Air Land Sea Application Center
Joint Base Langley-Eustis, Virginia
https://www.alsa.mil

# DOD Cyberspace: Establishing a Shared Understanding and How to Protect It

By Maj Eric Pederson (USAF), MAJ Don Palermo (USA), MAJ Stephen Fancey (USA), Mr. Tim Blevins (LCDR Ret.)
Air Land Sea Application Center

*We have no room for complacency and history makes it clear that America has no preordained right to victory on the battlefield.—Secretary James N. Mattis.*[1]

As the joint force shifts its focus towards trans-regional, all-domain, multi-functional (TAM) strategic competition, nowhere are these concepts more relevant than in cyberspace. The cyberspace domain itself cuts across all physical domains (land, maritime, air, and space) and historic adversary cyberspace activity has generally been below the level of armed conflict. From a defensive cyberspace perspective, the threat to the Department of Defense (DOD) has never been greater. Cyberspace defensive joint force doctrine is still being developed, defensive cyberspace DOD authorities are not well known, and the U.S. and its allies do not have cyberspace supremacy (i.e. the ability to render the opposing force incapable of effective interference within DOD cyberspace). The full consequences of potential adversary cyberspace operations (CO) in the DOD are still being fully understood. Yet, there is a lack of shared understanding about cyberspace across the DOD and the joint force and even less understanding of how the DOD should protect its cyberspace. Despite a desire to understand cyberspace and to protect ourselves, a dearth of clear, concise guidance for the joint force has led to a lack of emphasis on cyberspace and cyberspace security in planning and operations. This article establishes a clear, shared understanding of DOD cyberspace, provides guidance to the DOD to protect its cyberspace, and illustrates current and future efforts to improve DOD's cybersecurity.

**Changing Nature, Character of War**

The 2018 National Defense Strategy (NDS) and 2018 Joint Concept for Integrated Campaigning present the idea of global integration: arranging military actions in time, space, and purpose to address security challenges. Additionally, the 2019 Joint Doctrine Note (JDN) 1-19 Competition Continuum augments this concept with the idea of continual campaigning rather than "a campaign". Continual campaigning is when the joint force is continually competing and adapting in response to strategic conditions and policy objectives through different levels of cooperation, competition below armed conflict, and armed conflict. This is different from a traditional campaign designed around the idea that the world is either at peace or at war. Doctrinally the joint force is being pushed to plan operations from a global perspective, instead of focusing only on a

specific geographic area. These concepts describe the approach required for the cyberspace domain. Actions in cyberspace, particularly defensive actions within DOD cyberspace, should not be viewed as a traditional force-on-force competition. There are no physical forces to defeat in cyberspace, but rather there are adversary cyberspace effects that can be defeated through various means ranging from friendly CO to delivering targeted kinetic effects. Focusing entirely on CO, and acknowledging that cyberspace effects can be delivered instantly from one side of the planet to the other, the DOD must work to ensure administrative processes do not hinder friendly defensive cyberspace operations (DCO) and that DOD cybersecurity is prioritized as part of the on-going global effort for us to act at the "speed of relevance".

**Too Little, Too Late?**

> *The Russians and Chinese are playing a long game to threaten the international, rules-based order…and they are doing this with actions below the threshold of armed conflict. They use information operations, troop movements, proxy fighters, propaganda, diplomacy, economic pressures, and threats to coerce countries.—Jim Garamone*[2]

Arguably, the DOD's established processes and bureaucracy are not suited to the fast-paced world of cyberspace. The first US Air force chief software officer, Nicolas Chaillan, who spent three years on a Pentagon-wide effort to boost cyber security, resigned late in 2021, arguing, "we do not have a competing fighting chance against China in 15 to 20 years".[3] The Chinese are heading for global dominance because of their advances in artificial intelligence, machine learning, and cyber capabilities, and that these emerging technologies were far more critical to America's future than hardware such as big-budget fifth-generation fighter jets such as the F-35.

Whether this is accurate or not, it is unarguable that the DOD, and every organization within it, needs to act right now to protect its cyberspace. Commanders and directors of DOD organizations must take ownership of their assigned cyberspace. If their DOD cyberspace is not adequately protected, the adversary will exploit it and may even achieve physical effects such as shutting down critical infrastructure or weapon systems, while ensuring any digital footprint is not attributable. Accurate reporting of the cybersecurity status of DOD cyberspace is critical. Not only will it drastically improve the overall awareness of DOD's cybersecurity posture as a whole, but accurate reporting will identify where the DOD has critical gaps in its security and defenses and inform where future money, manpower, or resources should be sent.

**Cyberspace Missions and Actions**

There are three types of cyberspace missions: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense information network (DODIN) operations (DODIN Ops); and, four types of cyberspace actions: attack, exploitation, security, and defense (*Figure 1*).

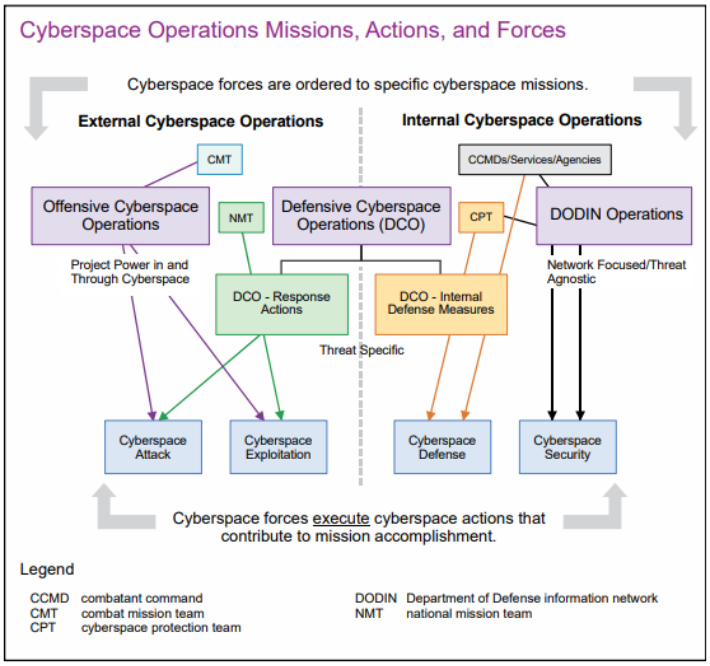


Figure1: Cyberspace Operations Missions, Actions, and Forces

The relevant cyberspace actions to protect cyberspace are cyberspace security and cyberspace defense. The difference between cyberspace security and defense actions is that security actions are taken to *prevent* malicious cyber activity in order to ensure system availability, integrity, authentication, confidentiality, and nonrepudiation, whereas defense actions are taken to *defeat* the adversary in order to restore the system to a secure configuration.

Within a given cyberspace mission, different types of cyberspace actions can occur. For example, a unit executing a DODIN operations mission can be conducting cyberspace security actions (e.g. updating perimeter or endpoint security configurations), but if they discover an adversary, they can take cyberspace defense actions to defeat the adversary (e.g. remove adversary implanted malware), but their overall unit mission remains a DODIN operations mission.

**DOD Cyberspace and Authorities**

The DOD cyberspace backbone is called the DODIN.[4] The DODIN is the biggest network in the world. It is composed of 44 different DOD components made up of service, agency, and combatant command constructed networks *(Figure 2)*. The DODIN is DOD's classified and unclassified enterprise. Within each DOD component constructed network are thousands of subordinate networks, information technology equipment, tools and applications, weapon system technologies and data spanning across bases, posts, camps, and station levels.

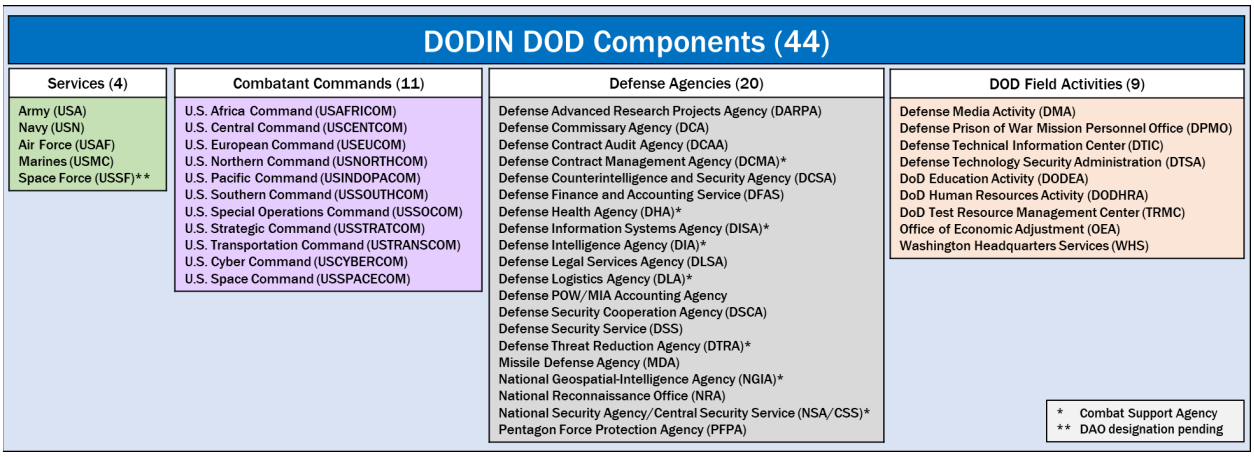


Figure 2: The 44 DOD Components of the DODIN.

The Defense Information Systems Network (DISN), managed by Defense Information Systems Agency (DISA), serves as the DODIN backbone *(Figure 3)*. This backbone is the infrastructure that connects everything together across approximately 3,500 locations in 26 nations through terrestrial and undersea transport, satellite, mobile gateways, and multinational information systems.

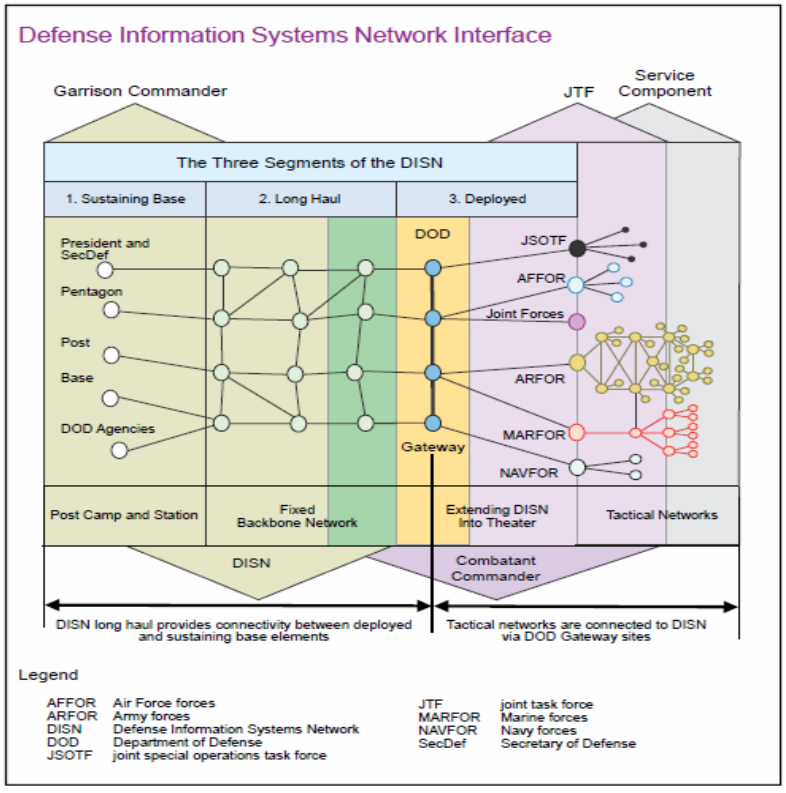


Figure 3: DISN Interface

Each of the 44 DOD components owns a portion of the DODIN area of operation (DAO) and is responsible for protecting it. USCYBERCOM has directive authority for

cyberspace operations (DACO), established by CJCS EXORD, that enables DOD-wide synchronized protection of the DODIN. DACO has been delegated to JFHQ-DODIN and provides authority to direct cyberspace operations related to global DODIN operations and DCO-IDM within each DOD component's DAO. *(Figure 4)*.

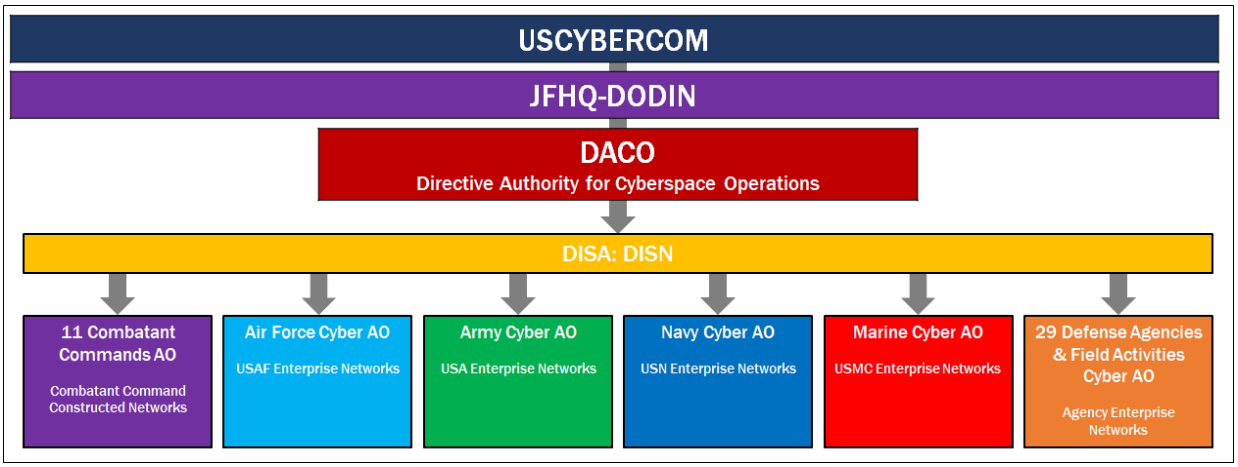


Figure 4: DACO Authority

**Joint Cyberspace Organizations, Structures, Roles, and Responsibilities**

There is a hierarchy based on roles and responsibilities *(Figure 5)* when it comes to protecting cyberspace as part of the joint force. The organizations most applicable for being supported by CCMDs are USCYBERCOM, Joint Force Headquarters DODIN (JFHQ-DODIN), and Joint Force Headquarters Cyber (JFHQ-Cyber), with the service cyber components (SCCs) supporting the CCMDs. Organizations within CCMDs that can provide cybersecurity expertise and support are cyber operations-integrated planning elements (COIPEs), joint cyber centers (JCCs), cybersecurity service provider (CSSPs), and network operation centers (NOCs). We will give a quick summary of these organizations as this will help you understand when we address the complications and solutions for CCMDs.

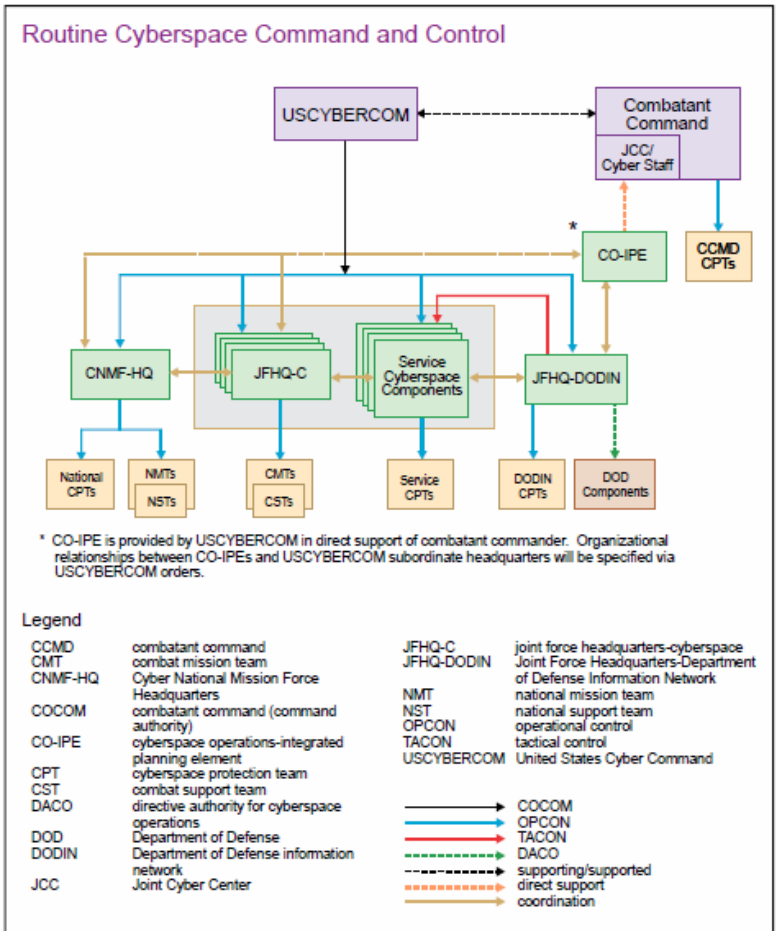


Figure 5: DOD Cyberspace C2

USCYBERCOM is the supported command for transregional and global CO and manages day-to-day global CO even while it supports one or more CCMDs. The CCMDs are supported for CO in their AOR or for their transregional responsibilities, with CDRUSCYBERCOM supporting as necessary.

JFHQ-DODIN which is a component command of USCYBERCOM is the organization that is responsible for securing, operating, and defending the DOD complex infrastructure of roughly 15,000 networks with 3 million users. JFHQ-DODIN leads unified actions across all DOD for DODIN operations and defeats, denies, and disrupts cyberattacks against the DODIN.

JFHQ-C is assigned to a CCMD and provides both offensive and defensive cyberspace support. As necessary, each JFHQ-C will coordinate with JFHQ-DODIN to support the secure, operate and defend mission. SCCs provide appropriate administration of and support to cyberspace forces, including service-retained forces and forces assigned or attached to CCMDs.

Each CCMD has DAO-level CSSPs and NOCs. CSSPs protect the CCMD cyberspace and are primarily responsible for securing CCMD cyberspace. NOCs configure, operate, extend, maintain, and sustain the CCMD cyberspace and are primarily responsible for

operating CCMD cyberspace. Under current doctrine, securing cyberspace falls within the DODIN operations mission. Additionally, the joint force function of protecting cyberspace consists largely of cyberspace security actions, and when required, cyberspace defense actions.

**Why Life is Complicated for Combatant Commands**

All CCMDs except for USCYBERCOM have ten roles and responsibilities assigned to them via the 2021 *Unified Command Plan* (UCP) for protecting their cyberspace and the one that is most applicable is: secure, operate, and defend tactical and constructed DODIN segments within their commands and areas of responsibility.

Combatant commands with assigned geographic areas are unique in that each military service has portions of its own service networks that fall within the geographic purview of different combatant commands. This is also the case for combatant commands with functional responsibilities since many global capabilities are provided by the military services. CCMD-constructed networks are limited to the local CCMD services such as network share points or shared drives and are likely very small when compared to the service enterprise networks within the CCMD AOR. The CCMD-constructed networks are the only portion of the DODIN that the CCMD is directly responsible for. Yet, the services have their own network operating independently within the CCMD AOR and, therefore, the CCMD is unaware of all activities that could have an impact on their current and future operations.

**The Way Forward**

There are three straightforward, but fundamental, steps that CCMDs and DOD organizations need to take to protect their cyberspace:

**1) Take Ownership**: Determine what portion of DODIN cyberspace the CCMD is responsible for. A CCMD should go to its COIPE, JCC, CSSP, and NOC to obtain its operationally assigned cyberspace from JFHQ-DODIN. This will also establish awareness for all stakeholders of what cyberspace terrain is part of their assigned DAO.

**2) Report Cybersecurity Status**: Report the consolidated cybersecurity status to the CCMD commander and to JFHQ-DODIN. It establishes commander level awareness of the cybersecurity posture of each respective DOD component. This vastly improves component awareness of potential operational impacts from a cyberspace perspective. By also sharing this information with JFHQ-DODIN, this establishes awareness of the DOD's cybersecurity posture, DOD-wide. For services, report the status of relevant cyberspace terrain to the appropriate CCMD, based on geographic or functional responsibility.

**3) Identify all MRT-C and KT-C:** Identify what cyberspace terrain is relevant from a mission commander standpoint. Often, there are pieces of cyberspace terrain that are critical for mission or network function that are not obvious (e.g. a lone server in a random unprotected closet that all operational data passes through). The process of identifying this terrain requires both *technical understanding* and *knowledge of the commander's missions*. This then translates into a critical task for CSSPs. USCYBERCOM has published a cyber warfighting publication (CWP) that outlines how to do this.[5] In a nutshell, it simply involves following a mission's data path across

networks. Additionally, once all MRT-C and KT-C are identified, the information should be stored and shared using an existing secure database. This step is critical to inform cyberspace defensive planning and operations. As this process matures, cyberspace planners will know what MRT-C and KT-C must be protected throughout all phases of the various scenarios in joint force plans and operations.

**Current and Future Cybersecurity Efforts**

There are other efforts to modernize cybersecurity within the DOD (and the federal government as a whole) that are relevant to CCMDs and all DOD organizations. These include:

- Standardizing network sensors (e.g. perimeter and endpoints sensors) and their deployment within each DAO and across the DODIN
- Standardizing data aggregation at local (local network log/data collection), regional (base/camp/post/station collection), and enterprise (big data) levels, as well as what data is fed to higher echelons
- Formalizing data access for network defenders, cyberspace operators, and cyberspace commanders to improve cyberspace awareness and establish a common operating picture (COP). This will result in increased cyberspace command and control and decrease DOD security incident response times.[6]
- Adopting cybersecurity best practices such as implementing zero trust architecture,[7] accelerating movement to secure cloud services, enhancing software supply chain security, and streamlining cybersecurity to drive data analytics for identifying and managing cybersecurity risks.[8]
- Adopting standardized cybersecurity reporting practices such as the DOD cybersecurity analysis and review (DODCAR) methodology and cyber threat framework that provide effective, and readily digestible, cybersecurity risk information.[9] This nests with industry governance, risk, and compliance (GRC) best practices that improve current DOD compliance operations and ensure operationally focused assessments augment compliance, rather than replace them, ensuring additional risk is not created.
- Updating contract language with DOD partners in a timely manner to address current cybersecurity issues such as enabling cybersecurity-related information sharing across the DOD and limiting/governing cleared defense contractors (CDC) remote access into the DODIN.

**Protecting DOD Cyberspace, Now and Beyond**

The stage is set to successfully consolidate multiple cybersecurity efforts. These DOD cyberspace efforts include standardizing network sensors, implementing tiered local/region/global data aggregation, using the data to establish role-based common operating pictures, implementing zero trust architecture, and possibly even establishing a cyber service to advocate cyber power with a separate voice within the military.

The end state of all these initiatives is that DOD cybersecurity efforts have moved away from localized efforts and expertise, and transitioned to established cybersecurity

standards across the DOD. Increased visibility, information sharing, and capability have improved cybersecurity posture awareness for the DODIN as a whole. All DOD organizations share cyberspace information and intelligence securely, and cyberspace is fully incorporated into joint force planning and operations.

**Case for a Cyber Service**

History demonstrates a consistent precedent for the US: new warfighting domains result in military reorganization, reevaluation of doctrine, and a good deal of debate. A new service emerges to ensure that warfighting in the domain receives the necessary focus for education, training, recruiting, doctrine development, force generation, and as a leading voice in the ongoing discussion of that domain at the strategic, operational, and tactical levels. Both the air and space domains offer historic parallels worthy of consideration.

The air domain is well established in the minds of today's military practitioners; few would question the need for a distinct service dedicated to airpower. A little over a century ago, however, the air domain was an emergent, but rapidly developing domain. Establishing a separate service in the air domain was not instantaneous or without controversy: creation of the US Air Force was gradational, spanned two world wars, and was marked by resistance from within the Army and Navy. Now the Air Force has its own identity, service culture, technology, tactics, and strategy. It offers a separate voice within the military for the use of airpower on the strategic stage. Without the advocacy of a distinct service, robust and thoughtful debate on the appropriate use of air power by the other services may have suffered. Although the existence of a separate Air Force is no longer controversial, its creation was often characterized by resistance from within the military amidst advocacy from civilian political pressures.

Unlike the air domain, the space domain is expanding as a realm of competition nearly simultaneously with another domain: cyberspace. Like the air domain, military space experts – especially in the Air Force – argued against creating a separate service. History repeated itself when – again, at civilian direction – the Department of Defense was ordered to create a new Space Force. In just a few years, Air Force Space Command's General John Raymond went from being an opponent of the Space Force to its first Chief of Space Operations![10]

Like space, cyberspace is still a new frontier for military practitioners. Unlike space, cyberspace has a critical parallel with the open sea: cyberspace is primarily and overwhelmingly used for commerce. Cyberspace is a "wild west" with a low barrier to entry where both nations and criminals can exploit it for their own ends. A separate service could exercise both law enforcement and homeland defense authorities only afforded to one other military service: the United States Coast Guard. Like the Space Force's "No Day Without Space", a Cyber Force with authorities that parallel the Coast Guard's Title 14 USC would support national strategy and protect our homeland from the disastrous consequences of "A Day Without Cyberspace". A dual identity (military and law enforcement) and alignment under the Department of Homeland Security allow a separate cyber service to protect our nation's global infrastructure from state actors who will be indistinguishable from criminal threats.

**Conclusion**

The DOD cyberspace is only going to continue expanding at an exponential rate utilizing the latest and greatest technology to meet the ever-growing demands for more information from commanders while conducting warfare. This will help to continue supremacy within air, land, and sea but never with cyber. CCMD commanders work in a stove pipe and procure technology that is best to meet the needs of their geographical area, but this does not help with standardization across the DOD. Since the US has experienced successful and harmful cyber-attacks on the critical infrastructures, protecting the DOD cyberspace from adversaries is more important than ever. But do we have an adequate level of protection and shared understanding of our cyberspace and does our current structure work for the foreseeable future. We have only created a band-aid solution and pieced together the infrastructure with the cheapest possible solutions. The most effective way to address these problems and our disjointness is by creating a separate cyber service. Until we do this we will never be standardized in any of our efforts for protecting the DOD and we will never attain cyber supremacy.

Endnotes

[1] "Secretary Mattis Remarks on U.S. National Defense Strategy," January 19, 2018, C-SPAN, video, 49:06, https://www.c-span.org/video/?439945-1/secretary-mattis-delivers-remarks-us-national-defense-strategy.
[2] Garamone, Jim, "Global Integration Seeks to Buy Leaders Decision Time, Increase 'Speed of Relevance'," *DOD News*, July 2, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1565240/global-integration-seeks-to-buy-leaders-decision-time-increase-speed-of-relevan/.
[3] Manson, Katrina, "US has already lost AI fight to China, says ex-Pentagon software chief," *Financial Times*, October 10, 2021, https://www.ft.com/content/f939db9a-40af-4bd1-b67d-10492535f8e0.
[4] Defense Information System Agency Joint Force Headquarters Department of Defense Information Network, *Capabilities: Connecting and Protecting the Warfighting in Cyberspace, 2019*, https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/DISA-Capabilities.ashx#:~:text=DISA%20Voice%20Services%20provide%20reliable, voice%20and%20voice%20messaging%20services.&text=Virtual%20Private%20Network%20(VPN)%20provides,through%20various%20means%20and%20modes.
[5] U.S. Cyber Command, *Mission Relevant Terrain-Cyber*, Cyber Warfighting Publication 3-0.1, 20 August 2021
[6] Russel, W. William, *Defense Acquisitions: Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance*, GAO-21-68, (Washington, DC: Government Accountability Office, 2020)
[7] Pomerleau, Mark, "The Pentagon is moving away from the Joint Regional Security Stacks", *C4ISRNET*, November 1 2021, https://www.c4isrnet.com/it-networks/2021/11/01/the-pentagon-is-moving-away-from-the-joint-regional-security-stacks/.
[8] Joseph R. Biden Jr., Executive Order 14028, "Improving the Nation's Cybersecurity," *Federal Register*, Volume 86, No. 93, May 17 2021
[9] Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan (Risk Report)*, (Washington, DC: Office of Management and Budget, 2018), https://www.hsdl.org/?view&did=811093.

*Disclaimer. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other agency of the Federal Government.*

[10] Raymond, John W., “We Need to Focus on Space, We Don’t Need a Space Corp,” *Defense One*, July 20, 2017, https://www.defenseone.com/ideas/2017/07/we-need-focus-space-we-dont-need-space-corps/139360/.; Raymond, John W., “How We’re Building a 21st Century Space Force,” The Atlantic, December 20, 2020, https://www.theatlantic.com/ideas/archive/2020/12/building-21st-century-space-force/617434/.