OSSERVATORIO SUGLI AFFARI STRATEGICI ED INTERNAZIONALI

ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

Breaking Up The Dual-Hat Leadership Of National Security Agency And United States Cyber Command

The Central Debate In The United States Cyber Community

Fabio Vanorio

Edizioni Machiavelli

www.strategicstudies.it

Maggio 2018

ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

L'***Osservatorio sugli affari strategici ed internazionali*** costituisce, all'interno dell'Istituto Machiavelli, il principale centro di analisi delle dinamiche e delle tendenze strategiche nel campo degli affari internazionali.

L'Osservatorio elabora con continuità, autonomamente e su commissione, analisi, scenari e studi previsionali su temi politici, militari ed economico-finanziari di rilevanza strategica per l'interesse nazionale italiano e per il decisore pubblico e privato.

ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

About the Author

Fabio Vanorio is an Executive Officer of the Italian Government. He has been servicing for almost 25 years at the Ministry of Foreign Affairs and International Cooperation and at the Presidency of the Council of the Ministers. Currently, he is on temporary leave to conduct academic research and resides in New York.
He holds one Degree in Economics, and three advanced Degrees in Economics and Law of European Communities, in Applied Econometrics, and in Islamic Banking and Insurance. His specializations are International Economics, Econometrics, and Economics of National Security.
He is also a contributor of the Hungarian Defense Review.

Acknowledgement

I would like to thank Frank Katusak for proofreading this paper, helping me keep things in perspective, and providing me patient advice and meaningful comments.

Disclaimer

The views expressed herein are my own and do not necessarily reflect the position of the Government of Italy or Ministry of Foreign Affairs and International Cooperation.
This paper was cleared for publication as required by my nondisclosure agreements.

Summary

Increasing the U.S. competitive advantage in cyberspace as a war-fighting domain is one of the priorities in Fiscal Years (FY) 2019-2023 Department of Defense (DoD) budgets.

The functional Combatant Command (CCMD or COCOM) of the U.S. military dedicated to the cyberspace is the U.S. Cyber Command (USCYBERCOM). On December 23, 2016, USCYBERCOM was elevated from a sub-unified command under U.S. Strategic Command (STRATCOM) to the fourth functional Combatant Command, making cyber security a major aspect of U.S. national security. On February 2018, the Army Cyber Commander, Lt. Gen. Paul Nakasone, was appointed by the President of the United States, Donald J. Trump, as the new USCYBERCOM Commander. Once confirmed, Lt. Gen. Nakasone will be also the new Director of the National Security Agency (NSA) according to a debated "dual-hat" arrangement.

Since its inception in 2009, USCYBERCOM has worked in a close relationship with the National Security Agency (NSA), an organization that is part of the Intelligence Community. The decision to keep close the two entities has been taken by putting the Signal Intelligence (SIGINT) and Cyber Warfare (CW) functions under the same command.

The DoD has set out a conditions-based approach to consider the opportunities of a breakup, fulfilling the National Defense Authorization Act for Fiscal Year 2017 mandate. According to Gen. Nakasone, any decision to terminate the dual-hat leadership arrangement must find prior well-established and operating processes and decisions which enable effective mutual collaboration and deconfliction. Any premature separation runs the risk of reducing speed and agility of cyber operations, as well as reduced cohesion and disruption of resources between the two agencies.

Like him, also some other key players, including the Secretary of Defense General Mattis, and the Chairman of the Senate Armed Committee, Senator John McCain, expressed concerns about the split.

Taking a corporate view as an example, the strategy of breaking up NSA and USCYBERCOM is like a spin off. Until the benefits of a combined organizational structure justify the negative cost of duplicative management structures and synergies costs, the structure allows USCYBERCOM to take advantage of synergy opportunities. As soon as synergies and economies of scale diminish or disappear, NSA can split off part of its operations into USCYBERCOM.

In this way, each part is enabled to become a separate player in its own sector (military and civilian cyber, in our case), focusing on its own game plan and valuing each distinct business more efficiently. The sum of the parts must usually be greater than the whole. Moreover, there can be a more efficient allocation of capital (network infrastructure, Hardware, Software, in our case) than within a merged organization. One size does not fit all when it comes to capital needs.

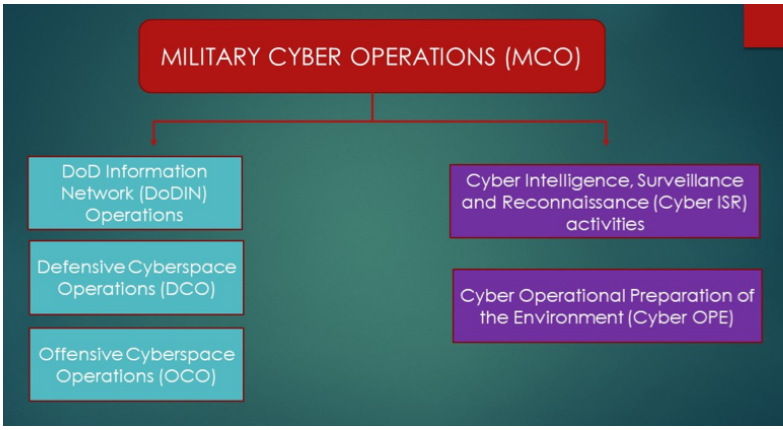
It appears, for now, the "dual hat" arrangement will endure, at least for the near term, surely for this election year. Congressional members are not pushing for a rapid separation of the dual hat. Instead, they would want to make sure any eventual split is done in a cautions and meaningful way. Each national security asset rationalization, as any splitting off of NSA and USCYBERCOM would be, must improve and increase - not damage - the single capabilities of both agencies which currently are synergically tied more in a symbiosis than in a simple coupling.

1. CYBERSPACE AS A WAR-FIGHTING DOMAIN

According to the declassified summary of the 2018 National Defense Strategy, increasing the U.S. competitive advantage in cyberspace as a war-fighting domain is one of the priorities in Fiscal Years (FY) 2019-2023 Department of Defense (DoD) budgets, supporting high-technology programs and resources, and the most innovative firms.[1]

"Cyberspace as a war-fighting domain" is an evolution of the Cyber Warfare (CW)[2] concept.

As Bray (2016) affirmed, often CW, Information Warfare (IW)[3] and Traditional Intelligence[4], CW are arbitrarily treated as synonyms, confused and overlapped. To make a distinction, an analysis of the military cyber operations can help. The Military Cyber Operations (MCO) are broken up into the following categories[5]:



1. See https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. The Attachment 1 (Cyberspace Operations Lexicon) of the Vice Chairman of the Joint Chiefs of Staff, General James E. Cartwright, Memorandum about Joint Terminology for Cyberspace Operations (11.2010) defines "Cyber Warfare" as follows: "An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber-attack, cyber defense, and cyber-enabling actions.
3. IW is not doctrinally defined by the U.S. Department of Defense (DoD). Wessley (2017) provided a good definition of IW as follows: "the means of creating non-kinetic effects in the battlespace that disrupt, degrade, corrupt, or influence the ability of adversaries or potential adversaries to conduct military operations while protecting our own.". See footnote 6 for a definition of non-kinetic effects.

4. Basically, traditional intelligence (developed from facts collected through clandestine activities, covert operations, human and electronic surveillance, and technical collection as well) provides frameworks and scenarios to government decision-makers. See Warner, M. (2017). U.S. military doctrine identifies as "1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities." See Department of Defense Dictionary of Military and Associated Terms, February 2018. Only information calibrated on protecting national security is considered intelligence. See Warner, M. (2017).

5. See Herr, T., Herrick, D. (2016).

1. DoD Information Network (DoDIN) operations, dealing with secure network configuration, systems administration, and patching.
2. Defensive Cyberspace Operations (DCO), focusing on both passive and active defense measures, including detecting, analyzing, and mitigating active threats.
3. Offensive Cyberspace Operations (OCO), deploying cyber capabilities to disrupt, deny, degrade, or destroy an adversary' system.
4. Cyber Intelligence, Surveillance and Reconnaissance (Cyber ISR) activities, collecting information on some adversary's systems (Hardware/Software configurations, personnel, and operational security) for effective targeting, and operational planning.
5. Cyber Operational Preparation of the Environment (Cyber OPE), focusing on the access to a target system, searching for advanced and up-to-date knowledge of the target system.

According to MCO's doctrine, then, CW requires the greatest awareness of the battle space, the most in-depth knowledge of an enemy's C2 (Command and Control) structure to enable "non-kinetic effects"[6] and the fastest and the most accurate targeting for information-driven weapons.[7]

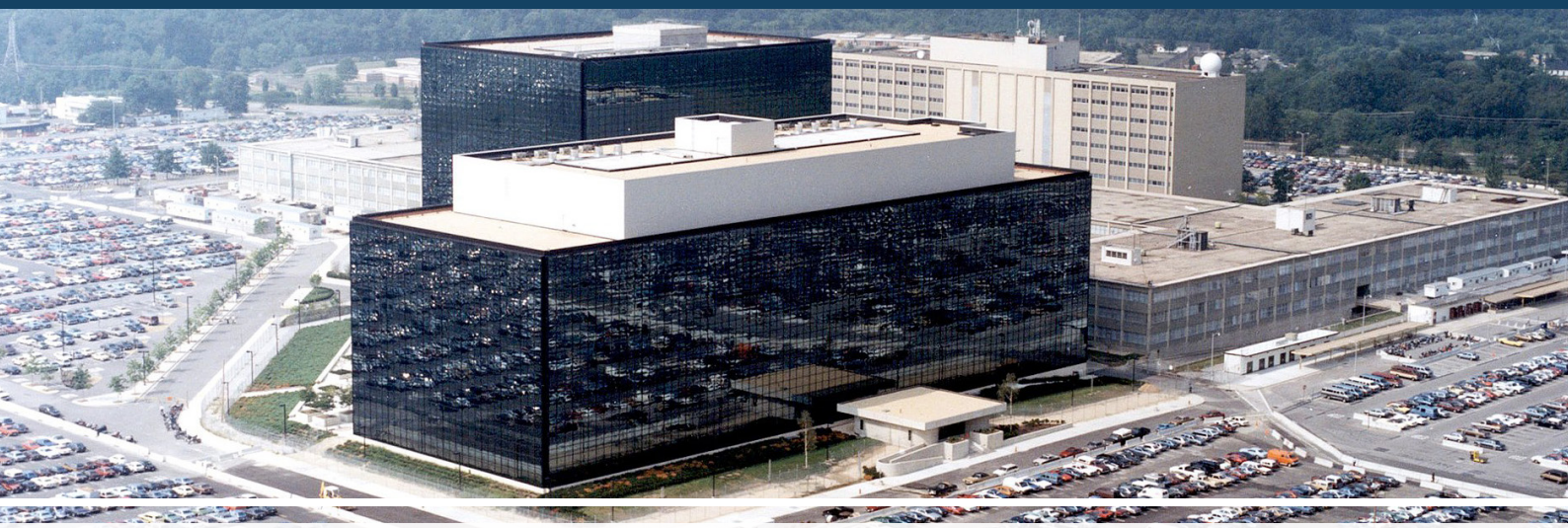
MCO is not the same concept as "cyber war." Cyber war, as usually expressed, focuses on combatants, deploying malicious cyber capabilities against the other side's systems to achieve explicit political goals. This formulation, however, ignores both existing U.S. military doctrine and the way modern forces deploy such capabilities. Instead of "cyber war," MCO focus on "cyber-enabled warfare," in which cyber capabilities are deployed in conjunction with conventional forces. See in the picture[8] an example of cyber-enabled Economic Warfare.
The war-fighting platform used by the Cyber Mission Force (CMF) to conduct war-fighting missions, according to the Title 10, United States Code (USC) that regulates the Armed Forces, is the Military Cyber Operations Platform (MCOP).[9]

6. Bob Woodward's book, "Bush at War", introduced the Washington retronym, "kinetic" warfare. The Washington meaning of the word "kinetic" derives from its secondary definition, "active, as opposed to latent." Dropping bombs and shooting bullets, killing people are kinetic. But the 21st-century military is exploring less violent and more high-tech means of warfare, such as, for example, messing electronically with the enemy's communications equipment or wiping out its bank accounts. These are "non-kinetic effects". See Noah (2002).

7. See Bray, W.R. (2016).

8. Source: Foundation for Defense of Democracies, http://www.defenddemocracy.org/project/cyber-enabled-economic-warfare/.

9. See Pomerleau, M. (2017a)



2. The Main Issue in U.S. Military Cyberspace Organization: The "Dual-Hat Arrangement" between USCYBERCOM and NSA

The functional Combatant Command (CCMD or COCOM) of the U.S. military[10] dedicated to the cyberspace is the U.S. Cyber Command (USCYBERCOM)[11]. Inside USCYBERCOM, the C2 (Command and Control) and the battle management visualization capability allow for the coordination of Defensive Cyber Operations (DCO), Offensive Cyber Operations (OCO) and Cyber Intelligence, Surveillance and Reconnaissance (Cyber ISR).

On February 2018, the Army Cyber Commander, Lt. Gen. Paul Nakasone, was appointed by the President of the United States, Donald J. Trump as the new USCYBERCOM Commander. Gen. Nakasone will be also the new Director of the National Security Agency (NSA) according to a debated "dual-hat" arrangement.

10. The U.S. military is currently organized into ten COCOMs: six geographic Combatant Commands (Pacific, Europe, Africa, Northern, Southern, Central) and four that field specialized capabilities (Special Operations, Cyber Operations, Strategic (Nuclear), and Transportation). "Combatant command" (CCMD) is "a unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff." See Department of Defense Dictionary of Military and Associated Terms, February 2018. According to Weisgerber (2014), since COCOM sounds like a compression of combatant command, it has become the de facto slang term for these military headquarters.

11. According to a recent statement of Admiral Rogers (See Senate Armed Service Committee (2018b)), USCYBERCOM's mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests. The mission objectives are three:

1. to ensure DoD mission assurance by directing the operation and defense of the DoDIN;
2. to deter or defeat strategic threats to U.S. interests and infrastructure;
3. to achieve Joint Force commander objectives in and through cyberspace.

USCYBERCOM comprises a headquarters organization and seven components: Cyber National Mission Force (CNMF), Joint Force Headquarters-DoDIN, plus joint force headquarters and forces at Army Cyber Command (ARCYBER), Marine Forces Cyberspace Command (MARCYBER), Fleet Cyber Command/Tenth Fleet (NAVCYBER), and Air Forces Cyber/24th Air Force (AFCYBER). A seventh partner, though not a component, is U.S. Coast Guard Cyber. See Senate Armed Services Committee (2016). In Fiscal Year 2018, USCYBERCOM is executing more than $600 million dollars in programs and projects. Its full-time staff amounts to 1,060 military members and civilians, plus contractors. At the end of December 2017, it had 5,070 service members and civilians in the Cyber Mission Force (CMF), building to a total of 6,187 people, meaning the CMF was staffed at 82 percent.

In his remarks before the Senate Armed Services Committee last March 1st,[12] Gen. Nakasone pointed two main goals: increasing deterrence and readiness in the U.S. military cyber strategy. According to him, a whole-of-nation approach (including government, military, industry and academia) is critical to success in deterring action in cyberspace. His way of changing will be based on:[13]

1. a new strategy and doctrine for how the U.S. operates;
2. new established norms;
3. new cyber-thinking as response and offense.

To understand the meaning of the above mentioned "Dual-Hat Arrangement", a brief explanation of USCYBERCOM origin can be useful. In 2009, then-President of the United States Barack Obama created the U.S. Cyber Command (USCYBERCOM) as a sub-unit of the U.S. Strategic Command (USSTRATCOM[14]) to address threats of cyber espionage and other cyber-attacks, to coordinate the ability of the DoD to conduct Cyber Warfare and to defend its own networks, including those that are used by combat forces in battle.[15]

Since its inception in 2009, USCYBERCOM has worked in a close relationship with the National Security Agency (NSA), an organization that is part of the Intelligence Community. The decision to keep close the two entities has been taken by putting the Signal Intelligence (SIGINT) and Cyber Warfare (CW) functions under the same command.[16] For this reason, the "dual-hat" arrangement has been introduced as follows:

- USCYBERCOM and NSA share the same military Commander and Director[17].
- USCYBERCOM and NSA share the location of Fort Meade, Maryland.
- USCYBERCOM and NSA personnel share the same networks built by the NSA[18]. Moreover, NSA supports USCYBERCOM's mission, providing critical support for target access and development, including linguists, analysts, cryptanalytic capabilities and sophisticated technological infrastructure.[19]

On December 23, 2016, with the approval of the National Defense Authorization Act (NDAA) for Fiscal Year 2017, USCYBERCOM was elevated from a sub-unified command under STRATCOM to the fourth functional Combatant Command[20],

12. Senate Armed Service Committee (2018a).

13. See Pomerleau, M. (2018b).

14. The same command responsible for military affairs in space and the nuclear arsenal.

15. See Baldor L.C. (2017).

16. See Sanger, D.E., Shankerdec, T. (2013).

17. The NSA is a civilian-military hybrid since its inception in 1952, and this is the reason for which it has been lead by a military official.

18. See Nakashima, E. (2016).

19. See Sanger, D.E., Shankerdec, T. (2013).

20. The National Defense Authorization Act (NDAA) for Fiscal Year 2017 allocated $75 million a year to CYBERCOM for upkeep of current facilities, training of personnel, acquisition of hardware, and development and deployment of new programs. See Park, J. (2017).

making cyber security a major aspect of U.S. national security. Now, the USCYBERCOM Combatant Commander can directly appeal to the Secretary of Defense and the President of the United States, and he has a voice regarding budgeting decisions. Moreover, he is the only official responsible for surveillance and to direct cyberweapons.

The debate about mixing-up military and civilian systems in the cyber security has pro and cons. According to Gen. Nakasone remarks,[21] the dual-hat arrangement has enabled an operationally close, mutually beneficial partnership, for instance, in mapping networks prior to operations.[22] Similarly, the experience has also brought some issues[23], such as for example a growing dependence of Military CYBERCOM Information Assurance (IA)[24] on the civilian NSA IA[25].

About the cyber issue, NSA and USCYBERCOM have fundamentally different missions. From an NSA perspective, cyber is about gaining access to networks; from a USCYBERCOM point of view, it's about every piece of software on the battlefield the adversary is using and preventing that software from working the way it was intended to work.[26] In cyberspace, while the military wants to attack networks, intelligence objectives prioritizes gathering information from them.[27] This keeps both agencies in potential disagreement about how to use intel and tools that they share.[28]

21. Senate Armed Service Committee (2018a).

22. "Dual-hatting optimizes the integration and synchronization of [signals intelligence] and cyberspace operations. It enables decision-making that balances competing equities under the judgment of a single individual directly responsible for both organizations critical missions". See Pomerleau, M. (2018a).

23. See White House (2013)

24. "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." See National Institute of Science and Technology (NIST) - Computer Security Resource Center (CSRC) Glossary, https://csrc.nist.gov/Glossary/?term=4763. The DoDI 8500.01 Instruction has transitioned from the term "information assurance" to the term "cybersecurity". DoD now defines "cybersecurity" as: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." See http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

25. The reliance upon the same infrastructure to conduct intelligence operations with the intent of being unidentifiable while performing loud, offensive military operations meant to disrupt a target's networks (and sometimes also with the intent of being identifiable) presents dangers from an intelligence perspective. Loud attacks, in fact, can be traced back through the channels on which they were carried, leading adversaries back to NSA servers and offering intel on capabilities. See Pomerleau, M. (2017a).

26. See Tucker, P. (2017).

27. See Baldor L.C. (2017).

28. See Tucker, P. (2017).

3. The "Title 10 - Title 50" Debate

There is another big concern related to the dual-hat role in implementing intelligence actions and military operations. Dual responsibilities, in fact, are also related to the "Title 10-Title 50 debate". Title 50 U.S. Code is the part of the federal regulations dealing in national defense and intelligence. It establishes authorities within the Intelligence Community, and it also clarifies that the Secretary of Defense controls two of the U.S. Intelligence Community agencies (the NSA and Defense Intelligence Agency, that are part of the DoD).

NSA's authority to conduct cyber surveillance comes from Title 50 of the U.S. Code. But this also interdict NSA, as an Intelligence organization, to destroy information, and to harm someone else's networks, as these actions constitute "a war-making Title 10 function."[29]

29. See Kohse, E., Mirasola, C. (2017).

Title 10 of the U.S. Code is related to Defense and military organizations. CYBERCOM's powers stems from this Title. NSA personnel may conduct intelligence gathering to support a Title 10 military operation and existing law does not preclude CYBERCOM from conducting a Title 50 operation.

Wall (2011) proposes a two-part test to determine whether an activity is an intelligence activity or a military operation. An intelligence activity is (1) conducted by an element of the intelligence community, and (2) in response to tasking from the U.S. Intelligence Community.

The activity in question is[30]:

1. a Title 50 intelligence activity if fulfills both requirements.
2. a Title 10-Title 50 military intelligence activity if the activity is conducted by a DoD agency of the intelligence community but under the Secretary of Defense direction.
3. a Title 10 military operation if the activity is conducted by a DoD agency that is not part of the Intelligence Community.

These three points are of the utmost relevance with respect to the Congressional oversight,

The Secretary of Defense possesses authorities under both Title 10 and Title 50. All DoD activities and operations, including military and tactical intelligence activities, and other departmental intelligence-related activities are under the Armed Services Committees oversight.

There also are assertions by the Congressional intelligence committees about a jurisdiction over the "intelligence-related" activities of the DoD. This could create overlapping jurisdiction with the Armed Services Committees and confusion over oversight and reporting requirements.

While the intelligence committees' claim can be justified over DoD Title 50-activities, the same cannot be said of DoD Title 10-activities, categorized as military operations and subject to the exclusive oversight of the armed services committees. Title 10-military operations are subject to the exclusive oversight of the Armed Services Committees, even if those activities are related to intelligence gathering since they provide information on Secretary of Defense's requests and remain under military direction and control.

The Senate and the House intelligence committees hold an exclusive jurisdiction only when an operation is a "covert action". In this case, they have jurisdiction even over military operations.

30. See Wall, A.E. (2011).

4. What To Expect

After revelations of NSA surveillance programs by Edward Snowden[31], then-President of the United States Barack Obama created the "Review Group on Intelligence and Communications Technologies". To distinguish the warfighting role from the intelligence role, the Review Group recommended splitting the military Cyber Command into a separate organization and bringing NSA to refocus on its core function: the collection and use of foreign intelligence information.[32]

The DoD has set out a conditions-based approach to consider the opportunities of a breakup, fulfilling the National Defense Authorization Act for Fiscal Year 2017 mandate.[33] Last March 1st, in his confirmation hearing before the Armed Service Committee, Lt. Gen. Paul M. Nakasone did not openly recommend splitting USCYBERCOM from the NSA, vowed (1) to evaluate the conditions expressed by the DoD and the appropriateness of the "dual-hat arrangement" within his first 90 days of taking office, and (2) to provide an assessment to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff.[34]

31. Criticism of NSA surveillance programs sparked by the documents leaked by former contractor Edward Snowden brought Chris Inglis, the NSA's Deputy director and its highest ranking civilian, to step down after serving as Deputy director since 2006. Inglis, and other top agency officials, were angry and dispirited about the weakness in the way of the Obama Administration to defend the agency. See Sanger, D.E., Shankerdec, T. (2013).

32. See White House (2013).

33. The Subtitle C - Cyberspace-Related Matters, Sec. 1642. (Limitation on Termination of Dual-Hat Arrangement for Commander of the United States Cyber Command), (b) Assessment says "The Secretary of Defense and the Chairman of the Joint Chiefs of Staff shall jointly assess the military and intelligence necessity and benefit of the dual-hat arrangement. The assessment shall include the following elements:
(A) An evaluation of the operational dependence of the USCYBERCOM on the NSA.
(B) An evaluation of the ability of the USCYBERCOM and the NSA to carry out their respective roles and responsibilities independently.
(C) A determination of whether the following conditions have been met:
(i) Robust operational infrastructure has been deployed that is sufficient to meet the unique cyber mission needs of the USCYBERCOM and the NSA, respectively.
(ii) Robust command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations.
(iii) The tools and weapons used in cyber operations are sufficient for achieving required effects.
(iv) Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations.
(v) Capabilities have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.
(vi) The cyber mission force has achieved full operational capability."

34. See Senate Armed Service Committee (2018a).

Gen. Nakasone, who witnessed the creation of USCYBERCOM while serving as executive officer to former NSA Director Keith Alexander[35], said that any decision to terminate the dual-hat leadership arrangement must find prior well-established and operating processes and decisions which enable effective mutual collaboration and deconfliction. Any premature separation runs the risk of reducing speed and agility of cyber operations, as well as reduced cohesion and disruption of resources between the two agencies.

Like him, also some other key players, including the Secretary of Defense General Mattis, and the Chairman of the Senate Armed Committee, Senator John McCain, expressed concerns about the split.

Taking a corporate view as an example, the strategy of breaking up NSA and USCYBERCOM is like a spin off[36]. From the CYBERCOM's point of view, the consequences can be identified similarly:

- Until the benefits of a combined organizational structure justify the negative cost of duplicative management structures and synergies costs, the structure allows USCYBERCOM to take advantage of synergy opportunities.
- As soon as synergies and economies of scale diminish or disappear, NSA can split off part of its operations into USCYBERCOM. In this way:
  - Each part is enabled to become a separate player in its own sector (military and civilian cyber, in our case), focusing on its own game plan and valuing each distinct business more efficiently. The sum of the parts must usually be greater than the whole.
  - There can be a more efficient allocation of capital (network infrastructure, Hardware, Software, in our case) than within a merged organization. One size does not fit all when it comes to capital needs.

Some believed (or simply hoped) with the Admiral Michael S. Rogers's retirement from his task of USCYBERCOM Commander and NSA Director, the Trump administration might take the opportunity to separate the "dual hat" and name distinct leaders. It appears, for now, the "dual hat" arrangement will endure, at least for the near term, surely for this election year.[37]

Congressional members are not pushing for a rapid separation of the dual hat. Instead, they would want to make sure any eventual split is done in a cautions and meaningful way. Each national security asset rationalization, as any splitting off of NSA and USCYBERCOM would be, must improve and increase - not damage - the single capabilities of both agencies which currently are synergically tied more in a symbiosis than in a simple coupling.

35. See Chalfant, M. (2018). In his remarks before the Senate Armed Services Committee last March 1st, Gen. Nakasone wrote "For the past ten years, I have had the privilege to lead, plan, and execute Joint and Army cyberspace operations supporting national, Combatant Command, and Service missions. In this decade I have seen incredible growth in cyber capacity and capabilities within the Department of Defense. When I first started working cyber, operations were often just concepts, and when conducted, performed ad-hoc by technical specialists on loan from other organizations. Today that is not the case. Now, a mature and highly-capable Cyber force is built and, in the fight, aggressively defending our network, conducting daily operations against adversaries, and strengthening the combat power and lethality of U.S. forces around the world." See Pomerleau (2018b).

36. When a corporation spins off a business unit that has its own management structure, it sets it up as an independent company. A spinoff may be conducted by a company, so it can focus its resources and better manage the division that has better long-term potential. See https://www.investopedia.com/terms/s/spinoff.asp.

37. DoD is quietly reorganizing USCYBERCOM hierarchy aimed at helping navigate the command through the elevation and eventual split from the National Security Agency without interrupting the regular day-to-day activities. See all this issue in Pomerleau (2018c). At first, in June 2017, Marine Corps Lt. Gen. Vincent Stewart, who most recently served as the director of the Defense Intelligence Agency (DIA), was nominated Deputy Commander. At second, a second Deputy, Army Lt. Gen. William Mayville, filled in a position that did not previously exist for 8 months until March 2018. (See Pomerleau (2018d)). Stewart is focused on the regular duties a deputy fills while Mayville was brought in to focus intently on the work necessary for elevation. This was viewed as a temporary setup. Congress, in fact, won't support making a two-deputy construct permanent.

4. What To Expect

Baldor L.C. (2017), U.S. to create the independent U.S. Cyber Command, split off from NSA, Associated Press, July 17, 2017

Bray, W.R. (2016), Intelligence Is Not Warfare!, Proceedings Magazine, U.S. Naval Institute, Vol. 142/12, December 2016

Chalfant, M. (2018), Meet Trump's popular nominee to lead NSA, The Hill, March 15, 2018

Heftye, E. (2017), Multi-Domain Confusion: All Domains Are Not Created Equal, The Strategy Bridge, May 26, 2017

Herr, T., Herrick, D. (2016), Military Cyber Operations: A Primer, The American Foreign Policy Council, Defense Technology Program Brief, No. 14, Washington D.C., January 2016

Hoffman, F. G., Davies, M. C. (2013), Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework?, Small Wars Journal, June 2013

Kohse, E., Mirasola, C. (2017), To Split or Not to Split: The Future of CYBERCOM's Relationship with NSA, www.lawfareblog.com, April 12, 2017.

Nakashima, E. (2016), Obama to be urged to split cyberwar command from NSA, Washington Post, September 13, 2016

Noah, T. (2002), Birth of a Washington Word, www.slate.com, November 20, 2002

Park, J. (2017), Should CYBERCOM Split From the NSA?, International Policy Digest, June 2, 2017

Pomerleau, M. (2018a), Nakasone not bullish on NSA/Cyber Command split, www.fifthdomain.com, March 15, 2018

Pomerleau, M. (2018b), Cyber Command nominee: attacks must come with a cost, www.c4isrnet.com, March 1, 2018

Pomerleau, M. (2018c), DoD quietly reorganizes Cyber Command, www.fifthdomain.com, January 9, 2018

Pomerleau, M. (2018d), New deputy at Cyber Command to retire, www.fifthdomain.com, March 23, 2018

Pomerleau, M. (2017a), Here's what Cyber Command's war-fighting platform will look like, www.fifthdomain.com, June 29, 2017

Pomerleau, M. (2017b), Why you'll hear about a 'cyber carrier' in 2018, www.c4isrnet.com, December 29, 2017

Sanger, D.E., Shankerdec, T. (2013), Obama to Keep Security Agency and Cyberwarfare Under a Single Commander, New York Times, December 13, 2013

Senate Armed Service Committee (2018a), Advance Policy Questions for Lieutenant General Paul Nakasone, U.S. Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, www.armed-services.senate.gov/imo/media/doc/Nakasone_APQs_03-01-18.pdf, March 2018.

Senate Armed Service Committee (2018b), Testimony of Admiral Michael S. Rogers, Commander U.S. CYBERCOM, www.armed-services.senate.gov/imo/media/doc/Rogers_02-27-18.pdf, February 2018.

Senate Armed Service Committee (2016), Statement of Admiral Michael S. Rogers, Commander U.S. CYBERCOM before the Senate Armed Services Committee, www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf, April 2016.

Tucker P. (2017), What the Announced NSA / Cyber Command Split Means, Defense One, August 18, 2017

Tucker P. (2016), Carter May Elevate CYBERCOM to a Full Combatant Command, Defense One

Wall, A.E. (2011), Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action, National Security Journal, Harvard Law School, December 2, 2011

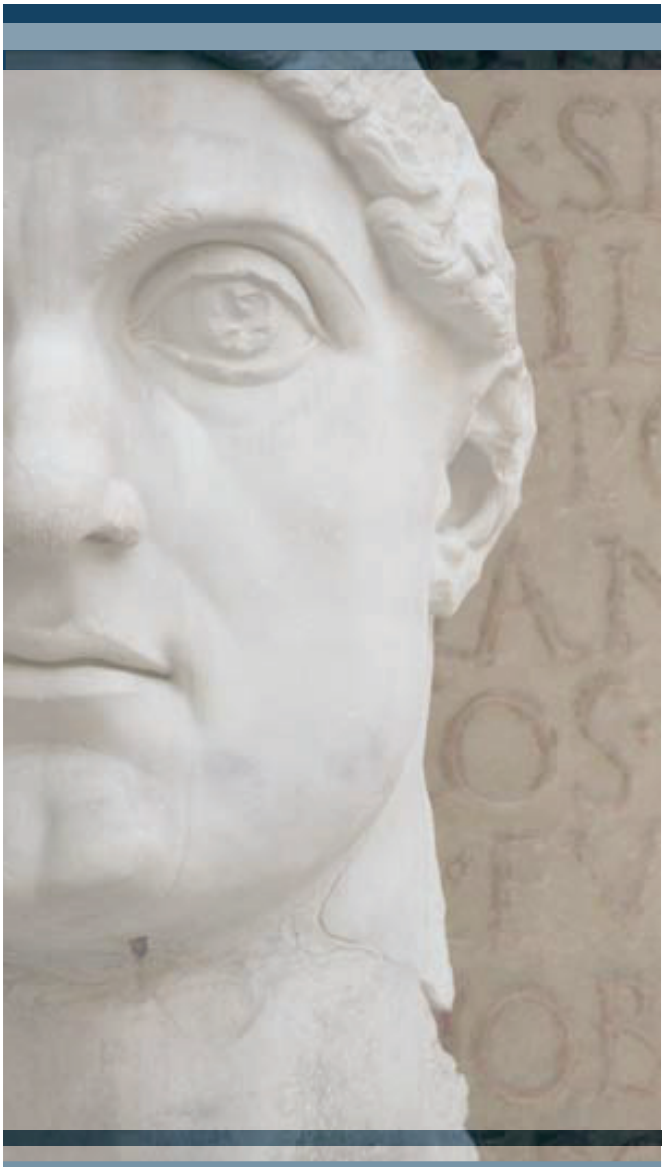
Warner, M. (2017), Intelligence in Cyber - and Cyber in Intelligence, Carnegie Endowment for International Peace, October 16, 2017

Weisgerber M. (2014), How to Abbreviate Combatant Command: COCOM vs. CCMD, intercepts.defensenews.com, March 24, 2014

Wessley, B. (2017), Evolution of U.S. Cyber Operations and Information Warfare, Divergent Options, May 25, 2017

White House (2013), Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, December 12, 2013

Williams, L. (2018), Nakasone talks cyber deterrence at confirmation hearing, Defense Systems



ISTITUTO ITALIANO
DI STUDI STRATEGICI
ITALIAN INSTITUTE
OF STRATEGIC STUDIES
Niccolò Machiavelli

L'Istituto Italiano di Studi Strategici *"Niccolò Machiavelli"* è un'associazione culturale senza scopo di lucro costituita a Roma nel 2010.

L'Istituto, think tank indipendente, nasce dall'iniziativa di un gruppo internazionale di personalità del mondo economico, accademico ed istituzionale civile e militare, con l'obiettivo di contribuire alla rinascita del pensiero strategico italiano.

La complessità e l'ampiezza delle sfide che attendono il Paese nel XXI secolo richiede conoscenza, consapevolezza e capacità prospettiche. L'Istituto Machiavelli, anche grazie al proprio network globale, promuove l'interscambio culturale tra il decisore italiano ed internazionale, pubblico e privato, e svolge attività di ricerca finalizzate ad elevare il livello di competitività globale del "Sistema Paese".

L'Istituto Machiavelli, autonomamente o in collaborazione con istituzioni, organizzazioni ed aziende nazionali ed estere, realizza studi ed analisi strategiche *policy-oriented*, organizza briefing, seminari e workshop, cura corsi di alta formazione per i *leader*.

Per ulteriori informazioni:

Istituto Italiano di Studi Strategici "Niccolò Machiavelli"
Via di S. Basilio, 64
00187 – Roma
Tel.: (+39) 06 45422952
Fax: (+39) 06 97259168
email: info@strategicstudies.it
www.strategicstudies.it