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

MP-IDSA
Issue Brief

# US–China Cyber Relations and the Weaponisation of Microsoft Platforms

*Ishanya Sharma*

November 11, 2025

## Summary

Cyber tensions between the United States and China show Microsoft's central yet fragile role in global cybersecurity, where its platforms serve as both assets and targets. While both nations have exploited vulnerabilities within the platform to conduct cyber-espionage against each other, China has been particularly persistent in its operations.

## Introduction

Accusations of state-sponsored cyber espionage have come to define the cyber relations between the US and China over the years. The widespread adoption of Microsoft products has also made them prime targets for state-sponsored cyber espionage. High-profile incidents, such as the SolarWinds breach and attacks on Microsoft 365, have demonstrated how nation-state actors exploit vulnerabilities in Microsoft's ecosystem to conduct sophisticated espionage operations. The same tactics have been deployed by both the US and China, deepening mistrust and diplomatic friction between the two.[1] In recent years, China, in particular, has increasingly weaponised vulnerabilities in Microsoft's platforms to execute espionage and influence operations.

## Historical Overview of US–China Cyber Relations

The trajectory of US–China cyber relations reflect a history of mutual espionage, strategic mistrust and technological competition. Since China's formal entry into the global Internet in 1994, cyberspace has emerged as a critical domain of tensions between the two powers.[2] What began as isolated intrusions has expanded into a repeated cycle of cyber espionage, countermeasures and retaliatory diplomacy. Though both China and the US have used cyberspace to gain strategic, economic and military advantages, China's campaigns, particularly those exploiting vulnerabilities in Microsoft systems, have been more frequent and globally disruptive.

For more than a decade, China-based advanced persistent threat (APT) groups have launched cyber espionage campaigns targeting US government agencies, critical infrastructure, defence contractors and technology firms. For example, the 2005 Titan Rain cyber-attacks, which compromised the unclassified networks of the US Departments of State, Homeland Security, and Energy, stand out as an essential incident.[3] Titan Rain represented the first publicly disclosed case of state-sponsored cyber espionage originating from China, and marked the first instance in which the US government publicly attributed such activities to Chinese state actors.

Another prominent example is the 2009 Operation Aurora, a series of cyberattacks that compromised the networks of Microsoft, Yahoo, Google, and other high-profile

[1] Juma Mdimu RUGINA, **"Economic Cyber Espionage: The US-China Dilemma"**, *Journal of International Relations Studies*, Vol. 3, No. 2, 2023, pp. 77–90.

[2] Manshu XU and Chuanying LU, **"China–U.S. Cyber-Crisis Management"**, *China International Strategy Review*, Vol. 3, No. 1, 2021, pp. 97–114.

[3] **"Titan Rain - How Chinese Hackers Targeted Whitehall"**, *The Guardian*, 5 September 2007.

companies to steal their trade secrets.[4] This prompted Google to close its offices and operations in China. The China threat became so evident that, in 2011, the US government's Office of the National Counterintelligence Executive issued a report naming China as the "most active and persistent" perpetrator of cyber intrusions into the United States.[5]

However, the US has not been passive in cyberspace—it has also conducted numerous cyber operations against Chinese networks and institutions. American intelligence, especially the National Security Agency (NSA), has used cyberspace for a long time to monitor and penetrate strategically. China has consistently claimed that the US is a leading perpetrator of cyberattacks and alleges tens of thousands of intrusions every year on Chinese systems.[6] In fact, independent research supports the view that a significant volume of global cyber activity originates from or transits through the US-based infrastructure, facilitated by major American Internet service providers.

Microsoft's dominance in both public and private sectors made its software a primary target for advanced persistent threats. As the world's largest provider of enterprise software, cloud infrastructure and productivity tools, Microsoft products such as Exchange, SharePoint, and Outlook underpin critical operations for governments, corporations and NGOs worldwide. This makes Microsoft a prime target for state and non-state actors seeking to penetrate sensitive networks, conduct cyber-espionage, or carry out disruptive attacks.

The historical evolution serves as an essential reference point for better understanding the present stage of US–China cyber competition, in which Microsoft has become both the *battleground* and the *barometer* of their technological and strategic contest. The following cases illustrate how China, in particular, has weaponised Microsoft's ecosystem. The three contemporary cases involving Hafnium, Antique Typhoon, and the combined efforts of Linen Typhoon, Violet Typhoon, and Storm 2603 highlight a clear pattern that has been unfolding for years. They show how China's cyber espionage tactics have not only increased but also grown more advanced and precise over time. These recent cases also highlight a transition from broad, data-theft-oriented attacks of the past to exact, zero-day-driven operations.

[4] Bill Gardner and Valerie Thomas, ***Building an Information Security Awareness Program***, Elsevier, 2014.

[5] Kenneth Lieberthal and Peter W. Singer, **"Cybersecurity and U.S.-China Relations"**, Brookings, 23 February 2022.

[6] Ibid.

## Chinese Cyber Operations Targeting the US via Microsoft Platforms

Serving as a critical gateway to US government, corporate and institutional networks, Microsoft offers Chinese actors a high-value “window” for espionage and economic theft. Because its tools are so widely adopted, and because many of them manage privileged access, hold private keys, or broker identity/trust, vulnerabilities in Microsoft’s systems are highly attractive. An exploit can give adversaries far-reaching potential: infiltrate multiple organisations simultaneously, move laterally within networks, exfiltrate intellectual property, observe or manipulate decision-makers, or launch ransomware. Chinese threat groups have repeatedly exploited these weaknesses, as evidenced in the cases discussed below.

The following sections discuss key instances of Chinese cyber operations targeting Microsoft, intended to gather intelligence and advance strategic interests against the United States. Table 1 outlines the attack timeline, the identified Chinese threat actor, the attack target, the tactics, techniques and procedures (TTPs) used, the attack objective, and Microsoft’s corresponding patching or mitigation measures.

### *2021 Hafnium Cyberattack on Microsoft Exchange Servers*

Hafnium, a threat group believed to be state-sponsored and operating in China, launched several cyberattacks on Microsoft Exchange Servers in January 2021. The attack exploited four zero-day vulnerabilities (CVE-2021-26855, 26857, 26858 and 27065).[7] By February, the incident had escalated into one of the most significant cyber incidents in recent history: approximately a quarter of a million systems worldwide were exposed, predominantly small and medium-sized businesses and organisations, with at least 30,000 confirmed compromises. What initially appeared to be targeted espionage quickly transformed into a widespread “smash-and-grab” operation.

The Microsoft Threat Intelligence Centre attributed the attack to a Chinese state-sponsored actor based on observed tactics and procedures.[8] The Biden administration later publicly accused China, attributing the operation to cyber actors connected to the Chinese Ministry of State Security, and stated that it had exploited zero-day vulnerabilities that Microsoft subsequently patched in March. China, however, firmly rejected these allegations. Zhao Lijian, the spokesperson for China's Ministry of Foreign Affairs, responded to the US-led accusations by stating that the United States, along with its allies, has fabricated allegations against China

[7] **“HAFNIUM Targeting Exchange Servers with 0-day Exploits”**, Microsoft, 2 March 2021.

[8] **“Microsoft Accuses China Over Email Cyber-attacks”**, *BBC*, 3 March 2021.

regarding cybersecurity, with no factual basis.[9] Hafnium is known to target entities in the US across various industry sectors, including law firms, infectious disease researchers, higher education institutions, policy think tanks, defence contractors and NGOs, reflecting a broad, strategic focus on intelligence collection.

### ***2023 Antique Typhoon Breaching Email Accounts Incident***

In May 2023, Antique Typhoon, a Chinese state-backed threat actor previously tracked by Microsoft as *Storm-0558*, carried out a cyber intrusion that compromised email accounts at roughly two dozen organisations across the United States and Europe, including the US Department of Commerce. Among those targeted were Commerce Secretary Gina Raimondo and several members of the House of Representatives.[10] China firmly denied the allegations, with the Ministry of Foreign Affairs accusing the US of engaging in its own hacking activities and labelling the Microsoft report as “highly unprofessional” and “disinformation”.

Active since at least August 2021, Storm-0558 is a cyber-espionage group linked to China that specialises in stealing credentials through phishing, manipulating OAuth tokens and forging authentication credentials to infiltrate the email systems of targeted organisations.[11] The group primarily targets government institutions in the United States and Europe, with a strategic focus on entities and individuals involved in geopolitical matters related to Taiwan and Uyghur interests.

### ***2025 Microsoft SharePoint Exploitation by Linen Typhoon, Violet Typhoon, and Storm 2603***

In a recent cyberattack, three threat groups, suspected to be Chinese government-affiliated, exploited zero-day vulnerabilities to target Microsoft SharePoint servers.[12] Several organisations across sectors, including government, critical infrastructure and education, have been impacted in countries such as the United States, Germany and Australia. The US National Nuclear Security Administration (NNSA) was among the organisations breached. However, reports suggest that no sensitive or classified information has been compromised. The identified threat groups include Linen Typhoon, Violet Typhoon and Storm-2603. Typhoon is a term Microsoft uses to designate Chinese nation-state threat groups, while Storm is a term it uses to refer to threat groups in development.

[9] David Jones, **“White House Ties Cyberattacks to China, But Private Sector Awaits Stronger Action”**, Cybersecurity Dive, 20 July 2021.

[10] David Shepardson and Christopher Bing, **“Chinese Hackers Breached US Commerce Chief's Emails; Blinken Warns Chinese Counterpart”**, *Reuters*, 14 July 2023.

[11] Kevin Lanier, **“Storm-0558 Forensic Analysis”**, University of Hawaii-West Oahu, 7 March 2025.

[12] **“Disrupting Active Exploitation of On-premises SharePoint Vulnerabilities”**, Microsoft, 22 July 2025.

China rejected the allegations, with Liu Pengyu, spokesperson for the Chinese Embassy in the US, emphasising that cyberattacks are a global challenge that affects all countries, and that China is also a target of such threats.[13] He reiterated the nation's "consistent and clear" stance, underscoring that China firmly opposes all forms of cyberattacks and actively combats cybercrime.

Linen Typhoon, active since 2012, primarily targets government, defence, strategic and human rights organisations to steal intellectual property, according to Microsoft.[14] Violet Typhoon, identified in 2015, conducts espionage against former officials, NGOs, think tanks, universities, media and sectors like finance and healthcare across the US, Europe and East Asia. Meanwhile, Storm-2603, another China-based actor, has been observed trying to steal MachineKeys from compromised SharePoint servers.

While much of the focus has been on China's offensive cyber operations, it is essential to recognise that exploitation of Microsoft systems is not one-sided—the US has also exploited Microsoft as a platform to target China to steal intelligence and conduct cyber espionage. However, such instances have been less direct and less frequent. For example, the Vault 7 CIA leak exposed how the CIA developed and deployed malware, backdoors and custom hacking tools to compromise operating systems like Microsoft Windows to penetrate computers and networks used by foreign targets, including Chinese government agencies and commercial entities.[15]

However, Vault 7 was not specifically directed at China; it revealed cyber tools and operations targeting multiple regions, including Europe, the Middle East and China. In a recent development, China's 2025 accusation against the US alleged that American agencies exploited unpatched Microsoft security flaws to spy on Chinese military networks, reflecting ongoing tit-for-tat cyber operations.[16] Unlike the Chinese cases, where detailed objectives, tactics, techniques and procedures (TTPs) of Microsoft exploitation have been documented, the 2025 Microsoft bug incident has not been confirmed or detailed by either Microsoft or the US government. This shows that Chinese operations are explicitly oriented towards espionage against Western entities, particularly the US, highlighting the asymmetry in targeting focus between US and Chinese cyber activities involving Microsoft vulnerabilities.

[13] Mitchell Labiak and Lily Jamali, **"Microsoft Servers Hacked by Chinese Groups, Says Tech Giant"**, *BBC*, 23 July 2025.

[14] Matt Kapko, **"Microsoft SharePoint Zero-day Attacks Pinned on China-linked 'Typhoon' Threat Groups"**, Cyberscoop, 22 July 2025.

[15] Matan Mimran, **"The Long-Term Threats Posed by the Vault 7 Leaks"**, Cybereason.

[16] **"China Accuses US of 'Using' Microsoft 'Bug' to Spy on Chinese Military"**, *The Times of India*, 1 August 2025.

## Cyber Crisis Management

The repeated cycles of accusation and denial following these Microsoft-related breaches reveal a deeper structural problem in US–China cyber relations: the absence of effective cyber crisis management frameworks. While cyber operations have become increasingly sophisticated, mechanisms to contain their diplomatic fallout remain underdeveloped. Crisis management in cyberspace involves controlling and mitigating cyber incidents that can escalate into tensions between countries, armed conflict, or war. The objective is to prevent cyberspace confrontations from escalating into a full-fledged war. Though disputes in cyberspace are low-intensity and involve limited confrontation, the need for cyber crisis stems from the recent rise in full-scale confrontation triggered by cyberspace conflicts between countries.[17]

One of the most critical objectives of crisis management is the establishment of shared attribution protocols and norms.[18] Joint technical teams should develop transparent, mutually-agreed processes for attributing attacks and reducing the "who-did-it" ambiguity that fuels retaliation. Attribution has, in fact, proved to be a significant challenge in US–China cyber crisis management. China's increasing sophistication of cyber threat actors over the years has made it difficult to attribute specific attacks to specific actors. This uncertainty makes it difficult for governments to respond to or diplomatically address the situation quickly.

Clear communication channels for de-escalating cyber crises are essential for cyber crisis management in the US–China context.[19] Historically, the absence of direct lines of dialogue during cyber incidents has frequently led to misunderstandings and tensions. Bilateral dialogue mechanisms have also seen limited success. For instance, the US–China Cyber Agreement in 2015 did not fully succeed in reducing the number of cyberattacks, especially in the long term. US cybersecurity experts observed a sudden decline in Chinese cyberattacks after the 2015 agreement.

However, they assigned four possible reasons for this decline—the first is the advancement in carrying out sophisticated cyberattacks which are challenging to be detected in cyberspace; second could be China's use of proxies in other countries to target victims in the US; third could be China's redirecting of attacks to other countries; and fourth could be that the agreement actually helped in putting a stop in Chinese cyberattacks by conducting an anti-corruption campaign in the

[17] Manshu XU and Chuanying LU, "**China–U.S. Cyber-Crisis Management**", no. 2.

[18] Arindrajit Das, "**International Cyber Incidents: On the Question of Public Attribution**", Observer Research Foundation, 4 November 2024.

[19] Manshu XU and Chuanying LU, "**China–U.S. Cyber-Crisis Management**", no. 2.

government and PLA after signing the contract. Similarly, the US–China Cyber Working Group saw limited success mainly due to mutual mistrust and differing national interests. These past bilateral efforts to institutionalise dialogue, such as the 2015 US–China Cyber Agreement and the US–China Cyber Working Group, demonstrate both the potential and the fragility of cyber crisis management.

When formal diplomatic channels fail during periods of tension, academic and civil exchanges play a crucial role in sustaining dialogue. Platforms such as the China–US Internet Forum (2007) and the Cyber Security Track-2 Dialogue (2009) have been successful in building mutual understanding and easing mistrust. Promoting collaborative research among think tanks and scholars enables both sides to address contentious issues more constructively, identify feasible policy recommendations and rebuild confidence. Such exchanges could further help revitalise past cooperative efforts, such as the 2015 six-point cybersecurity consensus, and align bilateral efforts with broader international norms developed by the UN Group of Governmental Experts.

## Microsoft’s Role in Cyber Crisis Management

Given how deeply Microsoft’s systems are embedded in government and private networks worldwide, its ability to anticipate and respond to large-scale cyber incidents has become a key concern for global security. Microsoft has built a fairly comprehensive system for managing cyber crises. This includes monitoring potential threats, coordinating incident response teams, public disclosure practices, and the regular release of intelligence through reports such as the Annual Digital Defence Report and Cyber Signals.

In the aftermath of major incidents such as the Hafnium and Antique Typhoon attacks, Microsoft demonstrated a structured, transparent approach to crisis management. The company’s Threat Intelligence Center (MSTIC) and Digital Security Unit (DSU) usually take the lead, identifying attackers, issuing emergency patches, and working closely with cybersecurity bodies such as the US Cybersecurity and Infrastructure Security Agency (CISA) and the UK’s National Cyber Security Centre (NCSC).

Microsoft also engages in attribution-based reporting. The company often names the threat actors involved (in cases such as Hafnium or Storm-0558) and explains the tactics and tools they used. This kind of transparency has two significant benefits: it improves global understanding of emerging threats and deters repeated attacks by exposing the methods behind them. However, not everyone views this positively.

Governments such as China's have criticised Microsoft's attributions, calling them politically biased or insufficiently backed by evidence.

Central to Microsoft's broader preparedness strategy is its Annual Digital Defense Reports (DDRs). These reports compile insights from an enormous amount of data: over 65 trillion security signals processed daily across Microsoft's cloud network. While they offer a look back at global cyber trends, they also serve as forward-looking tools to help governments and organisations evaluate their resilience against new forms of attack. The 2023 report, for example, highlighted the increasing sophistication of state-sponsored hackers, particularly those from China, Russia, Iran and North Korea.[20] It showed how these actors are shifting towards more covert tactics, such as credential theft and supply chain infiltration. Microsoft's quarterly *Cyber Signals* reports build on this work, offering more targeted insights by region and sector, effectively bridging technical threat analysis and high-level policy guidance.

Despite its active role in crisis management, Microsoft continues to face criticism over its complex position in the cyber landscape.[21] It often finds itself both as a primary target of attacks and as a major player in defending against them. This dual role raises a bigger issue: the world's growing dependence on a single company's digital infrastructure. When Microsoft is breached, the impact spreads far beyond its own systems. The ongoing US–China cyber rivalry has repeatedly exposed this vulnerability. While Microsoft's rapid crisis response and transparency help strengthen global resilience, they also reveal how much modern cybersecurity—and, by extension, national security—depends on a single corporate actor. In that sense, Microsoft's threat assessments and crisis responses have evolved into more than just technical exercises—they now play a part in shaping the global balance of power in cyberspace.

## Conclusion

The evolution of China's cyber operations against the United States highlights how cyberspace has become an increasingly contested frontier in great-power rivalry. From Titan Rain and Operation Aurora to Hafnium and Antique Typhoon, the pattern reveals a steady progression from rudimentary data theft to highly sophisticated campaigns that exploit global digital interdependence. Microsoft's platforms, which

[20] **"Microsoft Digital Defense Report 2023"**, Microsoft, 2023.

[21] Migo Kedem, **"The Microsoft Paradox | Dominance & Vulnerability in the World of Cybersecurity"**, *SentinelOne*, 2 October 2023.

anchor both US government and private infrastructure, have emerged as critical battlegrounds in this struggle, reflecting not only their technological ubiquity but also their geopolitical importance. While the US continues to accuse China of state-sponsored cyber espionage and intellectual property theft, China maintains that it too is a victim of cyberattacks, deflecting blame and challenging the credibility of US narratives. This dynamic has created a persistent cycle of accusation and denial, deepening mistrust between the two powers.

The cyber contest between the US and China ultimately reflects the broader struggle for influence in the 21st century global order. The Microsoft incidents serve as a reminder that technological dependence can become both a strength and a vulnerability. Unless both sides commit to developing trust-based frameworks and credible deterrence mechanisms, the current trajectory of cyber confrontation could continue to erode international stability and the very foundations of digital cooperation that underpin modern global life.

## About the Author

**Ms. Ishanya Sharma** is Research Intern 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.

*Disclaimer:* Views expressed in Manohar Parrikar IDSA's publications and on its website are those of the authors and do not necessarily reflect the views of the Manohar Parrikar IDSA or the Government of India.

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