INSTITUTE FOR DEFENSE ANALYSES

What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?

Michael P. Fischerkeller, Project Leader

April 2022

IDA Non-Standard D-33077

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project C5224, "Review and Editorial Prep for Non-sponsored Articles and Essays for External Publication," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Dr. Emily Goldman (NSA), Dr. Michael Warner (CYBERCOM), Dr. J.D. Work (National Defense University)

For More Information

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

Rigorous Analysis | Trusted Expertise | Service to the Nation

What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?

Michael P. Fischerkeller

The two-page fact sheet summarizing the 2022 National Defense Strategy (NDS) is notable when considered from a cyberspace strategy perspective.[1] Identifying campaigning as one way to advance Department of Defense (DoD) goals is consistent with lessons learned employing the doctrine of persistent engagement for operating in and through cyberspace. Additionally, three of NDS's campaigning objectives—to gain advantages against the full range of competitors' coercive actions, undermine acute forms of competitor coercion, and complicate competitor's military preparations—could be supported by persistent engagement. Further, although a fourth objective mentioned in the NDS fact sheet—resilience—is not listed as an objective of campaigning, persistent engagement has demonstrated that campaigning is critical to supporting anticipatory resilience in cyberspace, including ongoing efforts such as the use of hunt forward teams to inoculate the U.S. public and private sectors from malicious cyber activity. *In toto*, such cyber campaigns support integrated deterrence by undermining an opponent's confidence that they will prevail in crisis or armed conflict. As the forthcoming cyber strategy is to be nested within the NDS, we should anticipate it supporting these same objectives. This essay elaborates on each from a cyber strategy perspective and offers an additional objective unique to cyberspace—precluding exploitation and/or inhibiting the cumulation of strategic gains in and through cyberspace that can independently influence the international distribution of power.

Campaigning

The 2022 NDS fact sheet recognizes that a comprehensive national strategy intending to achieve security across the full spectrum of strategic competition must include strategic approaches for (integrated) deterrence and defense/resilience, as well as an approach that embodies initiative persistence (campaigning).[2] Shortly after assuming command at U.S. Cyber Command (USCYBERCOM), General Paul Nakasone described the need for a "cyber persistence force," rather than a "response force" to address the cyber strategic campaigns short of armed conflict through which U.S. opponents are reaping strategic political, economic, and military gains.[3] Persistent engagement, USCYBERCOM's doctrine, reflects an understanding that one-off cyber operations are unlikely to deter or defeat adversaries. Nakasone argues instead that U.S. cyber forces must compete with opponents on a recurring basis, making it far more difficult for them to advance their goals over time.[4] Persistent campaigning that seizes and maintains the initiative in and through cyberspace is the primary way to achieve security in and through the same. The

---

[1] *U.S. Department of Defense, Fact Sheet: 2022 National Defense Strategy*, https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF.

[2] Michael P. Fischerkeller and Richard J. Harknett, "Initiative Persistence as the Central Approach for US Cyber Strategy," *Kybernau* 1, no. 1 (August 2021), https://www.artsci.uc.edu/content/dam/refresh/artsandsciences-62/departments/political-science/ccsp/pdf_downloadableflyers/Kybernao_PaperSeries_Issue1_Final.pdf.

[3] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Forces Quarterly* 92, (1st quarter, 2019): 10-14, 12.

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

NDS's focus on campaigning to ensure favorable conditions in strategic competition may actually be a lesson learned from USCYBERCOM.

Targeting Coercive Activities

Cyber campaigning can address the full range of opponent's coercive actions, including day-to-day strategic competition from states—China, Russia, Iran, and North Korea—that employ coercive methods short of war.[5] This includes "gray-zone" challenges, which are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks.[6]

China's gray zone tactics in the South China and East China seas involve military and non-military coercion to achieve strategic goals without provoking armed conflict.[7] The U.S. challenged China's claim to an East China Sea air defense identification zone (ADIZ) in 2013 with unannounced military sorties through it.[8] In 2020, the *USS America*—a small carrier equipped with a handful of F-35 jets, helicopters, and a contingent of U.S. Marines—patrolled in close proximity to a Chinese maritime force that was trying to intimidate and disrupt Malaysia's energy exploration activities and coerce Southeast Asian littoral states into accepting joint development with China.[9] However, U.S. responses to China's gray zone tactics need not be limited to the air and maritime domains. The extraordinary breadth of China's activities presents opportunities for developing cyber campaigns that could disrupt ongoing coercive tactics or degrade the value or functionality of gains realized to-date in contested zones. Indeed, in recent testimony to the Senate Armed Services Committee, General Nakasone acknowledged the formation of a "China Outcomes Group"—a joint Cyber Command and NSA task force—to

---

[5] Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning*, March 16, 2018, 2, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

[6] For discussions of gray zone challenges, see *General Joseph L. Votel, Statement before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, March 18, 2015; https://docs.house.gov/meetings/AS/AS26/20150318/103157/HMTG-114-AS26-Wstate-VotelUSAJ-20150318.pdf; Joseph L. Votel, Charles T. Cleveland, Charles T. Connett, and Will Irwin, "Unconventional Warfare in the Gray Zone*," Joint Forces Quarterly* (80:1, 2016), pp. 101–109, https://ndupress.ndu.edu/Publications/Article/643108/unconventional-warfare-in-the-gray-zone/; Captain Philip Kapusta, "Defining Gray Zone Challenges," April 2015; http://www.soc.mil/swcs/ProjectGray/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf; Captain Philip Kapusta, "The Gray Zone," *Special Warfare*, October – December 2015), pp. 18–25, https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf; and, David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone,'" *War on the Rocks*, May 2015; https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/

[7] Peter Layton, *China's Enduring Grey Zone Challenge* (Air and Space Power Centre, Commonwealth of Australia, 2021), https://airpower.airforce.gov.au/publications/chinas-enduring-grey-zone-challenge.

[8] Ian E. Rinehart and Bart Elias, *China's Air Defense Identification Zone (ADIZ)* (Washington, DC: Congressional Research Service, January 30, 2015), https://sgp.fas.org/crs/row/R43894.pdf.

[9] Euan Graham, "U.S. Naval Standoff With China Fails to Reassure Regional Allies," *Foreign Policy*, May 4, 2020, https://foreignpolicy.com/2020/05/04/malaysia-south-china-sea-us-navy-drillship-standoff/.

ensure "proper focus, resourcing, planning, and operations" to counter Beijing's rising global influence, coercive or otherwise.[10]

In the cyber context, acute forms of competitor coercion referenced in the NDS fact sheet are akin to ransomware holding critical infrastructure at risk. USCYBERCOM, in a coordinated effort with the FBI and an unidentified third country, reportedly engaged in a limited campaign to disrupt the REvil ransomware group in November 2021.[11] Concerns regarding nations hosting ransomware groups and implicitly condoning their behaviors have fed forecasts that the groups or their capabilities could be co-opted by states wanting to leverage them for political rather than monetary gain. U.S. Department of Homeland Security officials, for example, feared that a ransomware attack on U.S. state or local voter registration offices and related systems could disrupt preparations for the 2020 presidential election or cause confusion or long lines on Election Day.[12] To preclude election disruption and interference, USCYBERCOM engaged in a campaign to temporarily disrupt what is described as the world's largest botnet—Trickbot, which is a collection of more than two million malware-infected Windows PCs that are constantly being harvested for financial data and are often used as the entry point for deploying ransomware within compromised organizations.[13] Additionally, in recent testimony, General Nakasone implied there is a similar ongoing campaign motivated by the current Russian-Ukraine conflict—"we're very, very focused on ransomware actors … that might conduct attacks against our allies or our nation."[14]

Complicating Competitor's Military Preparations

Cyber campaigns can complicate a competitor's military preparations through supply chain infiltration,[15] "left of missile launch" efforts,[16] and disruption of military exercises.[17] USCYBERCOM deployed "hunt forward" teams to Ukraine at the end of 2021 in anticipation of

---

[10] Martin Matishak, "Cyber Command Chief: U.S. Has 'Stepped Up' to Protect Ukraine's Networks," The Record, April 5, 2002, https://therecord.media/cyber-command-chief-u-s-has-stepped-up-to-protect-ukraines-networks/.
[11] Ellen Nakashima and Dalton Bennett, "A Ransomware Gang Shut Down after Cybercom Hijacked Its Site and It Discovered It Had Been Hacked," *The Washington Post*, November 3, 2021, https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html.
[12] Ellen Nakashima, "Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election," *The Washington Post*, October 9, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.
[13] Brian Krebs, "Attacks Aimed at Disrupting the Trickbot Botnet," *Krebs on Security*, October 2, 2020, https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/.
[14] "House Select Intelligence Committee Holds Hearing on Worldwide Threats," CQ Congressional Transcripts, March 8, 2022, https://plus.cq.com/doc/congressionaltranscripts-6475406?0#speakers.
[15] Greg Hadley, "Hacking the Supply Chain," *Air Force Magazine*, December 3, 2021, https://www.airforcemag.com/article/hacking-the-supply-chain/.
[16] Caroline Houck, "Left-of-Launch Missile Defense: 'You Don't Want to Have Just One Solution to the Threat'", DefenseOne, January 24, 2018, https://www.defenseone.com/threats/2018/01/left-launch-missile-defense-you-dont-want-have-just-one-solution-threat/145438/.
[17] China has reportedly engaged in the jamming of U.S. aircraft engaged in readiness and/or other exercises. Alex Lockie, "China May Be Jamming US Navy Jets Off Aircraft Carriers in the Pacific - and the US Will 'Not Look Kindly on It,'" *Business Insider*, April 18, 2018, https://www.businessinsider.in/china-may-be-jamming-us-navy-jets-off-aircraft-carriers-in-the-pacific-and-the-us-will-not-look-kindly-on-it/articleshow/63821014.cms.

a Russian invasion.[18] People familiar with the operation described an urgent hunt for dormant Russian malware that would be launched to support a military invasion.[19] Reportedly, a "hunt forward" team and civilians discovered and mitigated a "wiperware" malware in the Ukrainian Railways capable of disabling computer networks by deleting critical files. In the first 10 days of the Russian invasion, nearly one million Ukrainian civilians escaped to safety on the rail network. Had the malware remained undiscovered, "it could have been catastrophic," according to a Ukrainian official familiar with the issue.[20] Thus, the limited campaign disrupted Russia's military preparations for inducing post-invasion chaos among the population. By comparison, similar malware went undetected at the Ukraine-Romania border crossing of Siret during the first week of March, causing chaos as hundreds of thousands of Ukrainians sought to flee the country.[21]

USCYBERCOM's limited campaign to secure the 2018 U.S. mid-term elections from Russian interference serves as another example of complicating opponent's preparations. USCYBERCOM reportedly took the initiative to exploit vulnerabilities in the cyber infrastructure of Russia's Internet Research Agency (IRA) to constrain its ability to act against the U.S. 2018 elections.[22] This reportedly resulted in IRA organizational friction and Russia shifting its focus and efforts toward defense, both of which served a U.S. strategic objective of taking Russia's focus away from cyber-enabled information operations directed at U.S. elections.[23]

Resilience through Campaigning

The NDS fact sheet calls for the DoD to increase resilience—an ability to withstand, fight through, and recover quickly from disruption. Although not linked to campaigning per se, in cyberspace, campaigning to compete, deter, and win requires continuous maneuvering against adversaries that reveals insights about adversary tactics, techniques, and procedures that can be shared with inter-agency and industry partners (as well as allies and international partners) to

---

[18] See David A. Sanger and Julian Barnes, "U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault," *New York Times*, December 20, 2021, https://www.nytimes.com/2021/12/20/us/politics/russia-ukraine-cyberattacks.amp.html and Mark Pomerleau, "Ukraine Crisis Shows Effectiveness of Cyber Command's Persistent Engagement, Nakasone Says," Fedscoop, April 6, 2022, https://www.fedscoop.com/ukraine-crisis-demonstrates-cyber-concept-of-persistent-engagement/.

[19] Mehul Srivastava, Madhumita Murgia, and Hannah Murphy, "The Secret US Mission to Bolster Ukraine's Cyber Defences Ahead of Russia's Invasion," *Financial Times*, March 8, 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.

[20] Ibid.

[21] Ibid, and Kyle Alspach, "Ukraine Border Control Hit with Wiper Cyberattack, Slowing Refugee Crossing," VentureBeat, February 27, 2022, https://venturebeat.com/2022/02/27/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/.

[22] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *The Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

[23] U.S. Senate Committee on Armed Services Hearing, "Review Testimony on United States Special Operations Command and United States Cyber Command in Review on the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program," February 14, 2019, https://www.armed-services.senate.gov/imo/media/doc/19-13_02-14-19.pdf.

proactively inoculate vulnerable assets from cyber exploitation, disruption, and destruction.[24] This "anticipatory resilience" leverages insights gained from intelligence, hunt forward, and contest efforts against highly capable opponents to inform preclusion, preparation, mitigation, response, and recovery. An example of limited USCYBERCOM campaigns include hunt forward operations in Montenegro to improve American cyber defenses ahead of the 2020 election and current activities to inoculate U.S. systems from Russian cyber actors and/or any proxies supporting its war against Ukraine.[25]

Precluding and/or Inhibiting Exploitation

The NDS fact sheet focuses on adversary coercive activities. In cyberspace, these are necessarily preceded by cyber exploitation activities that are also independently consequential for cumulating strategic gains. Cyber exploitation is much more than an intelligence contest.[26] It is a strategic competition with states acting unilaterally—rather than interacting—to gain advantage by making use of another's cyberspace vulnerabilities.[27]

It is primarily through exploitation, not coercion, that states are harming U.S. national security interests in and through cyberspace. China's cyber-enabled intellectual property theft has led to a loss of U.S military overmatch in important areas.[28] North Korea has circumvented sanctions and continued to advance its ballistic missile and nuclear programs with illicit cyber-enabled acquisition of international currencies.[29] Russia's ubiquitous cyber-enabled efforts to stress-test alliances and erode confidence in democratic institutions continues largely unabated.[30] This exploitation-based cyber reality must be addressed in DoD's forthcoming cyber strategy. Campaigning to preclude exploitation and/or inhibit the cumulation of strategic gains should accompany DoD's other campaigning objectives.

---

[24] "An Interview with Paul M. Nakasone," *Joint Forces Quarterly* 92, (1st quarter, 2019): 4-9, 6.
[25] See, respectively, Nakasone and Sulmeyer, "How to Compete in Cyberspace" and Derek B. Johnson, "Cyber Command: Insights from Hunt Forward Teams in Ukraine Flow to US Private Sector," *SC Media*, April 5, 2022, https://www.scmagazine.com/analysis/critical-infrastructure/cyber-command-lessons-from-hunt-forward-teams-in-ukraine-flow-to-us-private-sector.
[26] 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/.
[27] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Rethinking National Security in Cyberspace* (New York: Oxford University Press, 2022), https://global.oup.com/academic/product/cyber-persistence-theory-9780197638255?cc=us&lang=en&.
[28] Lisa Ferdinando, "DoD Officials: Chinese Actions Threaten U.S. Technological, Industrial Base," *DOD News*, June 21, 2018, https://www.defense.gov/Explore/News/Article/Article/1557188/.
[29] Stephanie Kleine-Ahlbrandt, "North Korea's Illicit Cyber Operations: What Can Be Done?" *38 North*, February 28, 2020, https://www.38north.org/2020/02/skleineahlbrandt022820/.
[30] See *United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukasheb, Sergey Aleksandrovich Morgachecv, Nikolay Yuryvich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyovich Kovalev*, Filed July 13, 2018, https://www.justice.gov/file/1080281 and "House Select Intelligence Committee Holds Hearing on Worldwide Threats."

Conclusion

The NDS fact sheet makes clear that campaigning is important for achieving security across the full spectrum of strategic competition and supporting integrated deterrence. In cyberspace, it is *the essential way*, and so the fact sheet's discussion of campaigning and the objectives it intends to support offer a strong, albeit incomplete, outline for the forthcoming DoD cyber strategy. Given that exploitation must necessarily precede coercion in and through cyberspace, the strategy should prioritize efforts toward precluding the former to limit the number of times DoD must contest the latter. The forthcoming strategy should consider other questions such as which campaigns should be limited and event-based (e.g., helping to ensure the security of U.S. elections) and which must be enduring because they are threat-based (e.g., helping to secure intellectual property to prevent loss of overmatch, precluding or disrupting opportunities for states to circumvent sanctions, enabling anticipatory resilience). Campaigning in and through cyberspace could also increase the stability of the cyber strategic competition by helping to cultivate norms of acceptable and unacceptable behavior. Based on the content of the NDS fact sheet, the NDS promises to offer a strong operational framework for addressing these DoD cyber strategy issues.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-04-22	Non-Standard	

4. TITLE AND SUBTITLE
What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?

5a. CONTRACT NUMBER
HQ0034-19-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)
Michael P. Fischerkeller

5d. PROJECT NUMBER
C5224

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES
Institute for Defense Analyses
730 East Glebe Road
Alexandria, VA 22305

8. PERFORMING ORGANIZATION REPORT NUMBER
NS D-33077

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Institute for Defense Analyses
730 East Glebe Road, Alexandria, VA 22305

10. SPONSOR'S / MONITOR'S ACRONYM
IDA

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
Project Leader: Michael P. Fischerkeller

14. ABSTRACT

The two-page fact sheet summarizing the 2022 National Defense Strategy (NDS) is notable when considered from a cyberspace strategy perspective. Identifying campaigning as one way to advance Department of Defense (DoD) goals is consistent with lessons learned operating in and through cyberspace employing the concepts of defend forward and persistent engagement (DF/PE). Additionally, three of NDS's campaigning objectives—to gain advantages against the full range of competitors' coercive actions, undermine acute forms of competitor coercion, and complicate competitor's military preparations are objectives that DF/PE campaigning could support. Further, although a fourth objective mentioned in the NDS fact sheet—resilience—is not listed as an objective of campaigning, DF/PE has demonstrated that campaigning is critical to supporting anticipatory resilience in cyberspace, including ongoing efforts such as employing hunt forward teams to inoculate the U.S. public and private sectors from malicious cyber activity. *In toto*, such cyber campaigns support integrated deterrence by undermining an opponent's confidence that they will prevail in crisis or armed conflict. As the forthcoming cyber strategy is to be nested within the NDS, we should anticipate it supporting these same objectives. This essay elaborates on each from a cyber strategy perspective and offers an additional objective unique to cyberspace—precluding exploitation and/or inhibiting the cumulation of strategic gains in and through cyberspace.

15. SUBJECT TERMS
Cyber strategy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	10	19b. TELEPHONE NUMBER (Include Area Code)