THE 2023 NATIONAL CYBERSECURITY STRATEGY: HOW DOES AMERICA THINK ABOUT CYBERSPACE?

DIVYANSHU JINDAL & MOHAMMED SOLIMAN

May 2023

Background

On March 2, 2023, the Biden administration released the new National Cybersecurity Strategy, replacing the 2018 Trump administration Cybersecurity Strategy. The new strategy builds on the previous one, continuing the momentum on many of its priorities while seeking to carry forward and evolve many of the strategic efforts originally initiated by the 2008 Comprehensive National Cybersecurity Initiative.

Dividing the strategy into five pillars, the Biden administration focuses on defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, investing in a resilient future, and forging international partnerships to pursue shared goals.

The new strategy underlines two fundamental shifts: rebalancing the responsibility to defend cyberspace and realigning incentives to favor long-term investments. It takes a fresh look at the balance between the government and the private sector in terms of roles and responsibilities toward mitigating cyber risks. It recognizes the present realities where the end users bear a disproportionate burden for reducing such risks and, in an ambitious outlook change, seeks a legislative mechanism to enforce liability on providers when they fail to meet basic security standards. While underlining the government's role to protect its own systems and engage in diplomacy, law enforcement, and the collection of intelligence, the strategy places an emphasis on the need for private entities to protect their systems.

The Biden administration's strategy highlights the need to make substantial public sector investments in the sector to assure that the U.S. continues to stay ahead of the curve in modern technology and innovation, maintaining its global leadership role. For this, the Biden administration deems it necessary to incentivize decision-making while balancing short-term imperatives against a long-term vision.

An Overview of the Priorities in Five Pillars

1. Defend Critical Infrastructure

- Expand the use of minimum cybersecurity requirements in critical sectors and harmonize regulations to reduce the burden of compliance.
- Enable public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services.
- Defend and modernize federal networks and update federal incident response policy.

2. Disrupt and Dismantle Threat Actors

- Strategically employ all tools of national power to disrupt adversaries.

- Engage the private sector in disruption activities through scalable mechanisms.
- Address the ransomware threat through a comprehensive federal approach and in lockstep with international partners.

3. Shape Market Forces to Drive Security and Resilience

- Promote privacy and the security of personal data.
- Shift liability for software products and services to promote secure development practices.
- Ensure that federal grant programs promote investments in new infrastructure that are secure and resilient.

4. Invest in a Resilient Future

- Reduce systemic technical vulnerabilities in the foundation of the internet and across the digital ecosystem while making it more resilient against transnational digital repression.
- Prioritize cybersecurity R&D for next-generation technologies such as post-quantum encryption, digital identity solutions, and clean energy infrastructure.
- Develop a diverse and robust national cyber workforce.

5. Forge International Partnerships to Pursue Shared Goals

- Leverage international coalitions and partnerships among like-minded nations to counter threats to the digital ecosystem through joint preparedness, response, and cost imposition.
- Increase the capacity of partners to defend themselves against cyber threats, both in peacetime and in crisis.
- Work with allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology (ICT) and operational technology (OT) products and services.

Decoding the Strategy: What Does it All Mean?

Focus on Public-Private Cooperation

The strategy underlines that the industry and government must drive effective and equitable collaboration to correct market failures, minimize the harm from cyber incidents to society's most vulnerable members, and defend the shared digital ecosystem. It appreciates the commitments made by private sector entities to engage in collaborative defense efforts like the "Shields Up" campaign, which preceded the beginning of the ongoing Russia-Ukraine war, to proactively increase preparedness and promote effective measures to combat malicious activity.

The strategy encourages private sector partners to come together and organize efforts through one or more non-profit organizations that can serve as hubs for operational collaboration with the federal government.

This collaborative approach is of great interest to countries worldwide struggling to evolve a robust mechanism for policy inputs. Those working to craft a national cybersecurity strategy can benefit from policy inputs from non-profits through a structural and institutionalized framework. As countries look to decide whether or not to adopt strict data localization policies, factors like the identification of gaps in authorities to drive better cybersecurity practices in the cloud computing industry and other third-party services will be of great value. This is where expanded collaboration can play an important role.

Focus on Investments

Assuring the continued U.S. leadership in technology and innovation, the new strategy reemphasizes that a resilient and flourishing digital future tomorrow begins with investments made today. Toward this goal, it states that the federal government must leverage strategic public investments in innovation, R&D, and education to drive outcomes that are economically sustainable and serve the national interest.

The Biden administration also seeks to support non-governmental standards developing organizations (SDOs) to partner with industry leaders, international allies, academic institutions, and professional societies to secure emerging technologies. In particular, it aims to secure three families of technologies: quantum computing and AI, biotechnology, and clean energy. This investment focus will likely resonate in countries engaged in developing their own technology and governance visions for the decade ahead.

Calling Out Adversaries

The new strategy puts the spotlight on the governments of Russia, China, Iran, North Korea, and other autocratic states with revisionist intentions that are aggressively using advanced cyber capabilities to pursue objectives that run counter to accepted international norms as well as against U.S. interests.

Photo above: The White House in Washington D.C., United States on Jan. 10, 2023. Photo by Celal Gunes/Anadolu Agency via Getty Images.

It calls out the People's Republic of China as the broadest, most active, and most persistent threat to government and private sector networks and the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so.

It highlights that Russia remains a persistent cyber threat, refining its cyber espionage, attack, influence, and disinformation capabilities to coerce sovereign countries; harboring transnational criminal actors; aiming to weaken U.S. alliances and partnerships; and subverting the rules-based international system. It further recognizes the growing sophistication and willingness of the governments of Iran and North Korea to carry out malicious activities in cyberspace. The new strategy highlights the immediate need to counter further advances in both countries' capabilities, underlining in particular Iran's use of its cyber capabilities to threaten U.S. allies in the Middle East, chief among them Israel and the Arab Gulf states, and both Iran and North Korea's exploitation of cyberspace and cryptocurrency platforms to generate revenues to help reduce fiscal deficits caused by severe Western sanctions.

In recent years, the U.S. has — along with allies like the U.K. and Australia — taken an active stance toward public and collective attribution of malicious activities in cyberspace. As it looks toward expanding partnerships, Washington can aim to bring closer countries like India that face similar threats, but do not yet have an attribution framework or a clearly defined policy.

Focus on Values and Foundations

The core theme of the new strategy is an ambition for the further values-driven development of the digital ecosystem. It stresses that the U.S. must seize the opportunity to instill its most cherished values, as embodied by the Declaration for the Future of the Internet (DFI) and the Freedom Online Coalition, in future cyberspace governance models.

Taking note of the inherently vulnerable nature of cyberspace, it emphasizes the need to make fundamental changes to the underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and frustrating the forces that would threaten it.

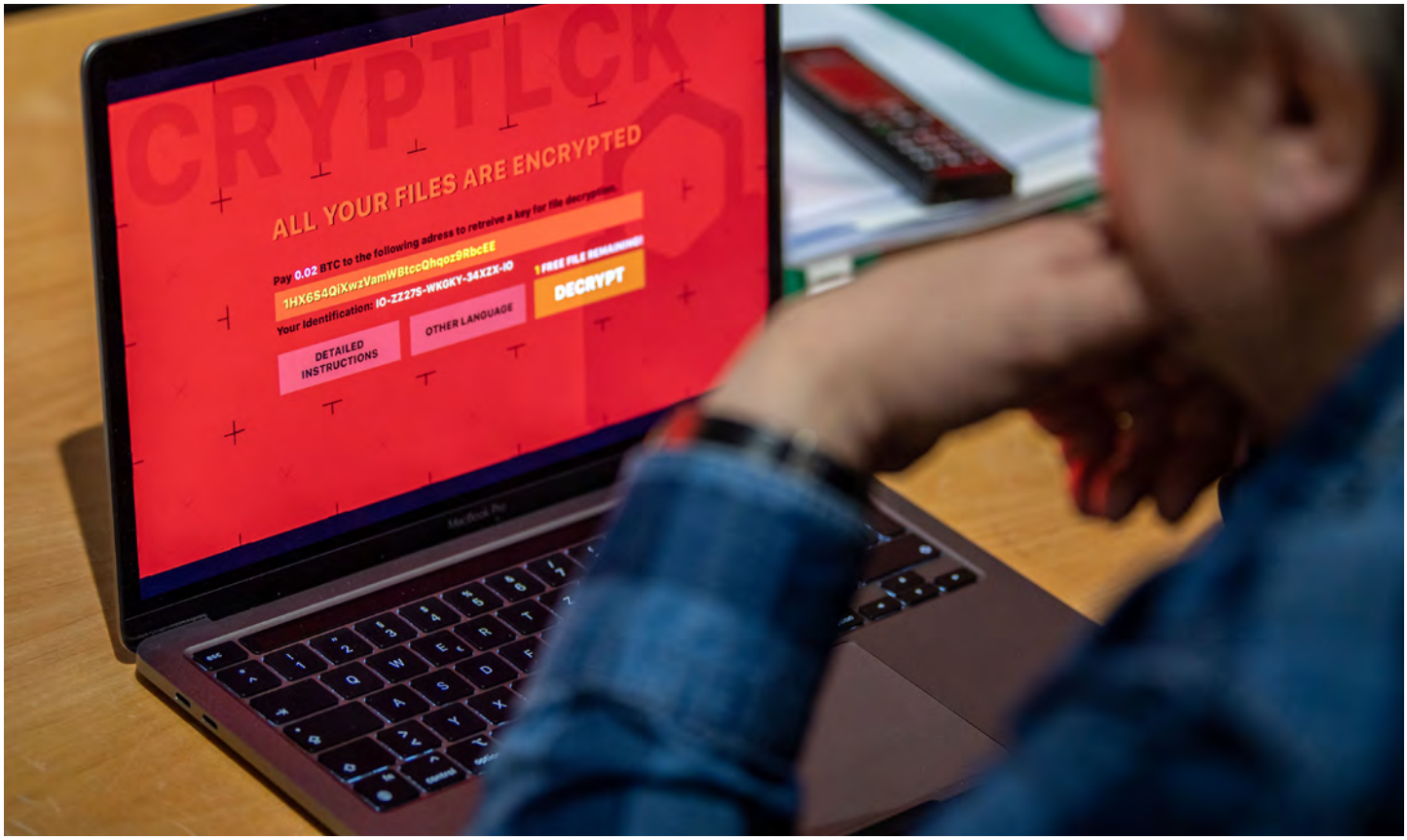

Photo above: A man sits in front of a laptop infected with ransomware. In attacks with extortion software, data on computers is encrypted and the hackers demand money for its release. Photo by Lino Mirgeler/picture alliance via Getty Images.

Focus on Resilience

The strategy states that the Biden administration is committed to improving federal cybersecurity through long-term efforts to implement a zero-trust architecture strategy and modernize IT and OT infrastructure. In doing so, it hopes that the federal cybersecurity program can be a model for critical infrastructure across the U.S. for how to successfully build and operate secure and resilient systems.

Along with this, the Biden administration seeks to embark on a clean-up effort to reduce systemic risks and the most pressing security challenges, without disrupting the existing platforms and services. This includes the technical foundations of the digital ecosystem, which are inherently vulnerable.

Considering the long-standing pioneer position of the U.S. in terms of digital innovation and in shaping the contours of cyber policies, how the U.S. government aspires to re-envision, re-shape, and re-vitalize this ecosystem will be critical for all countries.

Focus on Offensive Approach for Deterrence

The strategy states that the U.S. will use all of its instruments of national power to disrupt and dismantle threat actors whose actions threaten its interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities.

It complements the Department of Defense's strategic approach, as laid out in the 2018 Cyber Strategy, of "defending forward," stating that it has helped generate insights on threat actors, identify and expose malware, and disrupt malicious activity before it could affect its intended targets.

As active offense increasingly becomes the operational norm, countries worldwide might deem it necessary to refine and expand their capabilities. This could potentially lead to an accelerating arms race in the near future.

Focus on Threat Monitoring and Intelligence Sharing

The new strategy recognizes the need to increase the speed and scale of cyber threat intelligence sharing to

proactively warn cyber defenders and notify victims when the government has information that an organization is being actively targeted or may already be compromised. It affirms that the federal government will work with cloud and other internet infrastructure providers to quickly identify malicious use of U.S.-based infrastructure, share reports of malicious use with the government, make it easier for victims to report abuse of these systems, and make it more difficult for malicious actors to gain access to these resources in the first place.

Focus on Ransomware

Acknowledging ransomware's impact on key critical infrastructure services, the new strategy states that the U.S. will employ all elements of national power to counter the threat by leveraging international cooperation to disrupt the ransomware ecosystem, investigating crimes to disrupt infrastructure and actors, bolstering critical infrastructure resilience to withstand attacks, and addressing the abuse of virtual currency to launder ransom payments.

It highlights that the White House has convened the Counter-Ransomware Initiative (CRI) with participation from more than 30 countries.

Focus on Legislative Reform and Regulations

Underscoring that regulation can level the playing field and enable healthy competition without sacrificing cybersecurity or operational resilience, the Biden administration deems it vital that the new and updated cybersecurity regulations be calibrated to meet the needs of national security and public safety, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation.

The strategy states that regulations should be performance-based, leverage existing cybersecurity frameworks and international standards in a manner consistent with current policy and law, and when necessary, pursue cross-border regulatory harmonization to prevent cybersecurity requirements from impeding digital trade flows.

The administration supports legislative efforts to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data and aims to work with Congress and the private sector to develop legislation that establishes liability for software products and services.

With an increasing number of high-impact ransomware and other cyberattacks in recent years, cyber insurance has become a critical focus around the world. As private insurers continue to recalibrate their strategies to avoid overexposure to risk in cases of catastrophic mass-scale cyber events, there are growing calls for a greater federal role, including in the provision of insurance, in response to such events. The new strategy states that the federal government could be called upon to stabilize the economy and facilitate recovery and that the administration will assess possible federal insurance structures to support the cyber insurance market.

Focus on Capacity Building

The strategy highlights the hundreds and thousands of unfilled vacancies in cybersecurity positions nationwide and resolves to develop a national strategy to strengthen the U.S. cyber workforce. Recognizing that recruiting and training the next generation of cybersecurity professionals will require federal leadership, the document lays out plans to develop a National Cyber Workforce and Education Strategy to take a comprehensive and coordinated approach to expanding the national cyber workforce, improving its diversity, and increasing access to cyber educational and training pathways.

Establishing an effective cybersecurity workforce has been a thorn in the side of almost every country in the world. Standing as the lone cyber superpower, how the U.S. tackles this challenge will remain of great interest to all others.

Focus on International Partnerships

As the world watches the accelerating tech decoupling between the West and China, the focus on international partnerships is bound to take on increasing significance.

Aiming to rejuvenate U.S. cyber diplomacy on international platforms, the new strategy reinforces the applicability of existing international law and calls for upholding globally accepted voluntary norms of responsible state behavior during peacetime in cyberspace. It reaffirms the focus on securing global supply chains and commits to building on the National Strategy to Secure 5G in collaboration with partners around the globe. This underlines the U.S. commitment to international partnerships on cyber issues, emphasizing the importance of working with allies and partners to build a defensible, resilient, and values-aligned digital ecosystem. The strategy highlights that, through multilateral mechanisms

like the Quad, AUKUS, Indo-Pacific Economic Framework for Prosperity, and the Americas Partnership for Prosperity, the U.S. and its international allies and partners are advancing shared goals for cyberspace.

Taking note of the supply chain disruptions during the pandemic, the new strategy aims to secure global supply chains for ICT and OT products and services. Considering the emerging tech war and decoupling between China on the one hand and the West and many of its partners on the other, the new strategy mentions that the U.S. is partnering with allies to develop trustworthy and reliable supply chains for 5G and other critical technologies.

Data-Driven Implementation

The new strategy states that the U.S. is laying the foundations for real-time global collaboration by leveraging vast amounts of data and computing power that will unlock scientific discoveries. The federal government will take a data-driven approach toward the implementation of the new strategy and will measure investments made, progress toward implementation, ultimate outcomes, and the effectiveness of these efforts.

Opportunities for Partners and Allies in the Middle East

The U.S. cybersecurity strategy provides a framework for Washington to collaborate with its Middle Eastern partners in sharing threat intelligence and other critical information with the aim of identifying and addressing potential cyber attacks before they occur. Additionally, the U.S. can help build up its Middle Eastern partners' cyber capabilities through training and technical assistance, including establishing cyber defense teams, improving network security, and sharing cybersecurity best practices. In an even more advanced level of cyber cooperation, regional partners and the United States could jointly conduct cyber exercises to enhance their capabilities and coordination in responding to cyber attacks from malicious actors. The U.S. could also work closely with regional partners to develop norms of behavior for cyberspace, promote regional cooperation on cybersecurity, and address the malicious use of cyber tools.

Conclusion

The National Cybersecurity Strategy 2023 should be recognized as the product of U.S. ambitions to continue to shape the future of global cyberspace, which is highly dependent on U.S. infrastructure. The highlighted themes and objectives are consistent with how Washington is navigating the global technological decoupling and will surely support the U.S.'s economic resilience and cybersecurity in an age of multipolar global disorder. As recognized in the strategy, national cybersecurity cannot be future-proofed, and the government's response to current threats and those not yet conceived will rely on the ability of government agencies, regulators, the private sector, and users to collaborate on the Biden administration's approach.

In looking forward, implementation will be a key concern for this strategy and its impact on tech manufacturers, service providers, and users. The successful implementation of this strategy will dictate the security and resilience of U.S. cyberspace and also shape broader dynamics, as allies look to follow suit and adversaries look to use cyber tools to threaten U.S. security. The potential for the strategy to result in inclusive regulation will depend on how quickly and effectively lawmakers and the private sector can align on the tenets of the Biden administration's approach. Considering the diversity of ways in which private sector entities are relevant to the strategy and its proposed policy approaches, this could be simple in some areas but remain complex in most.

Divyanshu Jindal is a Non-Resident Scholar with MEI's Strategic Technologies and Cyber Security Program and a Research Associate at NatStrat, India. His work focuses on the geopolitics of tech and cyber and India's cyber diplomacy.

Mohammed Soliman is the director of MEI's Strategic Technologies and Cyber Security Program, and a Manager at McLarty Associates' MENA Practice. His work focuses on the intersection of technology, geopolitics, and business in emerging markets.