SECURING U.S. CRITICAL INFRASTRUCTURE AGAINST CHINESE CYBER THREAT – TRUMP 2.0 IMPERATIVE

by
Nistha Kumari Singh and Amrita Jash

On January 16, 2025, just days before leaving office, President Joe Biden issued an executive order on strengthening and promoting innovation in America's cybersecurity. Acknowledging the aggravating Chinese cyber menace, the order categorically states:

> Adversarial countries and criminals continue to conduct cyber campaigns targeting the United States and Americans, with the People's Republic of China presenting the most active and persistent cyber threat to United States Government, private sector, and critical infrastructure networks.

Against the series of recent high-profile attacks by Chinese hackers against U.S. agencies and companies, including a security breach into the U.S. Treasury Department, the outgoing National Security Advisor Jake Sullivan issued a warning to Beijing – "if they [China] actually took a physically destructive cyberattack in the United States – that there would be severe consequences."

In response to the looming Chinese cyber threat, on January 3, 2025, the U.S. Department of the Treasury sanctioned the Chinese company Integrity Tech for supporting the hacking group Flax Typhoon – which employs a "Living of the Land" strategy that involves implanting malware with legitimate admin tools and monitoring activities remotely. As cyberattacks will not just grow in intensity but also in sophistication, cybersecurity in all likelihood will rank high as one of the key national security concerns for the Trump administration. Clearly, there is a need for better preparedness under Trump 2.0

Change in Threat Landscape

Given the concerns over cybersecurity, on April 30, 2024, the Biden Administration issued a National Security Memorandum (NSM) addressing critical infrastructure cybersecurity, highlighting: the shift from counterterrorism to strategic competition, advances in technology like Artificial Intelligence, malicious cyber activity from nation-state actors, and the need for increased international coordination. This change in the threat landscape and increased federal investment in U.S. critical infrastructure prompted the need to update Presidential Policy Directives-21 (PDP-21).

Furthermore, the NSM replaced the PPD-21 from the Obama administration (2013), modernizing the approach to critical infrastructure protection. Data from KnowB4's August 2024 report exposed a 30 percent surge in cyberattacks targeting critical infrastructure, compared to 2022, as well as revealed that electric grids proved vulnerable, with blackouts causing economic losses amounting to trillions of dollars.

What called for the prioritization of critical infrastructure cybersecurity under the Biden administration was the May 2021 Colonial Pipeline attack – resulting in a national emergency. This attack carried out by a group named DarkSide, impacted 45 percent of the East Coast fuel supply, causing widespread gas shortages in many U.S states and airlines, with 100 GB of data stolen, and resulting in a payment of 75 bitcoin. The most significant aspect is the U.S.-China competition in cyberspace, which has acted as a catalyst in prioritizing critical infrastructure cybersecurity in Washington's policymaking. The Office of the Director of the National Intelligence's (ODNI) Annual Threat Assessment report in 2023 cautioned:

> If Beijing feared that a major conflict with the United States was imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.

The hint is quite clear. There is a surge in cyberattacks targeting critical infrastructure, such as ports and electric grids, which has been consistently warned about by FBI Director Christopher Wray and Microsoft, which have identified malicious Chinese state-sponsored groups such as Volt Typhoon, and Salt Typhoon as targeting American critical infrastructures.

For instance, Microsoft in its 2023 report identified Volt Typhoon as targeting critical infrastructure organizations in Guam and elsewhere in the U.S. Recently, Bloomberg reported Chinese cyberattacks targeting the Guam Power Authority (GPA) in particular, to wreak havoc – where Volt Typhoon is identified as the key suspect. The GPA is the island's only source of power, and the U.S. Navy is its biggest customer, consuming about 20 percent of the power it generated in 2023. In December 2024, the Salt Typhoon group was accused of breaching the U.S. telecommunication sector.

Highlighting the concerning evolution in Chinese targeting of U.S. infrastructure, in January 2024, Cyber Security & Infrastructure Security Agency (CISA) Director Jen Easterly remarked:

> Chinese cyber actors, including a group known as "Volt Typhoon," are burrowing deep into our critical infrastructure to be ready to launch destructive cyber-attacks in the event of a major crisis or conflict with the United States. This is a world where a major conflict halfway around the globe might well endanger the American people here at home through the disruption of our gas pipelines; the pollution of our water facilities; the severing of our telecommunications; the crippling of our transportation systems—all designed to incite chaos and panic across our country and deter our ability to marshal military might and citizen will.

By June 2024, Flax Typhoon had breached 260,000 computers globally, with significant attacks in Southeast Asia, North America, and Africa. It was mainly the U.S. which was especially affected, accounting for 47.9 percent of these botnet attacks, as reported by the U.S. Joint Cybersecurity Advisory in September 2024. Apart from this, in March 2024, the Treasury Department sanctioned the Wuhan XRZ for being a China-based Ministry of State Security front company that has served as cover for multiple malicious cyber operations

Apart from China, the U.S. has cited cyberattacks from other adversaries too. For instance, a report released by ODNI in April 2024 pointed out that cyberattack patterns in the health, agriculture, water and energy sectors, were notably from Iranian-affiliated groups like Cyber Av3ngers and other Russian hacktivist forces. The major implications of these attacks led to forced switches to manual operations, causing significant disruptions.

New Cybersecurity Posture

The upswing in cyberattacks does not mean there is no insight modification in cyberspace. The U.S. Department of Defense (DoD) has already adopted a "defend forward" and "persistent engagement" strategy to counter cyber threats. In May 2024, the White House released a report on the U.S. cybersecurity posture, reflecting the shift from a reactive to a proactive approach; and acknowledging that cyberattacks from Russia and China targeting U.S. critical infrastructures, were not merely espionage but pre-positioning for potential disruption.

So far, the Biden administration's approach towards cybersecurity has been that of "Act, Allies and Respond" – focusing on strengthening domestic infrastructure, aligning with like-minded countries, and responding to adversarial cyberattacks – by following a Zero Trust approach to support these goals. In addition, the Biden administration introduced the National Cybersecurity Strategy Implementation Plan, a long-term framework compromising 65 high-impact initiatives to fortify digital infrastructure.

Enhancing critical infrastructure resilience against cyberattacks is crucial to modernization and economic growth. Washington has taken many significant steps

in this direction. In June 2023, the U.S. Department of Justice created the National Security Cyber Section to jointly work with the Criminal Division's Computer Crimes and Intellectual Property Section and FBI's Cyber Division; while the U.S. Department of Defense's cyber strategy employs 'Hunt Forward' operations- leveraging insights from the Russia-Ukraine War.

Besides, the U.S. also closely monitors China's heavy investment in military cyber capabilities and has been vigilant on cyber operations by Russia, North Korea, and Iran. In April 2024, the National Infrastructure Risk Management Plan 2025 (National Plan) revised the National Cyber Incident Response Plan to address ransomware attacks and introduced cybersecurity standards. And, in December 2024, the ONCD and CISA issued a guide, Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure, to ensure the resilience of the next-generation infrastructure.

Military Preparedness

Also, budgetary allocations now prioritize the National Cybersecurity Strategy and allocate funding to the Office of Management and Budget and ONCD to promote cybersecurity and protect the critical infrastructure sector. Besides, steps were taken on the military front, where in 2010, the U.S. established the U.S. Cyber Command (USCYBERCOM), followed by the DoD's recognition of cyberspace as a strategic domain of warfare in 2011, calling for military preparedness in combating cyber threats.

Furthermore, in adding to public awareness, the U.S. government observes October as Cybersecurity Awareness Month and November as Critical Infrastructure Security and Resilience Month – aimed at integrating cyber-resilient critical infrastructure into public consciousness and ensuring cybersecurity. This indicates that Washington's cybersecurity shield for critical infrastructure is less about a single, unified defense mechanism and more about a layered approach combining technological, procedural, and legislative strategies.

Washington's current approach to strengthening critical infrastructure protection involves existing agencies (FBI, CISA, DoD) operating in highly centralized, sector-specific methods, often following distinct approaches. However, a unified framework for information sharing and an integrated approach across all relevant agencies is essential to enhance collaboration and sharing methods. Therefore, in light of the increasing threat from China, safeguarding America's critical infrastructure is vital for the agenda of Trump 2.0.

Nistha Kumari Singh is a Doctoral Candidate and a TMA Pai Fellow at the Department of Geopolitics and International Relations, Manipal Academy of Higher Education (Institution of Eminence), Manipal, Karnataka, India.

Dr. Amrita Jash is an Assistant Professor at the Department of Geopolitics and International Relations, Manipal Academy of Higher Education (Institution of Eminence), Manipal, Karnataka, India. She holds a PhD in Chinese studies from Jawaharlal Nehru University. She was also a Pavate Fellow at the University of Cambridge and an IAS Visiting Fellow at Loughborough University. Dr Jash is the author of China's Japan Policy: Learning from the Past (Palgrave Macmillan, 2023), and The Concept of Active Defence in China's Military Strategy (Pentagon Press, 2021). She can be reached at: @amritajash