The Heritage Foundation

BACKGROUNDER

No. 3403 | MAY 2, 2019

Should Cyber Command and the NSA Have Separate Leadership? How to Decide

James Di Pane

Abstract

The elevation of U.S. Cyber Command in 2018 to a unified combatant command has reignited the debate over whether to terminate the dual-hat arrangement, wherein the Director of the National Security Agency (NSA) simultaneously serves as the Commander of U.S. Cyber Command. This debate over whether to end this arrangement has gone on for years now, with many believing that a split is both inevitable and necessary to improve the cybersecurity of the United States, while others maintain that splitting the organizations could either have a detrimental effect on cybersecurity or would result in multiple inefficiencies. This Backgrounder *lays out the arguments for, and against, a split, with recommendations for a decision that is based solely on enhancing U.S. cyber operations.*

The elevation of U.S. Cyber Command in 2018 to a unified combatant command has reignited the debate over whether to terminate the dual-hat arrangement, wherein the Director of the National Security Agency (NSA) simultaneously serves as the Commander of U.S. Cyber Command.

This debate over whether to end this arrangement has gone on for years now, with many believing that a split is both inevitable and necessary to improve the cybersecurity of the United States, while others maintain that splitting the organizations could either have a detrimental effect on cybersecurity or would result in multiple inefficiencies. Ultimately, this decision should be based solely on whether a split would actually enhance the cyber capabilities of the United States.

Key Points

- Historically, the U.S. Cyber Command has relied heavily on the National Security Agency (NSA) for mission support, with the NSA providing much of the manpower, equipment, and know-how for the command's military operations.
- But Cyber Command has developed since then, both operationally and in manpower, and is now capable of a greater degree of autonomy in its ability to conduct operations.
- The debate over whether to end this arrangement—with both organizations operating under a single boss—has gone on for years now, with many believing that a split is both inevitable and necessary to improve the cybersecurity of the United States, while others maintain that splitting the organizations could either have a detrimental effect on cybersecurity or would result in multiple inefficiencies.
- Ultimately, this decision should be based solely on whether a split would actually enhance the cyber capabilities of the United States.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3403**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Evolution of U.S. Cyber Command and Its Relationship with the NSA

Since its inception, Cyber Command has had an incredibly close relationship with the National Security Agency. The organizations are both based at Fort Meade, Maryland, and Cyber Command historically depended on the NSA's workforce, computer networks, and intelligence to operate. The two also share singular leadership. Under what has been coined the dual-hat arrangement, a four-star flag officer heads both the NSA and Cyber Command.[1]

The evolution of Cyber Command, from a Joint Task Force in 1998, to a sub-unified command in 2009, and finally to a unified combatant command in 2018 coincides directly with the Department of Defense's (DOD's) increased focus on cyber defense over those two decades. By the mid-1990s, DOD officials had become increasingly concerned that adversaries were capable of disrupting U.S. military networks remotely, potentially affecting real-world operations.

In response, the officials created the Joint Task Force-Computer Network Defense (JTF-CND), the DOD's first organization with authority to "direct operations on individual military service and DoD networks."[2] In 2000, all DOD cyber operations were combined under the Space Command (SPACECOM), and when Space Command was dissolved two years later, cyber operations were absorbed into the Strategic Command (STRATCOM). In 2009, on orders of Secretary of Defense Robert Gates, Cyber Command was established as a sub-unified command, and continued to operate under the supervision of STRATCOM.[3] This elevation was in response to what the DOD considered a clear, persistent, and serious threat from foreign adversaries using cyberspace to attack the United States.[4]

Since 1952, the NSA's primary mission has been to clandestinely collect intelligence on actors outside the United States. It also supports U.S. military operations with equipment and intelligence. However, the military operations themselves, offensive and defensive alike, fall under the purview of Cyber Command:

> USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[5]

Besides having separate mission sets, the NSA and Cyber Command also operate under differing legal authorities. The NSA's authority comes from its creation in Title 50 of the U.S. Code, which outlines proper procedures for conducting intelligence collection, espionage, and cyber surveillance operations against foreign powers.[6] Cyber Command's authority, specifically the authority for offensive cyber operations, comes from Title 10 of the U.S. Code, which outlines the role of U.S. Armed Forces.[7] Title 50 does not give the NSA the authority to destroy or change an adversary's information, to harm someone else's network, or to seize control of an adversary's computers in order to create any physical destruction. These actions fall under Title 10.[8] However, the NSA can support a Title 10 military operation by providing intelligence, technology, and personnel. There is also no law precluding CYBERCOM from conducting a Title 50 operation.[9]

[1] U.S Cyber Command, "U.S. Cyber Command History," https://www.cybercom.mil/About/History/ (accessed March 27, 2019).

[2] Ibid.

[3] Ibid.

[4] Jim Garamone and Lisa Ferdinando, "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command," *DoD News*, April 18, 2017, https://dod.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/ (accessed March 27, 2019).

[5] U.S. Department of Defense, U.S. Cyber Command, *U.S. Cyber Command Fact Sheet*, May 2010, https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-038.pdf (accessed March 27, 2019).

[6] Andru E. Wall, "Demystifying the Title 10–Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal*, Vol. 3, No. 1 (September 2011), https://www.soc.mil/528th/PDFs/Title10Title50.pdf (accessed March 27, 2019).

[7] Ibid.

[8] Emma Khose and Chris Mirasola, "To Split or Not to Split: The Future of CYBERCOM's Relationship with NSA," *Lawfare*, April 12, 2017, https://www.lawfareblog.com/split-or-not-split-future-cybercoms-relationship-nsa (accessed March 27, 2019).

[9] Ibid.

Despite having distinct responsibilities and legal authorities, Cyber Command and the NSA maintain a close, cooperative relationship. Earlier this year, General Paul Nakasone—the current Commander of Cyber Command and Director of the NSA—told Congress, "The National Security Agency is our most important partner; the strength of this relationship will remain critical to the defense of the nation. The Agency's world-class expertise, technical capabilities, and accesses are crucial to USCYBERCOM's success."[10]

Background and Recent Activity

The Edward Snowden controversy in 2011 brought the issue of splitting the NSA and Cyber Command to the forefront of public debate. Snowden, a former NSA sub-contractor, brought a number of accusations about abuses of civil liberties into the public square when he leaked documents he copied from the NSA. The controversy raised questions of cyber operations and civil liberties, and led many to question if it was wise to have both cyber collectors and warriors under the same leadership.

Prompted by this leak, the Obama Administration explored a number of options to prevent such a situation in the future. A separation of the people collecting cyber intelligence and those conducting cyberwarfare was seen as a way to prevent abuse, and the Administration pushed for splitting Cyber Command and the NSA.[11] The Obama Administration also considered appointing a civilian as head of the NSA in an attempt to enhance civilian control over cyber and signals intelligence activities.[12] At the time, the push for the split was largely a political one rather than a matter of military necessity or as a means of enhancing cyber security.

This push for the split led Members of Congress to act. Fearing that a premature split of the NSA and Cyber Command would endanger the cybersecurity of the country by adversely affecting operations, the late Senator John McCain (R–AZ) and others vowed to block an attempt by President Obama's Defense Secretary Ash Carter and Director of National Intelligence James Clapper to separate the two organizations. Senator McCain argued that "given the very serious challenges we face in cyberspace," it would be unwise to split the two "prematurely."[13]

Congress included criteria for a possible end to the dual-hat relationship in the 2017 National Defense Authorization Act (NDAA), seeking to set conditions and criteria that must be met before a split occurs. These conditions were predominantly aimed at ensuring that cyber operations and effectiveness are not affected and included requirements for the Administration to verify that the necessary infrastructure for the NSA and Cyber Command has been deployed, along with command and control systems for planning and deconflicting cyber operations. Another condition is that capabilities are up to the tasks required and that personnel are adequately trained for the missions they are being asked to execute. Lastly, the cyber mission force has to have achieved full operational capability.

General Nakasone, his predecessor Admiral Michael Rogers, and Senator McCain all voiced concerns that prematurely severing the dual-hat relationship could slow down cyber operations and jeopardize the country's defenses.[14]

Cyber Command Maturity and Development

On May 4, 2018, the Trump Administration, in a desire to "streamline command and control and demonstrate increased resolve against cyberspace threats," elevated U.S. Cyber Command to a full unified combatant command. It joined the ranks of

[10] General Paul M. Nakasone, testimony before the Subcommittee on Intelligence, Emerging Threats, and Capabilities, Committee on Armed Services, U.S. House of Representatives, March 13, 2019, pp. 9 and 10, https://armedservices.house.gov/_cache/files/e/d/ed0549b9-c479-4ae0-943d-66cf8fd933c1/AEDF855100875FF9DBB6F5E7472F6E36.nakasone-cybercom-hasc-posture-statement-final-3-13-19.pdf (accessed March 27, 2019).

[11] Ken Dilanian and Courtney Kube, "Top Officials Want to Split Cyber Command from NSA," NBC News, September 9, 2016, https://www.nbcnews.com/news/us-news/top-officials-want-split-cyber-command-nsa-n645581 (accessed March 27, 2019).

[12] Warren Strobel, "White House Says Plans No Split of NSA, Cyber Command," Reuters, December 13, 2013, https://www.reuters.com/article/us-usa-security-nsa-idUSBRE9BC0MM20131213 (accessed March 27, 2019).

[13] Joe Gould, "McCain Vows to Block Potential NSA-Cyber Command Split," *Defense News*, September 13, 2016, https://www.defensenews.com/2016/09/13/mccain-vows-to-block-potential-nsa-cyber-command-split/ (accessed March 27, 2019).

[14] Ibid., and Joseph Marks, "CYBERCOM Chief Nominee Plans Recommendation on NSA Split Within Three Months," Nextgov, March 1, 2018, https://www.nextgov.com/cybersecurity/2018/03/cybercom-chief-nominee-plans-recommendation-nsa-split-within-three-months/146344/ (accessed March 27, 2019).

Pacific Command, Special Operations Command, and Strategic Command to become the newest and 10th Combatant Command.[15] This elevation is significant because it consolidates the authorities for training and operations under a single commander. It is designed to streamline cyber operations.[16]

Historically, Cyber Command has relied heavily on the NSA for mission support, with the NSA providing much of the manpower, equipment, and know-how for the command's military operations.[17] Both organizations' missions required a similar set of tools and skills, and often both infrastructure and personnel are used for Title 10 and Title 50 operations. Many employees of Cyber Command and the NSA participated in the dual-hat arrangement, conducting intelligence work for the NSA and then "flipping their hat" to perform military operations when needed.[18]

But Cyber Command has developed since then, both operationally and in manpower, and is now capable of a greater degree of autonomy in its ability to conduct operations. On May 17, 2018, Cyber Command reached full operating capacity earlier than anticipated, filling all of its 133 cyber mission forces, the units within Cyber Command responsible for conducting cyber operations.[19] Now the focus has shifted to improving the readiness of the cyber forces, and General Nakasone points to the opening of the Integrated Cyber Center, which enhances command and control of cyber operations, and is in the first dedicated building for Cyber Command.

Cyber Command has also conducted cyber operations against adversaries, gaining valuable experience in the process. Cyber operations worked together with kinetic and other operations to degrade the Islamic State and work to erode its caliphate. Admiral Rogers credits that campaign with providing key experience for operationalizing cyberwarfare tools against extremist organizations as part of a larger strategy.

Another example was the operation against Russia, known as the Russia Small Group, to defend the U.S. midterm elections in 2018. Cyber Command and the NSA worked together along with other combatant commands, the Department of Homeland Security, and the FBI to secure the elections.[20] Both of these operations against different targets demonstrated Cyber Command's successes in supporting broader objectives, as well as its ability to operate.

Arguments for Ending the Dual-Hat Arrangement

There are three key concerns that stem from the dual-hat arrangement.[21] The first is concern about unfair prioritization of requests for support. Whichever organization or mission set is favored by the commander could get special attention to the detriment of the other. If, for example, the Director/Commander favors the NSA and values the collection of signals intelligence over the execution of a cyber operation, Cyber Command could lose out to the NSA, or vice versa.

The second involves the ability of a single commander to manage two large organizations. Skeptics of the dual-hat arrangement wonder if one individual is really able manage the two large organizations, especially as Cyber Command continues to grow. This broad span of control could have a detrimental impact on organization management.

[15] News release, "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/ (accessed March 27, 2019).

[16] Katie Lange, "Cybercom Becomes DoD's 10th Unified Combatant Command," *DoD Live*, May 3, 2018, http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/ (accessed March 27, 2019).

[17] Scott Maucione, "CYBERCOM and NSA Leadership Needs to Evolve and That May Mean a Leadership Split," The Federal News Network, September 19, 2017, https://federalnewsnetwork.com/defense/2017/09/cybercom-and-nsa-leadership-needs-to-evolve-and-that-may-mean-a-leadership-split/ (accessed March 27, 2019).

[18] Mark Pomerleau, "What Would a CYBERCOM-NSA Split Mean?" C4ISRNET, October 10, 2016, https://www.c4isrnet.com/home/2016/10/10/what-would-a-cybercom-nsa-split-mean/ (accessed March 27, 2019).

[19] News release, "Cyber Mission Force Achieves Full Operational Capability," U.S. Department of Defense, May 17, 2018, https://dod.defense.gov/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/ (accessed March 27, 2019).

[20] General Paul M. Nakasone, testimony before the Subcommittee on Intelligence, Emerging Threats, and Capabilities, Committee on Armed Services, U.S. House of Representatives, p. 4.

[21] Robert Chesney, "Separating NSA and CYBERCOM? Be Careful When Reading the GAO Report," *Lawfare*, August 7, 2017, https://www.lawfareblog.com/separating-nsa-and-cybercom-be-careful-when-reading-gao-report (accessed March 27, 2019).

The third concern is the increased potential for exposure of NSA tools and operations. Maintaining the secrecy of the NSA's cyber tools is one of the highest priorities of the organization. Because the NSA shares its hacking tools with Cyber Command, the frequency of use for these tools has increased, leading to a correlating increased chance of release. This does not necessarily stem from the dual-hat relationship, but more from Cyber Command's close relationship with the NSA for support.

Some have also criticized the effect the close relationship has had on Cyber Command's operational development and culture. The NSA tends to be a more risk-averse organization, as the maintenance of access to intelligence sources requires a certain degree of caution. Since Cyber Command developed within the NSA, many of the processes for approving operations are based on a similar risk assessment as the NSA uses, but critics worry that this inhibits the ability of Cyber Command to deter adversaries. Cyberwarfare is an enterprise where aggressive and rapid actions are often necessary to be effective.[22] Ending the dual-hat relationship is one suggestion for allowing Cyber Command to develop its own operating culture that will better suit its mission set.

Arguments for Keeping the Dual-Hat Arrangement

DOD officials say that the benefits of the dual-hat arrangement include a close and collaborative relationship, a faster decision-making process, and more efficient resource allocation.[23] A closer look shows some compelling arguments to leave the two organizations dual-hatted.

A Single Commander Can Play Referee. The dual-hat arrangement leads to faster decision making because one person is ultimately responsible for both missions.[24] If there is a conflict between the two organizations, a single boss can make the call quickly on which course to take. This is especially important when the intelligence collectors and the cyber warriors are using the same access point in an adversary's network. If each organization had its own leader, a request would potentially go all the way to the Secretary of Defense and National Security Council to resolve a conflict, adding time to the decision-making process. Additionally, both organizations may be encouraged to become more protective of their particular mission set, as leaders would seek to maximize the effectiveness of their particular mission set. A single commander has responsibility for both mission sets, and would therefore be more likely to seek balance between the two.

Cyber Intelligence Collection and Warfare Are Different Missions, But Related. Unlike traditional military activities where intelligence and operations are very different, cyberspace is an area where the two functions are very closely related. Both collecting intelligence and conducting cyberwarfare requires accessing the networks of the intended target in the same way. This means that Cyber Command can utilize network access provided by the NSA and vice versa. According to General Hayden, "in the cyber domain the technical and operational aspects of defense, espionage, and cyberattack are frankly indistinguishable—they are all the same thing."[25] The skills required to create these various effects vary, but they are all related. When the two organizations operate together, they can take advantage of network access and work in tandem with one another, using their resources more efficiently. General Nakasone said, "My experience is that the dual-hat arrangement has enabled the operationally close partnership between USCYBERCOM and the NSA, which benefits both in the accomplishment of their respective missions."[26]

Typically in an organizational restructuring when an organization is divided to allow its components to better focus on disparate missions, it reflects a recognition that missions have grown to

[22] Andrew Schoka, "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat," War on the Rocks, April 3, 2019, https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/?utm_source=WOTR+Newsletter&utm_campaign=cbe74f8bfc-EMAIL_CAMPAIGN_10_30_2018_11_23_COPY_01&utm_medium=email&utm_term=0_8375be81e9-cbe74f8bfc-83053989 (accessed April 17, 2019).

[23] Chase Gunter, "Should NSA and CyberCom Split? A Watchdog Weighs In," *Federal Computer Week*, August 2, 2017, https://fcw.com/articles/2017/08/02/dual-hat-nsa-cybercom-gao.aspx (accessed March 27, 2017).

[24] Chesney, "Separating NSA and CYBERCOM? Be Careful When Reading the GAO Report."

[25] General Michael Hayden, "Cutting Cyber Command's Umbilical Cord to the NSA," *The Cipher Brief*, July 17, 2017, https://www.thecipherbrief.com/article/tech/cutting-cyber-commands-umbilical-cord-to-the-nsa (accessed March 27, 2019).

[26] Marks, "CYBERCOM Chief Nominee Plans Recommendation on NSA Split within Three Months."

the point where they need increased specialization and attention. This happens frequently in the commercial sector, where for example, a larger corporation, such as IBM or SAIC, spins off a unit to focus on a particular business sector. It often signifies a desire to increase the attention paid to a particular area.

In the case of the NSA and Cyber Command, however, that way of thinking may be faulty. Although the NSA focuses on intelligence, and Cyber Command focuses on offensive and defensive cyber operations, counterintuitively, it may be that cleaving NSA/Cyber Command via separate commanders, no matter which compensating enhancements are provided, will ultimately result in two less-viable organizations.

NSA and Cyber Command Pull from the Same Talent Pool. The NSA and Cyber Command operate jointly in many instances. Not only do they both hire the same type of employee, but a number of employees work for both organizations simultaneously, changing fluidly depending on the situation. Ending the dual-hat arrangement could result in personnel being forced to choose to work for either Cyber Command or the NSA, leading to personnel issues within both. Cyber Command still relies on NSA personnel for its command staff, even though it now operates independently of Strategic Command.[27]

This would be challenging under most circumstances, but is especially a problem given the challenges that the NSA and Cyber Command have with attracting and retaining top tech talent.[28] Additionally, cyber talent takes years to cultivate, meaning that the recruits filling the ranks would be less capable than their more experienced counterparts. Lieutenant General Stephen Fogarty, Commander of Army Cyber Command, testified before the Senate Armed Services Subcommittees on Cybersecurity and Personnel that the average operator can spend fully half of his or her six-year enlistment in training.[29]

Recent reporting shows that the U.S. government is struggling to attract and retain top cyber talent due to stiff competition from the private sector. The government has difficulty competing with the high salaries and swift onboarding processes large companies can offer. Cyber Command has outlined a series of initiatives to help improve talent recruitment and retention, including keeping close relationships with universities, increased pay scales, and retention bonuses. But the government may not be able to fill the necessary manpower demand it would create by splitting the organizations.[30]

The NSA and Cyber Command also share personnel because of the relative scarcity of cyber talent in the public sector. Despite Cyber Command's Cyber Mission Force teams filling all of its 6,200 billets, recent Senate testimony revealed lawmakers' concern about a "shortage of cyber-capable personnel."[31] As Cyber Command grows more independent of the NSA, Cyber Command will need to ensure its own robust workforce of coders, developers, and operators, as well as support staff and administrators.[32] General Nakasone says that hiring and retaining qualified personnel is the biggest challenge facing Cyber Command.[33] This makes the efficiency of scarce resources essential for the command, and sharing personnel is key to that efficiency.

Recommendations

The Administration and Congress should:

- **Re-evaluate the military necessity of splitting the NSA and Cyber Command, and should not assume that terminating the dual-hat arrangement is inevitable.** Large

[27] Mark Pomerleau, "Here Are the Cyber Staffing Issues Facing the Defense Department," *Fifth Domain*, August 3, 2018, https://www.fifthdomain.com/dod/cybercom/2018/08/03/can-cyber-command-overcome-its-staffing-shortage/ (accessed March 27, 2019).

[28] Ibid.

[29] Statement of Lieutenant General Stephen G. Fogarty, "Joint Hearing to Receive Testimony on the Cyber Operational Readiness of the Department of Defense (Open Session)," testimony before Subcommittee on Cybersecurity, Committee on Armed Services, U.S. Senate, September 26, 2018, p. 29, https://www.armed-services.senate.gov/imo/media/doc/18-60_09-26-18.pdf (accessed March 27, 2019).

[30] "Joint Hearing to Receive Testimony on the Cyber Operational Readiness of the Department of Defense (Open Session)."

[31] Ibid.

[32] Pomerlau, "Here Are the Cyber Staffing Issues Facing the Defense Department."

[33] General Paul M. Nakasone, "An Interview with Paul M. Nakasone," *Joint Force Quarterly*, Vol. 92 (January 2019), p. 9, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf (accessed March 27, 2019).

organizational shifts should not be made for their own sake, and sometimes the change itself can have unintended negative consequences. Given the demands on cyber-capable personnel and the intertwined nature of cyber espionage and warfare, there are plausible arguments for leaving the two organizations under the same leadership and infrastructure. A split would mean a large recruiting push for cyber personnel who may not be available. The benefits for cyber operations and the cybersecurity of the U.S. should be proven.

- **Refine the criteria used to decide whether a split is in the best interest of the United States.** If a split is ultimately pursued, the Administration should fully plan for what that would entail and share that plan with the congressional Armed Services and Intelligence Committees. This plan should involve the anticipated costs, both for personnel and infrastructure, and have a timeline. Support from Congress will be essential in making such a large change successful, and an understanding of the resources required will help Congress to provide that support.

- **Continue to develop Cyber Command's capacity and readiness to increase its ability to operate independently of the NSA.** Regardless of the ultimate outcome of the leadership and dual-hat situation, Cyber Command should continue to grow and mature into a premier cyberwarfare organization to enhance the offensive and defensive cyber operations of the United States. By improving its internal ability to operate, it will require the NSA's hacking tools less often, reducing the risk of those tools being discovered by adversaries and losing their effectiveness.

Conclusion

There are compelling arguments for both sides of the dual-hat question. The decision for ending or continuing the dual-hat arrangement should ultimately be based on what will enhance the cybersecurity of the United States, and it must protect the close relationship between the NSA and Cyber Command. Today, the logical course of action is to maintain the dual-hat arrangement. When and if that changes, a clear plan with the necessary resources should be developed and made available to Congress to ensure that both organizations receive the resources they need.

*—**James Di Pane** is Research Assistant in the Center for National Defense, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. The author thanks Will Thatcher, who contributed to this* Backgrounder *while he was a member of The Heritage Foundation's Young Leaders Program.*