Kybernao

Steering Toward the Nexus of Cyber Theory and Policy

The Advantage Gained:

Building on USCYBERCOM-NSA's "Dual Hat" Synergy Model

Jason Blessing, PhD and

Richard J. Harknett, PhD

University of CINCINNATI | CENTER FOR CYBER STRATEGY AND POLICY

Issue 2 February 2022

About the Authors

Dr. Jason Blessing is a Jeane Kirkpatrick Visiting Research Fellow at the American Enterprise Institute. He has previously held positions as a Consulting Fellow with the International Institute for Strategic Studies, a Postdoctoral Fellow at the Johns Hopkins University School of Advanced International Studies, and a USIP–Minerva Peace and Security Scholar with the U.S. Institute of Peace. Outside academia, Jason has worked in the financial sector as a fraud operations analyst. His research focuses on international relations and cybersecurity, civilian-military dynamics in cyberspace, cyber strategy, and topics related to NATO and transatlantic relations.

Dr. Richard Harknett is professor and Director of the School of Public and International Affairs at the University of Cincinnati. He co-directs the Ohio Cyber Range Institute and chairs the Center for Cyber Strategy and Policy. Professor Harknett has served as the inaugural scholar-in-residence at US Cyber Command and NSA and Fulbright Scholar at the University of Oxford, UK and the Diplomatic Academy, Austria. His published work covers international relations theory, cyber and international security studies.

Introduction

The "dual hat" leadership model between United States Cyber Command (USCYBERCOM) and the National Security Agency (NSA) – where one individual simultaneously serves as the Commander of USCYBERCOM and the Director of the NSA – has evolved into a critical asset to advance the interests of the United States in cyberspace. The United States established this synergistic model of leadership, in which the same military officer oversees the nation's cryptologic and cyber operations portfolios, in 2004 as the national security implications of cyberspace began to emerge.[1] This essay explains why the advantages gained through this distinct leadership model create operational effectiveness that is of strategic importance to the United States.

The United States established this synergistic model of leadership, in which the same military officer oversees the nation's cryptologic and cyber operations portfolios, in 2004 as the national security implications of cyberspace began to emerge.

This operationally driven arrangement predates the formal creation of USCYBERCOM by approximately six years. Despite this fact, arguments for ending the dual hat and creating separate leadership structures have periodically surfaced since USCYBERCOM's emergence in 2010.[2] A recent example includes the House of Representative version of the Fiscal Year 2022 Intelligence Authorization Act (IAA), which proposed to remove operational effectiveness as a critical assessment criterion. It had suggested that USCYBERCOM and the NSA need only meet certain capability conditions before initiating a new model of splitting responsibilities with two separate leaders.[3]

Removing measures of effectiveness from any policy consideration seems generically problematic. In this instance, such an approach would be a grave error that ignores the evolution of both the cyber threat environment and the USCYBERCOM-NSA operational relationship. In short, the relationship is not characterized by military reliance on the intelligence agency or by the borrowing of respective capabilities. Operational integration has occurred and evolved into a symbiotic relationship where both USCYBERCOM and the NSA both act effectively due to greater synergy. Moreover, lessons learned about achieving operational effectiveness have reshaped the nature and importance of the USCYBERCOM-NSA relationship and leadership model. Given the significance of securing cyberspace for U.S. interests, it is critical to understand how the dual-hatted leadership model fosters the USCYBERCOM-NSA relationship and confers strategic advantages to U.S. efforts.

We propose that, in the cyber strategic environment of 2022, the United States should focus on bolstering the operational effectiveness that has emerged from the intertwining of USCYBERCOM and the NSA. Both organizations have learned to advance their respective and complementary missions, and the dual hat arrangement has helped to maximize cooperation and to balance each organization's interests.

Thus, the United States should focus on building upon the dual hat as a linchpin for maximizing synergies between military and intelligence equities in an increasingly complex and interconnected operating environment. This requires understanding the on-the-ground organizational opportunities and contextualizing them within broader strategic trends that have occurred. Separating the dual hat now would be major strategic folly and a gift to adversaries who exploit the seams of U.S. segmentation in organizations and legal authorities. While capability standards are indeed crucial for both USCYBERCOM and the NSA, operational effectiveness in cyberspace must take center stage to support and advance U.S. national security interests.

The Challenges of the Cyber Strategic Landscape

The organizational intertwining of USCYBERCOM and the NSA is catching-up to a cyber threat environment that has evolved rapidly over the past ten years. That threat environment has become increasingly complex due to its interconnected nature. U.S. adversaries have been persistent in cyberspace, actively seeking to exploit vulnerabilities to advance their own interests. There are two major trends worth highlighting in this regard.

First, the cyber landscape has seen a proliferation of adversaries for the United States. This includes an increase in the number of formal and more capable military and intelligence cyber forces among state actors,[4] particularly adversarial states; persistence of terrorist groups online; and the emergence of criminal/ransomware groups as a national security threat. The sheer number of potential adversaries and attempted intrusions into U.S. networks, both military and civilian, is staggering. This presents an increasingly massive challenge for cyber defense efforts. The proliferation of adversaries also taxes U.S. efforts to simultaneously regain the cyber initiative and disrupt adversary campaigns. More potential targets require greater amounts of time, resources, personnel, and expertise to monitor and counteract.

Second, and perhaps more concerning, is the increased scope and scale at which adversaries operate. State actors such as Russia, Iran, North Korea, and China have dedicated more resources and capability to undertake and sustain long-term cyber exploitation. This increases the likelihood that these adversaries can maintain operational momentum and link cyber campaigns towards strategic outcomes.[5] Russia, Iran, North Korea, and China's increased scale and scope leverages the fact that they operate with little distinction between intelligence and military activities in cyberspace. For example, they are able to amplify interrelated efforts under the broad umbrella of cyber-enabled information operations.[6]

Additionally, these adversaries have diversified their operational portfolios. Russian operations have expanded in several ways. No longer limited to attempting targeted compromises of sensitive networks (such as via the agent.btz worm to infect DoD networks in 2008[7]), Russian operations now encompass the deployment of wiperware and ransomware, online election interference and influence operations to fray the fabric of U.S. society as well as compromising different elements of U.S. supply chains. As examples, two impactful operations include the NotPetya wiperware-masquerading-as-ransomware incident of 2017[8] and the more recent Solarwinds campaign that built on and improved upon the methods used for NotPetya.[9] Chinese cyber operations against the United States have similarly evolved from a focus on more narrow goals like intellectual property theft – for instance, stealing fighter jet plans from U.S. defense contractor Lockheed Martin[10] – to more widespread and, indeed reckless, efforts like the Microsoft Exchange exploitation.[11] Iranian capabilities continue to grow[12] and North Korea has continued its manipulation of digital financial streams to circumvent international sanctions.[13]

The public record indicates that adversaries are conducting cyber operations below the threshold of armed attack to undermine American power and achieve strategic gains. This has increased the importance of USCYBERCOM's Defend-the-Nation mission and the NSA's cybersecurity mission.[14] This evolving strategic cyber landscape has also made it increasingly clear that conflict and competition in cyberspace now require an unprecedented level of cross-capability collaboration that leverages the strengths of both military and intelligence organizations. Building on this interrelationship of military and intelligence cyber assets is critical as the *National Security Strategy of the United States* and *National Defense Strategy*, and the Biden Administration's interim national security guidance recognize that the United States is now in a period of great power competition in which cyberspace is being used to undermine American power and make strategic gains.[15]

This evolving strategic cyber landscape has also made it increasingly clear that conflict and competition in cyberspace now require an unprecedented level of cross-capability collaboration that leverages the strengths of both military and intelligence organizations.

Accordingly, in 2019 USCYBERCOM publicly stated it had moved from a "response force" to a "persistence force" that was more proactive in countering threats.[16] The NSA also launched its new Cybersecurity Directorate in 2019, which similarly reflected a new front-footed orientation of continuous engagement in cyberspace.[17] These shifts help align the two organizations not only to the logic of the cyber strategic environment itself, but also to the behavior of adversaries. If the goal is to enhance U.S. national security in the

globally interconnected cyber environment, then it would be a gift to our adversaries—indeed strategic folly—to divide two critical organizations into a new segmented leadership. It would be particularly detrimental as progress in operational effectiveness is gaining muscle memory.

Shifting from a Transition Mentality to a Synergy Orientation

These adjustments to the strategic nature of cyberspace have occurred as the United States has gained, absorbed, and built upon operational experience under the dual hat. As noted in our introduction, the dual hat leadership arrangement pre-dated the creation of USCYBERCOM by six years due to the recognition that operating in this domain required coordination between cryptologic activity and cyber operations. This dual leadership arrangement has enabled an effective way for the military to leverage NSA infrastructure, select capabilities, personnel, and expertise as the Department of Defense matured its capabilities in cyberspace. However, it is not simply the presence of those capabilities that matters—it is how they are employed operationally in a complex interconnected environment.[18] The dual hat model certainly was essential as a steward of USCYBERCOM's infancy and maturation. Yet today it should be understood in the context of its broader role that is operationally aligned to the domain upon which it must focus. It is, empirically, a linchpin for overseeing and leveraging resources and strategic connections across cybersecurity, intelligence, and military cyber operations and for maximizing integrated outcomes and effects.

USCYBERCOM's own organizational capacity has increased over time as the NSA's mission has evolved beyond Cold War cryptology toward cybersecurity. These evolving and critical developments in both organizations have progressed under the dual hat. Such developments include: USCYBERCOM's elevation to unified command status beyond its original structure under US Strategic Command;[19] the creation of the NSA's Cybersecurity Directorate; the Command's employment of acquisition authorities analogous to those of Special Operations Command—another entity that must be able to have accelerated procurement to meet rapidly changing mission requirements;[20] and an expanded force capacity in the form of the size, execution of mission, and skills of the Cyber Mission Force (CMF).[21]

Concomitantly, USCYBERCOM's process of organizational maturation has enabled its relationship with the NSA to better map to the initiative persistent strategic environment of cyberspace.[22] The original intent of the relationship in 2004 was for military cyber operations to benefit from close association with the NSA's infrastructure, capabilities, and intelligence. Yet, as USCYBERCOM's capacity has developed over time, its partnership with the NSA has deepened into a symbiotic and mutually beneficial arrangement.

A key dynamic underlying this organizational shift is the convergence of technical and operational requirements for military and intelligence cyber operations over time. These changes have effectively collapsed the "military as customer of intelligence" relationship, a stereotype that was never more than superficially accurate in the first place (because the military has always been a key contributor to intelligence).

In the conventional and nuclear realms – the strategic environments of militarized crises, coercion, and war – intelligence and military organizations differ in terms of their strategic ends and requirements for operational effectiveness. Traditionally, intelligence effectiveness hinges on the employment of fragile and often clandestine and tailored capabilities for collecting information. Conversely, military effectiveness hinges on sustained operations at-scale and usually on the production of visible effects and coercive signals as well.[23]

However, these dynamics differ in the cyber strategic environment, where almost all operations and campaigns occur below the threshold of armed conflict and take the form of strategic competition. While the different strategic ends of intelligence collection and military operations persist to a degree, the operational requirements for effectiveness have converged. Cyber-enabled intelligence collection can be nearly indistinguishable from preparation of the digital battlefield operationalized as planting disruptive payloads such as malware, for example. Both efforts require similar lines of code that can be developed, shared, and used for gaining access to an adversary network.[24] Both attacking a network and defending one's own can require collecting intelligence by exploiting an adversary's cyber vulnerabilities.[25]

While the different strategic ends of intelligence collection and military operations persist to a degree, the operational requirements for effectiveness have converged.

Military and intelligence effectiveness in the cyber domain thus rest on exploitation and a fluid setting and resetting of security through continuous operations on computing networks.[26] Overall U.S. effectiveness in cyberspace therefore requires the ability to shift seamlessly between intelligence collection goals and military operational effects and between respective organizational assets. In this sense, a single military commander and intelligence director is a linchpin for overseeing and leveraging the resources and connections between military cybersecurity, intelligence, and military cyber operations.

Instead, the dual hat model has fostered a 'synergy' orientation between the two organizations that seeks to persistently engage in sustaining initiative rather than ceding it to adversaries.

The effective and increasingly intertwined relationship between USCYBERCOM and NSA, which rests on a common leadership model, has moved the United States beyond a false 'tradeoff' mentality in cyberspace. Instead, the dual hat model has fostered a 'synergy' orientation between the two organizations that seeks to persistently engage in sustaining initiative rather than ceding it to adversaries.[27] This level of convergence, while retaining organizationally distinct expertise, would be impossible under a split leadership structure. This synergy orientation reinforces (and is reinforced by) the avoid-

ance of duplication of resources. It aligns both organization's effectiveness for combined impact, prevents a diffusion of strategic focus, and enables coordination to achieve the speed, scale, and unity of effort required to retain the initiative in securing cyberspace to advance U.S. interests. One example of this convergence is the NSA's Cybersecurity Directorate, which elevated cybersecurity as a mission and naturally aligned with USCYBERCOM's defensive missions.

The Way Forward with the Dual Hat

Cyberspace is evolving and there remains much to learn, but the United States should recognize what it has learned to date. Decisions on capabilities, organizational models, authorities, and strategy should be based first and foremost on measures of operational effectiveness. Interconnectedness, the core structural feature of the cyber strategic environment, demands continuous, integrated campaigning. Effectiveness in these conditions requires that operational players continuously collaborate, integrate, and synchronize across all relevant stages of cyber planning.

The United States is finally clawing back the initiative in cyberspace against its adversaries, in part, because it is leveraging the integrated leadership of two vitally important organizations under one military commander. As the Biden Administration's National Cyber Director John "Chris" Inglis recently pointed out, "cyber is a team sport."[28] The dual hat position can get the best out of both the NSA and USCYBERCOM by building out respective expertise while finding focal points to maximize their skills in parallel and combined operations. It is actually the best model for protecting the uniqueness of both organizations. A single commander/director can understand, filter, and advocate for their distinct contributions at the operational level. As a result, a dual-hatted leader can manage and leverage the two organizations' necessarily close relationship to focus on the best synergistic outcomes required for successful mission advancement.

The dual hat leadership model also more efficiently facilitates building interagency team coordination, as was the case with the Russia Small Group taskforce, a joint effort between USCYBERCOM-NSA and the FBI, DHS and CIA.[29] This USCYBERCOM-NSA operational synergy enhances the capacity to partner across the U.S. Government. Segmentation would introduce unnecessary complication to this endeavor. The U.S. "team" effort must also include coordination with allies since countering cyber campaigns requires operational synergy across allied expertise and space. Key U.S. allies have been moving toward greater coordination across their cyber assets, not less.[30] Having a single dual-hatted cryptologic and military cybersecurity leader in the largest allied cyber power works in favor of achieving operational effectiveness by reducing the complexity of working together across countries. From an ally perspective, breaking the dual hat would introduce significant disruption and unnecessary complexity to working with the United States that thankfully does not exist now.

It should also be noted that the military nature of this combined leadership position adds a layer of legal obligations under the Law of Armed Conflict, particularly in accountability for upholding civil liberalities and privacy. Confidence on accountability is a key element in sustaining the necessary public acceptance and trust

for any set of organizations so intimately involved with global networks and Big Data.

Given the operational integration that has occurred between USCYBERCOM and the NSA and the increasing complexity of the cyber landscape, Congress and the Biden Administration should lean forward rather than look backwards and focus on building up the utility of the dual hat.

Several areas for greater strengthening stand out. First, the United States needs to build greater cyber capability and capacity into other combatant commands. This will simultaneously require better integration of USCYBERCOM's tools into other commands while considering the impact on NSA effectiveness. This will be a complex evolution of U.S. overall capacity to compete in cyberspace and will be facilitated through having a single leader, who oversees the core dual operational anchor, in place to facilitate partnering with combatant commands.

Second, the United States must leverage the dual hat to facilitate greater coordination between the Intelligence Community and the Department of Defense overall. The interconnected structure of the cyber strategic environment requires continuous integrated campaigning supported by continuous collaboration, integration, and synchronization, across all relevant cyber planning and operational players and all instruments of national power. Building toward these ends by building on the dual hat model can give the United States an advantage over its adversaries, whose own bureaucratic seams should become targets of opportunity for the United States.

Building toward these ends by building on the dual hat model can give the United States an advantage over its adversaries, whose own bureaucratic seams should become targets of opportunity for the United States.

Third, a focus on synergy drawn from the dual hat model can also act as a springboard for wider intra-government cooperation and maximizing threat intelligence relationships with the private sector. Both are vital to create a true Whole-of-Nation-Plus solution to cyberspace insecurity.

Conclusion

Cyber policy, legal, and organizational frameworks should enable cyber operational persistence, agility, and initiative. A quick test policymakers should use in cyber-related policy decisions is to always ask, 'Does this policy create greater synergy or segmentation?' and choose solutions that favor synergy. Policy must be driven by strategic need, not by bureaucratic perspectives or in-fighting. When the United States created the dual hat leadership model eighteen years ago, it might not have fully understood the strategic challenges and dynamics of cyberspace or the significance of coupling cryptologic and cyber operations portfolios. However, that decision is perhaps one of the most important things the United States got right as cyberspace has emerged as a national security domain. It is time to build on this success and emphasize its strengths instead of creating an unforced error and unnecessarily giving away the fundamental advantages that it facilities.

Endnotes

1 The dual-hatted military element at the time would soon (in 2005) be renamed the Joint Functional Component Command—Network Warfare, whose three-star chief served as Director, NSA, and also reported to Commander, US Strategic Command. See Michael Warner, "US Cyber Command's First Decade," Hoover Institution, Aegis Series Paper No. 2008, December 2020, p.4; https://www.hover.org/sites/default/files/research/docs/warner_webready.pdf

2 For example, see: Robert Chesney, "Ending the 'Dual-Hat' Arrangement for NSA and Cyber Command?," *Lawfare*, December 20, 2020, https://www.lawfareblog.com/ending-dual-hat-arrangement-nsa-and-cyber-command.

3 Adam B. Schiff, "Intelligence Authorization Act for Fiscal Year 2022," Pub. L. No. H.R.5412 (2021), https://www.congress.gov/bill/117th-congress/house-bill/5412/text?r=34&s=1#HF6C-C5370EB1C432D85D810658656B80F.

4 Jason Blessing, "The Global Spread of Cyber Forces, 2000-2018," in *2021 13th International Conference on Cyber Conflict,* ed. T. Jančárková et al. (Tallinn, Estonia: NATO CCDCOE Publications, 2021), 233–55, https://ccdcoe.org/uploads/2021/05/CyCon_2021_Blessing.pdf

5 Richard Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes: The Other Means," *Journal of Strategic Studies* DOI: 10.1080/01402390.2020.1732354 (Spring 2020):1-34.

6 See, Mark Grzegorzewski and Christopher Marsh, "Incorporating the Cyberspace Domain: How Russia and China Exploit Asymmetric Advantages in Great Power Competition," Modern War Institute-West Point (March 15, 2021) https://mwi.usma.edu/incorporating-the-cyberspace-domain-how-russia-and-china-exploit-asymmetric-advantages-in-great-power-competition/.

7 Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 180–82; James A. Lewis, "Managing New Style Warfare: An Interview with Keith Alexander," Cyber From the Start, https://www.csis.org/podcasts/cyber-start.

8 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *WIRED*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/#.

9 Marcus Willett, "Lessons of the SolarWinds Hack," *Survival* 63, no. 2 (May 2021): 7–26, https://www.iiss.org/blogs/survival-blog/2021/04/lessons-of-the-solarwinds-hack; Richard Harknett,

Endnotes

"SolarWinds: The Need for Persistent Engagement," *Lawfare* (December 2020) https://www.lawfareblog.com/solarwinds-need-persistent-engagement

10 Peter Suciu, "China's New Stealth Fighter: Built From Stolen F-22 and F-35 Technology?," *1945*, September 25, 2021, https://www.19fortyfive.com/2021/09/chinas-new-stealth-fighter-built-from-stolen-f-22-and-f-35-technology/.

11 Dina Temple-Raston, "China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying," *National Public Radio,* August 26, 2021, https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying.

12 JD Work and Richard Harknett, "Troubled Vision: Understanding Recent Israeli-Iranian offensive cyber exchanges," *Issue Brief,* Atlantic Council Scrowcroft Center for Strategy and Security (July 2020): 1-12 https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/troubled-vision-understanding-israeli-iranian-offensive-cyber-exchanges/.; Catherine A. Theohary, "Iranian Offensive Cyber Attack Capabilities" (Washington, D.C.: Congressional Research Service, January 13, 2020), https://sgp.fas.org/crs/mideast/IF11406.pdf

13 Associated Press, "UN Experts: North Korea Stealing Millions in Cyber Attacks," *U.S. News & World Report,* February 6, 2022, https://www.usnews.com/news/world/articles/2022-02-06/un-experts-north-korea-seeks-to-produce-material-for-nukes.

14 Mark Pomerleau, "Cyber Command Task Force Focuses on Emerging Threats," *C4ISRNET*, March 8, 2021, https://www.c4isrnet.com/cyber/2021/03/08/cyber-command-task-force-focuses-on-emerging-threats/#:~:t

15 Joseph R. Biden, *Interim National Security Strategic Guidance* (White House, March 2021) https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

16 Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly,* January 2019.

17 Tom Temin, "NSA's Cyber Directorate Marks a Year in Operation," Federal News Network, February 3, 2021, https://federalnewsnetwork.com/cybersecurity/2021/02/nsas-cyber-directorate-marks-a-year-in-operation/

Endnotes

18 Jason Blessing, "The Diffusion of Cyber Forces; Military Innovation and the Dynamic Implementation of Cyber Force Structure" (Dissertation, Syracuse, NY, Syracuse University, 2020), 158–60, https://surface.syr.edu/etd/1190/.

19 U.S. Cyber Command, "U.S. Cyber Command History," accessed February 8, 2022, https://www.cybercom.mil/About/History/.

20 Mark Pomerleau, "US Cyber Command Touts Acquisition Advancements," *C4ISRNET*, July 27, 2021, https://www.c4isrnet.com/cyber/2021/07/27/us-cyber-command-touts-acquisition-advancements/.

21 United States Department of Defense, "Cyber Mission Force Achieves Full Operational Capability," May 17, 2018, https://www.defense.gov/News/News-Stories/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/; Mark Pomerleau, "Will the Cyber Mission Force Soon Receive More Personnel?," *C4ISRNET*, May 14, 2021, https://www.c4isrnet.com/cyber/2021/05/14/will-the-cyber-mission-force-soon-receive-more-personnel/.

22 Michael Fischerkeller and Richard Harknett, "Initiative Persistence as the Central Approach for US Cyber Strategy," *Kybernao* Issue 1 (July 2021): 1-29, https://www.artsci.uc.edu/content/dam/refresh/artsandsciences-62/departments/political-science/ccsp/pdf_downloadableflyers/Kybernao_PaperSeries_Issue1_Final.pdf

23 For a brief overview of these dynamics, see: Thomas Bruneau, "A Conceptual Framework for the Analysis of Civil-Military Relations and Intelligence," Defense & Security Analysis 34, no. 4 (2018): 345–64.

24 Michael P. Fischerkeller and Richard J. Harknett, "Cyber Persistence Theory, Intelligence Contests, and Strategic Competition," Texas National Security Review: Special Issue – Cyber Competition, September 17, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

25 Benjamin Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (Oxford: Oxford University Press, 2017)

26 On the structural imperative and strategic incentive to persist in exploitation and fluid re-

Endnotes

setting of cyber conditions, see Michael Fischerkeller, Emily Goldman and Richard Harknett, *Cyber Persistence: Redefining national security in cyberspace*, (UK: Oxford University Press, forthcoming, 2022).

27 Richard Harknett, "United States Cyber Command's New Vision: What it Entails and Why it is Important," *Lawfare* (March 2018). https://lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters

28 Inglis, Chris. Twitter Post. January 12, 2022, 3:48 PM, https://twitter.com/ncdinglis/status/1481367378835484678

29 Shannon Vavra, "NSA's Russia cyberthreat task force is now permanent," *Cyber Scoop* (April 29, 2019) https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/

30 For example, the UK Government announced, "In March 2021 the UK published its Integrated Review (IR) of Security, Defence, development and Foreign Policy, representing a significant shift in our posture towards persistent global engagement and constant campaigning. The UK will be more proactive, adaptable, and integrated with its partners to compete with adversaries, strengthen deterrence, and improve the ability to intervene and fight decisively." https://www.gov.uk/government/collections/the-integrated-review-2021.

About

Kybernao seeks to publish academic-based research applied to real-world policy and strategy questions. These short pieces (2500-8000) will be published on an occasional basis as an Issue Briefing/Policy Briefing with the goal of connecting academics with policymakers to improve security in cyberspace.

Kybernao is the Greek verb "to steer" (κυβερνάω, the first person singular present). The Greek noun for "steersmen" or "helmsman" is kybernetes (κυβηρνήτης), which many point to as the etymology behind the term cyber as it related to the concept of cybernetics, which focused on the relationship between communication and automatic control systems of both machines and humans.

Our image is inspired from ancient Greek pottery and depicts the guide navigating by the contours of the network (stars) through the core code that both serves as the terrain of cyberspace (seas) and the way one moves across the network.

The Center for Cyber Strategy and Policy (CCSP) image captures the challenge of securing cyberspace. The use of chess pieces is to emphasize the notion of strategy. The multiplying knights depicts the ever-changing character of malware that can morph into new versions and take advantage of new vectors for exploitation of vulnerabilities. The shadows depict the ever-present opportunity to leverage uncertainty regarding network intrusion, intruder, an intruder's intent, the scale and scope of a campaign, and even the game being played (perhaps you are playing GO instead of chess)--you may think you are playing against the knight and can anticipate those moves, when in fact you are playing against a bishop with very different operational capabilities and potential for strategic gain. The defeated pawn acknowledges the potential to win and lose in cyberspace (note that a draw is possible in chess, Go, and in cyberspace).

For more on the CCSP visit our website
For inquiries about the Kybernao series or CCSP in general, contact: cyberstrategy@uc.edu