Teneo

Following Publication of National Policies, U.S. President Joe Biden's Administration Releases International Cyber Strategy

June 2024

On May 13, U.S. President Joe Biden's administration rolled out its International Cyberspace and Digital Policy Strategy, which outlines a doctrine of "digital solidarity" and international coalitions to "promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem."

The Strategy is the first articulated U.S. global cyber strategy in over a decade and has the potential to elevate Washington's role in countering cyber threats on a global scale, create international consensus on artificial intelligence (AI), and position the U.S. against other countries in setting global cybersecurity norms.[1] The Strategy comes after a year of directives put forward by the Biden administration aimed at strengthening the country's approach to cyber and technology policy, including the White House's National Cyber Strategy and the National Cybersecurity Strategy Implementation Plan.

This article analyzes the driving forces and components of the Strategy, examines its potential to elevate Washington's role in countering global cyber threats, and outlines key considerations for

[1] https://www.politico.com/news/2024/05/06/biden-international-cybersecurity-plan-00156190

executives and organizations seeking to navigate evolving cyber threats within a rapidly evolving digital landscape.

An Emphasis on “Digital Solidarity”

On May 13, the U.S. State Department released its International Cyberspace and Digital Policy Strategy, aligning American foreign policy with a vision of an “open, resilient, defensible, and rights-respecting digital ecosystem” laid out by the Biden administration’s 2023 National Cybersecurity Strategy (NCS). Embracing the NCS’s emphasis on strengthening the digital landscape through international partnership, the Strategy outlines a doctrine of “digital solidarity” that champions the role of diplomacy and collaboration between allies and partners to shape the design, development, and governance of cyberspace and digital technology. Digital solidarity anchors coordination, integration, and mutual support between like-minded, rights-respecting nations as cornerstones of a more resilient digital ecosystem. As noted by U.S. Secretary of State Antony Blinken, the U.S. seeks to build an international coalition that capitalizes on “our solidarity with the majority of the world that shares [its] vision for a vibrant, open, and secure technological future” and will leverage “an unmatched network of allies and partners with whom [it] can work in common cause.”

Through proactive participation by government, business, and civil society across the globe, the approach envisions a strengthened rules-based order that aligns U.S. allies and partners on strategies to unlock the full benefits offered by the digital realm while minimizing its potential harms and vulnerabilities. Specifically, the Strategy identifies four key areas of action designed to foster digital solidarity over the next three to five years:

- Promoting an open, inclusive, secure, and resilient digital ecosystem
- Aligning rights-respecting approaches to digital and data governance with international partners
- Building international coalitions to counter cyber threats and advance responsible state behavior in cyber space
- Strengthening digital and cyber capacity by international partners

How We Got Here

The Strategy emerges at a time of rapid technological change and evolving threats to digital security. As executives are aware, the challenges emanating from this complex landscape are myriad. Adversarial state and non-state actors continue to craft sophisticated cyberattacks capable of hijacking national infrastructure, derailing private business functions, and threatening the privacy of individual citizens. Authoritarian states seek to impose an alternate vision of digital governance, underpinned by mass surveillance, online censorship, and the restriction of human rights online. Emerging economies are leveraging digital technologies to drive economic growth, while grappling with the challenge of preserving autonomy, neutrality, and safety. The nascent AI revolution promises expanding productivity and prosperity, as well as significant and unpredictable threats to equality, economic stability, competition, privacy, surveillance, and repression. These forces present a significant challenge to the U.S.-led effort to shape the digital landscape over the coming decade: How to best balance the risks and rewards of this ever-changing environment during a future of intensified geopolitical competition.

As a whole, the Strategy formalizes the Biden administration's approach to this challenge, which has already embraced the key principles underpinning digital solidarity across various initiatives fostering coordination and alignment on cyberspace issues with U.S. allies and partners. In 2021, the Biden administration convened the annual International Counter Ransomware Initiative, which today leverages the expertise of more than 60 countries to bolster business models within the ransomware ecosystem. In 2023, following destructive cyberattacks on Costa Rica and Albania, the White House granted $25 million in cybersecurity assistance to each country to strengthen their digital infrastructure and improve incident responses. Similarly, in 2023, the U.S. led the establishment of the Tallinn Mechanism, a donor coordination group designed to efficiently deliver cybersecurity assistance to Ukraine as it resists Russia's full-scale invasion. This past March, the U.S. galvanized pledges by nearly 20 countries to curb the misuse of commercial spyware. Additionally, the U.S. continues to play a key role in developing guidelines for safe and secure AI systems, leading the push for a landmark AI Safety resolution passed by the UN General Assembly in March. Recognizing that nearly all foreign policy issues unfolding over the coming decade – from international security to global health to climate change – will depend on decisions and investments in cyberspace and digital technology made today, the Biden administration's Strategy will streamline U.S. foreign policy efforts to continue crafting an open, secure, and resilient global digital ecosystem today and into the future.

Elevating the U.S.' Role in Cyber Diplomacy

In a concerted effort to strengthen Washington's leadership in cyber diplomacy, the Strategy emphasizes digital solidarity by fostering global consensus on cyber policies that uphold human rights and American values. By forging alliances with like-minded nations to defend against ideological adversaries, the Strategy targets foreign entities that undermine information integrity, pose threats to democracy, erode trust in institutions, or jeopardize electoral processes, further promoting U.S. principles and aims.

The Strategy details plans to initiate proactive dialogues at the UN, including establishing a framework for responsible behavior in cyberspace. By setting global governance standards, the Strategy aims to align emerging technologies with democratic principles and respect for human rights. The U.S. – in coordination with its allies – affirms that it will denounce harmful practices and may impose consequences on nations misusing technologies that endanger global safety and security.

Finally, the U.S. intends to use the Strategy to deter actors who stifle dissent through internet and telecommunications shutdowns, unlawfully intrude on privacy, restrict individuals' freedoms of expression, and perpetrate technology-facilitated gender-based violence (TFGBV). The Strategy commits to holding technology platforms accountable and implementing domestic cyber policies that uphold its core values.

Emphasizing the Importance of the Private Sector in International Cyberspace

The Biden administration’s Strategy for advancing an innovative, rights-respecting international cyberspace and digital technology environment emphasizes the private sector’s central role in expanding digital solidarity through diplomacy. It builds upon the framework laid by the 2023 NCS, which placed “responsibility for defending cyberspace onto the government and private sector organizations that are the most capable and best positioned to reduce risks” within the digital realm. As such, the Strategy recognizes that U.S. companies have been leaders in digitalization and therefore must leverage their positions to embrace leadership roles in promoting sustainability, security, and accountability in cutting-edge technology like AI. It hallmarks the private sector as a spring of innovation and encourages technology companies to apply their understanding of the drivers of systems development and deployment to urgent foreign policy efforts to ensure open, secure, and resilient global digital networks.

In practice, the Strategy envisions the private sector as impacting digital diplomacy in bold ways. For example, it references the private sector’s role in defending against malicious cyber activities, drawing on the history of private sector aid to Ukraine in the aftermath of Russia’s full-scale invasion to illustrate the direct role technology companies can play in U.S. foreign policy efforts to support the digital resiliency of allies and partners. In this example, technology firms provided services, tools, and threat intelligence to help Ukraine defend government and critical infrastructure networks, helping government agencies and business to continue operating in the face of open conflict. Imagining a wide range of public-private partnerships aimed at digital security and resiliency – from leveraging private partners to strengthen security of fifth-generation wireless networks (5G) to reducing the costs of secure cloud infrastructure for emerging economies – the Strategy has laid a framework that elevates the private sector’s role in shaping U.S. foreign policy on the most pressing issues shaping the digital landscape.

Considerations for Executives

In response to the publication of the U.S. International Cyberspace and Digital Policy Strategy, we provide several key considerations and actions as organizations innovate while mindful of cybersecurity amid an evolving global digital landscape.

- *Strategic Alignment:* Executives have an opportunity to be proactive and align with the guiding principles and action items outlined in the Strategy. This involves prioritizing investment and an operating structure that integrates robust cybersecurity measures and data governance frameworks in tandem with international partners that are compliant with emerging international standards and human rights laws. Companies should also conduct a thorough review of their current cybersecurity policies and practices to ensure they align with the frameworks and policies laid out by the U.S. federal government.

- *Cybersecurity as a Foundation for Innovation*: As stated in the Strategy, "cybersecurity, data security, and cyber-resilience are prerequisites for and enablers of economic growth." A focus on cyber risk mitigation and strategies such as zero trust architecture, supply chain vulnerability audits, diversification strategies, and business continuity planning will serve to protect digital assets, minimize disruption, and maintain resilience amid an ever evolving and volatile cyber threat environment. At the same time, this foundational resilience provides a platform to explore growth and innovation strategies and potentially take certain risks that would not have been sustainable in a more vulnerable environment.

- *Responsible and Inclusive Technology Use*: Executives should champion initiatives that promote the responsible and inclusive use of digital technologies. This may include initiatives to ensure that services are accessible to diverse populations. When utilizing emerging technologies such as AI, executives and their companies should work to protect user privacy and prevent the misuse of technology, including by malicious actors such as hacktivist groups and those seeking to leverage AI to spread disinformation. Executives should also ensure that their organization's employees receive thorough training on responsible and safe AI use and the detection of malicious communications that may have exploited generative AI technologies.

- *Enhanced Digital and Cybersecurity Capacity*: To support the Strategy's aim of building international partner capacity, the U.S. may seek out companies that can offer training and development programs to improve digital literacy and other cybersecurity skills, particular for a new generation of employees entering the workforce. Executives should consider forming or joining consortiums and other initiatives aimed at upskilling or reskilling resources in the cybersecurity arena with the goal of building capacity in digital technologies, particularly in regions that are important for their business operations.

- *International and Public-Private Partnerships:* Given the Strategy's focus on building digital solidarity and international cooperation, executives and their companies should proactively seek partnerships with global entities, including governments/government agencies, peer organizations in their respective sectors, and civil society organizations with a similar and vested interest in promoting an open, inclusive, secure, and resilient digital ecosystem. These partnerships can aid in navigating emerging international digital policies and standards. Executives can leverage these collaborations to share knowledge, resources, and best practices, thereby contributing to the Strategy's objectives.

- *Monitoring For Further Government Action, Including Implementation Plan:* Following the publication of the U.S. National Cyber Strategy, the government published an Implementation Plan, outlining steps to put the strategy into force. Executives should remain attuned to further updates to the international Strategy and the possible publication of a State Department implementation plan in the coming months.

By aligning corporate strategies with the U.S. International Cyberspace and Digital Policy Strategy, executives can set themselves on a path for compliance with emerging international norms as well as play a pivotal role in shaping the future of global digital technologies. This alignment will enhance their competitive advantage by fostering innovation and strengthening their organization’s cybersecurity posture.

For more information, email: Resilience&Intelligence@teneo.com

Authors

Rachel Cole
Senior Associate, Security Risk Advisory
Rachel.Cole@teneo.com

Liad Mansky
Associate, Security Risk Advisory
Liad.Mansky@teneo.com

Lauren Menzie
Associate, Security Risk Advisory
Lauren.Menzie@teneo.com

Eric Ryan
Associate, Security Risk Advisory
Eric.Ryan@teneo.com

Teneo

The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com

This material was produced by Teneo for use solely by the recipient. This communication is intended as general background research and is not intended to constitute advice on any particular commercial investment or trade matter or issue and should not be relied upon for such purposes. The views expressed here represent opinions as of this date and are subject to change without notice. The information has been obtained from sources believed to be reliable but no guarantees can be given as to its accuracy, completeness or reliability. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or otherwise, without the prior consent of Teneo. Teneo refers to Teneo Holdings LLC and its affiliates.