IDSS PAPER

27 March 2026

Doubling Down
The US Cybersecurity Strategy 2026

Kevin Chen Xian An

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No.054– 27 March 2026

Doubling Down: The US Cybersecurity Strategy 2026

Kevin Chen Xian An

KEY TAKEAWAYS

- *US cyber strategies were largely defensive and driven by risk management considerations until 2018, when they started taking on a more aggressive posture.*
- *The 2026 Cyber Strategy goes further to expand the scope of retaliation against cyberattacks while calling for the use of private firm capabilities in cyberattack campaigns.*
- *This offensive posture is paired with stronger defensive moves such as bans on foreign-made hardware like routers and drones.*

COMMENTARY

On the surface, the recent ban by the US Federal Communications Commission (FCC) on consumer routers produced in foreign countries has little in common with US cyber operations in Venezuela under Operation Absolute Resolve. Yet they are both manifestations of the US National Cybersecurity Strategy 2026 that was released in March.

In five pages of concise prose, US President Donald Trump's government expressed a vision for American cybersecurity with both a stronger offensive posture and a broader domestic shield against cyberattacks.

Understanding this strategy requires tracing the evolution of American cyber strategies since the National Strategy to Secure Cyberspace of 2003. It may appear as a sequel to Trump's 2018 cyber strategy and a departure from his predecessor Joe Biden's

cyber strategy of 2023. Yet it arguably takes ideas that were present in both documents and develops them further.

The Evolution of US Cyber Strategies

The core of every US cyber strategy has remained unchanged since 2003: to prevent cyberattacks against American critical infrastructure; reduce national vulnerability to cyberattacks; and minimise the damage and recovery time from cyberattacks.

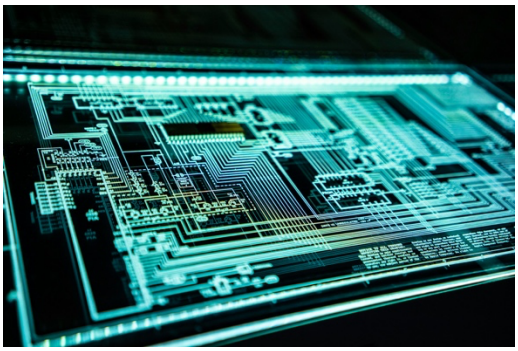
To fulfil these objectives, successive US governments sought to work with private firms to address cyberthreats instead of pushing for legislative solutions. Indeed, prior to 2018, the US cyber posture could be described as defensive and driven by risk management.

The concept of deterring cyberattacks had been present since the 2003 strategy, which called for stronger counter-intelligence efforts to name and shame "malicious actors". However, this push for deterrence first gained real teeth under the first Trump administration, which saw cyberspace as a key element of geopolitical competition.

Under the 2018 strategy, the best defence was seen as a fierce offence. National Security Presidential Memorandum 13 authorised offensive cyber operations to create what then-National Security Advisor John Bolton called "structures of deterrence" against malicious digital actors. Even Biden retained this focus on offensive capabilities, including methods to "disrupt and dismantle threat actors" as a strategic pillar of his cyber strategy.

Biden's 2023 strategy tried to leave its own mark on US cyber policy by prioritising clean energy to improve the resilience of the US electric grid and establish secure supply chains for telecommunications products. It sought to "shape market forces" by introducing liability for cybersecurity errors, taking a more interventionist stance towards the private sector. It also pledged to "forge international partnerships", going into detail about working through mechanisms such as the Quad, the quadrilateral security partnership between the United States, Australia, India and Japan, to advance shared goals for cyberspace.

This strategic direction, however, did not last. Trump's 2026 strategy retains some of the prognoses of its predecessor's strategy but offers more aggressive solutions.



Trump's 2026 cybersecurity strategy takes a more aggressive approach than previous administrations. *Image source: Unsplash*

A Greater Offensive Arsenal

The cyber strategies adopted by the Biden and first Trump administrations as well as the Obama administration all began with an enunciation of how the digital economy and cyberspace are important for Americans. The 2026 iteration eschews this for a blunt promise to act "swiftly, deliberately, and proactively to disable cyber threats", setting the tone for the rest of the document.

There are two key elements that make the 2026 strategy more aggressive than its predecessors. First, it declares that America "will not confine [its] responses to the "cyber" realm". This threat goes beyond the normal use of sanctions and could include diplomatic, intelligence, or even military solutions, raising the prospect of kinetic responses or even pre-emptive strikes against ostensible adversaries.

Second, the 2026 strategy calls on private companies to take on a bigger role in national cyber efforts. While liability for errors by private firms is mentioned, its inclusion in a section on "streamlin[ing]" cyber regulations hints at intentions more in line with market-driven approaches than Biden's. The ominous promise to "unleash the private sector" to "shape adversary behaviour" points to a posture of employing private companies to attack foreign parties.

Granted, the idea of private firms "hacking back" against digital adversaries is currently illegal. Yet we can already see private firms, particularly artificial intelligence firms such as Anthropic and Palantir, working with the US military in operations in Venezuela and Iran. The inescapable conclusion is that the US government no longer sees private firms just as partners for defence, but as offensive tools as well.

Fortress America

The 2026 strategy may have de-emphasised its 2023 predecessor's call for forging international partnerships, but it did zero in on one aspect: banning equipment from adversaries.

Since 2019, US federal agencies have been barred from using equipment or services by five Chinese companies, including Huawei and ZTE. In 2021, the FCC went further to include these companies in its Covered List, which restricts the sale or import of new equipment from these companies altogether for posing an "unacceptable risk" to US national security. This list was gradually expanded in 2022 and 2024, with the addition of service providers such as China Mobile.

Seen in this light, the FCC's 23 March ban on new foreign-made consumer routers was a drastic development, but not completely unexpected. The FCC announcement noted that foreign-made routers were "directly implicated" in recent attacks against American infrastructure by "advanced persistent threat (APT) actors" such as Volt, Flax and Salt Typhoon.

One can also draw links between this ban and the 2025 National Security Strategy, which argues that "the United States must never be dependent on any outside power for core components … necessary to the nation's defence or economy."

The bigger question is whether this sweeping ban will remain unchanged. While the FCC announced a similar ban on all foreign-made drones and components in December 2025, it subsequently exempted four non-Chinese models in March. In a similar fashion, the router ban may be a temporary measure while investigations continue behind the scenes. Alternatively, the ban could be an effort to gain leverage over foreign router companies and compel them to invest in American manufacturing.

Nonetheless, the 2026 strategy clearly shifts the US cyber posture towards a far more aggressive and isolationist direction. Subsequent governments may choose to limit hardware bans, emphasise cooperation with partners, or even place guardrails on the utilisation of private firms. However, the defensive, risk management-based approach firmly appears to be a thing of the past.

Kevin Chen Xian An *is an Associate Research Fellow in the US Programme at the Institute of Defence and Strategic Studies (IDSS), S. Rajaratnam School of International Studies (RSIS).*

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.