CYBER THREATS AND THE NEW *CYBER STRATEGY FOR AMERICA*

The remarks below were delivered at a symposium on "Cyber Threats and the New Cyber Strategy for America*" hosted by the National Institute for Public Policy on April 29, 2026. The symposium examined the growing threat of cyber warfare, the difficulties of attribution, and how the United States and allies should respond to cyber attacks. It also assessed the recently released March 2026 White House* Cyber Strategy for America *and how it compares and contrasts to previous cyber strategies, including the Biden Administration's 2023* National Cybersecurity Strategy *and the first Trump Administration's 2018* National Cyber Strategy*.*

David J. Trachtenberg (moderator)
David J. Trachtenberg is Senior Scholar at the National Institute for Public Policy and previously served as Deputy Under Secretary of Defense for Policy.

Cyber threats have become an inescapable part of the strategic environment and the landscape of the 21st century battlefield. And cyber security is more important today than ever before. I doubt there is anyone on this call who has not been affected in one way or another by cyber intrusions or hacking by malicious actors. Data breaches, phishing attempts, malware, ransomware, and other dangerous and destructive behaviors are now a growing part of the contemporary electronic information space.

They are also a tool for adversaries like Russia and China to use against the United States, its allies, and partners. For example, Ukraine's government, financial, and energy sectors, as well as satellite networks, have been targeted by Russian cyber attacks.[1] And the head of U.S. Cyber Command testified yesterday that foreign adversaries will likely try to interfere in this year's midterm elections.[2]

As a recent report noted, cyber attacks against U.S. critical infrastructures—presumably by pro-Iranian groups—have increased in number and severity in the wake of Operation Epic Fury. In March, the Los Angeles County Metropolitan Transportation Authority was breached, leading officials to shut down a part of its control network.[3]

Last week, the Chairman of the House Cyber, Information Technologies, and Innovation Subcommittee noted increased cyber targeting of telecommunications and other critical U.S. infrastructures. He also highlighted U.S. efforts to address these concerns, including growth

[1] Antony J. Blinken, Press Statement, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," Department of State, May 10, 2022, https://2021-2025.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

[2] Martin Matishak, "Cyber Command, NSA chief warns foreign adversaries likely to target midterms," *Recorded Future News* (*The Record)*, April 28, 2026, https://therecord.media/cyber-command-nsa-chief-midterm-election-threat.

[3] Chris Teale, "Pro-Iran hackers appear to increase critical infrastructure cyberattacks," *Defense One*, April 17, 2026, https://www.defenseone.com/threats/2026/04/iran-hackers-infrastructure-cyberattacks/412941/.

in the DoD Cyber Mission Force and establishment of an Assistant Secretary for Cyber Policy.[4]

Last month, the White House released *President Trump's Cyber Strategy for America*, which called for "unprecedented coordination across government and the private sector" and for making "the most of America's cyber capabilities for both offensive and defensive missions."[5] Along with the release of the cyber strategy, the president signed an Executive Order on "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens."[6] And the National Cyber Director recently stated that President Trump is expected to sign additional Executive Orders on cyber security in the near future.[7]

The unclassified strategy is only 4 pages long (excluding the president's cover letter) and does not name any adversaries that are known to engage in cyber warfare. This is a departure from the 2018 *National Cyber Strategy*, which stated, "Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains."[8] It lists six "pillars of action" intended to: shape adversary behavior; streamline regulations; modernize government networks; secure critical infrastructure; sustain American technological superiority; and build talent in the cyber workforce.

Some of these pillars seemingly align with the 2018 strategy and the five pillars of the Biden Administration's 2023 *National Cybersecurity Strategy*, which also prioritized defending critical U.S. infrastructure and disrupting adversary cyber threats. While the Biden *National Cybersecurity Strategy* superseded the 2018 *National Cyber Strategy* issued by the first Trump Administration, it acknowledged "continue[d] momentum on many of its [the Trump Administration's] priorities…."[9]

The 2023 *National Cybersecurity Strategy* and the *2024 Report on the Cybersecurity Posture of the United States* also suggested the need to deal with cyber threats by working with and strengthening the resilience of allies and partners—a theme only tangentially referenced in the new 2026 *Cyber Strategy*. While noting that "Defending cyberspace and safeguarding freedom is a collective effort," the 2026 strategy asserts that "the distribution

---

[4] Opening Statement of Rep. Don Bacon (R-NE), "Bacon: We're in a New Era of Cyber Warfare," House Armed Services Committee Subcommittee on Cyber, Information Technologies, and Innovation, Hearing on the Cyber Posture of the Department of Defense, April 21, 2026, https://armedservices.house.gov/news/documentsingle.aspx?DocumentID=6527.

[5] The White House, *President Trump's Cyber Strategy for America*, March 2026, p. 2, https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf.

[6] The White House, Executive Order on "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens," March 6, 2026, https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/.

[7] David Dimolfetta, "Expect more cybersecurity executive orders soon, national cyber director says," *NextGov/FCW*, April 15, 2026, https://www.nextgov.com/cybersecurity/2026/04/expect-more-cybersecurity-executive-orders-soon-national-cyber-director-says/412861/?oref=ng-author-river.

[8] The White House, *National Cyber Strategy of the United States of America*, September 2018, p. 2, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[9] The White House, *National Cybersecurity Strategy*, March 2023, p. 6, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

of cost and responsibility must be fair across the U.S. and allies who share our democratic values."[10]

In addition, although the 2026 strategy states that the United States "will deploy the full suite of U.S. government defensive and offensive cyber operations,"[11] it is left to the reader to imagine when, how, against whom, and under what circumstances offensive cyber operations will be considered or employed, though recent U.S. actions in Venezuela and Iran may provide a hint. On the other hand, despite its economy of words, the document does telegraph a forward-leaning approach, declaring that the United States will act "proactively" to counter cyber threats and "will not confine our responses to the 'cyber' realm."[12]

Of course, a strategy document cannot be expected to outline every detail on how the strategy will be implemented. But it should at least suggest how the administration will seek to align means with ends. By contrast, the 2024 report included a list of three dozen implementation initiatives and the agencies responsible for implementing them. How the 2026 strategy will be implemented, however, remains to be seen; though reportedly there is a classified implementation plan.[13]

* * * * * * * * * * *

Mathew Ferren
***Matthew Ferren is an International Affairs Fellow at the Council on Foreign Relations and previously served at the Office of the National Cyber Director, where he contributed to the 2023* National Cybersecurity Strategy.**

Thank you for the invitation. It is a privilege to be here.

The 2026 *National Cybersecurity Strategy* is more of a vision statement than a strategy. It sets out high-level aspirations, but offers little clarity on how to achieve them. A strategy is supposed to align clear end states with the resources and authorities required to reach them, organized around specific lines of effort. By that standard, the document falls short.

To some extent, the brevity is intentional. The administration has signaled that specific executive actions, such as the recent executive order on cybercrime, will follow and give the strategy operational content. That is a reasonable approach in principle. In practice, set against the cuts to United States cyber agencies and the absence of strong leadership at the Cybersecurity and Infrastructure Security Agency, there is little reason to expect that the follow-on actions will add up to significant progress. That is a problem, because the threat landscape is getting worse.

The strategy does not name China as the most significant cyber threat the United States faces. That omission is concerning because China is the only true strategic threat we face.

---

[10] The White House, *President Trump's Cyber Strategy for America*, op. cit., p. 5.

[11] Ibid., p. 4.

[12] Ibid.

[13] Emily Harding, "What Does the New Cyber Strategy Really Mean?," Center for Strategic and International Studies, March 9, 2026, https://www.csis.org/analysis/what-does-new-cyber-strategy-really-mean.

That is not to diminish the capabilities of Russia, Iran, and North Korea, or the very real consequences of ransomware and other cybercriminal activity, but they are not strategic threats in the same sense. They are economic and operational problems. China is the only adversary capable of using its advantages in cyberspace to generate cross-domain leverage that can alter or constrain U.S. decision-making. The strategy does not need to include a detailed threat analysis, which is better suited for the Annual Threat Assessment and other classified products. It does need to convey awareness of the nature and magnitude of the challenge, and this one does not.

The strategy's central move is to treat cyber offense as the principal tool of cyber defense. I do not think that approach will be sufficient, particularly against China, for three reasons.

First, the primary constraint on scaling offensive cyber operations is not political will, legal restrictions, or interagency process. It is access. Operations require time and persistent access to adversary networks to develop capabilities and produce effects. China is a hard target. It is not impenetrable, but Chinese authorities take cybersecurity seriously, and gaining and holding access to systems of consequence is difficult. Demanding that U.S. Cyber Command increase its operational tempo will not automatically deliver high-impact outcomes.

What it will deliver is one of two undesirable results. Either operators generate churn to demonstrate activity, with little tangible effect on adversary campaigns, or they take risks that compromise infrastructure, expose tradecraft, and degrade their ability to execute in the future. Better use of private sector partners and artificial intelligence may help at the margins, but neither changes the underlying constraint.

Second, the strategy does not articulate a clear strategic objective or end state. China's cyber apparatus is enormous. Between the People's Liberation Army, the Ministry of State Security, and the private sector contractors that enable both, the country can reconstitute operations and infrastructure faster than the United States can disrupt them. We are not going to stop Chinese cyber activity through offensive operations. At best, U.S. offensive operations buy time to make the structural changes and long-term investments that would actually improve U.S. security.

The trouble is that this strategy walks back many of the regulatory and market-shaping measures the previous administration was trying to use to drive those structural changes. The 2023 strategy treated critical infrastructure cybersecurity as a market failure: businesses will not invest up to the level required for national security and public safety, and government intervention is therefore necessary. It pursued that intervention along several lines at once. Sector-specific, outcome-oriented regulations, paired with regulatory harmonization where necessary. Software liability reform to shift responsibility upstream, toward the vendors that produce insecure code, and away from the downstream operators least able to fix it. Procurement requirements, product labeling, insurance, and utility-rate mechanisms to mobilize private capital toward security investment. The 2026 strategy retains the harmonization piece, recast as deregulation, and abandons the rest. We cannot play whack-a-mole forever and call it a strategy.

Third, U.S. military cyber operators have a growing responsibility to support conventional military operations, and the strategy's emphasis on persistent engagement risks crowding out that mission. We have already seen cyber and other non-kinetic capabilities employed in operations in Venezuela and against Iran. This is what modern warfare looks like.

Doing the same against China would be considerably harder. Chinese networks are hard to penetrate, and it is capable of doing to U.S. command and control, weapons systems, and civilian infrastructure what we would seek to do to its own. The priority for U.S. military cyber forces should be protecting U.S. command and control and weapons platforms against adversary disruption. The second is using cyber capabilities, alongside other non-kinetic effects, to enable joint fires and maneuver. Both require sustained investment in planning, exercising, and capability development today, for the peer conflict we may face tomorrow. If we over-prioritize persistent engagement against ongoing intrusions, we will not make those investments.

Strategies are ultimately about hard choices, coordination, and execution. This one looks for an easy button in cyber offense and avoids the costly investments in security and resilience that real progress would require. Even where the strategy does identify the right priorities, it is not clear that the Office of the National Cyber Director, as currently resourced and positioned, can drive the coordination across the interagency that implementation would demand. That was a hard problem under the previous administration, with a confirmed director and a fully staffed office. It is harder now. A serious strategy would name the threat, accept the limits of offense, and commit to the structural work that the United States has been deferring for a decade. This document does not do that. The follow-on executive actions may yet improve the picture. I would not count on it.

* * * * * * * * * *

Annie Fixler
Annie Fixler is Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies.

Thanks, David, for convening this group today. I'm glad to bat clean-up, which means I'll hit on some points again that you heard from Mark and Matt and raise a couple additional ideas for our audience's consideration.

First, I have to admit something embarrassing—I've never seen Clint Eastwood's *The Good, The Bad, and The Ugly*. I blame my parents. But still I'm going to use that framing to talk about the *National Cyber Strategy*. As with all administration's cyber strategies, there is some good, some bad, and some ugly.

The Good

First the good. The strategy is focused on action. "Pillars of Action" to be precise. David went over these, but let's list them again. They are:

1) Shape Adversary Behavior
2) Promote Common Sense Regulation
3) Modernize and Secure Federal Government Networks
4) Secure Critical Infrastructure
5) Sustain Superiority in Critical and Emerging Technologies
6) Build Talent and Capacity

I'd challenge anyone to say that these are not good priority action areas. Let's go through them briefly pillar by pillar.

Within the first pillar of shaping adversary behavior, the strategy articulates that this requires both better defense and better offense. Of particular note, the strategy pledges not only to disrupt and defeat adversarial activities but degrade the capabilities of our adversaries to launch attacks. I think we focus too heavily on detecting, mitigating, and defeating attacks themselves. That is, we have to do that too, but why stop there? Shouldn't we be actively undermining not just individual attacks but the capability of our adversaries to conduct attacks at all?

The strategy also uses this type of language to talk about criminal actors. We need to—and now I'm quoting—"uproot criminal infrastructure."

In pillar two, it rightfully notes that too much of cybersecurity has become a series of compliance checklists disconnected from actual security or resilience.

Pillar three—modernize and secure federal government networks—might simply be restated as "Doctor, heal thyself."

In pillar four, I particularly appreciate the statement that "we must be able to recover quickly." For many of us in the cyber policy community, the Cyberspace Solarium Commission's March 2020 report remains a touchstone. So let me paraphrase that report. Planning—and practicing—to ensure a quick recovery after an attack is necessary to demonstrate to our adversaries that we will survive and defeat them; that if they hit us, we will stand back up and punch back harder.

Pillar five—the prioritization of emerging technologies, particularly AI and Quantum—is vital. The intelligence community's annual threat assessment came out about a week after the *National Cyber Strategy*. Others can check my math, but I believe this was the first threat assessment that included an entire section devoted to technological challenges. Other assessments had cyber sections. This one had a cyber section but also a technology section where the assessment noted—and again, I'm quoting—"Leadership in emerging technologies is increasingly defining global power and influence."

The last pillar, pillar six of the strategy, prioritizes America's cyber workforce, calling it "an asset worthy of great investment and essential to our nation's economic prosperity and

security." America's cyber workforce is essential to each of the pillars of the strategy. Cyber and technology are fundamentally people problems. They are man-made problems with man-made solutions.

The Bad

But the strategy is not all good.

It is decisive. Across just four pages of text, the strategy uses the phrase "we will" 45 times. And yet, I'm not convinced it ever quite articulates the goal. The strategy talks about the importance of cyberspace to achieving American economic, technological, and military leadership. It affirms that President Trump will defend U.S. interests in cyberspace and punish adversaries for threatening those interests. But what is the affirmative statement of what we want to achieve?

The Biden Administration's strategy explicitly stated a goal. It read, "Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences."

The Trump Administration's strategy never states a goal. Not to get too philosophical, but if a man knows not to which port he sails, no wind is favorable.

But even though the strategy doesn't expressly state it, I think we all understand that this president's goal might simply be to win in cyberspace. What that means is that we will be stronger than and prevail over our adversaries.

The bigger problem with the strategy—as everyone has mentioned—is that it doesn't actually articulate who those adversaries are. Across the *National Security Strategy*, *National Defense Strategy*, and now the *National Cyber Strategy*, it seems this administration cannot articulate precisely who the bad guys are.

The Ugly

But now comes the really ugly part. It is not clear that the Trump Administration has any of the capabilities necessary to implement its strategy. Over the past year, the Trump Administration has systematically stripped away many of the federal government's cyber capabilities and so, I'm left responding to each of the administration's declarative statements about what it will do with the retort, "oh yeah? You and what army?"

But let's dig into the specifics so we can see how ugly the situation truly is.

I'm going to start with pillar four—secure critical infrastructure—because it is near and dear to my heart.

Securing critical infrastructure is fundamentally an issue of public-private collaboration. The private sector owns and operates the infrastructure. The federal government cannot unilaterally secure that which it does not operate—and frankly, does not really know how to operate. What it must do is provide owners and operators the information, tools, and—sometimes—resources they need to secure themselves.

Over the past year, the administration has gutted the mechanisms of public-private collaboration.

Here are a couple acronyms to throw at you—First, CIPAC—the Critical Infrastructure Partnership Advisory Council. When the Trump Administration assumed office, they purged advisory councils across the federal government. This is standard stuff. The new guy gets rid of people the old guy appointed and then appoints his own people. The problem is, the Trump Administration hasn't appointed new people.

Actually, the real problem is that CIPAC wasn't like other advisory councils. It was more than an advisory council. It was the convening authority that allowed sector coordinating councils—industry groups of specific critical infrastructure sectors—to come together and talk to the government about risks and threats without anti-trust or Freedom of Information Act (FOIA) concerns.

Another acronym: CISA 2015. Not CISA the agency but CISA the law. That is, the Cybersecurity Information Sharing Act. The law provided protections for sharing cyber threat information with the government. But it expired in September 2025, and has been limping along with temporary, short-term extensions since then. Technically, this is Congress' fault, not the administration's, but if the administration cares about public-private collaboration, it would work with Congress to get this done.

Let's talk about securing federal government networks. While all departments have their own CISOs and CIOs, the federal agency responsible for the cybersecurity of the ".gov" domain is CISA, the agency—the Cybersecurity and Infrastructure Security Agency. The Trump Administration has repeatedly attempted to slash the agency's budget. Last year, the president's budget called for a half billion-dollar reduction. This year, they asked for a $700 million cut. If Congress agrees, this would put CISA's budget at the level it was back in 2021, undoing years of growth and development of the agency.

How do we sustain U.S. leadership in emerging technology when we've fired or forced out technology experts across the federal government? Over the past few years, the federal government has rapidly hired technology experts. But using expedited processes meant that these experts were probationary employees, which was one of the first groups of federal employees that the administration targeted with workforce cuts. One metric to keep in mind: the federal government has a Center on AI Standards and Innovation. It has about 20 full-time staff. Britain's equivalent organization has about 200. It is hard to advance policies that foster U.S. innovation and encourage federal uptake of technology if you have very few technologists in government.

I could keep going. I'm concerned about the restructuring of cyber capabilities within the State Department. Three years ago, Congress consolidated what was then disparate cyber, technology, and digital infrastructure expertise into a single Bureau of Cyberspace and Digital Policy to work with partners and allies to secure their information and communication infrastructure, promote cyber norms that align with U.S. interests and security, and thwart U.S. adversaries. This past summer, as part of its reorganization of the department writ large, the Trump Administration reverted back to a situation of fractured and siloed expertise.

Ultimately, the problem with the administration's *National Cyber Strategy* seems to be that while it mostly says the right things—minus of course the inability to call out our adversaries by name—it is intent on ignoring the lessons of the past five years and relearning how to work with the private sector and resource itself appropriately for the fight in cyberspace.

I'll end on that somewhat somber note but look forward to the discussion and questions.

* * * * * * * * * *