ADARGA BRIEFLY

China in the changing world order

11th January 2025 | Volume 01 Issue No 21

adarga

NATIONAL SECURITY

US Treasury hacking allegations

On 30 December 2024, in a disclosure notice addressed to members of the United States House of Representatives, the U.S. Department of Treasury reported that it had been targeted in a cyber-attack.[1] According to the letter, the attack occurred in early December, and was linked to vulnerabilities in third-party software provided by BeyondTrust, which enabled hackers to steal an authentication key to bypass security and remotely access Treasury systems.[2 3]

The Treasury was reportedly notified by BeyondTrust on 8 December of a "major incident" whereby a threat actor overrode security and accessed some of the Treasury's workstations and "certain unclassified documents".[4 5 6] Following the event, the compromised system has been taken offline, and there is currently no evidence suggesting continued access to Treasury information by the attackers.[7 8] In its letter, the Treasury stated that the incident had been "attributed to a China state-sponsored Advanced Persistent Threat (APT) actor".

In statements, U.S. officials have described the incident as a 'major cybersecurity event' and are collaborating with the FBI and other agencies to investigate its repercussions.[9 10] Meanwhile, the department said it had been working with the Cybersecurity and Infrastructure Security Agency and third-party forensic investigators to determine the overall impact.[11] The initial response from the Treasury included a commitment to provide more details about the incident within 30 days as required by law.[12 13]

China has categorically denied these allegations, labelling them as baseless and a form of disinformation. In their read-outs, official channels asserted that China opposes all forms of cyberattacks and condemned the assertions made by Washington as smear tactics aimed at Beijing, highlighting that the US has not supplied any evidence that China is responsible.[14 15 16] At a regular press conference on 31 December, Mao Ning, a spokesperson for the Ministry of Foreign Affairs, reiterated these points, emphasising that China consistently rejects such unsubstantiated accusations.[17]

On 8 January, Bloomberg reported that according to "people familiar with the matter who did not want to be named to discuss information that hasn't yet been made public", the Biden administration is preparing an executive order aimed at enhancing U.S. cybersecurity measures, learning from this latest and other significant breaches.[18] This order includes robust requirements for identity authentication and encryption for government communications, particularly to safeguard against unauthorised access.[19 20]

Adarga Analysis: There is a realistic possibility that the recent cyberattack on the U.S. Treasury represents not just a significant cybersecurity breach but a broader geopolitical manoeuvre with potential medium-term and long-term implications. It is highly likely that the perpetrators were seeking information, rather than attempting to steal funds.[21] While the immediate impact on classified systems is highly likely minimal, based on official statements, it is likely that the potential exposure of sensitive, albeit unclassified, information could still have strategic consequences if weaponised. This is because, given the Treasury's role as the backbone of U.S. financial policy and debt issuance, the nature of information compromised could still provide adversaries with insight into U.S. financial strategies, vulnerabilities in economic policies, and internal decision-making. Consequently, even if limited in scope, compromised access to decision-making systems could enable adversaries to anticipate, and potentially pre-empt, U.S. fiscal or monetary policy actions. As such it represents information that could be weaponised in future economic or geopolitical competition.

The breach also underscores vulnerabilities in third-party software dependencies, such as those provided by BeyondTrust, which were exploited in this case. The increasing dependence on third-party software within government systems introduces significant cybersecurity vulnerabilities.[22] Consequently the event highlights the critical need for government departments and agencies to rigorously assess and manage those security risks posed by third-party software solutions. It also draws attention to a larger risk. While in this instance the breach and immediate impact was limited to the U.S. Treasury, the interconnected nature of critical infrastructure means that a future cyberattack on one component can have the potential to have cascading effects across multiple sectors.[23]

The cyberattack also aligns with a broader pattern of state-sponsored cyber activity where nations, particularly China, Russia, and Iran, have been accused of employing cyber espionage strategies to achieve asymmetric advantages. Consequently, this latest U.S. accusation made against China, if substantiated, reflects a continuation of the "grey zone" conflict paradigm — covert, non-military confrontations that are below the threshold of traditional armed conflict. It is almost certain that this incident has exacerbated tensions between the U.S. and China and further entrenched cybersecurity as a battleground for the geopolitical rivalry between the two countries. As seen in prior confrontations over intellectual property theft and technological espionage, incidents like these often serve to galvanise bipartisan support for more hawkish policies towards China. This has already been observed to some extent within the initial response. The cyberattack has already spurred policy adjustments on both sides, with the Biden administration reportedly preparing an executive order to strengthen cybersecurity defences, and with Republican lawmakers calling for briefings and further investigations into the breach's implications for U.S. security and foreign relations.[24]

It is likely that this could accelerate retaliatory measures from the U.S., potentially through sanctions or heightened restrictions on Chinese firms operating in the technology and software sectors. On 3 January, the U.S. Treasury announced it had imposed sanctions on Chinese cybersecurity firm Integrity Technology Group Inc, accusing the company of being a Chinese government-linked hacking group targeting U.S. critical infrastructure.[25 26] The firm, referred to as "Flax Typhoon" in private sector reports, was described by the U.S. State Department as a contractor for China's Ministry of State Security, and allegedly responsible for directing cyberattacks on U.S. and overseas infrastructure.[27 28] The Treasury Department has not publicly attributed this specific breach to Integrity Technology Group, and therefore it is highly likely the sanctions also relate to other incidents. It is likely that the U.S. could seek to target other Chinese firms in further sanctions as part of its medium-term response. There is also a realistic possibility that internationally, the U.S. may seek to leverage this incident to encourage allied nations towards a more unified stance on cybersecurity norms, potentially at forums like NATO or the G7. By framing the specific breach within the larger pattern of state-sponsored cyber aggression, Washington could work to isolate Beijing diplomatically while enhancing collaborative defence measures among its partners.

DIPLOMACY

Muted exchange between China and North Korea

Since 1 January, North Korea's state media has provided minimal coverage of President Xi Jinping's annual greetings to its leader, Kim Jong-un.[29 30] The official Korean Central News Agency (KCNA) reported the correspondence within an extended list of dignitaries, as follows: "The New Year cards came from the general secretary of the Central Committee of the Communist Party of China who is president of the People's Republic of China and his wife, the president of the Socialist Republic of Vietnam, and presidents of Mongolia, Tajikistan, Turkmenistan and Belarus."[31]

In contrast, Kim extended his "best wishes to the fraternal Russian people and all the service personnel of the brave Russian army in the name of his own, the Korean people and all the service personnel of the armed forces". In its coverage of the communications, several South Korean media outlets have suggested that this apparent lack of enthusiasm signifies strained ties between Pyongyang and Beijing, especially as North Korea strengthens its military relations with Russia. It also highlighted that the North Korean state media organs have not reported on whether Kim has delivered a new year message to Xi.[32 33 34 35]

Likewise, as at the time of writing, Chinese state media has not reported on Xi's New Year greetings to Kim.[36 37] Again, this contrasts with extensive coverage of Xi's interactions with Putin, hinting at an imbalance in how the two relationships are currently managed.[38] This silence is a clear diversion from previous years including the start of 2024 when Xi Jinping and Kim Jong-un exchanged New Year greetings, and marked 2024 as the "Year of Friendship between China and North Korea" to commemorate 75 years of diplomatic relations between the two countries.[39 40] At the time these messages proliferated across official channels and various state media outlets.[41 42]

Adarga Analysis: The muted exchange of New Year greetings between China and North Korea likely reflects underlying tensions in their relationship, as well as a shift in Pyongyang's diplomatic priorities.

The absence of typical celebratory rhetoric from North Korea's state media on its ties with China is striking, given the prominence of such messages in previous years. Paired with Beijing's official silence, this is a notable departure from the past. North Korea's enthusiastic messaging towards Russia – its heavily militaristic tone, and voicing of support, from one army to another – emphasises Pyongyang's contribution to Russia's war effort and stands in stark contrast to this minimal acknowledgment of China.

There is a realistic possibility that with this divergence, Kim Jong-un may be leveraging his relationship with Russia to signal independence from Beijing's shadow.

By pivoting toward Moscow, North Korea could be seeking to balance the perception of its reliance on China while fostering a narrative of diversification in its external alliances. Likewise, there is a realistic possibility that the shift may also reflect North Korea's broader frustrations with perceived constraints in its relationship with Beijing, which has historically oscillated between support and measured restraint.[43 44]

The relationship between China and North Korea showed several signs of deterioration during 2024, a year originally designated as a "Year of Friendship". Examples included the decline in the status of North Korean guests attending Chinese celebrations, and the absence of notable coverage by state media on both sides, leading some commentators to observe "abnormal air currents" in the bilateral relationship.[45]

The relationship dynamics are further complicated by North Korea's increasing reliance on Russia for military and economic support, while simultaneously moving away from Chinese influence.[46 47] In particular, China's resistance to being seen as directly involved in North Korea's military actions, particularly relating to troop deployments to aid Russia in Ukraine, has added to the strain. China's Ministry of Foreign Affairs has repeatedly expressed ignorance regarding North Korea's troop movements, and emphasised its projected stance of maintaining neutrality in the conflict.[48 49 50]

It would be premature to overstate any rift between Beijing and Pyongyang. The relationship remains rooted in mutual interests, from shared opposition to U.S. influence, to economic dependencies. Nevertheless, the absence of typical overtures is significant and merits attention, as such moments of reduced visibility hint at subtle recalibrations in bilateral ties. It likely highlights a subtle cooling, even if temporary, in a relationship long marked by ideological alignment and strategic necessity. Therefore, we assess that while the North Korea-China alliance highly likely remains foundational, the reduced visibility of their interactions, especially when compared to North Korea's overt support for Russia, signals a potential recalibration in Pyongyang's strategic outlook. North Korea's apparent prioritisation of Russia over China in its public communications offers insights into this evolving strategy — one that likely emphasises autonomy, opportunistic alliances, and a careful balancing act among its key partners.

This also highlights the importance of monitoring official communications and state media coverage; they should be understood not as a footnote, but as an indicator of how Pyongyang and Beijing are navigating their positions in an increasingly complex geopolitical landscape. Although easily overlooked in favour of more visible developments and gestures that dominate the geopolitical stage, the absence of something as routine as cordial New Year messages can often reveal more.

ABOUT

Briefly - China in the Changing World Order

Adarga is a leader in AI-driven information intelligence for defence, national security, and commercial organisations.

'Briefly' is brought to you by Adarga's geopolitical and geoeconomic experts, leveraging our highly curated data sets and Vantage software, which is designed to increase the quality, speed, and breadth of insight through the application of cutting-edge AI tools.

Time taken to generate research for this report with Adarga Vantage:
<10 seconds

Articles & papers scanned:
9.98 million

Including articles from:
China, France, Hong Kong, Russia, South Korea, Taiwan, UK, US

References

1 https://www.wired.com/story/us-treasury-hacked-by-china/
2 https://bit.ly/40tPuGA
3 China says US spreading 'disinformation' over Treasury hack claims - BBC monitoring - Adarga Vantage
4 https://bit.ly/40tPuGA
5 https://www.wired.com/story/us-treasury-hacked-by-china/
6 https://www.bbc.co.uk/news/articles/c3weye2j0e7o
7 https://bit.ly/40tPuGA
8 https://www.bbc.co.uk/news/articles/c3weye2j0e7o
9 https://bit.ly/40tPuGA
10 https://www.bbc.co.uk/news/articles/c3weye2j0e7o
11 https://www.bbc.co.uk/news/articles/c3weye2j0e7o
12 Cyberattack against the US Treasury: Beijing denounces 'baseless' accusations
13 https://www.bbc.com/news/articles/c3weye2j0e7o
14 https://www.bbc.co.uk/news/articles/c3weye2j0e7o
15 Cyberattack against the US Treasury: Beijing denounces 'baseless' accusations
16 https://www.bbc.com/news/articles/c3weye2j0e7o
17 China says US spreading 'disinformation' over Treasury hack claims - BBC monitoring - Adarga Vantage
18 https://www.bnnbloomberg.ca/business/international/2025/01/08/white-house-rushes-to-finish-cyber-order-after-china-hacks/
19 https://www.bnnbloomberg.ca/business/international/2025/01/08/white-house-rushes-to-finish-cyber-order-after-china-hacks/
20 https://www.scmp.com/news/world/united-states-canada/article/3293983/white-house-rushes-finish-cybersecurity-order-after-china-hacks
21 https://www.bbc.com/news/articles/c3weye2j0e7o
22 https://www.security.gov.uk/policy-and-guidance/secure-by-design/activities/managing-third-party-product-security-risks
23 https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00071-z
24 https://www.scmp.com/news/world/united-states-canada/article/3293661/no-indication-treasury-breach-affected-other-federal-agencies-us-cyber-watchdog-says
25 https://home.treasury.gov/news/press-releases/jy2769
26 https://www.reuters.com/technology/cybersecurity/us-issues-cybersecurity-sanctions-against-chinas-integrity-technology-2025-01-03/
27 https://home.treasury.gov/news/press-releases/jy2769
28 https://apnews.com/article/668371e717bea3ae7c7eb8a20fa81a99
29 https://www.koreatimes.co.kr/www/nation/2025/01/103_389541.html
30 https://www.scmp.com/opinion/asia-opinion/article/3293433/china-north-korea-relations-start-new-year-new-low
31 N Korea briefly reports on Chinese leader's new year greetings to Kim - BBC monitoring - Adarga Vantage
32 https://www.koreatimes.co.kr/www/nation/2025/01/103_389541.html
33 N Korea briefly reports on Chinese leader's new year greetings to Kim - BBC monitoring - Adarga Vantage
34 https://www.chosun.com/english/north-korea-en/2025/01/01/FVRERUXAFFCUNLEYAVOFI3IUJI/
35 https://en.yna.co.kr/view/AEN20250101003100315
36 BBCM China Watchlist 2 Jan 25 - BBC monitoring - Adarga Vantage
37 Verification by Adarga's internal analysts, correct as at the time of writing (10 Jan 25)
38 BBCM China Watchlist 2 Jan 25 - BBC monitoring - Adarga Vantage
39 https://news.sina.cn/gn/2024-01-01/detail-imzzyuwa0312701.d.html?vt=4&pos=108
40 https://www.asahi.com/articles/ASS116RV1S11UHBI00F.html
41 https://www.fmprc.gov.cn/zyxw/202401/t20240101_11215629.shtml
42 https://news.sina.cn/gn/2024-01-01/detail-imzzyuwa0312701.d.html?vt=4&pos=108
43 https://www.lowyinstitute.org/the-interpreter/will-north-korea-annoy-china-having-sent-troops-fight-alongside-russia
44 https://www.hani.co.kr/arti/opinion/column/1164949.html
45 https://www.yna.co.kr/view/AKR20240929000700083
46 https://www.foreignaffairs.com/china/strange-success-north-korea
47 "North Korea is China's potential enemy," but they can't break up
48 https://bit.ly/4gMbIcF
49 https://www.reuters.com/world/china-says-not-aware-north-korean-troops-russia-2024-10-24/
50 https://kyivindependent.com/china-not-aware-of-north-korean-troops-in-russia-preparing-to-fight-in-ukraine/

To provide feedback on *Briefly - China in the changing world order*, or suggest themes that you would like to see covered, please email **hello@adarga.ai**