Atlantic Council
CYBER STATECRAFT INITIATIVE

February 2026

Issue brief Understanding China's cyber capabilities: A view across the ecosystem

Written by Nikita Shah

Memo for the British Embassy in Beijing on China and cybercrime

Introduction

This memo is part of a project looking across China's evolving cyber ecosystem and provides an overview of cybercrime as it pertains to China, the Chinese state, and Chinese citizens. A network of China cyber experts developed in support of this project, as well as open-source research derived from cyber threat intelligence reporting, technical reporting, and academic literature inform these findings. The objective of this memo is twofold: first, to demonstrate how China is both perpetrator and victim of cybercrime, and plays an active part in sustaining aspects of the cybercrime industry; and second, based on this understanding, to identify vulnerabilities or weak points within China's relationship with cybercrime that could inform the British Embassy in Beijing's (BE Beijing) in-country engagement with China.

China's cyber capabilities and ecosystem have grown vastly in scale and sophistication over the last five to ten years. This is especially apparent in the maturation of cybercrime as an industry within that ecosystem: its industrialization both benefits the Chinese state and undermines Chinese society at the same time. Moreover, cybercrime in or relating to China is multifaceted: it comprises cyber-dependent crime such as ransomware; large-scale data breaches impacting citizens; and cyber-enabled crime, such as the scam compounds that depend on human trafficking to have effect. Each of these rest upon enabling actors, capabilities, and services whose presence also serves to blur the line between state and nonstate affiliations within this ecosystem. This is no coincidence; this complexity emboldens the Chinese state to carefully navigate clamping down on the cybercrime ecosystem while selectively allowing it to continue to exist and grow—particularly where it might serve broader Chinese foreign policy or national security objectives. For BE Beijing to approach the Chinese state on cybercrime, it should focus on the human impact of cybercrime and areas in which it can provide best practice examples, rather than on the technical aspects of cybercrime itself.

China as perpetrator

China's cyber ecosystem is uniquely characterized by the blurring of state actors and cybercrime enterprises, and is enabled by a thriving marketplace of tools, services, and (increasingly) stolen data. The Chinese government plays an active role in this ecosystem, whether through tacit support of cybercriminal operations, cultivating environments where cybercrime platforms thrive, or (increasingly) its crossover with serious and organized crime. The resulting 'intricate web' reflects an 'interplay between state policies, global events, and the innovative adaptability of [cybercriminals].'

APT use of ransomware

One of its defining features is the blending of 'state support with profit incentives,' including a 'vast network of actors driven by competition to exploit vulnerabilities and expand operations.' China is known to have cyber operators who work on both sides of the aisle, who can be characterized in two groups. The first group includes private sector employees moonlighting as cybercriminals in order to generate supplemental income, as in the case of the iSoon leaks. The second group consists of state cyber actors who use cybercrime for strategic disruption [usually tied to China's Ministry of State Security (MSS) and Ministry for Public Security (MPS)]. This is especially evident in ransomware cases as a specific subset of cybercrime, where Chinese Advanced Persistent (APT) groups have a history of suspected ransomware use, dating back to 2016. The most prominent examples include the use in 2020 of the ColdLock ransomware against Taiwanese organizations by APT41—a prolific cyber espionage group that also carries out financially motivated operations and is thought to be associated with the MSS, which is also known to deploy ransomware without an encryption key (effectively rendering it wiper malware). Another prominent example is the use of CatB ransomware by ChamelGang (also thought to be affiliated with the MSS) against the All India Institute of Medical Sciences (AIIMS), a high-profile medical platform in India, and the Brazilian presidential elections in 2022, in which then-President and candidate Jair Bolsonaro adopted a critical stance against China . In both cases, sensitive data was exfiltrated (i.e., stolen) and erased.

This crossover between state and criminal is especially useful to the Chinese state in a number of ways. Firstly, targeting patterns suggest that victims of Chinese cybercrime, particularly in the United States and Europe, and in sectors such a finance, healthcare, and manufacturing, are of high strategic intelligence value, whether in terms of sensitive data or supply chain access, or even strategic disruption in relation to geopolitical tensions. Secondly, the use of shared tooling and platforms between state and criminal actors (particularly publicly available, non-custom tooling) helps APTs to obfuscate their activity making it easier to evade attribution, save time and resources put toward capability development, and fills a gap in operations before the deployment of custom tooling. Some reporting has also identified the presence of Chinese-speaking hackers on non-Chinese hacking fora, hinting at the 'vast access' this provides to Chinese APTs in recruitment value, and access to databases for future targets.

Most importantly, as with the AIIMS and Brazilian election incidents noted above, the use of cybercrime tactics enhance China's plausible deniability. China has consistently blamed historical ransomware incidents on independent cybercriminal groups, as part of a broader effort to portray its espionage operations as cybercriminal activity. In 2024, its Computer Virus Emergency Response Centre (CVERC) published a report on Volt Typhoon claiming it was a ransomware operation and the actions of individual cybercriminals, as a means of publicly distancing itself and avoiding accountability.

The enabling marketplace

Another key aspect of Chinese cybercrime is the presence of 'enabler firms.' These can be understood as contractors that provide hack-for-hire services, who may also appear as freelancers within the Chinese cybercrime ecosystem (as with the iSoon leaks). For example, a small leak on the DarkForums by VenusTech (a Chinese company) pointed to individual actors hacking prospective targets, and then remaining dormant within these systems—effectively waiting to sell the stolen data to the Chinese government. To some extent, this explains the broad nature of Chinese cybercriminal targeting, in that what might sometimes look like prepositioning within victims' systems is in fact individual criminal actors maintaining a foothold until they are able to sell access or data that they have acquired to the Chinese government.

Critically, underlying both the enabling firms and state cyber actors is a vast and matured cybercriminal marketplace, comprising underground fora, Telegram channels (which are banned in China), and additional platforms. This marketplace supports: hacking and cyber-dependent crime, such as through Chinese-language fora, including the Darknet Forum, the Tea Horse Road Market, and Chang-An Sleepless Night; cyber-enabled crime, including the presence of SIM card dealers, account dealers, and money launderers; and participation in illicit trade (drugs, weapons, counterfeit goods, etc.). However, most critical to China's dual status as both perpetrator *and* victim of cybercrime is the illicit trade in personally identifiable information (PII) that has been established in recent years. Between Chinese hackers, data brokers, web crawlers, and vendors, the trade in PII is vast, in part owing to its global reach as Chinese-language cybercriminals increasingly target individuals and businesses overseas. Discretion and anonymity of users is prioritized in the Chinese cybercriminal underground, which some argue is a direct result of China's enforcement of regulations that restrict anonymity in data usage. One estimate placed the value of the black market in data at around 100-150 billion yuan.

Links to international serious and organized crime

Cyber-crime involving Chinese nationals also extends beyond China's borders and is often linked to serious organized criminal groups or activity in-region. This is illustrated in the growing number of Chinese nationals identified and arrested for their involvement in global cybercriminal operations. For example, in 2025, Pakistan's cybercrime unit made 150 arrests in relation to a cyber-enabled fraud operation, including 48 Chinese nationals, while Thai law enforcement authorities arrested Chinese nationals for their involvement in a transnational scam network and large-scale scam operations, the latter targeting victims across Thailand, China, Russia, and Japan, and involving Chinese syndicates.

These international links take a state-related turn in relation to the Democratic People's Republic of Korea (DPRK), where Chinese nationals have helped facilitate large-scale cryptocurrency thefts, now believed to total $6.75 billion for the DPRK, and with the largest heist involving the theft of $1.5 billion from cryptocurrency exchange ByBit. Analysis of these thefts revealed DPRK actors—including the state-affiliated Lazarus Group—to have 'clear preferences for Chinese-language money-laundering services, bridge services, and mixing protocols.' This is due in part to weak compliance controls for Chinese language platforms (that are linked to scam compounds, such as Huione) and is 'consistent with Pyongyang's historical use of China-based networks to gain access to the international financial system.' This demonstrates how Chinese nationals enable global crime beyond China's borders, and in the case of DPRK, contribute to its financially motivated cryptocurrency heists as a means of evading international sanctions.

China as victim of cybercrime

Though the above analysis demonstrates China's clear involvement in numerous facets of cybercrime, at the same time, China—specifically, its citizens, businesses, and organizations—is victim to the same forces.

Large-scale data theft and breaches

China is known to have suffered noticeable, large-scale data breaches in recent years, the largest of which took place in 2025, with around 4 billion records breached (with more than 805 million records originating from WeChat). The breach itself disappeared quickly, likely owing to the server or system operator (rather than the state) discovering and patching the breach. Nonetheless, researchers were able to discern that the dataset was 'meticulously gathered and maintained for building comprehensive behavioral, economic, and social profiles of nearly any Chinese citizen,' indicating an aggregated dataset that belongs to a cybercriminal.

Curated collections of breached data are a distinct feature of China's cybercriminal marketplace, which rests upon the illicit trade of PII—essentially monetizing the data breaches. The stolen data is then distributed via social engineering libraries, which curate aggregated data and help manage queries (i.e., supporting further criminality). The PII is marked for different purposes and motivations—primarily scams, phishing, doxing, stalking activity—that are usually facilitated or enabled through Telegram channels. This data trade in China tends to be focused on achieving persistent access to target systems—as opposed to in Europe, where cybercriminal actors pursue 'smash-and-grab' approaches to targets—where the data is either slowly leaked or sold outright. Researchers also point to the presence of insiders at telecommunications companies that siphon off and sell data on the side (sometimes responding to bespoke requests).

Cyber-enabled scams in-region

Scam compounds have surged in Southeast Asia in the past five years. Involving kidnap-to-scam operations that rely upon human trafficking by organized crime groups, these compounds act as industrial centers for the forced execution of 'pig-butchering,' cryptocurrency, and money-laundering operations. This means that oftentimes, the individual criminals executing pig-butchering or scam operations are themselves victims of crime.

These cyber-enabled scams reflect many aspects of China's cybercriminal ecosystem. Multiple conglomerates associated with the cyber scam centers are set up in similar ways (i.e., based on the sale of PII, malware, and money-laundering), switching these operations across platforms. Chinese-language platforms, such as the Huione Group (a Cambodian conglomerate), provide the platform for thousands of Telegram channels that facilitate the selling of PII. This is also where artificial intelligence (AI) is playing a growing role. With Southeast Asia at the 'epicenter' of AI's convergence with organized crime, automation is enabling the 'proliferation' of cyber-enabled fraud through the use of large language models for multilingual conversations with victims, and even to suppress China text in scams targeting non-Chinese speakers.

Selective enforcement (and displacement)

China's response to the proliferation of cyber scam operations is uneven and ambiguous, due to a 'confusing complex of mixed incentives and mutual opportunity.' Evidence suggests that Beijing does conduct 'clean-up' operations—closing smaller platforms, enforcing real-name registration, and targeting lower-level cybercriminals. However, this enforcement does not include significant underground marketplaces, such as Huione, FreeCity, or Chang-An, which enable many such operations to take place focus releasing Chinese nationals traf-

ficked to compounds, while leaving militia-linked organizations untouched.

Additionally, enforcement action against these centers will at times conflict with the Chinese government's foreign policy goals. Many of the scam compounds are located in 'special economic zones,' which are often fueled by investment coming from China, including casinos, or via Belt and Road (BRI) investment, in part bringing about 'pronounced geopolitical deference' to China, or as is the case with Myanmar, where China has given its support, recognition, and economic investment (including military investments). The Myanmar government relies upon this in part for its income, reflecting a trade-off for China, as it is in its interests to maintain the Myanmar state and relationship.

Where the Chinese government has taken action, this has had a 'squeezing effect;' with groups moving to friendlier locales, or targeting Western audiences instead. Scam compound operations have pivoted elsewhere, including Dubai and West Africa, where they are run by Chinese-speaking threat actors, or have moved overseas but subcontract to domestic hackers, while some money launderers have moved their operations to the Philippines, Australia, and the Middle East. Additionally, some cybercriminal actors involved in operating the scam compounds have devised alternatives to mainstream cryptocurrencies to circumvent law enforcement action against the likes of Tether—again, providing a model for other criminals or organized crime groups to pivot to other locations, platforms, or cryptocurrencies in order to continue their operating models or businesses in their local language. This also points to a broader enforcement gap—that law enforcement authorities will be able to shut down platforms, but not individual operators who will migrate their operations elsewhere.

Informing opportunities for engagement

Cyber crime as source of systemic vulnerability

The different types of cybercrime and cyber-enabled fraud discussed above are starting to have a real impact on China's economy and society. As personal data processed through 'industrialized chains' is facilitated by the same infrastructure that facilitates external cybercrime, the impact is felt foremost by Chinese citizens, risking eroding public trust in the state. Between the illicit trade of PII and large-scale data breaches, this points to a wider state of insecurity across Chinese platforms and services, making it a source of domestic vulnerability for China.

This is amplified by the negative impact of cybercrime on provincial economic growth across China. One study examining data from across 28 provinces shows that a 1 percent increase in cybercrime corresponded with a 0.019 percent decline in economic growth, suggesting that cybercrime is impeding provincial economic growth, and in the longer term risks undermining China's economic stability. This comes into tension with China's active role in maintaining cyber-dependent and cyber-enabled crime, whether for its foreign policy goals or the substantive national security value of PII (i.e., for domestic surveillance). Nonetheless, the domestic impact of cybercrime in China as a source of system vulnerability may provide a useful basis for approaching and engaging the Chinese state.

Recommendations

Below are suggestions for approaching and fostering diplomatic engagement with the Chinese state on different aspects of cybercrime, derived from expert discussion and consultation.

1. Humanitarian assistance

Expert opinion is divided regarding whether to directly engage the Chinese state on the operating of cyber scam compounds in Southeast Asia, owing to China's record of ambiguity in cracking down on such activity. However, the cyber scam industry continues to cause significant reputational harm to China, domestically, regionally, and globally.

Expert discussion suggested a **clear consensus to engage the Chinese state on the humanitarian impact of cybercrime, rather than on cyber incidents, actors, or capabilities.** From a humanitarian standpoint, many of the individuals that escape the scam compounds have nowhere to go, having had their passports confiscated, and often met with the cold shoulder from their home countries for the same reason—but also in part because they are considered the perpetrators of crime themselves. Though some nongovernmental organizations provide assistance, this is limited, and may be an opportunity for the UK government to consider offering humanitarian assistance, or to provide assistance or best practice in identifying victims and repatriating them, noting that China has forcibly returned around at least 60,000 Chinese nationals to China from the cyber scam compounds.

2. Sharing UK best practice and law enforcement cooperation

Though data breaches risk undermining public trust in the state, and are known to involve insider threats (or the 'corrupt insider') in some cases, discussing the breaches themselves may not be appropriate grounds for engagement, as they are likely to be cause for embarrassment to the Chinese state, given how widely known the breaches are domestically.

However, data breaches might form the basis of diplomatic **discussions around the use or application of the stolen data,** such as where it could be used to target high-profile individuals (or even politicians), as well as the harm stemming from doxxing—noting that cases of teenage suicide in China have been linked to doxxing incidents. Therefore, with an emphasis on the personal harm caused by data stolen in breaches, and

from scam compound operations, this could be an area for the UK government to approach the Chinese government, sharing best practice and lessons from the National Crime Agency to identify victims and provide Protect notifications at scale, as means to reduce societal harm from cybercrime.

Skepticism as to China's desire to take enforcement action is high among experts, not least as Chinese and Western law enforcement models differ greatly. Nonetheless, experts suggest approaching the Chinese government to discuss potential law enforcement cooperation on cybercrime. Noting the difficulties of targeting actors responsible for cyber-dependent crime, given links to the Chinese state, experts suggested **discussing targeted disruption efforts against applications or services that provide infrastructure to cybercriminal groups.** This includes the use of enabling infrastructure and clamping down on Chinese language money-laundering services. Targeting such services would have disproportionate impact, particularly where used by multiple cybercriminal groups, as well as significant secondary impact in also constraining a critical enabler of the DPRK's cybercriminal activity, denying access to its spoils.

3. Multilateral engagement

In 2025, at the Conference of Global Public Security Cooperation, the Chinese Ministry for Public Security (MPS) called for the creation of an international alliance against cyber scams. Seeking to establish a global framework for cooperation to combat this type of transnational crime, this initiative would provide for information-sharing between states, coordinated joint operations, the exchange of evidence, and ongoing judicial cooperation with China. This is also supported by the creation of a network of think tanks on public security governance as a means of encouraging expert participation. Though this should be met with a grain of salt, given China's mixed record in combatting cyber scams in-region, the MPS call for this initiative and framework was made at the direction of President Xi Jinping, demonstrating a political backing for the alliance, and followed on from statements made by Foreign Minister Wang Yi to the Association of Southeast Asian Nations (ASEAN) in January 2025 on tackling the threat that cyber scams pose. This could provide fertile ground for BE Beijing and wider Foreign, Commonwealth and Development Office engagement with China through this multilateral initiative, sequenced as a potential follow-up after a UK prime minister or other high-level visit to China.

Conclusion

China's complex relationship with cybercrime means that it is both active perpetrator and victim at the same time. Across cyber-dependent crime, cyber-enabled fraud, or cryptocurrency theft, China has a checkered record of taking enforcement action to tackle or counter such crime. This owes to the plausible deniability afforded to the state where its cyber actors moonlight or deceive in their use of cyber operations, the foreign policy benefits that limited crackdowns on the cyber scam compounds bring, or the national security value of personal identifiable data derived for domestic surveillance on its citizens. Despite these benefits, it is clear that cybercrime is a source of growing vulnerability to the state, risking undermining China's long-term economic stability, and causing significant reputational harm. This source of vulnerability provides small, if limited, openings for the UK government to consider approaching China through diplomatic engagement. Rather than engaging China on direct cyber or technical issues, such as specific cybercriminal incidents, actors, or capabilities, engagement should instead focus on the humanitarian impact of cybercrime, and the harm caused. Additional grounds for engagement should consider discussing potential law enforcement action on the critical enablers to cybercrime and fraud, and lastly, multilateral engagement via initiatives that offer mutual gain.

About the center

The **Cyber Statecraft Initiative** works at the nexus of geopolitics, technology, and security to craft strategies to help shape the conduct of statecraft and to better inform and secure users. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org