THE BIDEN ADMINISTRATION'S NATIONAL CYBERSECURITY STRATEGY: OPPORTUNITIES & CHALLENGES

NIRANJAN SHANKAR

FEBRUARY 2024

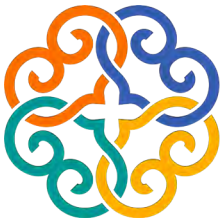
Middle East Institute

WWW.MEI.EDU

The Biden Administration's National Cybersecurity Strategy: Opportunities and Challenges

Niranjan Shankar

Middle East Institute
Washington, D.C.
February 2024



Middle
East
Institute

ABOUT THE MIDDLE EAST INSTITUTE

The Middle East Institute is a center of knowledge dedicated to narrowing divides between the peoples of the Middle East and the United States. With over 70 years' experience, MEI has established itself as a credible, non-partisan source of insight and policy analysis on all matters concerning the Middle East. MEI is distinguished by its holistic approach to the region and its deep understanding of the Middle East's political, economic and cultural contexts. Through the collaborative work of its three centers — Policy & Research, Arts & Culture, and Education — MEI provides current and future leaders with the resources necessary to build a future of mutual understanding.

INTELLECTUAL INDEPENDENCE

MEI maintains strict intellectual independence in all of its projects and publications. MEI as an organization does not adopt or advocate positions on particular issues, nor does it accept funding that seeks to influence the opinions or conclusions of its scholars. Instead, it serves as a convener and forum for discussion and debate, and it regularly publishes and presents a variety of views. All work produced or published by MEI represents solely the opinions and views of its scholars.

ABOUT THE AUTHOR

Niranjan Shankar is a non-resident scholar with MEI's Strategic Technologies and Cybersecurity Program focusing on great power rivalry, technology and cybersecurity policy, and U.S. policy in the Greater Middle East. He also works as a software engineer, and develops extensions to help provide zero-trust security and networking resiliency to applications hosted on cloud-based, distributed platforms. Niranjan's work at MEI focuses on the domestic and international cybersecurity landscape and the intersection of global geopolitics and tech and cyber policy. He also covers how digital trade and commerce, overseas tech and cyber partnerships, and the race for digital infrastructure development will shape political and economic trends in the Greater Middle East and other critical theaters in the developing world, as well as the implications of these transformations for the broader U.S.-China rivalry.

The views and opinions expressed are those of the author and do not necessarily reflect the official policy or position of entities, institutions, and/or organizations that the author may be associated with.

Cover photo: Exterior view of the northern side of the White House in Washington, DC as seen from Lafayette Square Park on May 8, 2023. Photo by Nicolas Economou/NurPhoto via Getty Images.

CONTENTS

Photo above: Raw computer programming code light boxes inside a science park in Jinhu County, Jiangsu Province, China. Photo by Costfoto/Barcroft Media via Getty Images.

EXECUTIVE SUMMARY

The Biden administration's National Cybersecurity Strategy (NCS), published in March 2023, outlines how the White House plans on defending America's digital ecosystem from malicious threat actors. The document, which has been rightly praised for its transformative agenda and ambitious vision, defines several key priorities for shaping a global cyber landscape that is more resilient and secure:

- Promoting multi-stakeholder cooperation with the private sector, international partners, and civil society organizations
- Modernizing legacy systems and transitioning to zero-trust architecture (ZTA)
- Investing in critical and emerging technologies and revitalizing America's cyber workforce
- Crafting cybersecurity regulations and shifting liability for vulnerable software while minimizing the impact on market dynamics
- Embracing an offensive approach to foreign cyber operations by augmenting disruption campaigns against adversaries and malicious actors

Nonetheless, the Biden administration will face several obstacles and challenges while putting its plan into action, namely:

- Navigating implementation barriers, budgetary restrictions, and political gridlock
- Protecting personal data and establishing interoperable data transfer frameworks with global partners without imposing major compliance costs on technology companies
- Addressing deficiencies in critical infrastructure operational technology and difficulties in adopting ZTA
- Emphasizing manufacturing, not just innovation, to secure American leadership in next-generation technologies
- Harmonizing regulations across critical infrastructure sectors and carefully designing regulatory frameworks and liability regimes
- Reconciling an offensive cyber posture with a commitment to promote and uphold norms of responsible state behavior for cyberspace
- Ensuring that U.S. cyber strategy does not neglect the dangers posed by non-state actors and proxy groups
- Promoting a values-driven digital ecosystem and countering the model of cyber-sovereignty without sidelining key non-democratic cyber and technological partners
- Expanding digital trade and commerce, increasing investments in digital infrastructure development, and integrating cyber diplomacy effectively with other instruments of statecraft

To address the growing threats in the digital domain and successfully executive the NCS's objectives, the Biden administration will need to overcome these obstacles by devising flexible, sustainable, and realistic policies at home and establishing robust cyber coalitions and trade frameworks with allies and partners abroad.

Introduction

In March 2023, the Biden administration published its National Cybersecurity Strategy (NCS),[1] which outlines how the executive branch will take on the proliferating threats facing the American digital landscape. The strategy, which consists of five pillars — Defend Critical Infrastructure, Disrupt and Dismantle Threat Actors, Shape Market Forces to Drive Security and Resilience, Invest in a Resilient Future, and Forge International Partnerships to Pursue Shared Goals — has been widely praised[2] for its embrace of an aggressive posture in cyberspace, calls for more regulations across critical infrastructure sectors, and advocacy for software liability reform.[3] Others, however, are skeptical[4] that its ambitions are achievable given the controversy over, and anticipated pushback against, some of its proposals and other implementation challenges.

Indeed, while the NCS is bold, expansive, and imaginative, it does leave many unanswered questions regarding the specific steps the administration will take to realize its vision for cyberspace. Though the July 2023 Implementation Plan[5] names specific initiatives for each pillar and assigns a federal agency[6] to lead and complete each of them by a target date, the White House still seems to have overlooked some critical issues — relating to data privacy and protection, migration to zero-trust architecture (ZTA), and digital infrastructure investment in the developing world, just to name a few — that it will need to address to foster a resilient digital ecosystem at home and abroad. The Biden administration also appears to be prone to repeating the same mistakes in the cyber domain that it has made in its overarching foreign policy.[7]

Thus, for the strategy's promising and ambitious agenda to succeed, the Biden administration will need to be more nuanced and realistic about how it will pursue the objectives it has laid out. The White House also must start accounting for other ambiguities and gray areas that both the NCS and Implementation Plan have either de-emphasized or omitted altogether. Finally, to secure American interests in international cyberspace, Washington needs to incorporate its technology initiatives[8] effectively into its broader foreign policy frameworks[9] and reconsider some of its approaches to cyber diplomacy.

1. "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy," *The White House*, March 2, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

2. Jason Healey, "The National Cybersecurity Strategy: Breaking a 50-Year Losing Streak," *Lawfare*, June 7, 2023, https://www.lawfaremedia.org/article/the-national-cybersecurity-strategy-breaking-a-50-year-losing-streak.

3. Stephen Weigand, "Biden cyber strategy a 'game changer' and 'revolutionary,' industry pros say," *SC Media*, March 3, 2023, https://www.scmagazine.com/news/biden-cyber-strategy-game-changer-revolutionary-industry-pros.

4. Chris Riotta and Natalie Alms, "National cyber strategy faces major implementation challenges, experts say," *Nextgov/FCW*, March 2, 2023, https://www.nextgov.com/cybersecurity/2023/03/national-cyber-strategy-faces-major-implementation-challenges-experts-say/383561/.

5. "National Cybersecurity Strategy Implementation Plan," *The White House*, July 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

6. "FY 2024-2026 Cybersecurity Strategic Plan," *U.S. Cybersecurity and Infrastructure Security Agency* (CISA), August 2023, https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.

7. Jeremy Stern, "Biden Promised to Confront China with an Alliance of Values. Europe Said No Thanks," *Newsweek*, February 4, 2021, https://www.newsweek.com/biden-promised-confront-china-alliance-values-europe-said-no-thanks-opinion-1566571.

8. Ngor Luong and Husanjot Chahal, "The Future of the Quads: Technology Cooperation Hangs in the Balance," *Council on Foreign Relations*, June 14, 2022, https://www.cfr.org/blog/future-quads-technology-cooperation-hangs-balance.

9. "U.S. Indo-Pacific Strategy," *The White House*, February 2022, https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.

Photo above: Gen. Paul Nakasone, Commander of U.S. Cyber Command; Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency; and Christopher Wray, FBI Director, testify before a House committee on Jan. 31, 2024. Photo by Kevin Dietsch/Getty Images.

What the National Cybersecurity Strategy Gets Right

To its credit, the National Cybersecurity Strategy highlights numerous important security priorities for Washington to tackle in the digital arena. Many of these efforts will build upon and complement President Joe Biden's previous executive orders[10] and directives,[11] as well as policies and frameworks[12] that were established under the Trump and Obama administrations.

A Multistakeholder Model for Cooperation with the Private Sector and International Partners

Firstly, the document rightly underscores the significance of collaboration for achieving its goals. At the domestic level, this entails integrating federal cybersecurity centers and disruption campaigns as well as expanding defense and security coordination and intelligence sharing between the public and private sectors. This latter objective will be facilitated by the Cybersecurity and Infrastructure Security Agency

10. "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks," *The White House*, May 12, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

11. Tom Kellermann, "Biden Administration Directs Federal Agencies to Patch Known Vulnerabilities," *VMware*, November 3, 2021, https://blogs.vmware.com/security/2021/11/biden-administration-directs-federal-agencies-to-patch-known-vulnerabilities.html.

12. Dave Weinstein, "The Pentagon's New Cyber Strategy: Defend Forward," *Lawfare*, September 21, 2018, https://www.lawfaremedia.org/article/pentagons-new-cyber-strategy-defend-forward.

(CISA)[13] and other sector-specific entities such as Sector Risk Management Agencies (SRMAs) and Information Sharing Analysis Organizations and Centers (ISAOs and ISACs). Given that leading technology companies own and maintain much of the infrastructure[14] upon which computer networks around the world are built, these public and private sector synergies will be crucial for gaining invaluable insights into adversarial activity in cyberspace.

On the global stage, the White House seeks to strengthen ties with its partners around the world and leverage international institutions to confront America's foreign adversaries, safeguard global digital commerce and supply chains, and enforce norms of responsible state behavior in cyberspace. The Biden administration also lists civil society organizations, nonprofits,[15] and local and regional entities as key partners in the fight against malicious cyber activity, reaffirming Washington's commitment to promoting a multistakeholder model of Internet governance.[16]

Transitioning from Legacy Systems to Zero-Trust Architecture and Investing in Critical and Emerging Technologies

Modernizing federal software and equipment and upgrading security architectures are other noteworthy goals set forth by the NCS. Building off of Executive Order 14028,[17] Memorandum 22-09,[18] and recommendations by the National Institute of Standards and Technology (NIST),[19] the Biden administration will work to expedite the federal government's shift[20] toward ZTA — security models in which no user or communication within a network is trusted, and access permissions are restricted to the "least privileges"[21] necessary to perform a given function. The administration will also assist federal agencies with replacing legacy systems and migrating on-premises workloads to the cloud.

Relatedly, the strategy appreciates that boosting R&D investments in cybersecurity, artificial intelligence (AI) (also emphasized in President Joe Biden's recent executive order[22] on the safe and secure development of AI), quantum computing, green energy, and biotechnology, along with fostering a stronger and more versatile cyber workforce,[23] will be vital for nurturing cybersecurity expertise and preserving American global leadership in critical technologies.

Issuing Cybersecurity Regulations and Shifting Liability for Insecure Software

Perhaps the most significant difference between the NCS and the strategies of previous administrations is

13. "FY 2024-2026 Cybersecurity Strategic Plan," *U.S. Cybersecurity and Infrastructure Security Agency* (CISA), August 2023, https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.

14. Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," *Carnegie Endowment for International Peace*, August 31, 2020, https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597.

15. "About EFF," *Electronic Frontier Foundation*, Accessed January 28, 2024, https://www.eff.org/about.

16. "Internet Governance: Why the Multistakeholder Approach Works," *Internet Society*, April 26, 2016, https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.

17. "Executive Order on Improving the Nation's Cybersecurity," *The White House*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

18. Shalanda Young, "M-22-09: Fiscal Year 2023 Federal Information Security Modernization Act Reporting Metrics," *The White House*, January 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

19. "Planning for a Zero Trust Architecture: White Paper," *National Institute of Standards and Technology* (NIST), May 6, 2022, https://csrc.nist.gov/News/2022/planning-for-a-zero-trust-architecture-white-paper.

20. Joseph Clark, "Pentagon Cyber Official Provides Progress Update on Zero Trust Strategy Roadmap," *U.S. Department of Defense*, May 18, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3400194/pentagon-cyber-official-provides-progress-update-on-zero-trust-strategy-roadmap/.

21. "Least Privilege," *National Institute of Standards and Technology* (NIST), Accessed January 28, 2024, https://csrc.nist.gov/glossary/term/least_privilege.

22. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," *The White House*, October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

23. Briana Reilly, "Lawmakers Outline Cyber Priorities for Pentagon," *Roll Call*, February 2, 2023, https://rollcall.com/2023/02/02/lawmakers-outline-cyber-priorities-for-pentagon/.

the unprecedented role that it designates for the federal government to play in the software market. Stressing that voluntary adhesion to critical infrastructure cybersecurity has yielded inconsistent and unsatisfactory outcomes,[24] the document instead advocates sector-specific, modern, and nimble regulatory frameworks that establish minimum expected cybersecurity best-practices and mandates but also take into account the cost of implementation to help level the playing field. To alleviate the private sector of potential burdens, reduce duplication, and avoid obstructing digital trade flows, regulators are expected to harmonize and streamline new and existing regulations. If federal agencies lack the authority to enforce certain requirements, Congress is expected to help bridge this gap.

Shifting liability from end-users and open-source developers onto the private sector is the other major component of the administration's ambition to realign incentives and shape market forces to drive security. Here, the strategy astutely observes that markets currently fail to hold software vendors accountable[25] when they maximize short-term profit at the expense of investing in security and overlook basic precautions[26] to prevent malicious users from infiltrating their networks. To shift the consequences of cybersecurity malpractice onto the entities "most capable of taking action to prevent bad outcomes," the White House plans to work with Congress to design and enact legislation that would make it illegal for companies to fully disclaim liability by contract. The strategy also aims to encourage coordinated vulnerability disclosures and the generation of a Software Bill of Materials (SBOM).[27]

Unsurprisingly, these declarations have ignited controversy among cybersecurity analysts and industry professionals, many of whom have warned[28] that government involvement — particularly in the highly complex and rapidly evolving software ecosystem — could lead to all sorts of unintended consequences and potentially stifle technological innovation. Critics are certainly correct that poorly designed regulatory frameworks and liability regimes could yield disastrous outcomes, and that determining accountability in cases where blame and root causes are difficult to pinpoint could be very problematic.

Nonetheless, the administration seems to have accounted for many of these concerns, even if it hasn't provided definitive answers for all of them. Pillar Three, for example, repeatedly stresses that Washington will strive to encourage vendors to prioritize the security of their products without undermining or diminishing the role of the market. The centrality of cooperation with the private sector and multistakeholderism to numerous NCS objectives, as well as the White House's appreciation of the private sector's unmatched talent pool and resources, seem to affirm that the Biden administration is wary of encumbering the industry with heavy-handed policies. It's also worth noting that the lack of specificity regarding implementation — while troubling in other respects — gives the administration some flexibility in adapting to emerging trends in the cybersecurity landscape.

The strategy also acknowledges that code vulnerabilities and errors are unavoidable even if enterprises diligently follow cyber-hygiene protocols. Through a safe harbor framework, the administration intends to shield companies that abide by best practices, such as the NIST Secure Software Development Framework,[29] from liability — only enterprises that fail to adhere to these standards and *knowingly* distribute vulnerable software will be held accountable. Moreover, the administration will leverage federal grants programs to create positive incentives for organizations to invest in secure-by-design software as opposed to solely

24. Janette Wider, "Hacktivist Group Responsible for Attacks on U.S. Hospitals," *Healthcare Innovation Group*, January 31, 2023, https://www.hcinnovationgroup.com/cybersecurity/news/21294198/hacktivist-group-responsible-for-attacks-on-us-hospitals.

25. "Colonial Pipeline Third-Party Lawsuits Dismissed," *CyberClan*, August 16, 2022, https://cyberclan.com/us/knowledge/colonial-pipeline-third-party-lawsuits-dismissed/.

26. Alexander Culafi, "Mandiant: Compromised Colonial Pipeline Password Was Reused," *TechTarget*, June 9, 2021, https://www.techtarget.com/searchsecurity/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused?Offer=abMeterCharCount_var2.

27. "Software Bill of Materials (SBOM)," *Cybersecurity and Infrastructure Security Agency* (CISA), https://www.cisa.gov/sbom.

28. Walter Haydock, "What is Software Security Regulation?" *StackAware Blog*, February 3, 2023, https://blog.stackaware.com/p/what-software-security-regulation.

29. "Software Supply Chain Risk Management (SSCRM) – Systems Security Engineering," *National Institute of Standards and Technology* (NIST), https://csrc.nist.gov/projects/ssdf.

relying on punishments to prod companies to bolster the security of their products and services.

Overall, there is widespread consensus[30] among policymakers and cybersecurity experts that despite the potential risks involved in legislating the technology industry, the status quo is unsustainable — change is both inevitable and necessary. Though some executives may decry these efforts, many have become more receptive[31] to cyber regulation in the aftermath of the Russo-Ukrainian war and the SolarWinds and Colonial Pipelines incidents, and the strategy's inclusion of safe harbors has made companies even more amenable to these proposals.[32] Many firms have also joined forces in campaigns like the Cybersecurity Tech Accord[33] to assist each other on their journey to enhanced software security.

The Best Defense Is a Good Offense

The Biden administration is not just focused on ramping up defenses — a salient aspect of its vision is an aggressive U.S. posture in cyberspace. In 2018, the Trump administration freed[34] the military of several restraints to pursue offensive cyber operations, and U.S. Cyber Command (CYBERCOM)[35] started proactively monitoring digital space and disrupting malicious actors overseas before they could attack U.S. networks. The 2023 NCS will take the "defend forward" and "persistent-engagement"[36] approaches even further by increasing "the volume and speed of these integrated disruption campaigns" and leveraging joint task forces[37] to conduct cyber operations against adversaries abroad (with an appropriate[38] emphasis on ransomware groups[39] in particular, as can be seen by the recent expansion[40] of the International Counter Ransomware Initiative [CRI]). Moreover, by pleading to use "all instruments of national power" to neutralize digital adversaries, the White House recognizes the importance of integrating[41] cyber capabilities with conventional modes of deterrence and warfare. The Pentagon reaffirms these concepts and articulates its planned use of integrated deterrence in its summary of its 2023 Cyber Strategy[42] as well.

While the nature of the offense-defense balance[43] in cyberspace and the coercive potential[44] of cyber

30. Paul Rosenzweig, "The Cyber Liability Fight Begins," *Lawfare*, January 6, 2023, https://www.lawfaremedia.org/article/cyber-liability-fight-begins.

31. Rishi Iyengar, "Biden's National Cybersecurity Strategy: Allies, Russia, China," *Foreign Policy*, March 2, 2023, https://foreignpolicy.com/2023/03/02/biden-national-cybersecurity-strategy-allies-russia-china/.

32. Chris Padilla and Jamie Thomas, "IBM's Letter to the Office of the National Cyber Director," *IBM*, March 2, 2023, https://www.ibm.com/policy/ibms-letter-to-the-office-of-the-national-cyber-director/.

33. "Accord," *Cyber Tech Accord*, Accessed January 28, 2024, https://cybertechaccord.org/accord/.

34. Ellen Nakashima, "Trump authorizes offensive cyber operations to deter foreign adversaries, Bolton says," *The Washington Post*, September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

35. Paul Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

36. "Cyber 101: Defend Forward and Persistent Engagement," *U.S. Cyber Command*, October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

37. "Joint Ransomware Task Force," *Cybersecurity and Infrastructure Security Agency* (CISA), https://www.cisa.gov/joint-ransomware-task-force/.

38. Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein, "Confronting Reality in Cyberspace," *Council on Foreign Relations*, July 2022, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace.

39. "Biden Declares Ransomware Attacks a National Security Threat," *IT World Canada*, March 6, 2023, https://www.itworldcanada.com/post/biden-declares-ransomware-attacks-a-national-security-threat#:~:text=U.S.%20President%20Joe%20Biden%20has,it%20a%20national%20security%20threat.

40. "International Counter Ransomware Initiative 2023 Joint Statement," *The White House*, November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

41. Sue Gordon and Eric Rosenbach, "America's Cyber Reckoning," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

42. "2023 DOD Cyber Strategy Summary," *U.S. Department of Defense*, September 12, 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

43. Brandon Valeriano, "Does the Cyber Offense Have the Advantage?" *OffensiveCyber*, December 20, 2021, https://offensivecyber.org/2021/12/20/does-the-cyber-offense-have-the-advantage/.

44. Erica Lonergan and Michael Poznansky, "Are We Asking

operations remain disputed, offensive campaigns have proven to be valuable in particular scenarios[45] and conditions, whereas purely defensive measures (like deterrence by denial) have often shown to be ineffective, given the impracticality of completely eliminating vulnerabilities from highly complex networks and systems. Moreover, Washington's passivity[46] in earlier instances, such as after Russia's devastating cyberattacks on Ukraine's electrical grid in 2015, eventually came back to bite it.[47] In contrast, the Trump administration's preemptive disruption of hostile networks and willingness to expose adversaries publicly[48] proved to be more effective in deterring[49] foreign attacks on U.S. digital infrastructure (though the NCS itself, in line with recommendations from experts,[50] opts for the phrase "resilience" over "deterrence"). However, despite these steps in the right direction, the Biden administration will still face several obstacles while putting its plan into action.

Challenges and Recommendations for the Road Ahead

Implementation Barriers

As many observers have noted,[51] the White House should expect to encounter numerous challenges as it embarks on its ambitious and revolutionary agenda. The administration has sought to address these concerns by revealing its Implementation Plan,[52] which defines a (somewhat) more actionable list of initiatives — some of which are already in progress or have been completed ahead of schedule[53] — and commits to revisiting and updating these milestones annually. As announced by Chris DeRusha, a senior White House cybersecurity adviser, in November 2023, the Biden administration is already working on a "version 2.0"[54] of the Implementation Plan. Additionally, the subsequent confirmation of Harry Coker, who has affirmed his commitment to the NCS and Implementation Plan, as the new national cyber director[55] is an encouraging development in terms of the strategy actually being put into action.

Nonetheless, the plan still does not fully clarify how the administration will tackle some of the NCS's most difficult goals. Several objectives' timelines even seem to have been pushed farther out into 2025, which calls into question the

Too Much of Cyber?" *War on the Rocks*, May, 2023, https://warontherocks.com/2023/05/are-we-asking-too-much-of-cyber/.

45. Max Smeets, "Cyber Security in the 21st Century: Threats, Challenges, and Opportunities," *Strategic Studies Quarterly*, 12(3), Fall 2018, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf.

46. Sue Gordon and Eric Rosenbach, "America's Cyber Reckoning," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

47. Patrick Howell O'Neill, "The Russian Hackers Who Interfered in 2016 Were Spotted Targeting the 2020 US Election," *MIT Technology Review*, September 10, 2020, https://www.technologyreview.com/2020/09/10/1008297/the-russian-hackers-who-interfered-in-2016-were-spotted-targeting-the-2020-us-election/.

48. David Sanger and Julian Barnes, "As States Finalize Vote Counts, Both Sides Prepare for Election Lawsuits," *The New York Times*, November 9, 2020, https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.

49. Timothy McKenzie, "Cyber Deterrence," *U.S. Department of Defense*, November 20, 2017, https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.

50. "Does cyber deterrence work? National security expert on cybersecurity and National Defense Strategy," *Government Matters*, January 12, 2022, https://www.youtube.com/watch?v=e27cLgyrwbM.

51. Tim Starks and David DiMolfetta, "Biden Administration Has a New Cybersecurity Strategy. Now Comes the Hard Part," *The Washington Post*, March 3, 2023, https://www.washingtonpost.com/politics/2023/03/03/biden-administration-has-new-cybersecurity-strategy-now-comes-hard-part/.

52. "National Cybersecurity Strategy Implementation Plan," *The White House*, July 13, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

53. "Administration Cybersecurity Priorities for the FY 2025 Budget," *The White House*, June 27, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf.

54. Matt Bracken, "Chris DeRusha: The Person Tasked With Overseeing the National Cybersecurity Strategy," *CyberScoop*, November 16, 2023, https://cyberscoop.com/national-cybersecurity-strategy-chris-derusha/.

55. John Sakellariadis, "Coker Confirmed as Next Cyber Director," *Politico*, December 12, 2023, https://www.politico.com/news/2023/12/12/coker-confirmed-as-next-cyber-director-00131345/.

Photo above: European flags wave in front of the Berlaymont building in Brussels, Belgium, in early 2019. Photo by Michele Spatari/NurPhoto/Getty Images.

feasibility of many of the Biden administration's aspirations. Many other key issues have also been omitted. For instance, aside from tasking the Department of Commerce with publishing a Notice of Proposed Rulemaking with cybersecurity standards, procedures, and requirements for Infrastructure-as-a-Service (IaaS) providers, the plan neglects cloud security,[56] an especially important subject given the centrality of cloud computing to IT modernization both for the federal government and the private sector.

Data Privacy and Protection and International Data Transfers

Data privacy and protection is another topic that receives short shrift in the strategy and the Implementation Plan. Given the inefficiency and complexity of the current "patchwork"[57] of state-wide privacy laws, the NCS is correct to support legislation "to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data and provide strong protections for sensitive data like geolocation and health information" and "set national requirements to secure personal data consistent with standards and guidelines developed by NIST." However, the strategy doesn't specify exactly what these regulations would entail, and the Implementation Plan leaves out the objective to "Hold the stewards of our Data Accountable" altogether.

The administration also overlooks some other risks involved with establishing data privacy requirements. A framework based directly on the oft-cited European

56. Tim Maurer and Garrett Hinck, "Cloud Security Primer for Policymakers," *Carnegie Endowment for International Peace*, August 31, 2020, https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597.

57. Jennifer Huddleston, "The Problem of Patchwork Privacy," *Technology Liberation Front*, August 15, 2018, https://techliberation.com/2018/08/15/the-problem-of-patchwork-privacy/.

Union's General Data Protection Regulation (GDPR) or the California Consumer Protection Act (CCPA) could impose major compliance costs[58] on technology companies, restrict productivity, and curtail innovation. Washington should avoid these pitfalls while also setting a baseline set of targeted privacy principles that is interoperable with the GDPR[59] and assuages EU citizens' unease about U.S. law enforcement's access to their data. In exchange, Brussels should drop some of its data localization requirements[60] that are currently impeding transatlantic data flows.

Unfortunately, meaningful progress on this front seems elusive in light of recent events. Previously, the Court of Justice of the European Union (CJEU) invalidated the former U.S.-EU Safe Harbor[61] and the Privacy Shield[62] agreements in the Schrems I[63] (2015) and Schrems II[64] (2020) decisions, respectively, on the grounds that the two frameworks didn't sufficiently protect EU citizens' data from U.S. government surveillance. Based on these complaints, President Biden signed an executive order[65] in October 2022 that limits U.S. law enforcement and intelligence collection agencies' access to and use of personal data for American and EU citizens, and also allows individuals in the EU to challenge how these agencies use their data through an independent Data Protection Review Court within the Department of Justice.

Earlier in 2023, President Biden fulfilled[66] all these commitments, and the European Commission's adequacy decision[67] in July 2023 to approve the new EU-U.S. Data Privacy Framework[68] initially seemed to be a hopeful sign that a clear consensus could soon be met on personal data transfers between America and the EU. Nonetheless, privacy groups such as NOYB are determined to challenge[69] the framework and bring it back to the CJEU, and other data privacy watchdogs and institutions claimed that the new measures still did not go far enough.[70] Indeed, despite European Commission President Ursula von der Leyen's praise[71] of Washington for implementing "unprecedented commitments to establish the new framework," experts[72] and commentators[73] are anticipating and preparing for an

58. Alan McQuinn and Daniel Castro, "The Costs of an Unnecessarily Stringent Federal Data Privacy Law," *Information Technology and Innovation Foundation* (ITIF), August 5, 2019, https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law/.

59. Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein, "Confronting Reality in Cyberspace," *Council on Foreign Relations*, July 2022, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace.

60. Luca Bertuzzi, "Is Data Localization Coming to Europe?" *International Association of Privacy Professionals* (IAPP), August 23, 2022, https://iapp.org/news/a/is-data-localization-coming-to-europe/.

61. "U.S.-EU Safe Harbor Framework," *Federal Trade Commission* (FTC), July 25, 2016, https://www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework.

62. "NIST Privacy Framework," *National Institute of Standards and Technology* (NIST), Accessed January 28, 2024, https://www.dataprivacyframework.gov.

63. "Schrems v Data Protection Commissioner," *Columbia Global Freedom of Expression*, Accessed January 28, 2024, https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/.

64. Sharp Cookie Advisors, "Schrems II Case Summary," *GDPR Summary*, November 23, 2020, https://www.gdprsummary.com/schrems-ii/.

65. Mark Scott, Alfred Ng, and Vincent Manancourt, "Biden's Data Privacy Executive Order Aims for EU-U.S. Agreement," *Politico*, October 7, 2022, https://www.politico.eu/article/joe-biden-data-privacy-agreement-executive-order-eu-us/.

66. "U.S. Finalizes EU-U.S. Data Privacy Framework Requirements, Awaits EU Adequacy Decision," *International Association of Privacy Professionals* (IAPP), July 3, 2023, https://iapp.org/news/a/us-finalizes-eu-us-data-privacy-framework-requirements-awaits-eu-adequacy-decision/.

67. Jennifer Bryant, "European Commission Adopts EU-U.S. Adequacy Decision," *International Association of Privacy Professionals* (IAPP), July 10, 2023, https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/.

68. "EU-U.S. Data Privacy Framework: Guidance and Resources," *International Association of Privacy Professionals* (IAPP), July 2023, https://iapp.org/resources/article/eu-us-data-privacy-framework-guidance-and-resources/.

69. "European Commission Gives EU-US Data Transfers a Third Round at CJEU," *None of Your Business* (NOYB), July 10, 2023, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

70. "New Biden Executive Order on EU-US Data Transfers Fails to Adequately Protect Privacy," *American Civil Liberties Union* (ACLU), October 7, 2022, https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy.

71. Jennifer Bryant, "European Commission Adopts EU-U.S. Adequacy Decision," *International Association of Privacy Professionals* (IAPP), July 10, 2023, https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/.

72. Mikołaj Barczentewicz, "Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States," *Law & Economics Center*, September 25, 2023, https://laweconcenter.org/resources/schrems-iii-gauging-the-validity-of-the-gdpr-adequacy-decision-for-the-united-states/.

73. "Schrems III: Are You Prepared?," *ShardSecure*, September

upcoming "Schrems III"[74] case. There's also the possibility of subsequent U.S. administrations overturning President Biden's executive order. With no imminent end in sight for these ongoing disputes with a major trading partner, Washington will struggle to boost international digital trade and commerce.

Setting Precedents for Negligence Liability Standards and Safe Harbor Laws

The White House will need to tread carefully when executing the liability regime for cybersecurity as well. Even with a legal safe harbor to limit the scope of undesirable outcomes, the administration must resolve several crucial questions to avoid punishing vendors that have actually incorporated security precautions throughout the software development lifecycle. How should a court of law decide, without being exclusionary or unfair, whether a company took "reasonable precautions" to secure their products? What makes an actor "most capable" of taking action? How will the Civil Cyber-Fraud Initiative (CCFI) determine whether an entity or individual "knowingly" provided deficient products or services? Should negligence liability standards be applied to small and medium-sized businesses that may be under-resourced?

Establishing precedents for these scenarios to ensure that well-intentioned firms are not targeted will take years, if not decades. Companies can also become more risk-averse and start significantly scaling back the functionality of their offerings. Furthermore, the executive branch will need to distance itself from, and push back against, other legislation (not mentioned in the NCS itself) proposed by lawmakers that could impair[75] technology companies' ability to invent secure-by-design solutions and discourage them from investing in cybersecurity and encryption research.

Promoting a Vibrant Technology Ecosystem Through Innovation, Manufacturing, and a Strengthened Cyber Workforce

The NCS acknowledges the indispensable roles of both the government and private sector in accelerating investments, achieving breakthroughs, and mitigating cybersecurity risks in existing and next-generation technologies. But safeguarding innovation[76] alone is not enough. To secure U.S. leadership in critical and emerging technologies, Washington must augment the country's manufacturing potential[77] in these sectors as well. The CHIPS and Science Act, Inflation Reduction Act, and Bipartisan Infrastructure Law will serve as important first steps in improving American industrial policy, but without overarching cultural changes[78] and structural adjustments to recalibrate the nation's conventional approaches to R&D and manufacturing — for instance, by pressing Silicon Valley to shift its focus back onto ultra-precision manufacturing, nurturing a business environment with favorable tax policies and environmental rules that encourage manufacturing, and reversing the consolidation of the American chip industry — the U.S. tech ecosystem could eventually fall behind those of the country's primary competitors, namely China.

Relatedly, as the document states, strengthening the American cyber workforce will be crucial for building more secure and resilient systems at home and crafting effective cyber diplomacy abroad. Fortunately, the

14, 2023, https://shardsecure.com/blog/schrems-iii-prepared.

74. William Alan Reinsch, "Privacy is Heading for Schrems III," *Center for Strategic and International Studies* (CSIS), October 11, 2022, https://www.csis.org/analysis/privacy-heading-schrems-iii.

75. Herbert Hovenkamp, "Why Breaking Up Big Tech Could Do More Harm than Good," *Knowledge@Wharton*, March 26, 2019, https://knowledge.wharton.upenn.edu/podcast/knowledge-at-wharton-podcast/why-breaking-up-big-tech-could-do-more-harm-than-good/.

76. Eric Schmidt, "Innovation and Power: Technology in Geopolitics," *Foreign Affairs*, February 28, 2023, https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.

77. Dan Wang, "China's Hidden Tech Revolution: How Beijing Threatens U.S. Dominance," *Foreign Affairs*, February 28, 2023, https://www.foreignaffairs.com/china/chinas-hidden-tech-revolution-how-beijing-threatens-us-dominance-dan-wang.

78. Chris Miller, "How Silicon Valley Lost the Chips Race," *Foreign Affairs*, October 19, 2022, https://www.foreignaffairs.com/united-states/how-silicon-valley-lost-chips-race.

Photo above: Harry Coker Jr., national cyber director nominee for U.S. President Joe Biden, speaks during a Senate Homeland Security and Governmental Affairs Committee nomination hearing on Nov. 2, 2023. Photo by Al Drago/Bloomberg via Getty Images.

National Cyber Workforce and Education Strategy[79] outlines various initiatives to ameliorate talent and staff shortages by promoting computer networking and security expertise, facilitating talent exchanges and joint fellowship programs with international partners, and developing immigration laws that will help retain foreign science, technology, engineering, and mathematics (STEM) students and researchers. That being said, cooperation from Congress (as is currently underway for the creation of a Cyber Workforce Development Institute[80]) will be necessary to enact these policies.

Budgetary Constraints and Political Obstacles

President Biden's budget request last March for Fiscal Year (FY) 2024 allocated[81] a notable increase in funds for cybersecurity across federal agencies,[82] for initiatives ranging from IT modernization to boosting Ukraine's digital defenses and augmenting digital transformation efforts[83] in the developing world. While the prospect of spending more

79. "National Cybersecurity Workforce Expansion Strategy 2023," *The White House*, July 31, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

80. Cate Burgan, "White House Working with Congress on Cyber Workforce Institute," *MeriTalk*, November 14, 2023, https://www.meritalk.com/articles/white-house-working-with-congress-on-cyber-workforce-institute/.

81. Edward Graham, "Biden Administration Seeks $26B for Cyber Funding in FY 2024," *Nextgov/FCW*, March 16, 2023, https://www.nextgov.com/cybersecurity/2023/03/biden-administration-seeks-26b-cyber-funding-fy-2024/384070/.

82. Christian Vasquez, "Biden's 2023 Budget Proposal Includes Nearly $11 Billion for Cyber," *CyberScoop*, March 9, 2023, https://cyberscoop.com/biden-budget-2023/.

83. "Fact Sheet: New Initiative on Digital Transformation with Africa (DTA)," *The White House*, December 14, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/.

on securing and modernizing federal network infrastructure and scaling public-private partnerships initially raised hopes[84] among cybersecurity and technology industry leaders that the administration's priorities could be fulfilled, the Republican Study Committee's fiscal blueprint[85] for the Congressional Budget Resolution — which promised to slash overall domestic spending — foreshadowed some major disagreements between Democrats and Republicans in Congress over a beefed up cybersecurity budget.

To be sure, some of the outcomes of the appropriations process have been conducive to the White House's goals. The National Defense Authorization Act[86] (NDAA), signed into law[87] by President Biden on Dec. 22, 2023, contains extensive cybersecurity-related provisions, namely for defense and security-oriented cyber operations like leveraging AI digital assets in cyberspace and bolstering defensive military cybersecurity operations with foreign partners and allies. Other developments, however, were less encouraging. Though House Republicans' attempt to slash CISA's funding by 25% in September[88] was unsuccessful, the House appropriations bill for Homeland Security provides CISA with $2.926 billion — $130 million less than what the Biden administration had requested and, when adjusted for inflation,[89] amounts to a cut in CISA's budget since FY23 — and also includes a policy rider to prohibit funding that would go toward countering misinformation. Other disparities[90] between the House and Senate appropriations bills remain to be resolved, but allocations for several other federal departments and agencies seem vulnerable to falling short of the requested amounts, which risks hindering their IT modernization and security objectives.

The recent conservative backlash against CISA, other federal agencies, and the Biden administration's cyber-related initiatives in general (including the appointment of Harry Coker as the new White House cyber director[91]) stem from a deep distrust of campaigns to combat misinformation on digital platforms,[92] which some hard-right lawmakers claim infringes upon freedom of speech and unfairly censors conservative voices online. In July 2023, U.S. District Judge Terry Doughty in Louisiana issued an order[93] to limit communications between the White House and several government agencies and social media platforms over taking down "content containing protected free speech." Though the Supreme Court in October temporarily froze[94] the (narrower) restrictions set[95] by the U.S. Court of Appeals for the 5th Circuit, the

84. Mark Montgomery and Jiwon Ma, "President's Cyber Budget Request Is Off to a Good Start — Congress Should Fill the Gaps," *The Hill*, April 15, 2023, https://thehill.com/opinion/cybersecurity/3952133-presidents-cyber-budget-request-is-off-to-a-good-start-congress-should-fill-the-gaps/.

85. Daniel Lerman, "Conservatives' Budget Plan Renews Battle Over Seniors' Benefits," *Roll Call*, June 14, 2023, https://rollcall.com/2023/06/14/conservatives-budget-plan-renews-battle-over-seniors-benefits/.

86. Cynthia Brumfield, "2024 US NDAA Boosts Nuclear Cybersecurity, Highlights Artificial Intelligence," *CSO Online*, December 18, 2023, https://www.csoonline.com/article/1265288/2024-us-ndaa-boosts-nuclear-cybersecurity-highlights-artificial-intelligence.html.

87. "Statement from President Joe Biden on H.R. 2670 - National Defense Authorization Act for Fiscal Year 2024," *The White House*, December 22, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/22/statement-from-president-joe-biden-on-h-r-2670-national-defense-authorization-act-for-fiscal-year-2024/.

88. John Sakellariadis, "Conservatives aim to gut CISA amid cyber fight," *Politico*, October 22, 2023, https://www.politico.com/news/2023/10/22/conservatives-cyber-cisa-politics-00122794/.

89. Elaine McCusker, "Don't Be Fooled by Biden's Budget: He's Cutting Military Spending as Our Needs Grow," *New York Post*, March 10, 2023, https://nypost.com/2023/03/10/bidens-budget-hes-cutting-military-spending/.

90. "How Do the House and Senate Appropriation Bills Differ?" *The Peter G. Peterson Foundation*, September 21, 2023, https://www.pgpf.org/blog/2023/09/how-do-the-house-and-senate-appropriation-bills-differ.

91. John Sakellariadis, "Coker Confirmed as Next Cyber Director," *Politico*, December 12, 2023, https://www.politico.com/news/2023/12/12/coker-confirmed-as-next-cyber-director-00131345/.

92. "Information Integrity," *United Nations*, Accessed January 28, 2024, https://www.un.org/en/information-integrity/.

93. John Berman, "Social media giants appeal lawsuit ruling," *CNN*, July 14, 2023, https://www.cnn.com/2023/07/14/politics/social-media-lawsuit-appeal/index.html.

94. Amy Howe, "Supreme Court allows federal government continued communication over social media content moderation," *SCOTUSblog*, October 20, 2023, https://www.scotusblog.com/2023/10/justices-allow-federal-government-continued-communication-over-social-media-content-moderation/.

95. Tierney Sneed, "Biden administration asks Supreme Court to weigh in on social media lawsuit," *CNN*, September 8, 2023, https://www.cnn.com/2023/09/08/politics/biden-administration-social-media-lawsuit/index.html.

bitter disputes over information integrity,[96] online content moderation, securing elections, and preventing foreign influence operations are unlikely to be resolved in the foreseeable future.

Unaddressed Vulnerabilities in Critical Infrastructure and Delays in Migration to Zero-Trust Architecture

Other attempts by the Biden administration to secure critical infrastructure have also faced major setbacks, due to political divides and unsettled disagreements over the role of government in protecting privately owned infrastructure. From the very outset of the NCS's publication, House Republicans have expressed their staunch opposition[97] to granting the executive branch additional authority to regulate business sectors (or for passing legislation that would impose liability on software companies). More recently, due to opposition from Republican states[98] and water industry groups, the Environmental Protection Agency (EPA) withdrew[99] its memorandum[100] from March 2023 requiring states to assess operational technology (OT) for public water systems for cybersecurity risks.

The failure to address these long-standing vulnerabilities in the nation's water infrastructure[101] was exploited[102] after the outbreak of the Israel-Hamas war[103] by Iranian-backed hackers, who launched a wave of cyberattacks against water facilities in the U.S. that use Israeli-made equipment. Though updates to the Implementation Plan[104] (which was announced as part of a broader discussion about managing risk to critical infrastructure) and the National Cyber Incident Response Plan (NCIRP),[105] a rewrite[106] of Presidential Policy Directive (PPD) 21 to more clearly define the role of government agencies and emphasize a greater role for CISA, and security-related mandates[107] in Biden's AI executive order will be important steps toward addressing these deficiencies across the water and other critical infrastructure sectors,[108] harmonizing regulations and technical standards for all these sectors and spurring investment in underfunded systems[109] will be enormous tasks that will likely span the course of several administrations.

96. "Information Integrity," *United Nations*, Accessed January 28, 2024, https://www.un.org/en/information-integrity/.

97. Mark Green and Andrew Garbarino, "Statement on the Release of the National Cybersecurity Strategy," *House Committee on Homeland Security*, March 2, 2023, https://homeland.house.gov/2023/03/02/green-garbarino-statement-on-the-release-of-the-national-cybersecurity-strategy/.

98. Eric Geller, "EPA Faces Lawsuit Over Biden's Cybersecurity Directive for Critical Infrastructure," *Wired*, May 11, 2023, https://www.wired.com/story/epa-lawsuit-biden-cybersecurity-critical-infrastructure/.

99. Christian Vasquez, "EPA Calls Off Cyber Regulations for Water Sector," *CyberScoop*, October 12, 2023, https://cyberscoop.com/epa-calls-off-cyber-regulations-for-water-sector/.

100. Christian Vasquez, "EPA Water Sector Ditches Plans for Cyber Regulations," *CyberScoop*, March 3, 2023, https://cyberscoop.com/epa-water-cyber-regulations/.

101. Mark Montgomery and Trevor Logan, "Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure," *Foundation for Defense of Democracies* (FDD), November 18, 2021, https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure/.

102. David Jones, "Water Utility Cyberattacks: The Threat to OT," *Cybersecurity Dive*, December 5, 2023, https://www.cybersecuritydive.com/news/water-utility-cyberattacks-threat-ot/.

103. "MEI Spotlight on the Israel-Hamas war," *Middle East Institute*, Accessed January 28, 2024, https://www.mei.edu/israel-hamas-war.

104. "White House Cybersecurity Implementation Plan Continuously Evolving," *SC Magazine*, November 17, 2023, https://www.scmagazine.com/brief/white-house-cybersecurity-implementation-plan-continuously-evolving.

105. "National Cyber Incident Response Plan (NCIRP)," *Cybersecurity and Infrastructure Security Agency* (CISA), October 20, 2023, https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp.

106. Christian Vasquez, "Critical infrastructure policy rewrite expected to 'emphasize' CISA, NSC official says," *CyberScoop*, November 16, 2023, https://cyberscoop.com/critical-infrastructure-policy-rewrite-expected-to-emphasize-cisa-nsc-official-says/.

107. Bridget Neill, John D. Hallmark, Richard J. Jackson, and Dan Diasio, "Key Takeaways from the Biden Administration Executive Order on AI," *EY*, October 31, 2023, https://www.ey.com/en_us/public-policy/key-takeaways-from-the-biden-administration-executive-order-on-ai.

108. Jonathan Mattise and Jake Bleiberg, "Ransomware attack prompts multistate hospital chain to divert some emergency room patients elsewhere," *AP News*, November 28, 2023, https://apnews.com/article/ransomware-attack-hospitals-emergency-rooms-0841defe1b881b71eccb8826ed46130e.

109. Sadek Wahba, "Water Cybersecurity Dispute Reveals Infrastructure Problem," *Forbes Finance Council*, August 25, 2023, https://www.forbes.com/sites/forbesfinancecouncil/2023/08/25/water-cybersecurity-dispute-reveals-infrastructure-problem/?sh=703c341d6ade.

The ongoing effort to adopt ZTA reveals even more hurdles on the path to a more resilient digital ecosystem. While the federal government has made progress[110] toward the mandates laid out in the Office of Management and Budget's (OMB) ZTA memorandum,[111] the Department of Defense[112] (DoD) and other agencies have encountered major challenges during their migrations to zero-trust frameworks, which has led some observers to question the feasibility of the September 2024 deadline.[113] The barriers[114] to federal agencies' shift away from traditional, perimeter-based defenses include outdated legacy systems, lack of urgency and technical expertise, and structural and organizational inefficiencies. Critical infrastructure owners[115] and companies[116] in the private sector also face similar problems in their adoption of ZTA. Government and industry leaders must therefore look beyond the technical dimensions of zero-trust security and start emphasizing the cultural and organizational factors involved in successful migrations to ZTA as well. Additionally, both the public and private sectors should treat the transition to zero-trust as a long-term process and be prepared for delays and growing pains along the way.

Managing Cyber-Escalation and Establishing Norms in Cyberspace While Going on the Offensive

As with securing critical infrastructure domestically, combating threat actors abroad will also be a formidable undertaking. In pursuing the aggressive stance outlined in both the NCS and the 2023 Cyber Strategy summary,[117] the DoD will need to carefully distinguish between situations and attack types in which offensive maneuvers are appropriate (typically for quick, targeted, and short-lived attacks) and those in which their benefits will be more limited, as opposed to treating the question of the offense-defense balance in cyberspace in a one-size-fits-all manner. Moreover, while both documents acknowledge the threat posed by transnational criminal organizations and non-state actors,[118] the growing (and warranted) emphasis on China's and Russia's cyber capabilities risks overshadowing the numerous problems[119] that proxy groups could also present for U.S. interests. The Pentagon should remain vigilant about non-state entities' malicious activity in cyberspace and differentiate tactics specifically tailored[120] to deal with these groups from those designed for established militaries and intelligence services.

Another pain point for the administration could be reconciling a more confrontational cyber doctrine with

110. "Federal Agencies Move Forward on Zero Trust," *MeriTalk*, May 3, 2023, https://www.meritalk.com/articles/federal-agencies-move-forward-on-zero-trust/.

111. Shalanda Young, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," *The Office of Management and Budget*, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

112. Jaspreet Gill, "DoD finding it 'hard to orchestrate' services on zero trust, holding monthly discussions: Resnick," *Breaking Defense*, June 8, 2023, https://breakingdefense.com/2023/06/dod-zero-trust-cyber-services/.

113. Kevin Finch, "Can federal agencies meet the 2024 zero trust deadline?," *Federal News Network*, October 12, 2023, https://federalnewsnetwork.com/commentary/2023/10/can-federal-agencies-meet-the-2024-zero-trust-deadline/.

114. Emily Harding, James Andrew Lewis, Suzanne Spaulding, Rose Butchart, Jake Harrington, Devi Nair, Harshana Ghoorhoo, and Paula Reynal, "Never Trust, Always Verify": Federal Migration to ZTA and Endpoint Security," *Center for Strategic & International Studies* (CSIS), June 16, 2022, https://www.csis.org/analysis/never-trust-always-verify-federal-migration-zta-and-endpoint-security.

115. "IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High," *IBM*, July 27, 2022, https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High.

116. Robert Lemos, "Companies Struggle With Zero Trust as Attackers Adapt to Get Around It," *Dark Reading*, January 26, 2023, https://www.darkreading.com/remote-workforce/companies-struggle-zero-trust-attackers-adapt.

117. "2023 DOD Cyber Strategy Summary," *U.S. Department of Defense*, September 12, 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

118. Brandon Valeriano and Jose Macias, "Paper Tigers: Proxy Actors Are True," *The National Interest*, April 12, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/paper-tigers-proxy-actors-are-true.

119. Sue Gordon and Eric Rosenbach, "America's Cyber Reckoning," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

120. Joseph Nye, "Deterrence in Cyberspace," *ASPI Strategist*, June 7, 2019, https://www.aspistrategist.org.au/deterrence-in-cyberspace/.

a commitment to reinforce global norms of responsible state behavior in cyberspace. As it is, setting standards for international cyberspace remains a struggle for the United Nations.[121] Though claims that "norms of behavior aren't well-established" in the cyber domain aren't always accurate,[122] scholars have often pointed out[123] that due to some of the digital arena's unique characteristics (erosion of distance, speed of interaction, low cost, and difficulty of attribution), as well as the relative novelty of the Internet, the process of defining rules for cyberweapons will follow a different trajectory than it did for nuclear or conventional arms, and will likely be an uneven,[124] uncertain work in progress for several decades.

Russia's numerous attacks against Ukraine's critical infrastructure,[125] interference in U.S. elections, and sponsorship of ransomware gangs — despite having formerly signed off on nonbinding, voluntary UN agreements[126] eschewing such conduct — are key cases in point of the difficulty of enforcing norms across the digital ecosystem. And though Washington and its overseas partners have made notable strides[127] in advancing international law in cyberspace, they too have failed to abide by and honor many of these standards consistently. This was evident in Western officials' overall muted response when their citizens helped "hacktivist" and digital vigilante groups, like Ukraine's "IT Army,"[128] launch distributed-denial-of-service (DDoS) attacks against Moscow, even though such operations rest on shaky legal ground.[129] Similarly, the U.S. has previously stated[130] that only espionage directed against the private sector should be off-limits, but at times has also tried to rule out breaches like the SolarWinds incident[131] that targeted government and military officials. Neither the NCS nor the Implementation Plan offer suggestions for crafting more enduring and consistent cyber-rules.

A growing reliance on offensive cyber operations risks jeopardizing this already fragile and delicate framework for developing standards for the digital domain. Indeed, fears of cyberwarfare escalating to physical conflict tend to be overblown,[132] and the Pentagon can clarify that defend forward missions are preemptive measures only directed at hostile actors intending to attack U.S. networks, not unprovoked acts of aggression. But even if such operations won't lay the groundwork for kinetic warfare, they could still risk inviting similar attacks by overseas actors, such as Iran and North Korea, which can justify their state-sponsored, cyber-enabled campaigns against the West

121. Arindrajit Basu, Irene Poetranto, and Justin Lau, "UN Struggles to Make Progress on Securing Cyberspace," *Carnegie Endowment for International Peace*, May 19, 2021, https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491.

122. Lloyd Austin, "Remarks by Secretary of Defense Lloyd J. Austin III at the Reagan National Defense Forum," *Department of Defense*, December 4, 2021, https://www.defense.gov/News/Speeches/Speech/Article/2861931/remarks-by-secretary-of-defense-lloyd-j-austin-iii-at-the-reagan-national-defen/.

123. Joseph Nye, "The End of Cyber Anarchy," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.

124. "Back to Square One: The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," *Cyber Defence Centre of Excellence*, Accessed January 28, 2024, https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/.

125. "Industrial Control Systems (ICS) Alert - IR-Alert-H-16-056-01," *Cybersecurity and Infrastructure Security Agency* (CISA), July 20, 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

126. "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," *Cyber Defence Centre of Excellence*, Accessed January 28, 2024, https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

127. "UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)," *Digital Watch*, Accessed January 28, 2024, https://dig.watch/processes/un-gge.

128. "The Ukrainian IT Army," *Council on Foreign Relations*, Access January 28, 2024, https://www.cfr.org/cyber-operations/ukrainian-it-army.

129. "'Hacktivists' and the Ukraine-Russia Conflict: Legal Considerations," *Congressional Research Service* (CRS), May 13, 2022, https://crsreports.congress.gov/product/pdf/LSB/LSB10743.

130. Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein, "Confronting Reality in Cyberspace," *Council on Foreign Relations*, July 2022, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace.

131. Tarah Wheeler, "The Danger in Calling the SolarWinds Breach an Act of War," *Brookings Institution*, March 4, 2021, https://www.brookings.edu/articles/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/.

132. Erica Lonergan, "The Cyber Escalation Fallacy," *Foreign Affairs*, April 15, 2022, https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy.

Photo above: U.S. President Joe Biden announces new sanctions against the Russia government, on April 15, 2021, in response to the 2020 hacking operation that breached U.S. government agencies and major American companies. Photo by Chip Somodevilla/Getty Images.

as disruptions of imminent threats to their security,[133] whether or not such claims have any credibility.

Given that democracies like the U.S. are highly vulnerable[134] to cyberattacks and influence operations due to their political openness, protection of individual freedoms, and digital dependencies, Washington needs to prosecute an assertive cyber doctrine while still discouraging and deterring hostile states and proxy groups from launching destructive attacks against the American digital landscape. As suggested by cybersecurity policy expert Jacquelyn Schneider,[135] one way for CYBERCOM to square this circle would be to explicitly call out what America won't do in the digital domain — such as attack critical infrastructure overseas — even as it embraces an offensive cyber strategy. Moreover, it's worth noting that the DoD's Cyber Strategy summary[136] does account for the possibility of unintended cyber escalation and reassures that "the Department will remain closely attuned to adversary perceptions." Nevertheless, some disruptive events are impossible to prevent altogether, and the U.S. must be willing to accept some of the risks involved with expanding its digital capabilities and adopting a more aggressive posture in

133. Josh Fruhlinger, "Stuxnet Explained: The First Known Cyberweapon," *CSO Online*, August 31, 2022, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

134. Erica Lonergan and Jacquelyn Schneider, "America's Digital Achilles' Heel: Technology," *Foreign Affairs*, September 7, 2023, https://www.foreignaffairs.com/united-states/americas-digital-achilles-heel-technology.

135. "Does cyber deterrence work? National security expert on cybersecurity and National Defense Strategy," *Government Matters*, January 12, 2022, https://www.youtube.com/watch?v=e27cLgyrwbM.

136. "2023 DOD Cyber Strategy Summary," *U.S. Department of Defense*, September 12, 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

cyberspace. Hence, investing in resilient civilian and military systems that can withstand such assaults will continue to be a pressing priority for Washington.

Balancing American Interests and Values in the Digital Domain

Still, the White House's aspiration to foster a "values-driven development of our digital ecosystem" internationally could face other major hindrances. To advance the liberal and democratic principles embodied in the Declaration for the Future of the Internet (DFI)[137] and the Freedom Online Coalition,[138] Washington plans to work with a broad, global coalition of "like-minded states" to counter transnational digital authoritarianism and nurture an "open, free, global, interoperable, reliable, and secure" Internet. Though the Trump administration's National Cyber Strategy[139] also frequently underscores the importance of furthering American values in cyberspace, President Biden has been especially emphatic about the role of democracy promotion and human rights in both the digital[140] and physical[141] worlds, and on numerous occasions has endorsed a binary foreign policy narrative of a global showdown between democracies and autocracies.

To be sure, the strategy is correct to highlight the threat that autocratic regimes pose to global Internet freedom and how the model of cyber-sovereignty[142] promulgated by Beijing and Moscow erodes Western efforts to advance a multistakeholder framework for governing cyberspace. Likewise, Washington should strive to respect individual freedoms to the greatest extent possible as it works with social media platforms to combat misinformation online, and must treat cybersecurity as a vital component of its mission to restore faith[143] in democratic institutions at home. But unrealistic expectations of a global digital landscape anchored in U.S. ideals and technological partnerships based predominantly on shared values will easily backfire.

For starters, as can be seen by the numerous[144] and unresolved[145] aforementioned disagreements on data privacy and protection between Washington and Brussels, democracies won't always see eye-to-eye on issues regarding cybersecurity and Internet governance. America's priorities also often conflict with those of its "like-minded" partners when it comes to Washington's technological competition with Beijing — the alarmingly slow progress by EU countries, especially Germany,[146] in excluding Huawei[147] from their 5G networks is a key case in point.

The other serious flaw of this strategic paradigm is that it risks harming technical cooperation with states in the developing world, particularly with illiberal or non-democratic ones. In the Greater Middle East,[148]

137. "Declaration for the Future of the Internet," *The White House*, April 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.

138. "Freedom Online Coalition," *Freedom Online Coalition*, Accessed January 28, 2024, https://freedomonlinecoalition.com.

139. "National Cyber Strategy," *The White House Archives*, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

140. Jessica Brandt, "How Biden Can Make His Internet Freedom Agenda a Success," *Brookings Institution*, December 8, 2021, https://www.brookings.edu/articles/how-biden-can-make-his-internet-freedom-agenda-a-success/.

141. Joseph Biden, "Why America Must Lead Again," *Foreign Affairs*, January 23, 2020, https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again.

142. Eric Rosenbach and Shu Min Chong, "Governing Cyberspace: State Control vs. Multistakeholder Model," *Belfer Center for Science and International Affairs*, August 2019, https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

143. Jacquelyn Schneider, "A World Without Trust," *Foreign Affairs*, December 18, 2021, https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust.

144. Sharp Cookie Advisors, "Schrems II Case Summary," *GDPR Summary*, November 23, 2020, https://www.gdprsummary.com/schrems-ii/.

145. William Alan Reinsch, "Privacy is Heading for Schrems III," *Center for Strategic and International Studies* (CSIS), October 11, 2022, https://www.csis.org/analysis/privacy-heading-schrems-iii.

146. Alina Clasen, "Why Germany Keeps Dragging Its Feet on the Huawei Ban," *Euractiv*, June 16, 2023, https://www.euractiv.com/section/5g/news/why-germany-keeps-dragging-its-feet-on-the-huawei-ban/.

147. Laurens Cerulus, "Europe's Cybersecurity Toolbox Explained: Huawei and 5G," *Politico*, January 29, 2020, https://www.politico.eu/article/europe-eu-huawei-5g-china-cybersecurity-toolbox-explained/.

148. Mohammed Soliman, "Middle East in the Era of Great Tech Competition," *Middle East Institute*, February 6, 2023, https://mei.

for example, governments have invested heavily in digitally transforming[149] their societies and shoring up their defenses against proliferating cyber threats.[150] Therefore, it is essential that Washington deepens digital partnerships[151] with countries throughout the Middle East and North Africa (MENA) if it wishes to preserve its hegemony in the region. This will entail scaling intelligence-sharing[152] and counterterrorism campaigns, fostering vibrant technology ecosystems and startup scenes[153] to enable economic growth and diversification,[154] promoting information sharing platforms[155] used to identify ransomware threats, expanding partners' AI capabilities,[156] countering the Iranian cyberthreat[157] by enhancing cyber cooperation between Israel and the Arab world,[158] and reversing[159] China's technological advances in the Middle East.[160]

Yet many countries in the MENA region are not fully on board with America's commitment to an open and free online ecosystem. This is also the case for nations in other parts of the world — digital authoritarianism[161] has been on the rise globally for over a decade,[162] and even democracies have struggled[163] to protect civil liberties while simultaneously moderating illegal content and fighting misinformation (as evidenced by the aforementioned polarization[164] over CISA's work to combat online misinformation) on the web. Nevertheless, many of the states that have seen drastic declines in Internet freedom are ones that Washington will inevitably need to engage with to maintain its technological competitiveness and defend its interests in international cyberspace. As an example, the fact that the CRI[165] consists of several

edu/publications/middle-east-era-great-tech-competition.

149. Eva Andren, "Technology Innovation: The Foundation of Egypt's Digital Future," *Ericsson*, September 12, 2022, https://www.ericsson.com/en/blog/5/2022/technology-innovation--the-foundation-of-egypts-digital-future.

150. Maria Harika, Eliza Campbell, "Ransomware in the UAE: Evolving Threats and Expanding Responses," *Middle East Institute*, July 27, 2022, https://www.mei.edu/publications/ransomware-uae-evolving-threats-and-expanding-responses.

151. Manuel Langendorf, "Enhancing U.S.-EU Collaboration in MENA's Digital Development," *Middle East Institute*, September 7, 2023, https://www.mei.edu/publications/enhancing-us-eu-collaboration-menas-digital-development.

152. David Schenker, "How the United States Should Help Protect Jordan from Chaos Next Door," *The Washington Institute*, February 22, 2017, https://www.washingtoninstitute.org/policy-analysis/how-united-states-should-help-protect-jordan-chaos-next-door.

153. Aynush Narayanan, "Non-oil Focus Fuels Optimism for Saudi, UAE Startups, Investors Amid Global Slump," *Al Arabiya*, July 24, 2023, https://english.alarabiya.net/business/economy/2023/07/24/Non-oil-focus-fuels-optimism-for-Saudi-UAE-startups-investors-amid-global-slump.

154. Mark Minevich, "Saudi Vision 2030: Key Lessons from the Kingdom's New Digital Leadership," *Fast Company*, September 1, 2022, https://www.fastcompany.com/90781638/saudi-vision-2030-key-lessons-from-the-kingdoms-new-digital-leadership.

155. Suzanne Smalley, "White House Counter Ransomware Initiative Summit Announces New Measures," *The Record*, October 31, 2023, https://therecord.media/white-house-counter-ransomware-initiative-summit-new-measure.

156. Madhumita Murgia, Andrew England, Qianer Liu, Eleanor Olcott, and Samer Al-Atrush, "Saudi Arabia and UAE race to buy Nvidia chips to power AI ambitions," *The Financial Times*, August 14, 2023, https://www.ft.com/content/c93d2a76-16f3-4585-af61-86667c5090ba.

157. Clint Watts, "DTAC: Iran Cyber Influence Operations and the Digital Threat Landscape," *Microsoft On the Issues*, May 2, 2023, https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/.

158. Thomas Warrick, "Cybersecurity in the Abraham Accords: A New Opportunity for Israel and the Gulf States," *Atlantic Council*, May 19, 2023, https://www.atlanticcouncil.org/blogs/menasource/cybersecurity-iran-abraham-accords-israel/.

159. Eric Geller, "Will the Saudis Help the U.S. Beat Huawei?," *Politico*, July 18, 2022, https://www.politico.com/newsletters/weekly-cybersecurity/2022/07/18/will-the-saudis-help-the-u-s-beat-huawei-00046280.

160. Mohammed Soliman, "Is China Winning the Middle East's Data?," *The National Interest*, April 13, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/china-winning-middle-east's-data.

161. Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," *Freedom House*, October 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

162. Adrian Shahbaz and Allie Funk, "Freedom on the Net 2021: Global Drive for Control Over Big Tech," *Freedom House*, October 2021, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

163. Janosch Delcker, "Germany's Controversial Legislation on Hate Speech on the Internet (NetzDG)," *Politico*, October 1, 2020, https://www.politico.eu/article/germany-hate-speech-internet-netzdg-controversial-legislation.

164. John Sakellariadis, "Conservatives are increasingly knives out for the nation's top cyber agency," *Politico*, October 22, 2023, https://www.politico.com/news/2023/10/22/conservatives-cyber-cisa-politics-00122794.

165. "International Counter Ransomware Initiative 2023 Joint Statement," *The White House*, November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

Photo above: A Huawei Technologies Co. sign outside the company's offices in Reading, U.K., in July 2020. Photographer: Jason Alden/ Bloomberg via Getty Images.

illiberal and non-democratic countries, and will likely be expanded in the future to include even more, illustrates how crucial it is for Washington and other liberal democracies to collaborate effectively with these nations.

This dilemma can also be partly seen in the U.S's vital partnership with India. The two countries have recently launched[166] numerous joint initiatives[167] on AI, telecommunications and wireless technology, quantum computing, space exploration, semiconductor supply chain resiliency, biotechnology, advanced weaponry, green energy, and talent exchanges. These engagements are expected to have a transformative impact on the strategic picture in the Indo-Pacific as both powers seek to offset Chinese hegemony[168] in the region. But government-initiated Internet shutdowns[169] have also been major points of tension between New Delhi and rights groups based in the West, and India (along with Brazil, another important technology partner[170] for the U.S.) has also not signed onto the DFI.[171]

166. "FACT SHEET: United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology (iCET)," *The White House*, January 31, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/.

167. Ved Shinde, "Technological cooperation is cementing U.S.-India security ties," *Nikkei Asia*, July 4, 2023, https://asia.nikkei.com/Opinion/Technological-cooperation-is-cementing-U.S.-India-security-ties.

168. Sumathi Bala, "India is a rising force in Southeast Asia as region seeks to counter China's dominance," *CNBC*, August 13, 2023, https://www.cnbc.com/2023/08/14/india-is-rising-force-in-southeast-asia-that-could-counter-china-dominance.html.

169. "Freedom on the Net 2022: India Country Report," *Freedom House*, October 2022, https://freedomhouse.org/country/india/freedom-net/2022.

170. "The Importance of Tech in the US-Brazil Relationship," *Information Technology Industry Council* (ITI), March 18, 2019, https://www.itic.org/news-events/techwonk-blog/the-importance-of-tech-in-the-usbrazil-relationship.

171. "India stays out of global declaration on future on

This is not to say that the U.S. should abandon its values-driven approach to cyberspace altogether. Initiatives such as the DFI and Freedom Online Coalition will still be useful for galvanizing global support against China and Russia, which have exploited digital tools and AI software to quell dissent and surveil their populations,[172] unfairly privileged[173] domestic companies over foreign competitors, and interfered[174] in the political affairs of democratic nations. Moreover, cross-border commercial activity is likely to suffer if more states start exerting extensive control of the Internet and enacting restrictive data localization and content-moderation policies.[175]

However, Washington should be wary of framing the global cyber coalitions it builds as pacts against digital autocracy and repression, which could alienate potential allies and partners. Such an outcome would not only be inimical to American interests but would also undermine American values by ceding additional ground to Beijing and Moscow and further enabling them to dictate[176] international standards for the online world, export their illiberal visions[177] for cyberspace, and exacerbate[178] the global fragmentation of the Internet.

A Better Approach: Digital Trade and Cybersecurity Collaboration

Instead, as recommended by Nathaniel Fick, Jami Miscik, Adam Segal, and Cordon M. Goldstein in their Council on Foreign Relations (CFR) Task Force Report on "Confronting Reality in Cyberspace," the U.S. should emphasize digital trade and commerce, secure and trusted data flows, and national security as the defining characteristics of a global cyber coalition.[179] Drawing in nations with tangible commercial benefits[180] and opportunities to augment offensive and defensive cyber capabilities can broaden these partnerships so that they can serve as effective counterweights to Beijing and Moscow. For instance, offering European nations higher-quality and cheaper 5G technology can help convince them to replace Huawei[181] as their provider for mobile network infrastructure. Likewise, given the proliferation of digital trade agreements[182] around the world, the U.S. must come off the sidelines in the global game on digital trade to remain a leading player in the world economy. This is especially true for the Indo-Pacific,[183] where Washington has been largely absent from

Internet," *The Hindu Business Line*, April 29, 2022, https://www.thehindubusinessline.com/info-tech/white-house-60-global-partners-launch-the-declaration-of-the-future-of-the-internet-india-not-on-the-list/article65366407.ece.

172. Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York Times*, May 22, 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

173. Dianjing Li, "Great firewall of China reinforced as foreign media banned from publishing online," *The Conversation*, March 10, 2016, https://theconversation.com/great-firewall-of-china-reinforced-as-foreign-media-banned-from-publishing-online-55091.

174. Michael Birnbaum and Craig Timberg, "E.U.: Russians interfered in our elections, too," *The Washington Post*, June 14, 2019, https://www.washingtonpost.com/technology/2019/06/14/eu-russians-interfered-our-elections-too/.

175. "Key Barriers to Digital Trade," *Office of the United States Trade Representative*, Accessed January 29, 2024, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade.

176. Charles Mok, "China and Russia Want to Rule the Global Internet," *The Diplomat*, February 22, 2022, https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/.

177. Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism: The Russian and Chinese models," *Brookings Institution*, August 27, 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

178. Christoph Meinel and David Hagebölling, "Russia's War Against Ukraine is Catalyzing Internet Fragmentation," *Council on Foreign Relations*, March 13, 2023, https://www.cfr.org/blog/russias-war-against-ukraine-catalyzing-internet-fragmentation.

179. Nathaniel Fick, Jami Miscik, Adam Segal, and Gordon M. Goldstein, "Confronting Reality in Cyberspace," *Council on Foreign Relations*, July 2022, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace.

180. Jay Heisler, "Smaller Economies See Big Opportunities in Digital Trade Pact," *VOA News*, April 21, 2021, https://www.voanews.com/a/economy-business_smaller-economies-see-big-opportunities-digital-trade-pact/6204836.html.

181. Ryan Browne, "Top EU official urges more countries to ban China's Huawei, ZTE from 5G networks," *CNBC*, June 16, 2023, https://www.cnbc.com/2023/06/16/eu-urges-more-countries-to-ban-chinas-huawei-zte-from-5g-networks.html.

182. Michelle Warren and Ziyang Fan, "Digital economy agreements are a new frontier for trade – here's why," *World Economic Forum*, August 24, 2022, https://www.weforum.org/agenda/2022/08/digital-economy-agreements-trade/.

183. Nigel Cory, "U.S. Options to Engage on Digital Trade and Economic Issues in the Asia-Pacific," *Information Technology & Innovation Foundation* (ITIF), February 8, 2022, https://itif.org/publications/2022/02/08/us-options-engage-digital-trade-and-economic-issues-asia-pacific/.

meaningful economic and trade engagement — a trend that will likely be exacerbated[184] by a recent decision by the U.S. to drop demands at the World Trade Organization (WTO) to protect cross-border data flows and prohibit data localization mandates. By contrast, China has attempted to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA) — the first digital-only trade agreement open to all members of the WTO.

Washington should launch new digital trade pacts and data transfer arrangements, see through the successful implementation of digital trade chapters in agreements such as the United States-Mexico-Canada Agreement (USMCA),[185] and determine a clear role for Congress in approving and shaping such frameworks. Incorporating digital trade updates to existing free trade agreements is another option, albeit less impactful than creating wider-ranging, digital-only initiatives.[186] Bridging the aforementioned differences in regulatory approaches and localization policies with European and Asian partners will also be necessary for establishing unimpeded and secure global information flows. Furthermore, incorporating cooperation on cybersecurity, as the USMCA does, can serve as an additional incentive for states to join these frameworks.

These strong political and commercial inducements won't just benefit America economically. With states more willing to forego more localized, protectionist systems to harness the full benefits of digital trade, the Biden administration can leverage these arrangements to gradually incentivize other nations to adopt practices that are more in line with America's vision of an open, free, secure, and trusted global digital ecosystem. And while full alignment on cyber norms or data protection and localization policies is unlikely, the U.S. and its partners can still find common ground on how citizens' data should be used, shared, and secured within interoperable frameworks. Additionally, Washington will be presented with ample opportunities (through subtle dialogues, as opposed to public naming and shaming[187]) to encourage its allies and partners to use digital tools and emerging technologies more responsibly. One way of doing this is to point out to world leaders and officials that excessive control and moderation of the Internet can hinder their countries' digital transformations.

Though such a network of alliances would still fall short of a united group of "techno-democracies,"[188] it will nonetheless allow American diplomats and policymakers to play an extensive role in shaping norms and standards on a broad range of economic and security issues in cyberspace. Over the long term, a more holistic and inclusive definition of what it means to be "like-minded" will therefore not only leave the U.S. well-positioned to safeguard its vital interests, but will also enable it to push back against the top-down, closed model of Internet governance espoused by Russia and China.

Investing in Digital Infrastructure Development and Reinvigorating American Cyber Diplomacy

Relatedly, Washington needs to work with its international partners to finance digital infrastructure projects in the developing world. Through the Digital Silk Road (DSR),[189] the technological component of the Belt and Road Initiative (BRI), the Chinese government has

184. David Lawder, "U.S. suspends Indo-Pacific talks on key aspects of digital trade -lawmakers," *Reuters*, November 8, 2023, https://www.reuters.com/business/finance/us-suspends-indo-pacific-talks-key-aspects-digital-trade-lawmakers-2023-11-08/.

185. Miranda Alamilla & Gabriel Cabañas, "Digital Trade under the USMCA: A Modern Opportunity for North American Economic Growth," *The Wilson Center*, March 21, 2022, https://www.wilsoncenter.org/article/digital-trade-under-usmca-modern-opportunity-north-american-economic-growth.

186. Nigel Cory, "U.S. Options to Engage on Digital Trade and Economic Issues in the Asia-Pacific," Information Technology & Innovation Foundation (ITIF), February 8, 2022, https://itif.org/publications/2022/02/08/us-options-engage-digital-trade-and-economic-issues-asia-pacific/.

187. Cole Bunzel, "Partner Or Pariah? Saudi Arabia, The Biden Administration, And Human Rights," *The Hoover Institution*, March 9, 2021, https://www.hoover.org/research/partner-or-pariah-saudi-arabia-biden-administration-and-human-rights.

188. Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies: How to Build Digital Cooperation," *Foreign Affairs*, October 13, 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

189. "Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms?," *Council on Foreign Relations*, December 18, 2020, https://www.cfr.org/china-digital-silk-road/.

invested billions of dollars in building 5G networks, cloud computing platforms, data centers, mobile payment services, AI systems, smart cities, and surveillance technologies for participating countries. This diffusion of Chinese technology throughout Latin America,[190] Africa,[191] and the Middle East[192] has presented Beijing with numerous opportunities[193] to conduct espionage against foreign governments and military facilities, augment its offensive cyber capabilities, promote technical standards that favor its geopolitical and economic interests, and undercut American efforts to establish international cyber norms. Over time, China will likely prioritize[194] the DSR over other traditional BRI projects; hence, it will be paramount that America and its allies fulfill the growing global demand for technology infrastructure.

Though the U.S. has warned the international community of the cybersecurity risks of using Chinese technology and shed light on how DSR-provided software and tools entrench digital authoritarianism, it has struggled to provide developing nations with realistic alternatives. Beijing has heavily subsidized[195] companies like Huawei to undercut foreign competitors and has also provided countries with low-interest loans to use Huawei's equipment. Washington should expand initiatives such as the International Development Finance Corporation (DFC),[196] Blue Dot Network,[197] USAID Digital Strategy,[198] and the digital components of the Partnership for Global Infrastructure and Investment (PGII)[199] to offer countries low-cost hardware, software, and services to realize their digital connectivity and technological modernization aspirations. Drawing in the private sector into these programs will also be crucial for ensuring their success. While President Biden has allocated funding[200] for digital development in his budget proposal, the West's financial commitment to building technological infrastructure abroad is still well behind Beijing's investment in the DSR,[201] and the likely funding cuts[202] to the State Department[203] suggest that this trend is unlikely to be reversed anytime soon, expansions of other initiatives notwithstanding. Moreover, the failure of the NCS and Implementation Plan to mention digital infrastructure development as a pressing priority reflects a lack of urgency toward the issue.

190. Nahal Toosi, "'Frustrated and powerless': In fight with China for global influence, diplomacy is America's biggest weakness," *Politico*, October 23, 2022, https://www.politico.com/news/2022/10/23/china-diplomacy-panama-00062828.

191. Motolani Agbebi, "China's Digital Silk Road and Africa's Technological Future," *Council on Foreign Relations*, February 1, 2022, https://www.cfr.org/blog/chinas-digital-silk-road-and-africas-technological-future.

192. Mohammed Soliman, "China Is Winning the Middle East's Data, Cyber, and Technology Race," *The National Interest*, April 13, 2022, https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/china-winning-middle-east%E2%80%99s-data.

193. Jacob J. Lew, Gary Roughead, Jennifer Hillman, and David Sacks, Project Directors, "China's Belt and Road: Implications for the United States," *Council on Foreign Relations*, March 2021, https://www.cfr.org/task-force-report/chinas-belt-and-road-implications-for-the-united-states/findings.

194. "China's Rise in the Global South: The Middle East, Africa, and Beijing's Alternative World Order," *National Committee on U.S.-China Relations*, August 29, 2022, https://www.youtube.com/watch?v=qckQNlkLYAs&t=1914s.

195. Noah Berman, Lindsay Maizland, and Andrew Chatzky, "Is China's Huawei a Threat to U.S. National Security?," *Council on Foreign Relations*, February 8, 2023, https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security.

196. "U.S. International Development Finance Corporation (DFC)," *USA.gov*, Accessed January 31, 2024, https://www.usa.gov/agencies/u-s-international-development-finance-corporation.

197. "Blue Dot Network," *U.S. Department of State*, Accessed on January 31, 2024, https://www.state.gov/blue-dot-network/.

198. "USAID Digital Strategy," *U.S. Agency for International Development (USAID)*, Accessed on January 31, 2024, https://www.usaid.gov/digital-development/usaid-digital-strategy.

199. "FACT SHEET: Partnership for Global Infrastructure and Investment at the G7 Summit," *The White House*, May 20, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/fact-sheet-partnership-for-global-infrastructure-and-investment-at-the-g7-summit/.

200. Christian Vasquez, "Biden's budget seeks increase in cybersecurity spending," *CyberScoop*, March 9, 2023, https://cyberscoop.com/biden-budget-2023/.

201. Russell Deeks, "The Digital Silk Road - China's $200 billion project," *BBC Science Focus*, December 8, 2018, https://www.sciencefocus.com/future-technology/the-digital-silk-road-chinas-200-billion-project.

202. "How Do the House and Senate Appropriation Bills Differ?" *The Peter G. Peterson Foundation*, September 21, 2023, https://www.pgpf.org/blog/2023/09/how-do-the-house-and-senate-appropriation-bills-differ.

203. "Rep. Bera Raises Alarm on Republican Budget Cuts to State Department and USAID, Hampering Ability of U.S. to Outcompete Beijing," *Office of U.S. Representative Ami Bera*, July 19, 2023, https://bera.house.gov/news/documentsingle.aspx?DocumentID=400169.

Most importantly, the Biden administration needs to understand that technical solutions and advanced cyber capabilities alone are not sufficient for defending American interests in the digital realm. As Dimitri Alperovitch, the co-founder and former CTO of CrowdStrike, has argued,[204] countering the Chinese, Russian, Iranian, and North Korean cyberthreats requires addressing them in their wider geopolitical contexts. Additionally, despite important differences[205] between the cyber and physical realms, missteps in conventional diplomacy[206] will inevitably hinder deterrence of overseas adversaries in the digital domain. Thus, for Washington's cybersecurity and cyber diplomacy initiatives to succeed, the broader foreign policy framework of which they are part must also be robust and well executed. Similarly, advancing an open, free, global, interoperable, reliable, and secure Internet will entail more than just denouncing the "splinternet"[207] and rebuking the model of cyber-sovereignty.[208] If American policymakers wish to make the case for online freedom and the unrestricted flow of data to countries around the world, they must wed these with other parallel efforts to rectify and clarify perceived faults with globalization,[209] free trade, and democracy[210] in general.

204. Dmitri Alperovitch, "The Case for Cyber-Realism: Geopolitical Problems Don't Have Technical Solutions," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism.

205. Sarah Kreps and Jacquelyn Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics," *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, https://doi.org/10.1093/cybsec/tyz007.

206. "The Biden-Iran Hostage Deal," *The Wall Street Journal*, August 13, 2023, https://www.wsj.com/articles/the-biden-iran-hostage-deal-house-arrest-middle-east-jail-sanctions-evin-prison-3d736837.

207. Shira Ovide, "The Internet Is Splintering," *The New York Times*, February 17, 2021, https://www.nytimes.com/2021/02/17/technology/the-internet-is-splintering.html.

208. Eric Rosenbach and Shu Min Chong, "Governing Cyberspace: State Control vs. The Multistakeholder Model," *Belfer Center for Science and International Affairs*, Harvard Kennedy School, August 2019, https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

209. Sinan Ülgen and Ceylan Inan, "From the Local to the Global: The Politics of Globalization," *Carnegie Europe*, February 17, 2022, https://carnegieeurope.eu/2022/02/17/from-local-to-global-politics-of-globalization-pub-86310.

210. "Democracies in Decline," *Freedom House*, Accessed January 31, 2024, https://freedomhouse.org/issues/democracies-decline.

Conclusion and Summary

The Biden administration's NCS lays out a bold and transformative agenda for safeguarding America's digital landscape. Some of these noteworthy undertakings include:

- Promoting multi-stakeholder cooperation with the private sector, international partners, and civil society organizations
- Modernizing legacy systems and transitioning to ZTA
- Investing in critical and emerging technologies and revitalizing America's cyber workforce
- Crafting cybersecurity regulations and shifting liability for vulnerable software while minimizing the impact on market dynamics
- Embracing an offensive approach to foreign cyber operations by augmenting disruption campaigns against adversaries and malicious actors

While many of these objectives build off of ones set forth by Donald Trump[211] and CYBERCOM Director Paul Nakasone,[212] others — like realigning market incentives to favor secure software design, shifting liability for vulnerable products and services from end-users onto the best-positioned actors in the private sector, and establishing stronger regulatory regimes to enforce cybersecurity requirements — set the White House's approach apart from that of previous administrations. The document also implicitly acknowledges that cyberattacks against the United States and its allies cannot be completely prevented, and instead outlines steps to nurture a resilient digital ecosystem at home and abroad.

Nonetheless, even after the publication of the Implementation Plan[213] and agency-specific strategies,[214]

211. "The National Cybersecurity Strategy of the United States," *The White House*, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

212. Paul Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

213. "National Cybersecurity Strategy Implementation Plan," *The White House*, July 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

214. "FY 2024-2026 Cybersecurity Strategic Plan," *U.S.*

the Biden administration will still face numerous challenges on the domestic and international stages while striving to achieve its ambitious vision, such as:

- Navigating implementation barriers, budgetary restrictions, and political gridlock
- Protecting personal data and establishing interoperable data transfer frameworks with global partners without imposing major compliance costs on technology companies
- Addressing deficiencies in critical infrastructure OT and difficulties in adopting ZTA
- Emphasizing manufacturing, not just innovation, to secure American leadership in next-generation technologies
- Harmonizing regulations across critical infrastructure sectors and carefully designing regulatory frameworks and liability regimes
- Reconciling an offensive cyber posture with a commitment to promote and uphold norms of responsible state behavior for cyberspace
- Ensuring that U.S. cyber strategy does not neglect the dangers posed by non-state actors and proxy groups
- Promoting a values-driven digital ecosystem and countering the model of cyber-sovereignty without sidelining key non-democratic cyber and technology partners
- Expanding digital trade and commerce, increasing investments in digital infrastructure development, and integrating cyber diplomacy effectively with other instruments of statecraft

To enhance its competitiveness in today's digital world, the United States will need to devise effective and sustainable policies for triumphing over these obstacles and confronting the growing threats throughout the global cybersecurity landscape.

Cybersecurity and Infrastructure Security Agency (CISA), August 2023, https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.

Middle
East
Institute

WWW.MEI.EDU