13

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-02-2023	FINAL	N/A

4. TITLE AND SUBTITLE
Enacting the U.S. Cyber Force: The Key to Winning the Great Cyber Competition with China

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Henry L. Sims Jr.

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The enactment of a U.S. Cyber Force (USCF) combined with increased integration of Artificial Intelligence (A.I.) and automation will help win the great cyber competition with China. The 2022 National Security Strategy (NSS) highlights the President's desire to enhance cybersecurity partnerships and stresses the importance of out-competing China by improving U.S. cyber resilience. The U.S. must enact the USCF as the final service branch to remain competitive in the cyber fight. This thesis will be proven by expounding on China's cyber dominance, using the U.S. Space Force (USSF) as a model, highlighting the positive impact on talent management, and demonstrating the USCF is instrumental in helping counter China's cyber superiority. Senior leaders challenged with "strengthening norms that mitigate cyber threats and enhance stability in cyberspace" should take heed.

15. SUBJECT TERMS (Key words)
Cyber, China, National Security Strategy, National Defense Strategy, Space, Competition

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A		19b. TELEPHONE NUMBER *(include area code)* 401-841-6499

Standard Form 298 (Rev. 8-98)

Enacting the U.S. Cyber Force:

The Key to Winning the Great Cyber Competition with China

INTRODUCTION

The enactment of a U.S. Cyber Force (USCF) combined with increased integration of Artificial Intelligence (A.I.) and automation will help win the great cyber competition with China. The 2022 National Security Strategy (NSS) highlights the President's desire to enhance cybersecurity partnerships and stresses the importance of out-competing China by improving U.S. cyber resilience. The U.S. must enact the USCF as the final service branch to remain competitive in the cyber fight. This thesis will be proven by expounding on China's cyber dominance, using the U.S. Space Force (USSF) as a model, highlighting the positive impact on talent management, and demonstrating the USCF is instrumental in helping counter China's cyber superiority. Senior leaders challenged with "strengthening norms that mitigate cyber threats and enhance stability in cyberspace" should take heed.[1]

China's cyber forces are becoming superior to U.S. cyber forces, and "many experts view China as the greatest cyber threat on Earth (Duke, 2020)."[2] Unfortunately, today's U.S. cyber posture cannot stay ahead of this pacing threat. Most cyber professionals have concluded that the U.S. is "either just as vulnerable to cyberattacks or even more vulnerable today than it was five years ago."[3] In fact, 81% of experts believe the U.S. cyber security posture has been on a steady decline for more than half a decade (figure 1).

---

[1] National Security Strategy, Washington, D.C.: *Office of Homeland Security, (October 12, 2022),* https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[2] Klevering, Griffin, "A Brief Look at Chinese Cyberwarfare", *Small Wars Journal* (January 26, 2022), https://smallwarsjournal.com/jrnl/art/brief-look-chinese-cyberwarfare

[3] Marks, Joseph and Schaffer, Aaron, "The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say", The Cybersecurity 202 (January 6, 2022), https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/

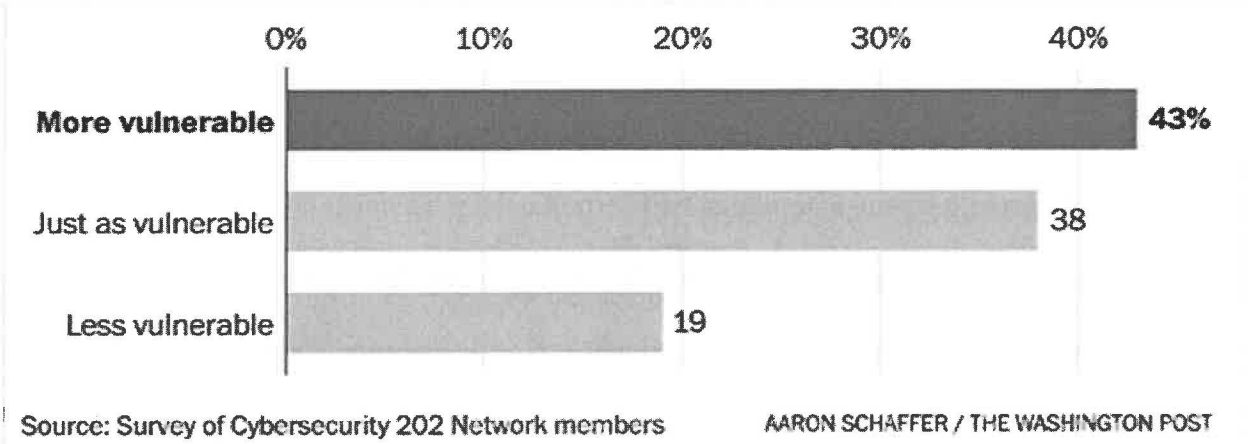

Figure 1. Is the U.S. more vulnerable, less vulnerable, or just as vulnerable to cyberattacks now as it was five years ago?

China initiates daily cyberattacks to exploit U.S. vulnerabilities, and the "NSA, CISA, and FBI continue to assess [People's Republic of China] PRC state-sponsored cyber activities as being one of the largest and most dynamic threats to U.S. government and civilian networks."[4] For example, "Atlassian" is a top Common Vulnerability and Exposure (CVE) used by the PRC that could enable China to execute malicious code on U.S. servers.[5] Attacks against the U.S. present a global danger to national peace and security, and if left unchecked, "cyber warfare as planned by the Chinese can take the nation down."[6] China's global threat was illustrated when the U.K. accused Chinese hackers of attacking many U.K. businesses. China has also struck Taiwan with cyber espionage.[7] Additionally, border disputes are increasingly becoming a point of contention in the quest for global dominance. Furthermore, China has used cyberwarfare as a

---

[4] "Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors", *Cybersecurity and Infrastructure Security Agency*, October 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

[5] "Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors", *Cybersecurity and Infrastructure Security Agency*, October 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

[6] Kannan, Saikiran and Bhalla, Abhishek, "Inside China's cyber war room: How PLA is plotting global attacks", *India Today*, August, 6, 2020, https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06

[7] Klevering, Griffin, "A Brief Look at Chinese Cyberwarfare", *Small Wars Journal* (January 26, 2022), https://smallwarsjournal.com/jrnl/art/brief-look-chinese-cyberwarfare

weapon of choice to intimidate its neighboring country, India. Intelligence suggests China has enacted a secret People's Liberation Army (PLA) to use cyber tactics to degrade India's information and defensive security.[8] The U.S. must reassess its cyber posture to protect against this form of irregular warfare.

The U.S. has also become increasingly vulnerable to cyberattacks due to a lack of dedicated cyber resources. China is becoming dominant in the Great Cyber Competition with its dedicated cyber force, and the U.S. cannot defeat China without diminishing the dichotomy of cyber presence. The 2022 National Defense Strategy (NDS) identified China as the pacing threat, and this adversary has dedicated substantial resources to prepare for cyber warfare. China's PLA is dedicated full-time to imposing cyber threats on neighboring countries to further its global dominance. During a time of limited resources and DoD funding, the U.S. cannot sustain global power when faced with cyber war. China currently outnumbers the U.S. active and reserve military by approximately 1.12M (figure 2).[9] This large population provides more opportunities for China to recruit and retain dedicated cyber personnel.

Top 10 Countries with the Highest Number of Active-Duty and Reserve Military Personnel (in members):

1. Vietnam: 5,482,000
2. South Korea: 3,699,000
3. China: 3,355,000
4. Russian Federation: 3,014,000
5. India: 2,610,550
6. United States: 2,233,050
7. North Korea: 1,880,000
8. Taiwan: 1,820,000
9. Brazil: 1,706,500
10. Pakistan: 1,204,000

Figure 2. Top 10 countries with the highest number of military members

[8] Kannan, Saikiran and Bhalla, Abhishek, "Inside China's cyber war room: How PLA is plotting global attacks"
[9] "Military size by country 2023," World Population Review, accessed January 2, 2023, https://worldpopulationreview.com/country-rankings/military-size-by-country

China's dedicated cyber army places the U.S. at a disadvantage regarding global dominance, and the U.S. must consolidate forces to counter China's cyber power. Once done, the U.S. can focus on interoperability within the Joint Information Environment (JIE) and utilize A.I. and automation to reduce the loss of human life, supplement military recruiting shortages and manning deficits, and capitalize on emerging military technologies. These actions will also enable the U.S. to increase its focus on A.I. and automation to supplement military manning deficiencies and reallocate existing personnel to help create the USCF as its sixth branch of service. A.I. can complement limited military personnel and fill cyber recruiting and training gaps. Therefore, the U.S. should integrate more A.I. into its military Operations Plans. Additionally, automation can help sustain military forces and justifies the need for the establishment of the USCF to have a full-time focus on the cyber domain to compete with China. This concept successfully established the USSF to focus on the space domain.

A DEDICATED FORCE

General George S. Patton famously said, "A good plan violently executed today is better than a perfect plan executed next week." This statement still holds today as the U.S. must initiate steps to enact the USCF as soon as possible. According to the Small Wars Journal, "Within the next 5-10 years, China could overtake the United States and become the most powerful cyber nation."[10] Since China has a dedicated cyber army, the U.S. needs a dedicated cyber force to combat the power of China's cyber supremacy. Just as China has effectively capitalized on its PLA's massive workforce of well-trained cyber warriors, the U.S. must also

[10] Klevering, Griffin, "A Brief Look at Chinese Cyberwarfare", *Small Wars Journal* (January 26, 2022), https://smallwarsjournal.com/jrnl/art/brief-look-chinese-cyberwarfare

dedicate troops to protect the world against China and other bad cyber actors. This can be accomplished by modeling the establishment of the USSF, created to institute dominance in the space domain. According to USSF history, the space domain was identified as a national security imperative determined by "the growing threat posed by near-peer competitors in space, [and] it became clear there was a need for a military service focused solely on pursuing superiority in the space domain."[11] Similarly, the cyber domain impacts every aspect of warfare and requires a dedicated service to conduct unceasing offensive and defensive cyber warfare. To capitalize on emerging military technologies and create interoperability within the JIE, the U.S. military needs to make a solitary service with the mission of creating a collaborative environment on a global scale.

As outlined in the NSS, "The United States has a vital interest in deterring aggression by PRC behavior below, and above the traditional threshold of conflict [and] we cannot afford to rely solely on conventional forces."[12] The way wars of the past were fought will not suffice in modern times. Stove-piped efforts in combat will exacerbate the U.S.'s loss of global power. According to the NSS, "Our National Defense Strategy relies on integrated deterrence: the seamless combination of capabilities to convince potential adversaries that the costs of their hostile activities outweigh their benefits."[13] To accomplish these goals, we must secure cyberspace, and "as an open society, the United States [must establish] a clear interest in strengthening norms that mitigate cyber threats and enhance stability in cyberspace."[14] The

---

[11] United States Space Force History. Accessed January 4, 2023. https://www.spaceforce.mil/About-Us/About-Space-Force/History/#:~:text=The%20establishment%20of%20the%20USSF,superiority%20in%20the%20space%20domain.

[12] National Security Strategy, Washington, D.C.: *Office of Homeland Security, (October 12, 2022),* https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

[13] NSS

[14] NSS

cyberspace domain is rapidly evolving, and currently, China is using cyberspace to conduct coercive activities in what the NDS refers to as the gray zone.[15]

Also stated in the NDS, cyber and space domains empower the entire joint force, and increased resilience in each environment is necessary.[16] However, establishing the USSF only covers 50% of the resiliency strategy highlighted. In December 2022, steps were made toward protecting the remaining threat by establishing the Cyber National Mission Force (CNMF) as the DoD's newest subordinate unified command.[17] While this is a step in the right direction, a subordinate unified command embedded within U.S. Cyber Command only protects a portion of the cyber mission. Specifically, this organization primarily defends the Department of Defense Information Network (DoDIN) and focuses less on cyber-like irregular warfare.

The U.S. must continue the momentum to cover the remaining 50% of the national security imperative by enacting the USCF. Advances in non-nuclear capabilities, such as cyber, will produce complicated and volatile pathways for conflict where collective understandings and behavioral norms are not clearly defined.[18] Currently, the U.S. Cyber Command oversees regionalized Service cyberspace components: ARCYBER, AFCYBER, FLTCYBER, and MARFORCYBER. However, "much of the work of Cyber Command is performed by its Service cyberspace components."[19] Each entity works on important but separate ventures to combat

---

[15] National Defense Strategy, Washington, D.C., *(2022),* https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[16] NDS

[17] U.S. Cyber Command. Accessed January 4, 2023. https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe/#.Y6EDPFyUDLg.linkedin

[18] NDS

[19] U.S. Cyber Command. Accessed January 4, 2023.

China and other adversaries. The evolution must continue to create unity of effort and eliminate confusion, and the current construct (figure 3) should be further evolved to create the USCF.[20]

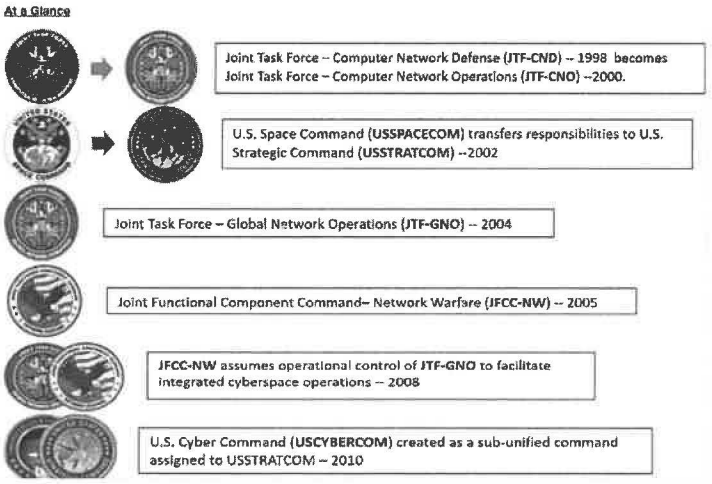

Figure 3: The evolution of the cyber organization.

A.I AND AUTOMATION/RECRUITING AND RETENTION

World War III (WWIII) is possible, with constant international vying for global dominance. However, unlike the previous two World Wars, the next one will not likely involve boots on the ground nor rely on ships on the seas. If WWIII is initiated, there will likely be a heavy cyber emphasis instigated by China to gain global dominance. Therefore, the Great Cyber Competition cannot be won solely with human assets. This will be the first unconventional global war, and the best way for the U.S. to win is through the enactment of the USCF. Creating the USCF will help establish interoperability of information technology and cyber systems where A.I. and automation will be the premise. To maximize combat power and extend operational reach, A.I. and automation employment must be amplified. Manpower resources are finite in the

[20] U.S. Cyber Command. Accessed January 4, 2023. https://www.cybercom.mil/About/History/#:~:text=Its%20mission%20is%20to%20direct,with%20domestic%20and%20international%20partners.

U.S. military. Therefore, emerging technologies are required to help reduce the loss of human life, supplement military recruiting shortages and manning deficits, and create interoperability within the JIE.

Technological innovation shows that "new applications of artificial intelligence, quantum science, autonomy, biotechnology, and space technologies have the potential not just to change kinetic conflict, but also to disrupt day-to-day U.S. supply chain and logistics operations."[21] The U.S. must lead the charge in implementing technological advancements by making suitable investments in technology and "be a fast-follower where market forces are driving the commercialization of militarily-relevant capabilities in trusted artificial intelligence and autonomy."[22] Modern warfighters rely on data-driven technologies and data integration that enhance intelligence efforts and provide prompt delivery to the warfighter.[23] Since the U.S. has a limited force size, "we [need to] aggressively seek to fill specific technology gaps, including in cyber, data, and artificial intelligence specializations, and work with colleges and universities to help build our future workforce."[24] This will be a crucial step toward cyber resilience.

Simultaneously, the U.S. must make a valiant effort to recruit and retain its cyber talent. The private sector has better technology, training programs, and resources. It is becoming more challenging to compete with the civilian cyber market. In fact, "troops who receive extensive cyber training, lured by the lucrative private sector, are parting ways with the military services

---

[21] National Defense Strategy, Washington, D.C., *(2022),* https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[22] NDS

[23] NDS

[24] NDS

quicker than some branches can offset the cost of that training."[25] The USSF is acquiring cyber troops from the USAF among the current service branches. Still, the USAF is adding three-year service obligations to retain its own cyber personnel. The U.S. Army is trying to double its cyber force, the U.S. Marine Corps (USMC) is not getting a good return on cyber training, and the U.S. Navy is trying to retain visibility on cyber billets.[26] The National Defense Authorization Act (NDAA) has pinpointed a lack of service obligation for cyber-trained personnel. This is a monumental problem since it could take up to three years and cost up to $500,000 to fully train a cyberwarrior, only to lose them to the private sector.[27] While the U.S. has already spent roughly $160 million to retain its cyber talent, it still lags behind countries like China. The best way to rectify this shortfall is to eliminate each service's separate recruiting and retention efforts and create a unified recruiting effort via the enactment of the USCF.

Continual steps must be made to attract cyber knowledge and retain the talent already acquired. For instance, the USAF recently released its Initial Enlistment Bonus (IEB) plan for 2023, offering up to $20,000 for six-year enlistments and a new "quick ship" program to foster faster recruitment efforts.[28] Additionally, physical fitness standards of the past are not conducive to attracting the cyber talent the U.S. military needs today. The world is not fighting the same conventional war fought previously. Cyber warriors don't need to run three miles nor complete a certain number of push-ups or sit-ups in an allotted time. The U.S. Army is the largest and oldest branch of service in the U.S., yet it still understands that old ways of thinking will cause demise

---

[25] Lawrence, Drew. "Troops Are Getting Cyber Training and Then Rapidly Leaving the Military, Report Finds". *Military.com,* Accessed January 5, 2023. https://www-military-com.cdn.ampproject.org/c/s/www.military.com/daily-news/2022/12/27/troops-are-getting-cyber-training-and-then-rapidly-leaving-military-report-finds.html/amp

[26] Lawrence, Drew. "Troops Are Getting Cyber Training and Then Rapidly Leaving the Military"

[27] Lawrence, Drew. "Troops Are Getting Cyber Training and Then Rapidly Leaving the Military"

[28] U.S. Air Force Careers. Accessed January 8, 2023. https://www.airforce.com/careers/pay-and-benefits/enlistment-bonuses

in combat superiority.[29] Without unified guidance, the U.S. Army intends to initiate job-specific fitness scoring. This furthers the theory that a cyber soldier needs to be held to a different standard of physical fitness than a soldier in the infantry.[30]

Grooming standards also need to be reevaluated. The U.S. military requires the brainpower and cyber talent of those with beards, tattoos, piercings, pink hair, etc., that may be able to join the USCF in a military, civilian, or contractor capacity. These nuances are hindering cyber recruitment and retention across the joint force. The USMC is renowned for its high appearance and grooming standards; however, it still recognizes the need for change. The Force Design 2030 Annual Update highlights the desire "to change the recruit and replace paradigm, implement measures to professionalize career retention, and further incentivize retaining talented Marines."[31] The U.S. Navy strongly desires to work with joint partners to build cyber-secure information technology systems. The 2022 Navigation Plan (NAVPLAN) states, "We owe it to our people to create an ecosystem that recruits and retains diverse and technically skilled personnel, educates them to out-think our adversaries, and trains them to work with new technologies."[32] Winning the next major war also requires domestic cyber protection. Over $54 million of the U.S. Coast Guard's fiscal year 2023 budget has been allocated to cybersecurity and command, control, communications, computers, combat systems, and intelligence (C5I).[33] "The

---

[29] U.S. Department of Defense. Accessed January 8, 2023. https://www.defense.gov/About/our-forces/#:~:text=The%20largest%20and%20oldest%20service,that%20protect%20the%20United%20States.

[30] Beynon, Steve, "The Army's Fitness Test Might Be Revamped Yet Again for Gender-Neutral and Job-Specific Standards", (December 7, 2022). https://www.military.com/daily-news/2022/12/07/armys-fitness-test-might-be-revamped-yet-again-gender-neutral-and-job-specific-standards.html

[31] Force Design 2030 Annual Update. Accessed January 8, 2023. https://www.marines.mil/Portals/1/Docs/Force_Design_2030_Annual_Update_May_2022.pdf (pg. 13).

[32] Chief of Naval Operations Navigation Plan 2022. Accessed January 8, 2023. https://media.defense.gov/2022/Jul/26/2003042389/-1/-1/1/NAVIGATION%20PLAN%202022_SIGNED.PDF (pg. 19, 22)

[33] "Taking the Helm: The Commandant's Vision for the U.S. Coast Guard", (July 14, 2022). https://www.congress.gov/117/chrg/CHRG-117hhrg49364/CHRG-117hhrg49364.pdf (pg. 11)

Coast Guard is committed to maritime border security, full participation in crisis response, and the protection of critical infrastructure, including in the cyber domain."[34] The U.S. cannot continue to allow individual services to maintain their missions while also trying to tackle a global cyber threat.

Additionally, the DoD cannot monetarily compete with the private sector and should focus on job satisfaction to help recruit and retain the necessary cyber talent. Every current branch of service is working independently to solve the problems with cyber talent recruitment and retention; however, these efforts need to be managed on a USCF scale versus being conducted through individual services. Single-service efforts assist with the short-term problem, but a sustainable solution should be the priority.

COUNTERARGUMENTS/RECOMMENDATIONS

Some may argue that creating an independent cyber force is too costly and unsustainable. Since the USSF was easier to develop from the USAF, it would be illogical to model that process for the USCF. "In a time of flat or declining Pentagon budgets, the notion that the department should create an entirely new service when interservice competition for resources is already fierce may seem an unaffordable luxury."[35] Each service will still have requirements for maintaining the existing command, control, communication, and computer (C4) systems. Each service still needs its cyber personnel to operate and maintain traditional information technology and communications requirements.

---

[34] "Taking the Helm: The Commandant's Vision for the U.S. Coast Guard", (pg. 10)

[35] Barno, David and Bensahel Nora, War on the Rocks: "Why the United States Needs an Independent Cyber Force." (May 4, 2021). https://warontherocks.com/2021/05/why-the-united-states-needs-an-independent-cyber-force/

To accomplish this feat, the recommendation is to capitalize on a program recently adopted by the USAF called Enterprise I.T. as-a-service (EITaaS). "The EITaaS program is meant to outsource basic I.T. services so that the Air Force can free up airmen for more specialized, cyber-focused network defense and mission assurance."[36] EITaaS is being implemented in two waves. Wave one includes working with civilian industry to implement best practices into the government, and wave two involves overhauling antiquated base infrastructure. EITaaS will free up uniformed personnel to focus on military support, reduce costs, and limit risk by optimizing technology, people, processes, and data interaction.[37] Each service should follow suit and adopt a similar approach to maintain service-specific I.T. systems.

Some may also argue that U.S. Cyber Command is sufficient to combat global cyber threats, and a dedicated USCF would be a redundant effort. The individual services have repelled adversarial cyber threats and continue to do so with the overarching guidance of the U.S. Cyber Command. The CNMF's mission is to defend the U.S. by operating as a joint force "through full-spectrum operations, including offensive, defensive, and information operations."[38] This construct enables interoperability and promotes joint service collaboration to utilize the strengths of each branch.

However, individual service efforts have proven futile and cannot stay current with the nation's pacing threat. The overarching mission to protect and defend the domain should not be conducted in stovepipes. AFCYBER, ARCYBER, MARFORCYBER, FLTCYBER should all

---

[36] Harper, Jon, Defense: "Air Force awards $5.7B contract for enterprise IT as a service". (August 31, 2022). https://www.fedscoop.com/air-force-awards-5-7b-contract-for-enterprise-it-as-a-service%ef%bf%bc/

[37] Peraton: "*Enterprise IT as a Service, Air & Space Force Mission Focus Starts with Enterprise IT.*" Accessed January 8, 2023. https://www.peraton.com/eitaas/

[38] U.S. Cyber Command. Accessed January 4, 2023. https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe/#.Y6EDPFyUDLg.linkedin

be consolidated to form the USCF. For example, in April 2021, the USAF removed the words' Space' and "Cyber' from its mission statement. According to sources, the term space was removed due to the momentum made after the enactment of the USSF. The term cyber was initially added to the USAF mission statement in 2005 due to the increased threats to the U.S.'s network security but was still later removed.[39]

Nevertheless, removing the terms did not remove the threats. Threats to the space domain are more prevalent than ever, and the USSF has a firm grasp on combatting those threats. That leaves a persistent threat in the cyber domain. Just as a dedicated service branch was established to create and maintain space superiority, the USCF should be enacted to develop and maintain dominance in the cyber domain. The Air Force Chief of Staff initiated these changes, so the Air Force [could] now focus solely on Airpower and maintain a sustained focus on core air domain missions. Other service branches can also be relieved of global protection in the cyber domain, with the sole responsibility being shifted to the USCF.[40] Combatting threats from China is not a problem that can spread throughout individual services with service-specific missions. As per the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, presents a growing influence threat, and is conducting operations worldwide."[41]

Others may contend that A.I. and automation cannot resolve recruiting and retention issues since these options are poor substitutes for human intelligence. A.I. and automation lack

---

[39] Pawlyk, Oriana, "Air Force Drops 'Space,' 'Cyber' from Mission Statement as Space Force Gains Momentum" (April 8, 2021), https://www.military.com/daily-news/2021/04/08/air-force-drops-space-cyber-mission-statement-space-force-gains-momentum.html

[40] Pawlyk, Oriana, "Air Force Drops 'Space,' 'Cyber' from Mission Statement as Space Force Gains Momentum" (April 8, 2021), https://www.military.com/daily-news/2021/04/08/air-force-drops-space-cyber-mission-statement-space-force-gains-momentum.html

[41] Cybersecurity & Infrastructure Security Agency. "China Cyber Threat Overview and Advisories", Accessed January 8, 2023. https://www.cisa.gov/uscert/china

the cognitive assessments required in combat, and this skill can only be found in humans. The military should reassess its recruiting and retention processes and focus less on technological advancements since A.I. is still in its infancy.

However, A.I. can compute faster and make judgments without emotion.[42] Discovering ways to streamline and effectively operate in the JIE with human assets has remained unresolved for over a decade. In fact, in 2013, the Chairman of the Joint Chiefs of Staff, Martin Dempsey, signed a whitepaper stating, "Globally integrated operations demands a far greater capacity to see, understand, operate in and defend cyberspace."[43] He later mentions, "JIE will allow better integration of information technologies, operations, and cyber security at a tempo that supports today's fast-paced operational conditions."[44] In modern warfighting areas, joint efforts are hindered by varying service branch goals, lack of collaboration, and limited resources. The responsibility to protect the entire cyber domain is too much to bear. Just as these sentiments were highlighted by the DoD Chief Information Office in 2016, the "DoD [still] stands at a crossroads facing a future I.T. environment that is fast-moving, connected, and highly contested."[45] The cyber threat that China poses spans beyond the traditional protection of hardware.

---

[42] Eliacik, Eray. Dataconomy. "Artificial intelligence vs. Human Intelligence: Can a Game-changing Technology Play the Game?" (April 20, 2022). https://dataconomy.com/2022/04/is-artificial-intelligence-better-than-human-intelligence/#:~:text=making%20better%20judgments%3F-,Is%20Artificial%20Intelligence%20better%20than%20Human%20Intelligence%3F,go%20unnoticed%20by%20a%20person.

[43] Dempsey, Martin. Joint Information Environment Whitepaper. (January 22, 2013). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjcs_wp_infoenviroment.pdf?ver=2017-12-28-162048-650

[44] Dempsey, Martin. Joint Information Environment Whitepaper. (January 22, 2013).

[45] Office of the Deputy DoD CIO for Information Enterprise. "*Additional Information about the Joint Information Environment (JIE)".* (July 2016). https://dodcio.defense.gov/Portals/0/Documents/JIE/Additional%20Info%20on%20the%20Joint%20Information%20Environment%20-%20DISTRO.pdf

The USCF would be responsible for protecting other aspects of the cyber domain, as highlighted by Frank Kendall, Secretary of the Air Force, "our personnel system, our medical system, our transportation system, our logistics system, [and] you have to think about all those things as well as all the weapons systems."[46] Kendall also expressed the importance of looking beyond traditional cyberattacks and focusing on disinformation's human influence.[47] These strengths, weaknesses, opportunities, and threats can be overcome and exploited with a consolidated USCF.

CONCLUSION

Cyber capabilities are the most potent weapons in the U.S.'s arsenal, and a dedicated force is needed to ensure they are appropriately utilized. The cyber domain impacts all other domains, and superiority in this domain will determine the winner of the Great Cyber Competition. Bad actors can use cyber to gain dominance in every instrument of national power: Diplomatic, Informational, Military, and Economic. The entity with the most cyber sovereignty can gain an advantage with diplomacy during negotiations. Disinformation can be used to alter the mind of citizens and damage civil infrastructure. Additionally, cyber can be used to infiltrate military communications and I.T. systems. A nation's economy can be jeopardized by damaging financial systems. "Often backed by adversaries, these cyberattacks threaten the United States and the rules-based order on which the global economy relies."[48] Whether overt or covert, the U.S. must take the necessary steps to reign supreme in cyber.

---

[46] Gordon, Chris, Air and Space Forces Magazine: *"Disinformation, Data Collection are Cybersecurity Concerns, Kendall Says"* (December 4, 2022). https://www.airandspaceforces.com/disinformation-data-collection-are-cybersecurity-concerns-kendall-says/

[47] Gordon, Chris, Air and Space Forces Magazine: *"Disinformation, Data Collection are Cybersecurity Concerns, Kendall Says"* (December 4, 2022). https://www.airandspaceforces.com/disinformation-data-collection-are-cybersecurity-concerns-kendall-says/

[48] Securing Defense-Critical Supply Chains. *"An action plan developed in response to President Biden's Executive*

Supporting the President's goals to enhance cybersecurity partnerships, out-compete China, and improve U.S. cyber resilience will require innovation and strategic planning. Deterring PRC aggression will necessitate unconventional methods by unconventional means. "Therefore, cybersecurity standards and enforcement mechanisms that recognize shared national interests need to be developed."[49] Winning the Great Cyber Competition will require integrated deterrence and the combination of capabilities via the USCF to convince China that hostile activity threatening global security will be futile. Individual service efforts should be consolidated to remain dominant in the cyber domain. Bottomline, the U.S. needs to enact the USCF as the final service branch to win the Great Cyber Competition with China.

Order 14017". (February 2022). https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF (pg. 55)

[49] Securing Defense-Critical Supply Chains. *"An action plan developed in response to President Biden's Executive (pg. 54)*

BIBLIOGRAPHY

Barno, David and Bensahel Nora, War on the Rocks: "Why the United States Needs an Independent Cyber Force." (May 4, 2021). https://warontherocks.com/2021/05/why-the-united-states-needs-an-independent-cyber-force/

Beynon, Steve, "The Army's Fitness Test Might Be Revamped Yet Again for Gender-Neutral and Job-Specific Standards," (December 7, 2022). https://www.military.com/daily-news/2022/12/07/armys-fitness-test-might-be-revamped-yet-again-gender-neutral-and-job-specific-standards.html

Chief of Naval Operations Navigation Plan 2022. Accessed January 8, 2023. https://media.defense.gov/2022/Jul/26/2003042389/-1/-1/1/NAVIGATION%20PLAN%202022_SIGNED.PDF

Cybersecurity & Infrastructure Security Agency. "China Cyber Threat Overview and Advisories," Accessed January 8, 2023. https://www.cisa.gov/uscert/china

Dempsey, Martin. Joint Information Environment Whitepaper. (January 22, 2013). https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cjcs_wp_infoenviroment.pdf?ver=2017-12-28-162048-650

Eliacik, Eray. Dataconomy. "Artificial intelligence vs. Human Intelligence: Can a Game-changing Technology Play the Game?" (April 20, 2022). https://dataconomy.com/2022/04/is-artificial-intelligence-better-than-human-intelligence/#:~:text=making%20better%20judgments%3F-,Is%20Artificial%20Intelligence%20better%20than%20Human%20Intelligence%3F,go%20unnoticed%20by%20a%20person.

Force Design 2030 Annual Update. Accessed January 8, 2023. https://www.marines.mil/Portals/1/Docs/Force_Design_2030_Annual_Update_May_2022.pdf

Gordon, Chris, Air and Space Forces Magazine: *"Disinformation, Data Collection are Cybersecurity Concerns, Kendall Says"* (December 4, 2022). https://www.airandspaceforces.com/disinformation-data-collection-are-cybersecurity-concerns-kendall-says/

Harper, Jon, Defense: "Air Force awards $5.7B contract for enterprise I.T. as a service". (August 31, 2022). https://www.fedscoop.com/air-force-awards-5-7b-contract-for-enterprise-it-as-a-service%ef%bf%bc/

Kannan, Saikiran and Bhalla, Abhishek, "Inside China's cyber war room: How PLA is plotting global attacks," *India Today*, August 6, 2020, https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06

Klevering, Griffin, "A Brief Look at Chinese Cyberwarfare," *Small Wars Journal* (January 26, 2022), https://smallwarsjournal.com/jrnl/art/brief-look-chinese-cyberwarfare

Lawrence, Drew. "Troops Are Getting Cyber Training and Then Rapidly Leaving the Military, Report Finds." *Military.com,* Accessed January 5, 2023. https://www-military-com.cdn.ampproject.org/c/s/www.military.com/daily-news/2022/12/27/troops-are-getting-cyber-training-and-then-rapidly-leaving-military-report-finds.html/amp

Marks, Joseph and Schaffer, Aaron, "The U.S. Isn't Getting Ahead of the Cyber Threat, Experts Say," The Cybersecurity 202 (January 6, 2022), https://www.washingtonpost.com/politics/2022/06/06/us-isnt-getting-ahead-cyber-threat-experts-say/

"Military size by country 2023," World Population Review, accessed January 2, 2023, https://worldpopulationreview.com/country-rankings/military-size-by-country

National Defense Strategy, Washington, D.C., *(2022),* https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

National Security Strategy, Washington, D.C.: *Office of Homeland Security, (October 12, 2022),* https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Office of the Deputy DoD CIO for Information Enterprise. "*Additional Information about the Joint Information Environment (JIE).*" (July 2016). https://dodcio.defense.gov/Portals/0/Documents/JIE/Additional%20Info%20on%20the%20Joint%20Information%20Environment%20-%20DISTRO.pdf

Pawlyk, Oriana, "Air Force Drops' Space,' 'Cyber' from Mission Statement as Space Force Gains Momentum" (April 8, 2021), https://www.military.com/daily-news/2021/04/08/air-force-drops-space-cyber-mission-statement-space-force-gains-momentum.html

Peraton: "*Enterprise I.T. as a Service, Air & Space Force Mission Focus Starts with Enterprise I.T.*" Accessed January 8, 2023. https://www.peraton.com/eitaas/

Securing Defense-Critical Supply Chains. *"An action plan developed in response to President Biden's Executive Order 14017".* (February 2022). https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

"Taking the Helm: The Commandant's Vision for the U.S. Coast Guard" (July 14, 2022). https://www.congress.gov/117/chrg/CHRG-117hhrg49364/CHRG-117hhrg49364.pdf

"Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors," *Cybersecurity and Infrastructure Security Agency*, October 6, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

U.S. Air Force Careers. Accessed January 8, 2023. https://www.airforce.com/careers/pay-and-benefits/enlistment-bonuses

U.S. Cyber Command. Accessed January 4, 2023. https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe/#.Y6EDPFyUDLg.linkedin

U.S. Department of Defense. Accessed January 8, 2023. https://www.defense.gov/About/our-forces/#:~:text=The%20largest%20and%20oldest%20service,that%20protect%20the%20United%20States

United States Space Force History. Accessed January 4, 2023. https://www.spaceforce.mil/About-Us/About-Space-Force/History/#:~:text=The%20establishment%20of%20the%20USSF,superiority%20in%20the%20space%20domain