MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Commentary

Beyond Defence: The Offensive Turn in US Cybersecurity Strategy

Rohit Kumar Sharma

March 13, 2026

Summary

Offensive cyber operations are increasingly becoming an integral component of modern military campaigns.

On 6 March 2026, the Trump administration released its long-awaited National Cybersecurity Strategy, laying out a national vision to address threats in cyberspace. It encapsulates policy approaches based on a broader vision to secure American interests and leadership in cyberspace. Compared to the comprehensive and detailed cybersecurity strategy released during Trump's first term, the new document provides fewer specifics. Still, it reflects continuity with the earlier approach, albeit with some minor yet notable shifts.

The strategy consists of six pillars, outlining approaches towards adversaries while also advancing broader objectives such as regulatory measures and strengthening security across federal government networks. The first pillar *shaping adversary behaviour* clearly illustrates the US's intention to deploy offensive cyber operations, either in response to or to deter potential threat actors.[1] While emphasising the necessity of imposing costs on adversaries, the strategy also underlines the importance of collective action with US allies. Further, it makes it amply clear that the US response would consider cross-domain operations, potentially combining cyber operations with other non-kinetic measures and conventional military capabilities. As part of a broader offensive strategy in the cyber realm to 'create real risk for adversaries', the document also suggests an expanded role for private companies in supporting cyber offensive operations.[2]

The second pillar emphasises policy measures to streamline cybersecurity regulations, including data governance, to enhance the private sector's agility in developing and deploying adequate solutions to emerging cyber threats. The third pillar expounds on the need to 'modernise and secure federal government networks' by implementing best practices available and integrating emerging technologies such as post-quantum cryptography and AI-powered cybersecurity solutions.[3] Pillar four focuses on securing critical infrastructure by safeguarding the entire supply chain while also promoting disengagement from products and vendors linked to adversary states.

To sustain superiority in critical and emerging technologies, the strategy places special emphasis on securing the AI stack. It also highlights the potential of promoting agentic AI to enhance network security. Positioning the workforce as a strategic asset, the strategy argues for harnessing existing resources to develop a skilled talent pool capable of delivering next-generation cybersecurity solutions.

[1] **"White House Unveils President Trump's Cyber Strategy for America"**, The White House, 6 March 2026.

[2] Ibid.

[3] Ibid.

The key question, however, is whether the strategy signals any shift from, or continuity with, the cybersecurity approach adopted during Trump's first term. While the new vision openly mentions the US's willingness to deploy 'offensive cyber operations' to counter and deter threats in cyberspace, the earlier strategy adopted a more measured tone, referring to cyber operations merely as one option among the broader instruments of national power.[4]

The role of the private sector has also been elevated, with the strategy envisaging a greater involvement of companies in cyber offensive efforts, including actively disrupting adversary infrastructure. Reports indicate that industrial officials and experts familiar with the draft strategy were privy to the shifting stance.[5] That said, the private sector has not been entirely insulated from such collaborative efforts. In fact, the companies possess unique insights and visibility into adversary activity due to the scale of their operations, making close cooperation with government entities essential. However, the cooperation has always been predicated on defined roles and responsibilities, with the private sector sharing insights and capabilities coupled with the federal agencies' authority to act.[6]

The shift signals growing private-sector adoption of active defence, commonly referred to as 'hack back'.[7] This aspect is particularly intriguing and may raise both legal and practical concerns regarding the role of companies in cyber operations, which are conventionally closely guarded state activities.[8] Furthermore, experts point to potential legal hurdles in creating a mechanism that allows the private sector to participate in offensive cyber operations actively. For instance, the absence of a federal legal framework authorising such operations poses a stark challenge to this approach.[9]

Delineating clear legal boundaries for private sector involvement would also be a formidable task, particularly if a company were to overstep its mandate. This is particularly challenging given the amorphous nature of cybersecurity and the emergence of new threats. Involving the private sector could also make such companies legitimate targets in the eyes of adversaries, potentially leading to wider

---

[4] Ibid.

[5] Jamie Tarabay, **"Trump Administration Turning to Private Firms in Cyber Offensive"**, *Bloomberg*, 12 December 2025.

[6] **"National Cybersecurity Strategy"**, Biden White House Archives, March 2023.

[7] Aaron R. Cooper, Philip Chertoff and Shoba Pillay, **"Trump Admin Cyber Strategy Centers Private Sector in Offensive Cyber Operations"**, *Lawfare,* 9 March 2026.

[8] Adam Sella, **"Trump Calls On Private Companies to Take On a Bigger Role in Cyber"**, *The New York Times,* 6 March 2026.

[9] Aaron R. Cooper, Philip Chertoff and Shoba Pillay, **"Trump Admin Cyber Strategy Centers Private Sector in Offensive Cyber Operations"**, no. 7.

repercussions given the global dependencies and interconnected services they provide. The envisioned enhanced role also comes at a time when reports indicate that the Trump administration is reducing the cybersecurity workforce in agencies such as the Cybersecurity and Infrastructure Security Agency (CISA), raising the possibility that critical national infrastructure may be left without a well-prepared federal partner.[10]

The strategy further notes that the US may impose sanctions on 'lawless foreign hacking companies', signalling a tougher approach towards firms that sell spyware and other intrusive technologies that threaten American interests.[11] This could also be viewed as a double standard in the US approach, as it encourages the domestic private sector's role while penalising foreign companies engaged in similar activities.

Another notable development is the recognition of AI-powered cyber operations, particularly the use of agentic AI. The strategy also calls for the rapid deployment of AI-enabled tools to scale not only network defence but also disruption capabilities, laying bare the intent to employ AI in offensive cyber operations.

Interestingly, the strategy also references past successful US cyber operations, including actions against cybercriminal networks, support to military strikes on Iranian nuclear infrastructure and cyber-enabled measures used during the operation targeting Nicolas Maduro. This appears to underscore the growing role of offensive cyber capabilities in supporting broader US military and law enforcement operations.

The recent joint US–Israel strikes against Iran demonstrated the growing significance of offensive operations in the cyber realm. During a press briefing, Chairman of the Joint Chiefs of Staff General Dan Caine noted that multiple combatant commands, including US Cyber Command (USCYBERCOM), delivered "synchronised and layered effects designed to disrupt, degrade, deny and destroy Iran's ability to conduct and sustain combat operations".[12] USCYBERCOM was among the first to act, "layering non-kinetic effects" to hinder Iran's operational capabilities.[13] The coordinated, multi-domain operation enhanced speed, precision and the element of surprise.

One notable aspect of successful military strikes in the initial phase of the war was the culmination of years of persistent cyber and intelligence operations against Iran.

[10] Sam Sabin, **"Exclusive: One-third of Top U.S. Cyber Force Has Left Since Trump Took Office"**, *Axios*, 3 June 2025.

[11] **"White House Unveils President Trump's Cyber Strategy for America"**, no. 1.

[12] **"Secretary of War Pete Hegseth and Chairman of the Joint Chiefs of Staff Gen. Dan Caine Hold a Press Briefing"**, US Department of War, 2 March 2026.

[13] Ibid.

These included hacking into Tehran's traffic cameras and infiltrating Iranian mobile phone networks to build a detailed "pattern of life" for key targets, tracking their routines, movements and security arrangements before the strikes were executed.[14] This illustrates that cyber operations are not restricted to layering non-kinetic effects but also assist in "layering of those effects with intelligence collection", a pattern that has become increasingly evident in recent US operations, including last year's military strikes against Iranian nuclear infrastructure.[15] Here, 'layering' refers to the synchronised use of non-kinetic methods, such as cyberattacks, electronic warfare and influence operations, before conventional strikes, as clearly demonstrated in recent military operations against Iran.[16] These developments also underscore the growing integration of cyber capabilities in US military operations.

Carefully reading the strategy alongside observations of ongoing Israel–US joint operations against Iran makes it clear that offensive cyber operations are no longer merely an option reserved for exceptional circumstances but have become integral to state military operations. Moreover, cyber campaigns such as pre-positioning within strategic networks are actively supporting reconnaissance and precision strikes, underscoring that cyber capabilities are most effective when integrated with other military tools and intelligence sources.[17]

The growing integration of cyber operations into conventional military conflicts across multiple battlefields, such as in the Ukraine–Russia armed conflict and the ongoing war in West Asia, reflects an increasing reliance on such capabilities before, during, and even when military conflict ends, where cyber operations continue to support intelligence gathering and reconnaissance, to prepare for future contingencies. By incorporating this aspect into its cybersecurity strategy, the US is, in effect, institutionalising these operations or rather belligerent behaviour in cyberspace, which may lead to further distress in the existing understanding of norms and governance frameworks in cyberspace.

[14] Mehul Srivastava, James Shotter and Neri Zilber, **"Inside the Plan to Kill Ali Khamenei"**, *Financial Times*, 2 March 2026.

[15] Mark Pomerleau, **"Cyber Command Supports Strikes on Iran's Nuclear Facilities, But Officials Keep Details Under Wraps"**, *Defense Scoop*, 23 June 2025.

[16] Tom Uren, **"The Four Hour Cyber War on Iran"**, *Lawfare,* 6 March 2026.

[17] Louise Marie Hurel, **"Fog, Proxies and Uncertainty: Cyber in US-Israeli Operations in Iran"**, RUSI, 5 March 2026.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses