service Should Own Cyber Warfare," Modern War Institute, July 16, 2020, https://mwi.westpoint.edu/a-combat-role-for-space-force-why-the-newest-armed-service-should-own-cyber-warfare/.

[57] Jaspreet Gill, "'Be Careful What You Wish For': DoD Official Warns Separate Cyber Force Could Pose New Challenge," Breaking Defense, September 15, 2023, https://breakingdefense.com/2023/09/be-careful-what-you-wish-for-dod-official-warns-separate-cyber-force-could-pose-new-challenges/.

B. The Current Approach

U.S. Cyber Command's operations are direct though various subordinate organizations. These include the 133 cyber mission teams of the Joint Force Headquarters-DoDIN; the Cyber National Mission Force; Joint Task Force Ares; and the respective Service Cyber Commands, which include Army Cyber Command, Fleet Cyber Command/10th Fleet, Marine Corps Forces Cyberspace Command, Air Force Cyber/16th Air Force, and Coast Guard Cyber Command. To provide planning, targeting, intelligence and cyber capabilities to the CCMDs, each of U.S. Cyber Command's Service component commands, except the Coast Guard Cyber Command, also mans a Joint Force Headquarters – Cyber (JFHQ-C). Some JFHQ-Cs support three CCMDs while others support two CCMDs. The JFHQ-Cs also oversee a portion of the 133 cyber mission teams that conduct operations for the supported CCMD. To provide a cyberspace presence on the CCMD staff, U.S. Cyber Command and its components have also established Cyber Operations – Integrated Planning Elements (CO-IPEs) at each CCMD headquarters. The CO-IPEs facilitate the CCMD's requirements for cyber support in the accomplishment of the CCMD's mission. The CO-IPEs also offer lessons learned and new options for the CCMD's planners based on insights from fellow CO-IPEs at other commands. The Space Force takes a slightly different approach for supporting the CCMDs.

One of the challenges to understanding how the U.S. military is organized for space operations is understanding the different roles of the U.S. Space Force versus the U.S. Space Command. The U.S. Space Force is one of the five Armed Services of the DoD. Its role is to organize, train, and equip space forces. As a CCMD, U.S. Space Command actively employs assigned forces from each of the military services to accomplish directed missions in the space domain. The U.S. Space Force recently reorganized its command structure in an effort to streamline operations.

On December 12, 2023, the U.S. Space Force established the U.S. Space Forces – Space, which is a U.S. Space Force Component Field Command directly subordinate to the Chief of Space Operations for execution of the Secretary of the Air Force's responsibilities for administration and support functions under Section 9013 of Title 10, U.S. Code (U.S.C.). U.S. Space Command's commander has also designated the U.S. Space Forces – Space Commander, Lieutenant General Schiess, to serve simultaneously as the Combined Joint Force Space Component Commander, granting Schiess authority over all space forces assigned by the services to the CCMD. Space Forces – Space is responsible for ensuring that space forces are efficiently trained and ready for U.S. Space Command while also meeting the challenges found in the dynamic national security environment.[58] This

[58] U.S. Space Command, "SecAF Redesignates Space Operations Command West as U.S. Space Forces – Space," December 12, 2023, https://www.spacecom.mil/Newsroom/News/Article-

reorganization combines duties and responsibilities previously assigned to two organizations with two separate commanders: Combined Force Space Component Command (CFSCC) and Joint Task Force Space Defense (JTF-SD). CFSCC provided U.S. Space Command planning, integration, and the execution and assessment of global space operations that deliver combat-relevant space capabilities to combatant commanders, coalition partners, the joint force, and the nation. JTF-SD provided U.S. Space Command and its mission partners with space superiority operations to deter aggression, defend U.S. and allied interests, and defeat adversaries throughout the continuum of conflict.[59] U.S. Space Command also lists U.S. Army Space and Missile Defense Command; U.S. Marine Forces – Space; U.S. Navy Space Command; First Air Force, Space Operations Command; and Joint Functional Component Command for Integrated Missile Defense as warfighting units on its web page.[60] As a Service, the U.S. Space Force is also readying Space Force Service Component Commands at geographic CCMD headquarters locations.

The first Space Force Component Command resides with U.S. Indo-Pacific Command (INDOPACOM). INDOPACOM's Space Force Component Command consists of 21 military and civilian personnel, who help INDOPACOM coordinate and synthesize space offerings from commercial companies, the intelligence community, the NRO, and allies and partners. These space experts are also expected to improve the processes CCMDs use for identifying their space operational needs.[61] More recently, Space Force has installed Space Forces Europe and Africa at Ramstein Air Base in Germany. Like the INDOPACOM Space Component, Space Forces Europe and Africa will coordinate and synthesize space offerings from commercial companies, the intelligence community, the NRO, and allies and partners for both U.S. European Command (EUCOM) and U.S. Africa Command (AFRICOM).[62] It is not clear how effective these approaches will be in achieving the synergy between cyberspace and space that General Dickinson described or how well these approaches will be in addressing similar threats or coordinating the use of the electromagnetic spectrum and the IT infrastructure.

Display/Article/3614643/secaf-redesignates-space-operations-command-west-as-us-space-forces-space/.

[59] Sandra Erwin, "Space Force Reorganizes Command Structure to Streamline Operations," *SpaceNews*, December 13, 2023, https://spacenews.com/space-force-reorganizes-command-structure-to-streamline-operations/.

[60] https://www.spacecom.mil/About/Warfighting-Units/

[61] Lauren C. Williams, "Space Force Is Setting Up Inside Combatant Commands," *Defense One*, November 22, 2022, https://www.defenseone.com/policy/2022/11/space-force-setting-inside-combatant-commands/380095/.

[62] Theresa Hitchens, "Space Force Gets a New Command, New Geographic Component in Latest Reorg," *Breaking Defense*, December 13, 2023, https://breakingdefense.com/2023/12/space-force-gets-a-new-command-new-geographic-component-in-latest-reorg/.

C. Achieving Unity of Effort in Cyberspace and Space Operations

A series of stress tests would determine whether current command and support approaches can achieve the necessary synergy between cyberspace and space, enable a coordinated response to similar threats, and support the dual use of both the electromagnetic spectrum and IT infrastructure. These stress tests would use the command and support relationships in existing combatant commander contingency plans as the starting point for the evaluations. The first step entails developing a detailed schematic of the planned chain of command for the contingency plan being evaluated. The chain of command would include both the CCMD chain of command and the administrative control (ADCON) exercised through the Secretaries of the Military Departments. *Joint Publication 1, Volume 2, The Joint Force* details the command authority combatant commanders have over assigned forces.[63] The CCMD chain of command runs from the President to the Secretary of Defense to the commanders of the CCMDs. Secretaries of the Military Departments exercise administration and support of forces assigned to combatant commanders in accordance with the provisions of Section 165, Title 10 U.S.C. The ADCON chain of command[64] runs from the President through the Secretary of Defense and Secretaries of the Military Departments to the forces assigned to CCMDs.

The schematic would show the levels of authority[65] the combatant commander has established for Service forces assigned under the command's component commands and any other subordinate headquarters found in the contingency plan. Since the contingency plan likely has other CCMDs in supporting roles, the type of support[66] provided by other CCMDs would also be shown in the schematic. The schematic would also identify combat support or combat service support provided by any of the combat support agencies (CSAs). Finally, the reporting requirements. along with the supporting IT infrastructure that allows the organizations in the chain of command schematic to communicate with one another

---

[63] combatant command (command authority) — Nontransferable command authority, which cannot be delegated, of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Also called COCOM. See also combatant command; combatant commander; operational control; tactical control. Department of Defense, *Joint Publication 1, Volume 2, The Joint Force*, June 19, 2020, p. xix. https://jdeis.js.mil/jdeis/new_pubs/jp1vol2.pdf.

[64] Administrative control – direction or exercise of authority over subordinate or other organizations in respect to administration and support, Ibid, p. GL-4.

[65] Levels of authority – the specific command relationship; combatant command authority, operational control, tactical control, coordinating authority and direct liaison authorized, Ibid, p. xix.

[66] Support – support is a command authority. A support relationship is established by a common superior commander between subordinate commanders when on organization should aid, protect, complement, or sustain another force. The Secretary of Defense establishes support relationships between combatant commanders for the planning and execution of joint operations. Ibid, p. xx.

and share data and information will be overlaid on top of the chain of command schematic. Once the schematics are complete, the Joint Staff would sponsor a series of tabletop exercises or wargames using different scenarios to stress the levels of authority, CCMD and support relationships, CSA combat and combat service support relationships, staff coordination procedures, and information sharing systems. The exercises will demonstrate where these elements work effectively and contribute to mission success, where they generate friction that hampers mission accomplishment, and where they fail and contribute to mission failure.

This methodology is essentially an attempt to apply Martin van Creveld's model of a "Command System" from his book *Command in War*. As van Creveld explained,

> Although the functions of command are thus not subject to change (it is certainly conceivable for the way in which they are carried out to vary, however, and for their relative importance and relationship to each other to do the same), the means at its disposal as we know them today are, without exception, the result of long and continuous development. A useful method for classifying these means is to divide them into three categories: organizations, such as staffs or councils of war; procedures, such as the way in which reports are distributed inside a headquarters; and technical means, ranging from the standard to the radio. The combination of these three should make it possible, in principle, to describe the structure of any command systems at any given time and place.[67]

Some issues will be obvious and easily corrected. One obvious and potentially easily fixed issue, for example, is that the NRO is not designated as a CSA in DoDD 3000.06, "Combat Support Agencies."[68] Technically, this means the NRO is not required to support U.S. Space Command. Other issues might be more difficult to address. One potentially difficult issue is intel gain/loss or deciding whether the value of collecting information from an enemy target is more worthwhile than destroying it. Due to the number of CCMDs, CSAs, and intelligence agencies potentially involved in the intel gain/loss problem, should the Secretary of Defense, or even the President, be the ultimate arbiter? Do procedures exist to provide the necessary information to the individual that will be required to make the intel gain/loss decision? If procedures exist, are they agile enough to meet the demands of conflict in the current and emerging operating environment? The tabletop exercises or wargames will likely identify areas where the law or joint doctrine does not provide sufficient guidance to the joint force in areas like the coordination of supporting terrestrial space operations and the coordination of Service space operations.

---

[67] Martin Van Creveld, *Command in War*, (Cambridge: Harvard University Press, 1987), 9–10.

[68] Combat Support Agencies (CSA) are designated in Department of Defense Directive (DoDD) 3000.06. Department of Defense, *DoDD 3000.06, Combat Support Agencies (CSAs)*, June 27, 2013. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300006p.pdf?ver=2019-01-24-093121-273.

7. Conclusions

This paper examined the similarities and differences between cyberspace and space and presented three related national security issues for the U.S.

Addressing the national security relationship between the government and the commercial sector in both cyberspace and space will require the active participation of several government agencies, including DoD. The Department will have a significant role in the government's efforts to establish the national security relationship between the government and the commercial sector. DoD's needs will be particularly critical when discussing those national security systems that operate in or transit through cyberspace or space.

Similarly, addressing the underlying shortage of a technically capable uniformed and civilian workforce for both cyberspace and space will require a whole-of-nation approach. However, the Department must ensure that its internal policies, procedures, and resourcing levels for recruiting, retaining, and professionally developing both its uniformed and civilian cyberspace and space workforces enables it to be competitive with the rest of government and the commercial sector to secure the necessary talent to accomplish its current and future missions in both domains in the current and emerging operational environments.

Finally, the Department should conduct a series of stress tests of the current approaches for support relationship between CYBERCOM and the NSA, between SPACECOM and the NRO, and between both CYBERCOM and SPACECOM and the geographic and functional CCMDs. These tests will be critical components of the Department's efforts for achieving key future capabilities for the Joint Force, such as the unified ecosystem of sensors and data streams through JADC2 and tracking emerging threats like hypersonic missiles.

Appendix A. References

Barton, Rachel. *Technology and the History of Commercial Spaceflight.* West Lafayette: Purdue University Online, 2022. https://polytechnic.purdue.edu/purdue-online/blog/technology-and-history-of-commercial-spaceflight.

Ben-Itzhak, Svetla. "Companies Are Commercializing Outer Space. Do Government Programs Still Matter?" *Washington Post*, January 11, 2022.

Boneberger, Adrian. "Space Force: Surprisingly Good at Recruiting." *Military Media*, August 28, 2023. https://www.militarymedia.org/p/recruiting-space-force-success

Brooks, Chuck. "Cybersecurity Trends and Statistics for 2023: What You Need to Know." *Forbes*, March 5, 2023. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=4c3f91f519db

Brown, Ethan. "A Combat Role for The Space Force: Why the Newest Armed Service Should Own Cyber Warfare." Modern War Institute, July 16, 2020. https://mwi.westpoint.edu/a-combat-role-for-space-force-why-the-newest-armed-service-should-own-cyber-warfare/.

Creedon, Madelyn R. "Space and Cyber: Shared Challenges, Shared Opportunities. Edited Remarks to the USSTRATCOM Cyber and Space Symposium." *Strategic Studies Quarterly* 6, no. 1, (Spring 2012): 3–8. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/creedon.pdf.

Crothers, Brian, Jeff Lanphear, Brian Garion, Paul P. Konyha, and Edward P. Byrne. *U.S. Space-Based Intelligence, Surveillance, and Reconnaissance.* Montgomery: Air University Press, 2009. https://www.jstor.org/stable/resrep13939.20.

Daniel, Michael. "Why Is Cybersecurity So Hard?" *Harvard Business Review*, May 22, 2017. https://hbr.org/2017/05/why-is-cybersecurity-so-hard#:~:text=But%20if%20you%20look%20at%20the%20challenge%20more,policy%2C%20and%20practice%20are%20not%20yet%20fully%20developed.

Defense in a Digital Era: Artificial Intelligence, Information Technology, and Securing the Department of Defense, Statement by John B. Sherman, Department of Defense Chief Information Officer, before the House Armed Services Committee Subcommittee on Cyber, Innovative Technologies, and Information Systems, March 9, 2023. https://docs.house.gov/meetings/AS/AS35/20230309/115478/HHRG-118-AS35-Wstate-ShermanJ-20230309.pdf.

Department of Defense. *DoDD 3000.06, Combat Support Agencies (CSAs)*. June 27, 2013.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300006p.pdf?ver=2019-01-24-093121-273.

Department of Defense. *DoDI 8140.02, Identification, Tracking, and Reporting on Cyberspace Workforce Requirements*. December 21, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/814002p.PDF?ver=XEaIhBYPP_Ib2wnHOnA7xw%3d%3d

Department of Defense. *Joint Publication 1, Doctrine for the Armed Forces of the United States*. May 2003 (Change 1, March 2009).

Department of Defense. *Joint Publication 1, Volume 1, Joint Warfighting*. August 2023. https://jdeis.js.mil/jdeis/new_pubs/jp1_vol1.pdf.

Department of Defense, *Joint Publication 1, Volume 2, The Joint Force*, June 19, 2020, https://jdeis.js.mil/jdeis/new_pubs/jp1vol2.pdf.

Department of Defense. *Joint Publication 3-12, Cyberspace Operations*. June 8, 2018. https://nsarchive.gwu.edu/document/16681-joint-chiefs-staff-joint-publication-3-12.

Department of Defense. *Cyber Workforce Strategy Implementation Plan 2023–2027*, Washington, DC: Department of Defense, 2023. https://dodcio.defense.gov/Portals/0/Documents/Library/CWF-Strategy.pdf.

Dwyer, Morgan, Lindsey Sheppard, Angelina Hidalgo, and Melissa Dalton. "To Compete, Invest in People: Retaining the U.S. Defense Enterprise's Technical Workforce." Center for Strategic & International Studies, November 23, 2020, https://www.csis.org/analysis/compete-invest-people-retaining-us-defense-enterprises-technical-workforce.

Electrical Academia. "What Distinguishes Cyberspace, the Internet, and the World Wide Web?" https://electricalacademia.com/tech-articles/distinguishes-cyberspace-internet-world-wide-web/.

Erwin, Sandra. "Space Force Embraces Unconventional Ways to Attract and Retain Talent." *SpaceNews*, April 5, 2023. https://spacenews.com/space-force-embraces-unconventional-ways-to-attract-and-retain-talent/.

Erwin, Sandra. "Space Force Reorganizes Command Structure to Streamline Operations." *SpaceNews*, December 13, 2023. https://spacenews.com/space-force-reorganizes-command-structure-to-streamline-operations/.

Gill, Jaspreet. "'Be Careful What You Wish For': DoD Official Warns Separate Cyber Force Could Pose New Challenge." Breaking Defense, September 15, 2023. https://breakingdefense.com/2023/09/be-careful-what-you-wish-for-dod-official-warns-separate-cyber-force-could-pose-new-challenges/

Graham, Edward. "How Space Force Is Raising Its Cyber Defenses." *Defense One*, January 9, 2024. https://www.defenseone.com/policy/2024/01/how-space-force-raising-its-cyber-defenses/393197/.

Hitchens, Theresa. "NGA to Gather More Unclassified Economic, Military Intel From Commercial Sats." *Breaking Defense*, January 22, 2024.

https://breakingdefense.com/2024/01/nga-to-gather-more-unclassified-economic-military-intel-from-commercial-sats/.

Hitchens, Theresa. "Space Force Gets a New Command, New Geographic Component in Latest Reorg," *Breaking Defense*, December 13, 2023, https://breakingdefense.com/2023/12/space-force-gets-a-new-command-new-geographic-component-in-latest-reorg/.

Kamarck, Kristy N., and Catherine A. Theohary. *FY2023 NDAA: Cyber Personnel Policies*. Washington, DC: Congressional Research Service, March 6, 2023. https://crsreports.congress.gov/product/details?prodcode=R47270

Kemp, Tracy. "Unconventional Recruiting Methods That Can Help Fill The Tech Talent Gap." *Forbes*, July 14, 2023. https://www.forbes.com/sites/forbestechcouncil/2023/07/14/unconventional-recruiting-methods-that-can-help-fill-the-tech-talent-gap/?sh=fcd8b7d75be7

Lambakis, Steven. *On the Edge of Earth: The Future of American Space Power*. Lexington, KY: University Press of Kentucky, 2001.

Lehrfeld, Jonathan, and Rachel S. Cohen. "Congress Approves Space Force Part-Timers, but Still No Space Guard." *Air Force Times*, January 16, 2023. https://www.airforcetimes.com/news/your-military/2024/01/16/congress-approves-space-force-part-timers-but-still-no-space-guard/

Mahsie, Abraham. "Dickinson: Space Command and Cyber Command 'Inseparable.'" *Air & Space Forces Magazine* July 27, 2021. https://www.airandspaceforces.com/dickinson-space-command-cyber-command-inseparable/.

Mather, Matthew. 2013. "How Space and Cyberspace are Merging to Become the Primary Battlefield of the 21st Century." *Space Quarterly Magazine*, March 15, 2013. https://matthewmather.com/how-space-and-cyberspace-are-merging-to-become-the-primary-battlefield-of-the-21st-century/.

Morgan, Daniel. *Commercial Space: Federal Regulation, Oversight, and Utilization*. Washington, DC: Congressional Research Service: November 29, 2018. https://crsreports.congress.gov/product/pdf/R/R45416.

National Security Agency/Central Security Service. "Signals Intelligence (SIGINT) Overview." https://www.nsa.gov/Signals-Intelligence/Overview/.

Office of the Director of National Intelligence. "What Is Intelligence?" https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

Redwire Press Release, "Redwire Acquires Made in Space, the Leader in On-Orbit Space Manufacturing Technologies, June 23, 2020. https://redwirespace.com/newsroom/redwire-acquires-made-in-space-the-leader-in-on-orbit-space-manufacturing-technologies/.

Redwire. "Redwire's Trailblazing OSAM-2 Mission Passes Critical NASA Milestone." April 6, 2022. https://redwirespace.com/newsroom/redwires-trailblazing-osam-2-mission-passes-critical-nasa-milestone/.

Schneier, Bruce. “Computer Network Exploitation vs. Computer Network Attack.” *Schneier on Security*, 2014. https://www.schneier.com/blog/archives/2014/03/computer_networ.html.

Shepardson, David. “Internet Sector Contributes $2.1 Trillion to U.S. Economy: Industry Group.” Reuters, September 26, 2019. https://www.reuters.com/article/idUSKBN1WB2QB/.

Starks, Tim, and David DiMolfetta. “Inside the White House Blueprint for Filling U.S. Cyber Jobs.” *The Washington Post*, August 1, 2023. https://www.washingtonpost.com/politics/2023/08/01/inside-white-house-blueprint-filling-us-cyber-jobs/.

Starling, Clementine G., Mark J. Massa, Christopher P. Mulder, and Julia T. Siegel. *The Future of Security in Space: A Thirty-Year U.S. Strategy*. Atlantic Council, April 2021. https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/the-future-of-security-in-space/.

Sweetman, Bill, and Kimberly Ebner. *Jane’s Space Systems and Industry: 2007–2008*. Alexandria: Jane’s Information Group, 2007.

Turk, Robert W. *Preparing a Cyber Security Workforce for the 21st Century*. Carlisle: U.S. Army War College, 2013. https://apps.dtic.mil/sti/pdfs/ADA590251.pdf.

Ugarte, Michael. *Challenges and Way Ahead for Cybersecurity Workforce in Today’s Federal Government*. Washington, DC: Defense Information Systems Agency, 2022. https://www.disa.mil/en/NewsandEvents/2022/Cybersecurity-Workforce.

U.S. Government Accounting Office. “High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas.” March 2, 2021. https://www.gao.gov/products/gao-21-119sp#:~:text=GAO%27s%20High-Risk%20Series%20identifies%20government%20operations%20with%20vulnerabilities,transformation%20to%20address%20economy%2C%20efficiency%2C%20or%20effectiveness%20challenges.

U.S. Naval Academy. “Cyber Operations: The Discipline and the Major. https://www.usna.edu/Academics/Majors-and-Courses/Majors/Cyber-Operations.php

U.S. Space Command. “SecAF Redesignates Space Operations Command West as U.S. Space Forces – Space.” December 12, 2023. accessed at https://www.spacecom.mil/Newsroom/News/Article-Display/Article/3614643/secaf-redesignates-space-operations-command-west-as-us-space-forces-space/.

U.S. Space Force. “The Guardian Ideal.” September 17, 2021. https://media.defense.gov/2021/Sep/21/2002858512/-1/-1/1/GUARDIAN%20IDEAL%20-%20FINAL.PDF.

Van Creveld, Martin. *Command in War*. Cambridge: Harvard University Press, 1987.

Warner, Michael. “Intelligence in Cyber–and Cyber in Intelligence.” In *Understanding Cyber Conflict: 14 Analogies*, edited by George Perkovich and Ariel E. Levine, 17–

30. Washington D.C.: Georgetown University Press, 2017. https://carnegieendowment.org/2017/10/16/introduction-to-understanding-cyber-conflict-14-analogies-pub-73392.

Weinzierl, Matthew, and Mehak Sarang. "The Commercial Space Age Is Here." *Harvard Business Review*, February 12, 2021. https://hbr.org/2021/02/the-commercial-space-age-is-here.

White House. "Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity," August 25, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

Williams, Lauren C. "Space Force Is Setting Up Inside Combatant Commands." *Defense One*, November 22, 2022. https://www.defenseone.com/policy/2022/11/space-force-setting-inside-combatant-commands/380095/.

Zakrzewski, Cat, Joseph Marks, and Jay Greene. "Biden Tells Top CEOs at White House Summit to Step Up on Cybersecurity." *The Washington Post*, August 25, 2021. https://www.washingtonpost.com/technology/2021/08/25/white-house-cybersecurity-summit-apple-amazon/

Appendix B.Abbreviations

ADCON	Administrative Control
AFRICOM	U.S. African Command
AI	Artificial Intelligence
ARPA	Advanced Research Projects Agency
CCMD	Combatant Command
CES	Cyber Excepted Service
CFSCC	Combine Force Space Component Command
CMF	Cyber Mission Force
CO-IPE	Cyber Operations – Integrated Planning Element
CSA	Combat Support Agency
CSIS	Center for Strategic and International Studies
CYBERCOM	U.S. Cyber Command
DARPA	Defense Advanced Research Projects Agency
DCWF	Defense Cyber Workforce Framework
DoD	Department of Defense
EUCOM	U.S. European Command
GAO	Government Accountability Office
GEOINT	Geospatial Intelligence
HUMINT	Human Intelligence
IMINT	Imagery Intelligence
INDOPACOM	U.S. Indo-Pacific Command
IoT	Internet of Things
ISS	International Space Station
IT	Information Technology
JADC2	Joint All Domain Command and Control
JFHQ	Joint Force Headquarters
JFHQ-C	Joint Force Headquarters – Cyber
JFHQ-DoDIN	Joint Force Headquarters – Department of Defense Information Network
JTF-SD	Joint Task Force – Space Defense
MASINT	Measurement and Signature Intelligence

NASA	National Aeronautics and Space Administration
NGA	National Geospatial-Intelligence Agency
NIST	National Institute for Standards and Technology
NRO	National Reconnaissance Office
NSA	National Security Agency
NSF	National Science Foundation
NSG	National System for Geospatial Intelligence.
OSINT	Open-Source Intelligence
SIGINT	Signals Intelligence
SPACECOM	U.S. Space Command
UHF	Ultra-High Frequency
U.S.	United States
VHF	Very High Frequency

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-04-24	Key Deliverable	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace and Space Similarities, Differences, and Related National Security Issues	HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Thomas H. Barth	C5237
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	3001828

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release: distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Thomas H. Barth

14. ABSTRACT

The similarities and differences between cyberspace and space present several national security issues for the U.S. Three of these issues concern (a) defining the national security relationship between the government and the commercial sector in each domain; (b) the recruiting, professional development and retention of a technically capable workforce; and (c) achieving unity of effort within each and between both, which includes determining the appropriate - relationships between U.S. Cyber Command (CYBERCOM) and the National Security Agency (NSA); U.S. Space Command (SPACECOM) and the National Reconnaissance Office (NRO); and between CYBERCOM AND SPACECOM and the geographic and functional combatant commands.

15. SUBJECT TERMS

Cyberspace, space, acquisition, operations, manpower and personnel

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	33	19b. TELEPHONE NUMBER (Include Area Code)