International Security at the NUCLEAR NEXUS

PROJECT ON NUCLEAR ISSUES

OCTOBER 15, 2020

Cross-domain Competition

HOW ORGANIZATIONAL STOVEPIPES CREATE RISKS FOR SHARED MISSIONS

By **Morgan Dwyer**

Within the national security community, institutional interactions are shaped by how responsibility, authority, competency, and budgets are allocated across separate organizations with shared missions. Organizational lines have to be drawn somewhere; indeed, boundaries enable organizations to develop specialized knowledge and tackle problems which might otherwise be intractable by breaking them down into more manageable chunks.[1] But

Banner Image: *Cyber operators executing the persistent engagement strategy.* Source: U.S. Fleet Cyber Command/U.S. Tenth Fleet, https://www.fcc.navy.mil

organizational stovepipes can also create risks to shared missions, especially when separate institutions must develop interoperable technology.

Today, traditional nuclear missions increasingly intersect with emerging technical domains such as space and cyber. And while much has been written about the technical intersection among nuclear, space, and cyber, comparatively little attention has been paid to the nexus among nuclear, space, and cyber institutions. This brief explores that institutional nexus within the U.S. military, where new organizational stovepipes may create risks to shared missions. To mitigate these risks, policymakers should proactively counter bureaucratic competition among the separate organizations which share the mission of defending the nuclear command, control, and communications (NC3) system.

Cross-domain Competition

The Department of Defense (DOD) manages technology development and operations for the space and cyber domains in separate, stovepiped institutions. When these institutions interact with one another or with DOD's established nuclear bureaucracy, the resulting dynamics can affect what technology is developed and how that technology is operated. Frequently, however, bureaucratic dynamics are an afterthought in technology policy, where new organizations are often created as a means to prioritize specific technologies or technical domains.[2]

For instance, President Donald Trump stated that elevating Cyber Command to a unified combatant command would ensure "that critical cyberspace operations are adequately funded."[3] Similarly, former Acting Defense Secretary Patrick Shanahan supported the Space Force's creation by stating that "To move forward effectively, space needs an advocate. That advocate will be the Space Force."[4] Although separate institutions do have dedicated budgets and advocates, they also have boundaries, and in the case of space and cyber, policymakers created institutional seams that cut across shared missions. To effectively execute those shared missions, DOD's separate organizations will need to bridge institutional divides and cooperate.

Bureaucratic dynamics are frequently an afterthought in technology policy, where new organizations are often created as a means to prioritize specific technologies or technical domains.

[1] Graham Allison, "Conceptual Models and the Cuban Missile Crisis," American Political Science Review 63, no. 3 (1969), 700, doi:10.2307/1954423.

[2] Morgan Dwyer, "An Alternative to the Defense Department's New, Technology-Focused Organizations," CSIS, Commentary, January 22, 2020, https://www.csis.org/analysis/alternative-defense-departments-new-technology-focused-organizations.

[3] "Statement by President Donald J. Trump on the Elevation of Cyber Command," The White House, August 18, 2017, https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

[4] "Keynote Address by Acting Secretary of Defense Patrick Shanahan," (speech, Strategic National Security Space: FY2020 Budget and Policy Forum, CSIS, March 20, 2019), https://www.csis.org/analysis/strategic-national-security-space-fy-2020-budget-and-policy-forum.

Research, however, suggests that the interactions among separate government institutions are frequently competitive rather than cooperative.[5] For example, researchers at RAND described DOD's budget process as a continuous competition among the separate military services for resources, personnel, missions, and institutional influence.[6] MIT's Owen Cote observed that inter-service relationships oscillate between cooperation and competition, and that the nature of inter-service interactions can profoundly impact doctrine, budgets, roles, and missions.[7] My dissertation observed that when separate government agencies are forced to surrender their autonomy and execute missions jointly, they resist cooperation and compete for power and influence instead.[8]

When policymakers create new, separate institutions—such as Cyber Command or the Space Force—they empower those organizations to operate semi-autonomously. But by drawing organizational lines across shared missions, policymakers also create a requirement for interorganizational cooperation. Unfortunately, cooperation across organizational stovepipes is hard—because it disturbs each institution's ability to operate semi-autonomously.[9] Therefore, in the absence of a strong governance structure to compel cooperation, organizations may shirk their joint responsibilities and compete for resources and authority instead.[10] This competition, in turn, can create risks to the shared missions that cross organizational seams.

Nuclear, Space, and Cyber Stovepipes

Despite these risks, DOD's nuclear bureaucracy has successfully existed in an organizational stovepipe—one which separates it from conventional, non-nuclear technology—for decades. DOD develops nuclear-armed capabilities—submarines, inter-continental ballistic missiles (ICBMs), and bomber aircraft—in dedicated programs within the military services. Strategic Command—a separate, functional combatant command—operates these capabilities globally, with the mission of deterring strategic attack.

Importantly, an organizational stovepipe separates Strategic Command from conventional operations in the geographic combatant commands. Operational decoupling is possible because U.S. nuclear weapons exist to deter war, rather than to fight it, and can only be employed under presidential direction. As such, there is only one

---

[5] For example, see: Anthony Downs, Inside Bureaucracy (Boston: Little, Brown, and Company, 1972); James Q. Wilson, Bureaucracy: What Government Agencies Do and Why They Do It (New York: Basic Books, 1989); H. Seidman, Politics, Position, and Power, 5th ed. (New York: Oxford University Press, 1998); F.E. Rouke, Bureaucracy, Politics, and Public Policy (New York: Little, Brown, and Company, 1969); H.M. Sapolsky, The Polaris System Development: Bureaucratic and Programmatic Success in Government (Cambridge, MA: Harvard University Press, 1972); L.P. Temple, "Organizing Space: the Political-bureaucratic Dynamics through 1961," PhD dissertation, George Washington University, 1999, http://search. proquest.com/docview/304500442?accountid=12492; and Owen Cote, "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles," PhD dissertation, Massachusetts Institute of Technology, 1982, http://edocs.nps.edu/AR/topic/theses/1996/Feb/96Feb_Cote_PhD.pdf.

[6] S. Rebecca Zimmerman et al., Movement and Maneuver: Culture and the Competition for Influence Among the Military Services (Santa Monica, CA: RAND Corporation, 2019), xiii, https://www.rand.org/pubs/research_reports/RR2270.html.

[7] Cote, "The Politics of Innovative Military Doctrine."

[8] Morgan Dwyer, "The Cost of Jointness: Insights from Environmental Monitoring Systems in Low-Earth Orbit," PhD Dissertation, Massachusetts Institute of Technology, 2014, http://systemarchitect.mit.edu/docs/dwyer14e.pdf.

[9] For example, see: Downs, Inside Bureaucracy; Wilson, Bureaucracy: What Government Agencies Do and Why They Do It; Cote, "The Politics of Innovative Military Doctrine"; Seidman, Politics, Position, and Power; Rouke, Bureaucracy, Politics, and Public Policy; and Morgan Dwyer, Zoe Szajnfarber, Bruce Cameron, and Edward Crawley, "A model for understanding and managing cost growth on joint programs," Acta Astronautica 152 (November 2018): 59-70, doi:10.1016/j.actaastro.2018.07.004.

[10] Dwyer, Szajnfarber, Cameron, and Crawley, "A model for understanding and managing cost growth on joint programs"; and Dwyer, "The Cost of Jointness."

instance—when deterrence has failed and the president has authorized the use of nuclear weapons—in which DOD must integrate strategic and conventional operations across organizational stovepipes.

With strategic and conventional operations decoupled, there is little reason for their supporting technology to interface or interoperate. Therefore, for decades, DOD's nuclear bureaucracy has enjoyed relative autonomy. The emerging importance of the space and cyber domains, however, will change that.

Unlike nuclear capabilities, which can be decoupled from conventional operations, space and cyber technologies generate, share, and process information that all systems—strategic and conventional—require to operate. Space capabilities, for example, generate intelligence, weather, position, navigation, and timing data. Communications satellites relay that information to Earth-bound operators and create communications links between systems that operate in the air, land, and sea.

An Advanced Extrenely High Frequency (AEHF) satellite, built by the U.S. Air Force to provide survivable communications in the event of a nuclear attack.
Source: Los Angeles Air Force Base

Computers, of course, enable operators to process data, and computer networks allow operators to share data. Today, DOD's weapons systems (e.g., its aircraft and submarines) have onboard processing capabilities that are both increasingly powerful and increasingly networked with other systems. The F-35 aircraft, for example, has been described as a "flying computer."[11]

Although space and cyber activities are not easily decoupled, especially across a range of potential conventional or nuclear operations, policymakers recently created stovepipes to manage the space and cyber domains separately. For instance, in 2017, President Trump elevated Cyber Command to a unified combatant command with the purpose of preparing "cyber operations forces to carry out assigned missions."[12] Cyber Command's forces, in turn, are manned, trained, and equipped by DOD's military services. Within each military service, there is a distinct cyber component that is responsible for developing cyber technology and training cyber operators. For example, the Air Force manages its cyber capabilities within the 16th Air Force of the Air Combat Command.[13]

In 2019, President Trump recreated Space Command by elevating it to unified combatant command status.[14] As a geographic combatant command, Space Command will manage all operations that occur 100 km above the Earth's

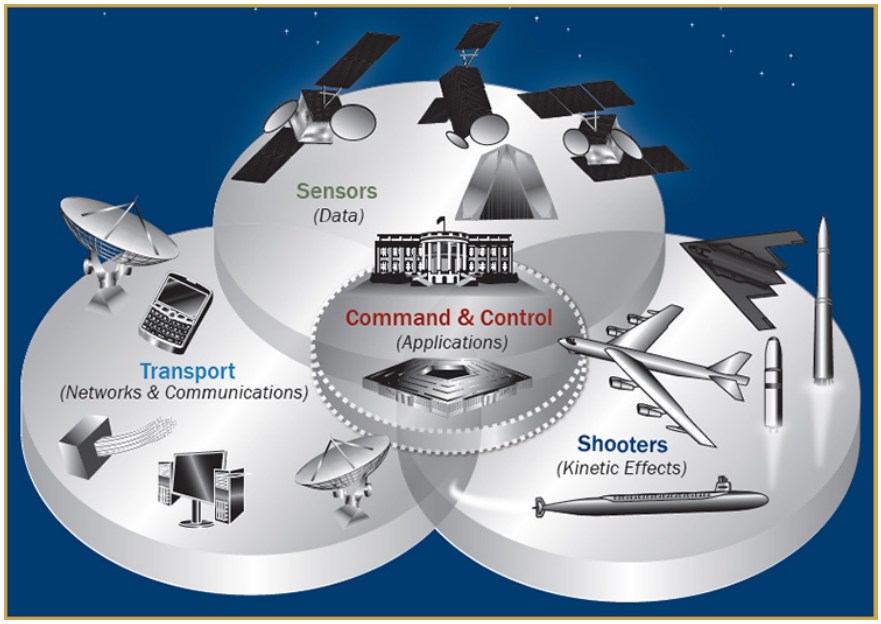
[11] Kris Osborn, "The F-35 is More 'Flying Computer' than Fighter Jet, And That's Changing How America Fights," National Interest, February 19, 2020, https://nationalinterest.org/blog/buzz/f-35-more-flying-computer-fighter-jet-and-thats-changing-how-america-fights-125156.
[12] Title 10 U.S. Code, §167b – Unified combatant command for cyber operations, https://www.law.cornell.edu/uscode/text/10/167b.
[13] "Sixteenth Air Force (Air Forces Cyber)," United States Air Force, August 27, 2020, https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/.
[14] "Department of Defense Establishes U.S. Space Command," Department of Defense (DOD), August 29, 2019, https://www.defense.gov/Newsroom/Releases/Release/Article/1948288/department-of-defense-establishes-us-space-command/.

surface.[15] DOD's Space Force—a new and separate military service within the Department of the Air Force—will man, train, and equip Space Command's operators.

Shared Nuclear, Space, and Cyber Missions

Separated by organizational stovepipes, DOD's nuclear, space, and cyber institutions are able to operate semi-autonomously. As such, these organizations can establish internal budget priorities and make decisions independently. This behavior, of course, can create problems when separate stovepiped organizations must cooperate in support of shared missions.

Importantly, DOD's nuclear, space, and cyber institutions share the mission of defending the NC3 architecture. NC3 enables strategic deterrence by sensing potential attacks and connecting sensors with decisionmakers. It also facilitates communication among decisionmakers, advisers, and DOD's nuclear forces.



The NC3 architecture, linking shooters, sensors, and transport networks.
Source: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters

Nuclear, space, and cyber capabilities all integrate and interoperate within the NC3 architecture.[16] For example, satellites contribute sensors and communications links. Sensors and communications links all require cyber capabilities—in the form of secure networks and software—to operate. Unfortunately, both space and cyber capabilities are vulnerable to attacks that could prevent the NC3 system from fulfilling its strategic deterrence mission.[17]

Because the NC3 architecture is vulnerable in both the space and cyber domains, DOD's space and cyber institutions share the mission of defending it. Therefore, to develop and operate the "right" mix of defensive capabilities, DOD's nuclear, space, and cyber institutions should cooperate. For example, rather than making decisions based upon which defensive capabilities might be optimal within a single domain, ideally, DOD's separate institutions would make decisions collaboratively, by working together to assess decision options across domains and to evaluate how those options impact the end-to-end NC3 architecture.

---

[15] Kaitlyn Johnson, "Bad Idea: Designating Space Command as a Geographic Command," CSIS, December 13, 2019, https://defense360.csis.org/bad-idea-designating-space-command-as-a-geographic-command/.

[16] For a more detailed description of NC3, see: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *Nuclear Matters Handbook* (Washington, DC: DOD, 2020), Chapter 2, https://www.acq.osd.mil/ncbdp/nm/nmhb/chapters/chapter2.htm.

[17] For a summary of space and cyber threats facing NC3, see: David Deptula, William LaPlante, and Robert Haddick, *Modernizing U.S. Nuclear Command, Control, and Communications* (Arlington, VA: Mitchell Institute for Aerospace Studies, 2019), 25-27, http://docs.wixstatic.com/ugd/a2dd91_ed45cfd71de2457eba3bcce4d0657196.pdf.

Without a mandate to cooperate, however, DOD's nuclear, space, and cyber institutions will operate semi-autonomously. This means that they will be empowered to make decisions which might be locally optimal, but which might be globally—and with respect to the cross-domain NC3 architecture—suboptimal. Furthermore, rather than making decisions collaboratively, DOD's separate stovepipes are more likely to compete with one another for resources and authority. This competition, in turn, can create additional risks to the shared mission of defending NC3.

Competition for Resources

All institutions compete to win some fraction of DOD's fixed resources.[18] And to compete effectively, institutions should offer distinct capabilities—those which cannot be provided by other organizations—to the joint force.[19] Distinct capabilities, almost by definition, rarely support shared missions. Therefore, in the battle for fixed resources, shared missions will likely lack both a dedicated budget and a champion that is willing to advocate on their behalf.

Space and cyber defense are, by definition, shared missions. Cyber defense involves monitoring and hardening the networks that power other organizations' systems and that enable their missions. Space defense involves designing space architectures that are resilient and capable of supporting air, land, and sea operations even when satellites are attacked.

For example, to increase the resiliency of its space architectures, DOD could replace constellations that are composed of only a few large satellites with constellations that contain many smaller satellites.[20] In theory, by disaggregating capabilities onto smaller and more numerous satellites, DOD could complicate its adversaries' decision to target individual systems.[21] DOD could also develop the capability to rapidly reconstitute any satellite—especially those which support NC3—and which might become disabled or destroyed by attacks.[22]

Although DOD's space and cyber stovepipes are responsible for defense in their respective domains, in the competition for fixed resources, they may be more likely to advocate for their distinct —rather than their shared—missions.[23] And within the space and cyber domains, distinct capabilities tend to be offensive rather than defensive. It is perhaps for this reason that the Union of Concerned Scientists warned that by establishing separate, space-

---

[18] For example: see Harvey M. Sapolsky, "The Interservice Competition Solution," *Breakthroughs* 5, no. 1 (Spring 1996): 1-4, http://web.mit.edu/SSP/publications/breakthroughs/1996-Spring.pdf; Susanna V. Blume and Molly Parrish, "Interservice rivalries: A force for good," Defense News, January 21, 2020, https://www.defensenews.com/opinion/commentary/2020/01/21/interservice-rivalries-a-force-for-good/; and Zimmerman et al., *Movement and Maneuver*.

[19] Downs, *Inside Bureaucracy*; Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It*; Clark and Wilson, "Incentive systems"; Selzncik, *Leadership in Administration*; and Seidman, *Politics, Position, and Power*; and H.M. Sapolsky, *The Polaris System Development: Bureaucratic and Programmatic Success in Government.*

[20] Jon Harper, "BREAKING: Space Command Hints at New Capabilities to Counter China, Russia," National Defense Magazine, August 21, 2020, https://www.nationaldefensemagazine.org/articles/2020/8/21/us-space-command-hints-at-new-capabilities-to-counter-china-russia.

[21] "Resiliency and Disaggregated Space Architectures," United States Air Force, 3, http://www.acqnotes.com/Attachments/AFSPC%20Resiliency%20and%20Disaggregated%20Space%20Architectures.pdf.

[22] "Building a Resilient Space Architecture," Aerospace Corporation, December 15, 2018, https://aerospace.org/Annual-Report-2018/building-resilient-space-architecture/

[23] Downs, Inside Bureaucracy; Wilson, Bureaucracy: What Government Agencies Do and Why They Do It; Clark and Wilson, "Incentive systems"; Selzncik, Leadership in Administration; and Seidman, Politics, Position, and Power; and H.M. Sapolsky, The Polaris System Development: Bureaucratic and Programmatic Success in Government.

focused institutions, DOD would "create bureaucratic incentives to hype the space weapons threat and build new weapons."[24]

DOD's space and cyber communities are secretive; however, publicly available information suggests that the Union of Concerned Scientists' worries—that separate institutions will prioritize distinct, offensive capabilities—may not be unfounded. For example, although the 2018 *Nuclear Posture Review* stressed the importance of space and cyber defense, neither DOD's space strategy nor its cyber strategy mentioned NC3.[25] Instead, both strategies struck a more aggressive, offensive tone when describing how DOD plans to operate in the space and cyber domains.

For example, the 2018 *Department of Defense Cyber Strategy* introduced a new operational concept whereby DOD "will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept or halt cyber threats" before those threats reach DOD networks.[26] Defense Secretary Mark Esper further explained this offensive approach by stating: "We need to do more than just play goal line defense . . . the department's 2018 cyber strategy articulates a proactive and assertive approach to defend forward of our own virtual boundaries."[27] Cyber Command's General Nakasone explained that this "more effective, proactive posture called 'persistent engagement'" would broaden the command's focus from planning for future wars to also include competing with adversaries today.[28]

Faced with budget constraints, however, Cyber Command's focus on persistent engagement may require trade-offs, such as allocating less funding towards preparing for future kinetic conflicts.[29] Already, several reports have noted that DOD has insufficiently prioritized efforts to identify and mitigate cyber threats to its weapon systems, including threats to NC3.[30] In 2018, the Government Accountability Office (GAO) stated that DOD did not know the full extent of the cyber vulnerabilities in its weapon systems.[31] In 2020, the Cyberspace Solarium Commission echoed the GAO's concerns and recommended that Congress require DOD to annually assess the NC3 system for potential cyber vulnerabilities.[32] More broadly, American University's Joshua Rovner noted that Cyber Command's focus on "persistent engagement" may create risks to the command's support to traditional DOD missions; in particular, Rovner warned that "if great-power hostilities continue to rise, Cyber Command may have to pump the brakes on

---

[24] "Creating a Space Force Would Trigger a Space Arms Race and Threaten US Satellite Security, Science, Group Says: Statement by Laura Grego, Union of Concerned Scientists," Union of Concerned Scientists, December 10, 2019, https://www.ucsusa.org/about/news/space-force-would-trigger-arms-race.

[25] DOD, Summary: Department of Defense Cyber Strategy (Washington, DC: 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF;
DOD, Defense Space Strategy Summary (Washington, DC: June 2020), https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF; and DOD, 2018 Nuclear Posture Review (Washington, DC: 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

[26] DOD, Summary: Department of Defense Cyber Strategy.

[27] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy," DOD, September 20, 2019, https://www.defense.gov/Explore/News/Article/Article/1966758/esper-describes-dods-increased-cyber-offensive-strategy/.

[28] Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs,* August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[29] Ibid., and for additional discussion see: Joshua Rovner, "More Aggressive and Less Ambitious: Cyber Command's Evolving Approach," War on the Rocks, September 14, 2020, https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/.

[30] For example, see: Government Accountability Office (GAO), *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities* (Washington, DC: October 2018), https://www.gao.gov/assets/700/694913.pdf.

[31] Ibid., 21.

[32] U.S. Cyberspace Solarium Commission, *The Cyberspace Solarium Commission Report* (Washington, DC: March 2020), 119, https://www.solarium.gov/report.

persistent engagement and devote more attention to the missions for which it was originally designed."[33] Those missions, of course, include preparing for future wars—presumably by defending DOD's weapon systems, including NC3.

Compared to cyber, DOD's space institutions are relatively new; as such, they are still working to define their priorities. It remains an open question whether DOD's space institutions will prioritize traditional approaches to defense—such as developing resilient space architectures—or will adopt a more offensive posture.[34] As in the cyber domain, however, offensive capabilities may help distinguish space organizations from the rest of the joint force, which has traditionally considered space to be an enabler rather than a distinct warfighting domain.

It is perhaps for this reason that the 2020 *Defense Space Strategy* stresses that space is, in fact, a "warfighting domain" and pledges to "advance space power."[35] Furthermore, in just its first year, the Space Force has already introduced new, warfighting-focused training and has unveiled its first offensive space weapon.[36] It remains to be seen, however, whether DOD's space organizations will mature according to a similar trajectory as Cyber Command, which intentionally evolved away from its focus on "reactive defense" and instead assumed a "proactive" and offensive posture.[37]

Going forward, if DOD's new space and cyber stovepipes truly develop institutional preferences for offense, how might the shared mission of NC3 defense be affected? The answer lies in the competition for fixed resources, wherein separate stovepiped organizations can set priorities and allocate budgets autonomously. This means that DOD's space and cyber stovepipes will likely invest in higher-priority offensive capabilities first and will allocate smaller budget shares to lower-priority defensive capabilities and shared missions.

Competition for resources may result in a systemic underinvestment in capabilities that support shared missions such as NC3 defense.

Importantly, although creating new space and cyber organizations may have garnered both domains a larger fraction of DOD's budget, the overall defense budget remains largely fixed. Faced with constant or declining budgets in the future, DOD organizations will be forced to prioritize capabilities that contribute to their distinct missions and to compete with each other for resources. Competition for resources, in turn, may result in a systemic underinvestment in capabilities that support shared missions such as NC3 defense.

Competition for Authority

Passive defense, of course, is not the only way to defend NC3. Offensive space and cyber weapons—the very capabilities that may be prioritized by DOD's space and cyber organizations—can deter attacks as well. But

---

[33] Rovner, "More Aggressive and Less Ambitious."

[34] For example, see the discussion here: Theresa Hitches, "Space Chief Targets Red Tape to Speed New Tech," Breaking Defense, September 15, 2020, https://breakingdefense.com/2020/09/space-chief-targets-red-tape-to-speed-new-tech/; and Theresa Hitchens, "U.S., Allies Agree on Threats in Space but Struggle with Messaging, Breaking Defense, September 11, 2020, https://breakingdefense.com/2020/09/us-allies-agree-on-threats-in-space-but-struggle-with-messaging/.

[35] DOD, *Defense Space Strategy*, 1.

[36] Kyle Mizokamni, "U.S. Space Force's First Offensive Weapon Is a Satellite Jammer," *Popular Mechanics*, March 17, 2020, https://www.popularmechanics.com/military/a31703515/space-force-first-weapon/.

[37] Nakasone and Sulmeyer, "How to Compete in Cyberspace."

deterrence requires organizations to communicate credible threats, and organizational stovepipes—as well as the competition for authority across them—may create barriers to both communications and credibility.

Unfortunately, DOD's space and cyber institutions have intelligence community roots and secretive cultures that tend to overclassify capabilities and operations rather than communicate them.[38] For example, DOD's 10-page space strategy is vague about which capabilities and actions DOD will take to "ensure space superiority."[39] DOD's 7-page cyber strategy is similarly opaque, stating that DOD will operate "persistently" in cyberspace but failing to specify to what end operators will persist and under what circumstances operations might change.[40] By comparison, DOD's 75-page *Nuclear Posture Review* clearly articulates how the United States perceives adversary actions, how it might respond to aggression, and which capabilities it might use.[41]

Clearly, organizational cultures conflict here, with the nuclear community prioritizing the deterrent value of communication and the space and cyber communities viewing communication as an inherent security risk. Unfortunately, even in the context of shared missions, DOD's separate institutions can make classification decisions independently. For DOD's space and cyber institutions, which value their autonomy, there is little incentive to declassify any capabilities, even those which might deter attacks to NC3.[42] DOD's nuclear institutions, in turn, lack the authority to compel the space and cyber institutions to act.

When separate authority stovepipes intersect but values conflict, cooperation is challenging, even in the context of shared missions.[43] In these circumstances, outside intervention is required to determine which organization is actually in charge. For example, in the traditional nuclear community—which not only includes the military services and Strategic Command but also the Department of Energy (DOE)—policymakers established the Nuclear Weapons Council.[44] The authorities and responsibilities for council participants are specified by law, policy, and memorandums of agreement between DOD and DOE.[45] Without a similar governance structure or single authority capable of compelling interorganizational change, it seems unlikely that DOD's separate space or cyber institutions will poactively declassify any capabilities, even those which might help deter attacks on NC3.[46]

Separate authority stovepipes may also create barriers to employing offensive weapons. For example, if an adversary attacks the NC3 architecture in the cyber domain, and DOD does not wish to retaliate using a nuclear weapon,[47] which combatant command is in charge of the response, Strategic or Cyber Command? DOD's cyber

---

[38] For example, see: Jamie Morin, "Moving toward a need-to-collaborate culture for national security space," C4ISRNet, May 6, 2020, https://www.c4isrnet.com/opinion/2020/05/06/moving-toward-a-need-to-collaborate-culture-for-national-security-space/; Todd Harrison, "Congressional Testimony: Space Warfighting Readiness," CSIS, March 14, 2018, https://aerospace.csis.org/congressional-testimony-space-warfighting-readiness/; and Dennis Blair and Robert Work, "Stovepipes in space: How the US can overcome bureaucracy to improve capabilities," Defense News, July 13, 2020, https://www.defensenews.com/opinion/commentary/2020/07/13/stovepipes-in-space-how-the-us-can-overcome-bureaucracy-to-improve-capabilities/.

[39] DOD, *Defense Space Strategy*, 1.

[40] DOD, *Summary: Department of Defense Cyber Strategy*.

[41] DOD, *2018 Nuclear Posture Review*

[42] Blair and Work, "Stovepipes in space."

[43] Dwyer, Szajnfarber, Cameron, and Crawley, "A model for understanding and managing cost growth on joint programs"; and Dwyer, "The Cost of Jointness."

[44] For more on the history of the Nuclear Weapons Council, see: "Chapter 6 Nuclear Weapons Council" in DOD, *Nuclear Matters Handbook 2020* (Washington, DC: 2020), https://www.acq.osd.mil/ncbdp/nm/nmhb/docs/NMHB2020_Ch6_NWC.pdf.

[45] Ibid., 89-90.

[46] For example, these authors argue that an outside commission of experts is required to recommend strategy for declassifying space capabilities: Blair and Work, "Stovepipes in space."

[47] Note that the 2018 Nuclear Posture Review (p. 21) states that DOD may consider employing a nuclear weapon in response to "significant non-nuclear strategic attacks" such as attacks on "U.S. or allied nuclear forces, their command and control, and warning and attack assessment capabilities." If DOD were to respond to non-nuclear (i.e., space or cyber) attacks to NC3 using nuclear weapons, it is assumed Strategic

doctrine specifies that Cyber Command's role vis-à-vis the other combatant commands varies as a function of whether operations are local or global.[48] Furthermore, it states that the support/supporting relationships between commands are established on a by-mission basis.[49] These public statements, of course, leave the unanswered the question of which combatant command—Cyber or Strategic Command—is in charge of non-nuclear responses to cyberattacks on NC3.

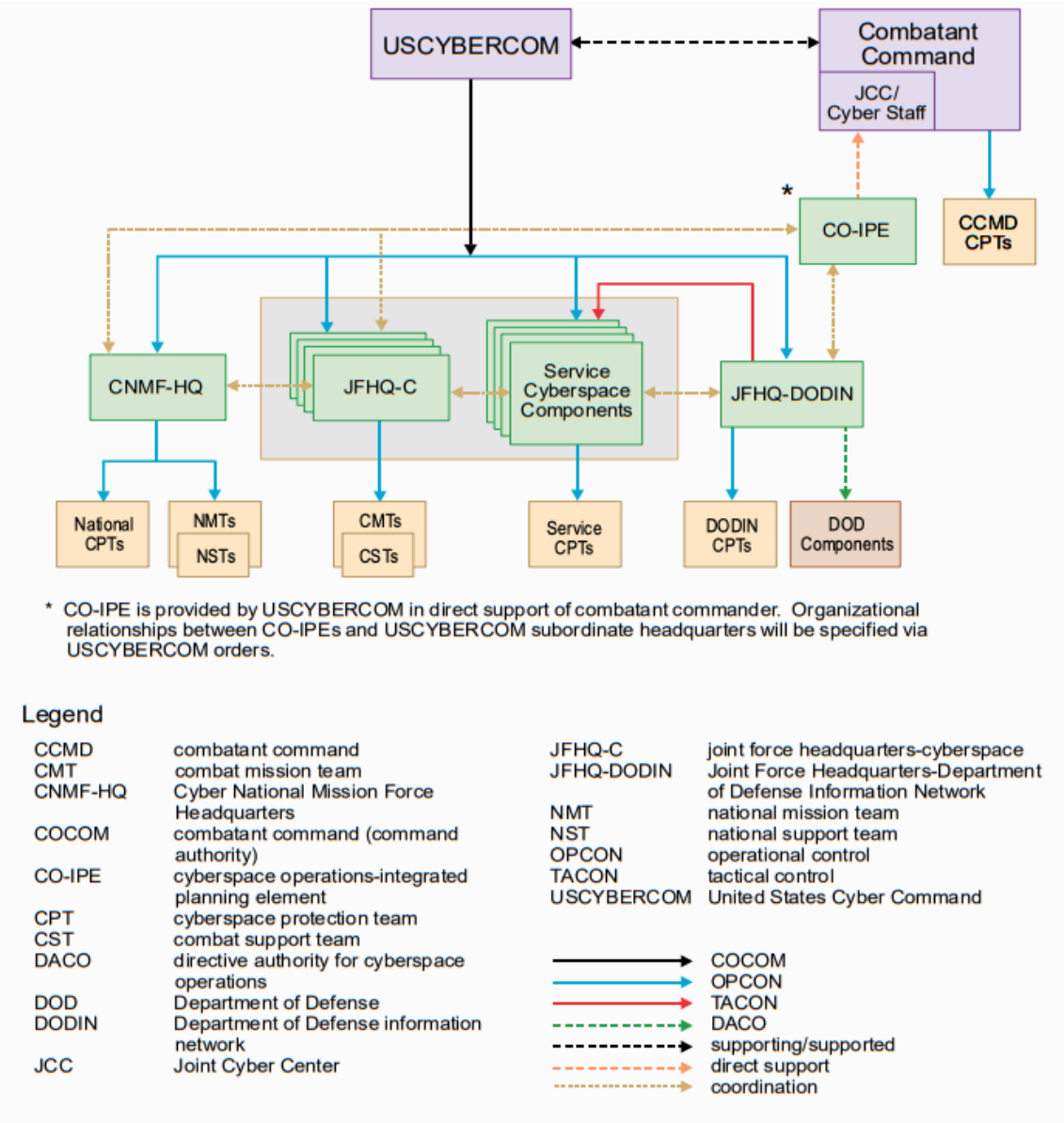


Figure 1: *Cyberspace command and control structure, which shows a bi-directional support/supporting relationship between Cyber Command and the other combatant commands.*
Source: Joint Staff, Joint Publication 3-12 Cyberspace Operations

Command would have decision authority. The discussion that follows assumes that DOD does not respond to such attacks using nuclear weapons.

[48] Joint Staff, *Joint Publication 3-12 Cyberspace Operations* (Washington, DC: DOD, June 2018), IV-11, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[49] Ibid.

Furthermore, what happens if attacks cross domains? How then should DOD integrate three separate authority stovepipes—in the Strategic, Space, and Cyber Commands—to effectively and efficiently respond? If DOD is to credibly threaten any response to space or cyber-based attacks on NC3, these basic unity of command questions deserve answers.[50] To date, however, Vice Chairman John Hyten admits that DOD has not sufficiently addressed these questions, noting: "We just decided that we'd call each other combatant commands, and not put an adjective on the front."[51] By failing to specify a critically important adjective—whether a command is supporting or supported—DOD leaves unanswered the question of who is in charge when attacks cross domains.

Because independent commands value their autonomy, they have little incentive to proactively integrate their operations across domains. Instead, outside intervention will again be required to determine who is in charge of non-nuclear responses to space or cyber-attacks on NC3. DOD's forthcoming update to its Unified Command Plan does offer policymakers an opportunity to intervene and to clearly specify who is in charge of the response when attacks cross domains.[52] Absent such intervention and clearly specified support/supporting command relationships, organizational stovepipes may create barriers to cross-domain operations, especially when operations support the shared mission of defending the NC3 system.

Mitigating Risks

As described above, competition across organizational stovepipes can create risks to the shared mission of defending NC3. Competition for resources may result in a systemic underinvestment in the space and cyber capabilities that are required to passively defend NC3. And competition for authority may create barriers to communicating and operating the offensive space and cyber weapons which might deter attacks. Thankfully, by proactively countering bureaucratic competition, policymakers can mitigate both of these risks.

Since nuclear, space, and cyber capabilities are separated within DOD, risk mitigation has to start at the top of the department, where policymakers in the Office of the Secretary of Defense and the Joint Staff have authority over all relevant institutions. Within these offices, policymakers should:

- Fully leverage the benefit of having separate space and cyber institutions that prioritize offensive capabilities by ensuring that the entire department develops cross-domain concepts of operation.
- Clearly specify supported/supporting roles for all combatant commands involved in cross-domain operations.
- Leverage new or existing governance structures to ensure that investments made across institutions appropriately balance offense and defense. To achieve this aim, policymakers might include relevant space and cyber capabilities under the purview of existing governance structures such as the Nuclear Weapons Council. They might also choose to manage a limited set of passive space and cyber defense capabilities within nuclear institutions, which might place a higher priority on investments in NC3 defense.

---

[50] For example, this discusses how DOD will need to rethink relationships between combatant commands: Theresa Hitchens, "All-Domain Ops Require Rethinking Combatant Commands: Goldfein," Breaking Defense, March 10, 2020, https://breakingdefense.com/2020/03/all-domain-ops-require-rethinking-combatant-commands/.

[51] Ibid.

[52] For discussion of DOD's intent to release a new Unified Command Plan, see: Theresa Hitchens, "Exclusive: Milley to OK New Unified Command Plan; Defines SPACECOM's Roles," Breaking Defense, August 26, 2020, https://breakingdefense.com/2020/08/exclusive-milley-to-sign-new-unified-command-plan-defines-spacecoms-roles/.

- Finally, work to actively counter space and cyber institutions' secretive cultures, at least as they relate to NC3 defense. Managing a limited set of space and cyber capabilities within the comparatively open nuclear community, as suggested above, may help. But policymakers could also direct space and cyber institutions to declassify intent and capabilities that are relevant to NC3 defense.

Overall, although the nexus among nuclear, space, and cyber institutions may create risks for the shared mission of NC3 defense, these risks can be mitigated. By anticipating and proactively countering competition across stovepipes, policymakers can ensure that separate institutions develop interoperable technology that supports shared missions. Furthermore, they can leverage the benefit of having separate institutions in the first place. In the case of space and cyber, DOD's new organizations appear poised to cultivate the type of specialized expertise and technology that will critically enable cross-domain operations in the future—including operations that support NC3 defense.

AUTHOR

Morgan Dwyer *is a fellow in the International Security Program and deputy director for policy analysis in the Defense-Industrial Initiatives Group at the Center for Strategic and International Studies (CSIS).*

ABOUT CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic in-sights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).