THE SOUFAN CENTER
IntelBrief

Friday, February 2, 2024

CHINA POSES MAJOR HACKING THREAT TO U.S. CRITICAL INFRASTRUCTURE

Bottom Line Up Front:

- In testimony delivered before Congress this week, FBI Director Christopher Wray detailed China's ongoing efforts to hack into U.S. critical infrastructure, including the power grid, oil pipelines, and water systems.
- The U.S. government on Wednesday announced it had taken down a hacking network operated by a group known as Volt Typhoon, believed to be state-sponsored Chinese actors, that was setting itself up with capabilities to disrupt U.S. critical infrastructure.
- The sophistication of Chinese cyberattacks is bound to proliferate as emerging technologies will increasingly be used to orchestrate cyberattacks.
- The integration of emerging technologies in the modernization efforts of critical infrastructure in the United States may further increase cyber risks.

When U.S. President Joseph Biden met with Chinese leader Xi Jinping in November, Xi promised Biden that Beijing would not interfere **with the November 2024 U.S. presidential election, a promise reiterated over the weekend by China's Foreign Minister Wang Yi during a meeting with U.S. National Security Adviser Jake Sullivan.** But few within the Biden administration are sanguine about Xi's reassurance, especially as FBI Director Christopher Wray testified this week before the U.S. House of Representatives select committee on competition with China, laying out a range of nefarious activities that China is allegedly conducting against the U.S. - particularly in targeting critical civilian infrastructure. Wray detailed how a Chinese hacking network named "Volt Typhoon," which private sector cyber actors that have been tracking the threat believed to be state-sponsored has targeted critical infrastructure throughout the United States and Guam, including naval ports, the power grid, oil pipelines, and water systems. On Wednesday, the United States announced it had taken down an ongoing Volt Typhoon operation. In a blog post published last May, Microsoft warned the operation was not merely aimed at intelligence gathering but focused on disrupting infrastructure in the United States.

Speaking about the threat, committee chairman Rep. Mike Gallagher (R-WI) said, "This is the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants. There is no economic benefit for these actions. There is no intelligence gathering rationale." Earlier this week, the cybersecurity director of the National Security Agency, Rob Joyce, said that artificial intelligence and machine learning are being applied to uncover stealthy digital infiltration operations, which he said had become a staple of Chinese efforts aimed at U.S. critical infrastructure.

China has long been comfortable operating in the so-called "gray zone," the ill-defined middle ground

between peace and war. Gray zone activities, as described by U.S. Special Operations Command (USSOCOM), “rise above normal, everyday peacetime geopolitical competition and are aggressive, perspective-dependent, and ambiguous.” Some see China’s hacking efforts akin to phase zero shaping operations, preparation in the event that China and the U.S. go to war at some point in the future over the status of Taiwan. A massive Chinese cyber-attack would seek to cripple U.S. networks while also breaking the will of the American people to engage in any conflict. A sophisticated cyberattack could tamper with everything from the safety of drinking water to aviation security. Jen Easterly, the director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA) said that a Chinese cyberattack that disrupted pipelines, severed telecommunications, polluted water facilities, and crippled transportation would be aimed at ensuring that Beijing can incite societal panic and chaos, while simultaneously deterring Washington’s ability to marshal military might and breaking civilian will.

Volt Typhoon has been known to be active since at least mid-2020. Analysis of the group’s functioning has highlighted that it prioritizes operational security in its hacking efforts, likely originating from the global scrutiny of China following its exposure. The group demonstrates a high degree of sophistication and operational patience. It focuses on a limited number of carefully selected targets over extended periods using an arsenal of difficult to trace repurposed legitimate applications, all hallmarks of a highly capable state-supported actor. Concretely, the group works by taking control of more accessible digital devices such as routers and subsequently uses these to launch attacks on more sensitive targets in their strategic interest, including critical infrastructure.

The sophistication of Chinese cyberattacks is bound to proliferate as emerging technologies will increasingly be used to orchestrate cyberattacks. The rise of malicious large language models (LLMs), for example, stems from the increasingly democratized access to Artificial Intelligence and Machine Learning technologies for the general public. WormGPT, for example, is a chatbot that emerged in 2021 to aid hackers with the development of malware. Additionally, the integration of emerging technologies in the modernization efforts of critical infrastructure in the United States may further increase cyber risks.

The vulnerability of U.S. critical infrastructure to cyber intrusion is by no means a revelation. In 2013, an Iranian proxy group infiltrated a small dam’s industrial control system north of New York City. Although the incident itself was inconsequential, it served as an early warning that America’s adversaries now had the capability and intent to target U.S. infrastructure, be it military or civilian. More recently, the 2021 Colonial Pipeline cyberattack, perpetrated by a Russia-based cybercrime group known as DarkSide, forced massive disruptions in fuel distribution along the U.S. East Coast. The attack was criminal in nature, but it highlighted a concerning level of unpreparedness across U.S. infrastructure. Following this attack, the Biden Administration began introducing regulations requiring owners and operators of critical infrastructure to modernize and standardize their cybersecurity. This policy shift was later outlined in the 2023 National Cybersecurity Strategy, which called for a rebalancing of corporate and government responsibility for cyber defense.