中国简报 China Brief
a journal of analysis and information
The JAMESTOWN FOUNDATION

VOLUME 24 • ISSUE 7 • MARCH 29, 2024

IN THIS ISSUE:

When The Chips Are Down: Taiwan's Water and Energy Conundrum

by Arran Hope

Reservoir in Taiwan at low water level. (Source: Sohu)

Executive Summary:

- Taiwan's heavy reliance on energy imports, coupled with high energy demands, poses significant challenges, with semiconductor manufacturing being a major consumer.
- Environmental concerns such as droughts, exacerbated by climate change, and Taiwan's fossil fuel-heavy energy mix raise serious alarm bells for the island's energy security.
- TSMC, Taiwan's semiconductor giant, faces water scarcity issues, which are forecasted to impact its production capabilities.
- The People's Republic of China (PRC) poses additional threats, with potential military actions targeting Taiwan's energy supply routes heightening concerns over the island's security and economic stability.

Earlier this month, the Taiwan Center for Security Studied (TCSS) hosted 170 experts to participate in an annual tabletop exercise (TTX) (TaiwanCSS, March 15). The theme of the TTX was "Gray Zone Strategy and Crisis Management," which was analyzed across eight scenarios set in the year 2032. One item highlighted as being particularly vulnerable was the island's energy supply (Digitimes Asia, March 26). Energy security, and resource scarcity more generally, is an increasing problem for Taiwan. It is made all the more acute by the exorbitant needs of its most valuable industry, semiconductor manufacturing, and of its most valuable company, Taiwan Semiconductor Manufacturing Corporation (TSMC; 台積電). As the island prepares to transition to a new government, environmental and policy problems at home, an uncertain external context, and the looming threat of a blockade instituted by the People's Republic of China (PRC) conspire to push Taiwan into a precarious position. While progress is being made, short- and medium-term fixes do not seem readily available or politically viable. This is a situation that most of the rest of the world has substantial interest in resolving, not least because 90 percent of advanced chipmaking capacity is based in Taiwan, as well as 18 percent of total global capacity.

Taiwan is home to around 24 million people and is one of the most densely populated countries in the world. As a small island with relatively few natural resources, it is constrained in terms of its capacity for autonomy in the production and generation of electricity. Currently, Taiwan imports almost 98 percent of its energy in various forms and from a variety of sources (Taipower, accessed March 29). In 2022, almost 80 percent of total generation came from fossil fuels, of which natural gas constituted 43 percent, coal 35 percent, and oil 1.4 percent. Nuclear contributed 9.1 percent, renewables 8.6 percent, and hydroelectric 1.2 percent. A lack of available land is a contributing factor to the low level of solar and wind power on the island, though offshore wind projects in the Taiwan Strait have been steadily growing since 2017 (FOW1, accessed March 29).

Despite Taiwan's high dependence on energy imports, it has unusually high energy demands. It ranks 17th in the world in terms of CO2 emissions per capita (the PRC ranks 35th) (Our World in Data, accessed March 29). The average person in Taiwan uses an equivalent amount of electricity as their American counterpart despite the United States having a per capita GDP that is twice as large. Taiwan's per capita energy and electricity demand are three times higher than the average across Asia (Baker Institute, December 21, 2023). The surge in demand has outpaced population growth by orders of magnitude. This is largely down to industry, which accounted for 56 percent of power consumption in 2022. Electronic components manufacturing constituted over half of this figure.

Taiwan's fossil fuel-heavy energy mix and rapidly rising demand raises serious concerns, particularly as the effects of global warming take their toll. Fewer typhoons reaching the island have led to four droughts in the last decade, two of which were the most severe since 1947. Government estimates suggest that rainfall could decline a further ten percent by 2050 (S&P Global Ratings, February 26). Rolling blackouts have had to be implemented in both 2017 and 2021 (Center for American Progress, January 19, 2022). If such occurrences become more common during extended periods of extreme heat, there would be severe costs to human life and to Taiwan's economy. Moreover, Taiwan imports much of its carbon-based energy from parts of the world that are themselves less stable, or could be influenced by the PRC, such as Russia, Qatar,

and Indonesia (Qianhai Institute of International Affairs, September 27, 2023). The PRC has a track record of starving Taiwan of diplomatic allies. It is not inconceivable that it could also make it difficult for the island to source its energy.

The 2022 "National Electricity Resources Supply and Demand Report (全國電力資源供需報告)" explicitly revised projections for the proportion of renewable energy in the island's mix down from 20 percent to 15 percent in 2025 (TWReporter, July 22, 2022). Even this number seems somewhat ambitious, given that renewables only rose from 6.0 percent to 9.9 percent of the island's generated energy between 2019 and 2023. Experts have diagnosed problems in "finding space," the "lack of a national white paper on spatial development," and "grid technology" ("尋找空間"、"缺乏全國空間發展白皮書"、"電網技術"三大面向) (TWReporter, May 25, 2022).

The Democratic Progressive Party (DPP) government's approach to nuclear power over the last eight years has exacerbated the situation. President Tsai Ing-wen (蔡英文) has pursued an agenda labeled "Nuclear-free Homeland 2025 (2025 非核家園)," which has sought to decommission the island's remaining nuclear power plants (New Bloom Magazine, January 11). This policy has strong public support, particularly following the 2011 Fukushima disaster in Japan, which heightened fears about nuclear safety on the island. Over 70 percent of Taiwan citizens oppose bringing the currently unfinished Lungmen Nuclear Power Plant online, reflecting widespread concern over the risks posed by earthquakes, tsunamis, and floods—dangers that Taiwan's nuclear facilities are uniquely exposed to according to risk assessments conducted by Maplecroft (FTV News, March 11, 2021). Although Tsai's successor, Lai Ching-te (賴清德), did not specify a specific timeline for nuclear energy to be eliminated during his campaign, the aspiration to be "nuclear-free" is still part of his agenda—in contrast with the platform of candidates whom he defeated in February's election. The policy is also in contrast with other countries, such as Japan, South Korea, India, and even the PRC, who are currently expanding their use of nuclear power.

These adverse conditions will affect TSMC to some extent. S&P Global Ratings published a report in February titled "TSMC And Water: A Case Study Of How Climate Is Becoming A Credit-Risk Factor," which was picked up by local news outlets, but received little attention in Western media (S&P Global Ratings, February 26; C114, February 29; CTEE, March 1). Water scarcity has long been a problem in Taiwan. A 2005 study by the World Economic Forum ranked the island as 18th lowest in terms of freshwater availability per capita among 146 countries (Commonwealth Magazine, May 30, 2023). The situation is acute for TSMC, whose factories are largely located in the south of the island, where shortages are most serious.

The report's headline conclusion was that poor execution of water supply management "could cause TSMC's output to drop as much as 10 percent" from their forecast for 2030. This is because of increasing water scarcity coupled with skyrocketing demand. TSMC's water consumption per unit grew over 35 percent since 2015. The company's demand for feedwater could double from 2022 levels by 2030. As processing technology advances, more steps are required in the process; as wafers must be rinsed between each step in the process, more water—in the form of "ultra-pure water" (to which water is converted in an energy-

intensive process)—will be needed (Semiconductor Digest, October 24, 2022). To put this in perspective, Taiwan's industry required 10 billion liters of water annually in 2022. Every day, TSMC alone used the equivalent amount of water as 170,000 US households. This level of demand, in a deteriorating climatic environment, will impact the company's ability to maintain stable production levels. In fact, this has already occurred. In 2021, a drought forced officials to require the industry to cut water usage by up to 20 percent (S&P Global Ratings, February 26).

The S&P Global Ratings report describes TSMC's water security issues as "meaningful, but modest relative to its peers." The company itself is reported to have estimated that a serious drought could impact its revenues by between 0.7 and 1.1 percent (Commonwealth Magazine, June 30, 2022). However, some experts fear that droughts in consecutive years would be intolerable (Commonwealth Magazine, May 30, 2023). Others, meanwhile, believe that the issue of water and electricity supply are key factors in TSMC's decisions to set up overseas factories in Japan and the United States (ETToday, March 27, 2023; TSMC, February 6, August 8, 2023).

All these concerns are compounded by potential actions that the PRC might take toward Taiwan. The People's Liberation Army (PLA) has conducted live-fire exercises for the apparent purpose of "blocking the country's important energy supply routes"—systematically encompassing Taiwan's eastern, northern, and southwestern regions (TWReporter, August 2, 2022). Given that Taiwan maintains only seven or eight days of LNG reserves, a blockade would not have to be long-lasting before its impact would be felt (Storm.mg, August 19, 2022). One report calculates that Taiwan's oil reserves can support military and civilian needs for four to five months and coal reserves for an additional month. It also suggests that a total shutdown of the manufacturing could allow the island to sustain itself for six months (Storm.mg, August 17, 2022). This is, of course, contingent on the PLA not targeting fuel reserves, many of which are relatively exposed.

The PRC is well aware of the problems Taiwan faces. Official media has responded to droughts on the island with schadenfreude and Beijing has attempted to leverage previous water crises to increase dependance on the mainland by integrating Taiwan's outlying islands with its own water, electricity, and gas supplies—the "Four Mini-Links (小四通)" (see China Brief, July 2, 2021). While the PRC remains reliant on Taiwan's semiconductor industry to an extent, this dynamic will likely lessen as it grows its indigenous industry. TSMC has done much to mitigate risks, including dramatically improving its wastewater recycling, conservation, and efficiency. But some factors are simply beyond the company's control. Taiwan's incoming government could raise its ambitions in energy policy and reduce the contradictions in its current trajectory, bringing its approach in line with similar countries in the region. The wider community will also require better understanding of Beijing's strategic framing of Taiwan's energy and water troubles, and how that informs its own calculus.

Arran Hope is the Editor of China Brief.

Foreign Intelligence Hackers and Their Place in the PRC Intelligence Community

by Matt Brazil

Advertisement for the 2018 "Anxun Cup" hacking competition, jointly hosted by Sichuan Anxun (iS00N) and Chengdu University. (Source: iS00N)

Executive Summary:

- Leaked files from iS00N reveal deep insights into the PRC's intelligence operations, highlighting an intensified global security offensive as well as issues within the intelligence community.
- iS00N's growth is tied to Xi Jinping's aggressive policies and demonstrates the importance of private contractors in fulfilling the PRC's increased intelligence and security needs.
- The leaks expose employee dissatisfaction and underscore iS00N's critical role in intelligence gathering and job provision, reflecting the contractor's complex relationship with the PRC government.
- The exposure raises questions about the role and regulation of hacking contractors in the PRC, potentially leading to investigations and reforms that could affect the PRC's intelligence strategy and international relations.

In the month since the leak of over 570 files from the Shanghai-based hacking contractor iS00N (安洵信息), we have seen much reporting about their company culture, leaders and clients, whom they try to recruit, and what iS00N was actually doing (some of the best analysis on the leaks and the overall nature of the threat can be read at Natto Thoughts and Recorded Future).

At the same time, the leaks are an opportunity to advance our understanding of how the opaque People's Republic of China (PRC) intelligence and security community is changing. The data, which continues to be mined by various analysts, provides a window into how Beijing's intelligence and security community (IC) is using cyberspace to meet the many threats perceived by the Party. It indicates continued issues in China's IC regarding standards, training, and discipline, while also confirming the long-held idea in the West that Beijing's worldwide intelligence and security offensive is intensifying, while the Chinese side continues to blithely deny everything.

The Leaks in a Nutshell

Confirmed as genuine, the leaked data shines a light on the freelance hacking contractor's operations, targets, and personnel (Associated Press, February 21). They reveal tasks that might be considered low-level but are now priorities because of Chinese Communist Party (CCP) General Secretary Xi Jinping's more aggressive policies at home and abroad. The added work necessary to meet the expectations of the CCP's supremo appears to have fostered a division of labor between the direct-hire officers of the Ministries of Public Security and State Security (MPS, MSS) and the People's Liberation Army (PLA) on the one hand, and their contractors—like iS00N—on the other. That contractors are being engaged by the security agencies at what appears to be a significant level also indicates that they have a limited supply of manpower at their disposal to meet enhanced intelligence tasking.

The leaks also contain revealing information about the kind of work these contracting firms pursue and employee attitudes toward both the work itself and their employers. Any retaliation against iS00N may be mitigated by its utility to the government, in terms of both the intelligence it produces and the employment it provides to recent university graduates amid rising unemployment.

In addition, the Chinese side does not seem to mind being exposed as engaged in spying abroad. They meet all such revelations with the same denials and rote statements that the United States is guilty of being the "world's largest hacking empire and cybercriminal" (Global Times, July 12, 2023).

iS00N Clients and Targets

The cohort of hacking contractors which include iS00N has been developing since the November 2015 military and intelligence reorganization initiated by Xi Jinping (see China Brief, February 4, 2016). The reforms probably redirected military cyber resources away from civilian targets in favor of those with military significance. The affected units could include the famous Unit 61398, alleged to be responsible for numerous hacking operations over the last two decades (Mandiant, December 30, 2021).

It is difficult to confirm the number of contractor hacking firms without further leaks. But the demand for their services seems to have risen with Xi Jinping's more aggressive domestic and foreign policies. These logically require more and better intelligence on China's targets and perceived antagonists. The utility of these contractors seems to be due in part to how well they work with the security apparatus, which appears to have increased responsibilities under Xi.

The MSS conducts most of its actual foreign intelligence collection through their provincial state security departments (SSDs) or municipal state security bureaus (SSBs). Different regional departments and bureaus appear to focus on targets in different parts of the world. For example, the Shanghai SSB carries out operations against the United States and its main Western allies, perhaps in part because so many Americans and other Westerners running factories and corporate offices in China are based there. The nearby Zhejiang SSD has been observed working against northern Europe, the Qingdao SSD against Japan and the Koreas, and so on. **[2]** This arrangement is probably dynamic, changing in response to shifting intelligence requirements and other considerations.

The Ministry of Public Security (the national police) has long conducted most of its work through provincial Public Security Departments (PSDs) and its municipal and county Public Security Bureaus (PSBs). This organizational structure has spawned work by agents of local PSBs and PSDs in illegally established "police stations" abroad. These police stations are illegal, as they are foreign government missions reportedly lacking the permission of the host government to operate—with the prominent exception of police stations set up with host government permission in South Africa (Africa-China Reporting, October 10, 2023; 60 Minutes Australia, July 30, 2023). These entities keep tabs on dissidents and others from their respective cities and provinces in China (Safeguard Defenders, December 5, 2022; CNN, February 2021). This same model seems to hold in PSD and PSB work with hacking contractors. Municipal bureaus and provincial departments that have intelligence requirements appear to solicit hacking contractors to help fulfill them.

Natto, an analyst group focused on Asia that has analyzed the leaks, count 66 of the 120 agreements in the data showing iS00N Chengdu contracts with PSBs and PSDs, and 22 with SSBs and SSDs. One contract was with the PLA, and was the only one classified as "SECRET" (Natto, February 28). 31 additional contracts were with other government agencies, institutes, state-owned enterprises, and universities. Subject expert and former DOD official Drew Thompson corroborated this analysis but added that his research indicates that none of their clients were at the ministry level. Instead, all were at the provincial level and below. Some State Security Bureau clients had unit designators in Yunnan and Hubei provinces, including Yunnan Province Unit 59 and Unit 938 (云南省 59 号单位 and 938 单位).

The iS00N leaks show that contractors specialize in several functions, including helping local PSBs and PSDs monitor their émigrés which have been deemed significant threats. For instance, the contract drawn up between iS00N's Chengdu office and a Public Security Bureau in the Xinjiang Uyghur Autonomous Region (XUAR), the Bayingolin PSB, is an illustrative example (XUAR Statistic Bureau, June 14, 2021). **[3]** The undated contract is likely from late 2022, given its proximity to other documents in the iS00N leak collection. In it, iS00N's Chengdu office offers these services:

1. Obtain data on Uyghur "terrorists" who might return to the XUAR from iS00N's penetration of the postal services of Afghanistan and Pakistan, the foreign ministries of Malaysia and Mongolia, the Malaysian military, the Thailand Ministry of Finance and Commerce, and commercial entities including Air Macau, Air Astana, and telecom operators in Kazakhstan, Mongolia, and Pakistan, and finally from other operations aimed at Syria, Uzbekistan, and Iran.
2. Technical services to assist PSB operators in passing proficiency verification assessments, training in network attack and defense theory, and practical exercises in terminal remote control and penetration attacks.
3. Design and initiation of a talent training plan between the Bayingolin PSB and local schools.
4. Construction of facilities and fit-out of required equipment for the PSB to run its own hacking operations to enhance offensive capabilities abroad, per previous requirements laid down by MPS in 2010. These include a Twitter evidence collection platform, and remote-control management capability for Windows, Mac, Android, and Linux based systems.

iS00N seems focused on the pathways back and forth between Xinjiang and Asian countries to which Uyghurs have emigrated, according to Thompson. The leaked material also indicates a division of labor. While the MSS and PLA use HUMINT resources to go after strategically important intelligence such as military assessments and plans at the strategic level, a lot of iS00N's work is low-level and specialized, tasked against soft targets such as email and phone systems in countries like Thailand, Malaysia, and central Asian states. **[4]**

Clandestine technology acquisition is another area of activity in which PRC hacking contractors like iS00N excel. This involves the theft of trade secrets to help China upgrade its military and civilian industry. Recent analysis indicates that iS00N was behind the 2022 "supply chain attack" against the Canadian firm Comm100, which provides chat and other industrial connectivity solutions to thousands of corporate clients (Unit 42, February 23; Comm100, accessed March 21).**[5]** The same analysis indicates that iS00N also goes after dissidents and political irritants. The contractor can be linked to a large-scale attack (dubbed "POISON CARP") in 2018–19 against Tibetan groups. The intrusions into iOS and Android devices owned by senior members of Tibetan groups were carried out by operators posing as NGO workers, journalists, and other fake personas. Links offered to the Tibetan users led to code designed to install spyware. The exploits were documented but not linked to iS00N until last month (Citizen Lab, September 24, 2019).

Central to iS00N's communications collection against such targets of interest is the "email analysis intelligence decision system (邮件分析情报决策系统)" and the "secret email extraction platform (邮件密取平台)," both of which specialize in the intercept and analysis of Gmail and Outlook messages. The latter "can achieve long-term and covert acquisition of target email data and intelligence, grasp evidence of the target's illegal crimes, and achieve prevention" for RMB 900,000 ($125,000) a year or RMB 2.4 million ($330,000) for three years. **[6]**

The leaks suggest that iS00N's access only lasts as long as a system remains vulnerable but can be locked out if that changes, Thompson argues. However, soft targets like university systems are an exception. For instance, they appear to have been inside the system of French university Sciences Po for almost 10 years. Simply changing passwords and implementing system updates can prevent the exploitation of many vulnerabilities, though universities may tend to lag private companies or some government agencies in terms of cybersecurity best practices. **[7]**

iS00N offers clients the "Twitter Control and Forensics Platform (Twitter 舆论导控 or 控制取证平台)" for RMB 700,000 ($97,230) per year or RMB 1.5 million ($210,000) for three years. It uses "exclusive non-sensory forensics" technology and big data "intelligent crawler technology" to implement countermeasures and monitoring of Twitter accounts.

iS00N Chengdu Employees and Salaries

In a table listing iS00N personnel at their Chengdu office who were cleared for secret duties (涉密人员花名册), each is categorized as either a "party member (党员)" or one of "the masses (群众)," along with their education level and, if a university graduate, their major. Another column lists each employee's "[o]verseas background of immediate family members (直系亲属的境外背景)," though all reported "none (无)." Job titles included:

- Legal representative and team leader;
- Confidentiality director and deputy team leader;
- Operations and maintenance engineer;
- Software development engineer (and manager);
- Software development manager;
- Multimedia design and production;
- Confidentiality administrator;
- Human resources manager; and
- Classified computer security administrator (涉密计算机安全管理员). **[8]**

A table of salaries, benefits, and taxes collected for the month of October 2022 indicates that the pay scale for non-management employees at iS00N varied. The highest monthly salaries (RMB 19,000–21,500; $2,640–2,990) were awarded to three people in the technology department (技术部) and the lowest (RMB 3,500–10,000; $490–1,390) to those in support roles. Most of the employees at the technology department drew monthly salaries in the range of RMB 10,000–16,000 ($1,390–2,220). **[9]**

For those in the top half of the iS00N Chengdu pay distribution, these salaries are reasonable. Monthly rent for a one-bedroom apartment outside the city center in Chengdu averaged about RMB 2,000 ($280) in May

2022, while the same in the city center cost about RMB 2,800 ($390). Larger apartments go for about twice as much, above RMB 4,500 ($625) (Travel Safe-Abroad, May 10, 2022). Those earning well below RMB 10,000 ($1,390) per month likely became disgruntled at their perceived low pay. One chat includes the message:

> *"I'm really drunk…Public Security clients are such stupid c***s [公安的客户太傻逼] ... I'd like to get the f**k out of the Public Security business this year. Too much heartache. Still no f**king money."* **[10]**

Ding Xiaoyang accepts an award for young leaders from China's Ministry of State Security in May 2018 while he and other MSS intelligence officers were allegedly hacking and stealing sensitive intellectual property from around the world. (Source: DOJ, July 19, 2021)

Contrasts and Similarities with Two State Security Front Companies

In the leaked materials, iS00N occasionally refers to itself as an "APT." The term—which stands for Advanced Persistent Threat—was coined by Western security researchers to refer to state-sponsored hacking groups. iS00N, as a freelance and seemingly private organization not under any ministry or department, takes ironic ownership of the term. But iS00N exhibits both similarities and differences with APTs known to be directly controlled by PRC authorities.

The now defunct Hainan Xiandun (海南仙盾) Technology Company Ltd. provides a useful comparison. Hainan Xiandun was directly set up as a front company by the Hainan SSD with management and other support from a local university. Before identifying Hainan Xiandun by name, private sector security researchers initially assigned it several codenames, eventually settling on APT40. By contrast, iS00N was established as a freelance, for-profit business to seek various clients among PSBs, SSBs, and so on.

However, both pursued an eclectic selection of targets: aviation, defense, education, government, healthcare, biopharmaceutical, and maritime industries in the United States, Austria, Cambodia, Canada, Germany, Indonesia, Malaysia, Norway, Saudi Arabia, South Africa, Switzerland, and the United Kingdom. Despite their different business models, the two companies' intelligence tasking also displayed some parallels, and both were working for PRC government and military clients.

Hainan Xiandun was an MSS front company and probably immune from pursuit in court by a competitor. iS00N, meanwhile, has been embroiled in business disputes with their own ex-employees and with an erstwhile collaborator and competitor, Chengdu 404 (aka APT41). Reporting has revealed chat messages from iS00N showing that executives from their firm and Chengdu 404 worked together to fix bids to the disadvantage of their PRC government clients (CloudSEK, February 23; Hunt & Hackett, March 11; Associated Press, March 8).

Another front company is the Wuhan Xiaoruizhi S&T Co Ltd (Wuhan XRZ; 武汉晓睿智科技). According to a US Justice Department indictment filed on 30 January, the company was set up in approximately 2010 by the Hubei State Security Department (HSSD) (DOJ, January 30). The seven defendants named in the indictment worked on behalf of HSSD, targeting Hong Kong democracy activists, commercial entities, journalists, and researchers to support unnamed MSS foreign intelligence and economic espionage objectives. They sent emails to "thousands of US and foreign politicians, foreign policy experts, academics, journalists, and democracy activists," as well as companies in the defense, IT, telecommunications, manufacturing, trade, legal, and research industries. Notably, the emails themselves were hazardous, according to the indictment:

> *"The messages contained an embedded hyperlink that served as a tracking link. If the recipient activated the tracking link by opening the email, information about the recipient, including the recipient's location, IP addresses, network schematics and specific devices used to access the pertinent email accounts, was transmitted to a server controlled by the Conspirators."* **[11]**

Again, an eclectic mix, but not specific enough to analyze what intelligence requirements are being levied on which SSDs and SSBs. It is a situation which may be in flux, might be disorganized, or may be intentionally duplicative to drive competition and distrust between agencies so that they do not conspire together against the CCP elite.

Future Prospects: Too S00N to Tell

iS00N has CCP members among its management and staff, which in theory opens them to the same sort of investigations that disciplined domestic tech giants in recent years (DavisPolk, February 17, 2022). Investigations by the Central Commission for Discipline Inspection (CCDI), the party's anti-corruption arm, would at a minimum be warranted for fixing bids to artificially inflate the prices paid by MPS and MSS bureaus for services. It would also be warranted to get to the bottom of the leak, which likely violated laws on state secrets and counterespionage, and are likely considered more urgent following extensive foreign media coverage.

The apparent dissatisfaction by at least one iS00N employee raises other questions. Do freelance companies engage in wage theft or other types of fraud? Do underpaid operators, equipped with the skills of a cyber burglar, use them against PRC entities such as state-owned enterprises? PRC media is yet to report any such investigations, but they would likely be kept secret until the hammer falls on a set of designated criminals. Reforms may lead to significant restrictions, not only on iS00N but on other freelance hacking contractors. The MPS and MSS may point out the relative reliability, in theory, of front companies closely managed by themselves. It remains to be seen if the need to exert discipline outweighs the value of iS00N's skilled operations against the CCP's perceived enemies and the imperative to supply the demand for jobs for university graduates amid the PRC's high youth unemployment rate.

"Naming and shaming" do not seem to deter Beijing's agencies and companies from various forms of espionage. But stopping the activity cold is not the point. Indictments and imprisonments may breed caution among active operatives and discourage some prospective candidates from joining up, as being caught can result in permanent travel restrictions to the United States and nations with which it has extradition agreements. This is the case for Xu Yanjun, now serving 20 years in prison for corporate espionage (Reuters, November 21, 2022).

Matt Brazil is a Senior Analyst at BluePath Labs and a Senior Fellow at The Jamestown Foundation. He pursued Chinese studies as an undergraduate at UC Berkeley, as an Army officer with tours in Korea and NSA, and as a graduate student at Harvard in their Regional Studies East Asia program. After a stint as the China specialist for the Commerce Department's Office of Export Enforcement, he was assigned as a Commercial Officer with the US Embassy, Beijing, where he both promoted and controlled US high technology exports to China.

Afterward, Matt spent 20 years as a security professional, performing investigations in China for a chip manufacturer, and leading the development of a security organization in China for an American specialty chemicals firm. His PhD dissertation at the University of Sydney (2013) described the place in the Chinese Communist Party of their intelligence organs. That and further research led to his contribution as the coauthor of Chinese Communist Espionage, An Intelligence Primer (2019). Matt is also the author of the China chapter in the Handbook of Asian Intelligence Cultures (2022). His next book concerns Beijing's contemporary worldwide espionage and influence offensive.

Notes

[1] Intelligence failures that came close to being fatal include missing signs of an impending coup by the Nationalist Chinese enemy (1927) and the defection of the leader of CCP Intelligence operations (1931). Successes that saved the party from disaster include the Three Heroes spy ring (1929–31), the CCP agents who uncovered Nationalist plans to attack the Red Army in 1934 and 1947, and the operation that discovered a Nationalist plot to kill Chinese president Liu Shaoqi during a state visit to Cambodia in 1963. Peter Mattis and Matthew Brazil, *Chinese Communist Espionage, An Intelligence Primer* (Annapolis: Naval Institute Press, 2019), 215-216, 6-7, 93. John Gittings, "Obituary, Xiong Xianghui," *The Guardian*, 26 September 2005, https://www.theguardian.com/news/2005/sep/26/guardianobituaries.china. 开诚, *李克农 中共隐蔽战线的卓越领导人* (北京: 中国友谊出版公司 2012), 2-3. David Ian Chambers, "Edging in from the Cold: the Past and present State of Chinese intelligence Historiography" *Studies in Intelligence*, Vol. 56. No. 3, September 2012, https://www.cia.gov/resources/csi/studies-in-intelligence/volume-56-no-3/edging-in-from-the-cold-the-past-and-present-state-of-chinese-intelligence-historiography/

[2] Nigel Inkster, *China's Cyber Power* (London: The International Institute of Strategic Studies, 2016), 55.

[3] The Bayingol PSB contract consists of five pages rendered in five files, beginning with leaked iS00N document d410e4aa-fb52-4ed4-9078-4483267a02b3_0 and ending with d410e4aa-fb52-4ed4-9078-4483267a02b3_4

[4] Drew Thompson, former senior DOD official, Visiting Senior Research Fellow at the Lee Kuan Yew School of Public Policy at the National University of Singapore. Interview with the author via audio link, March 11.

[5] A supply chain attack infects the target through a trusted third-party vendor like Comm100, that offers services or software, infecting all the users of the application.

[6] Document aedc6a39-7862-4bbc-99e7-780ab3980282_4_0.png

[7] Drew Thompson interview with the author via audio link, 11 March 2024.

[8] Document 6d7fc7b3-c892-4cb5-bd4b-a5713c089d88_0.png

[9] Document 2db27de1-d5c5-4f89-8572-da697a6329e4_3_0.png

[10] iS00N text (Markdown) document 36.md

[11] US Justice Department, Indictment 24-CR-43, 30 January 2024, para. B16, https://www.justice.gov/opa/media/1345141/dl?inline

ChinaBrief • Volume 24 • Issue 7 • March 29, 2024

Beijing's Increasing Maritime Gray Zone Operations Around Taiwan's Outlying Islands

by John Dotson

Taiwan Coast Guard personnel conduct rescue and salvage operations about the small craft that capsized after a chase involving a coast guard vessel, resulting in the deaths of two of the four men aboard the boat (February 14, 2024). (Source: ROC Coast Guard Administration)

Executive Summary:

- On February 14, an incident occurred to the east of Taiwan's Kinmen Island, in which an unidentified PRC small boat capsized while allegedly fleeing from an attempted inspection by the Taiwan Coast Guard. The incident resulted in the deaths of two of the four men aboard.
- In the wake of the incident, the PRC government has accused—without evidence—Taiwan authorities of maliciously causing the accident. The PRC Coast Guard has stepped up its presence and "law enforcement" activities in the area and engaged in limited harassment of Taiwan vessels and incursions into waters declared restricted by Taiwan's government.
- Beijing appears to be leveraging the incident to create an "opportunistic crisis"—using the event as a pretext to further escalate "gray zone" operations intended to assert Beijing's claimed sovereignty over both Taiwan and the waters of the Taiwan Strait.

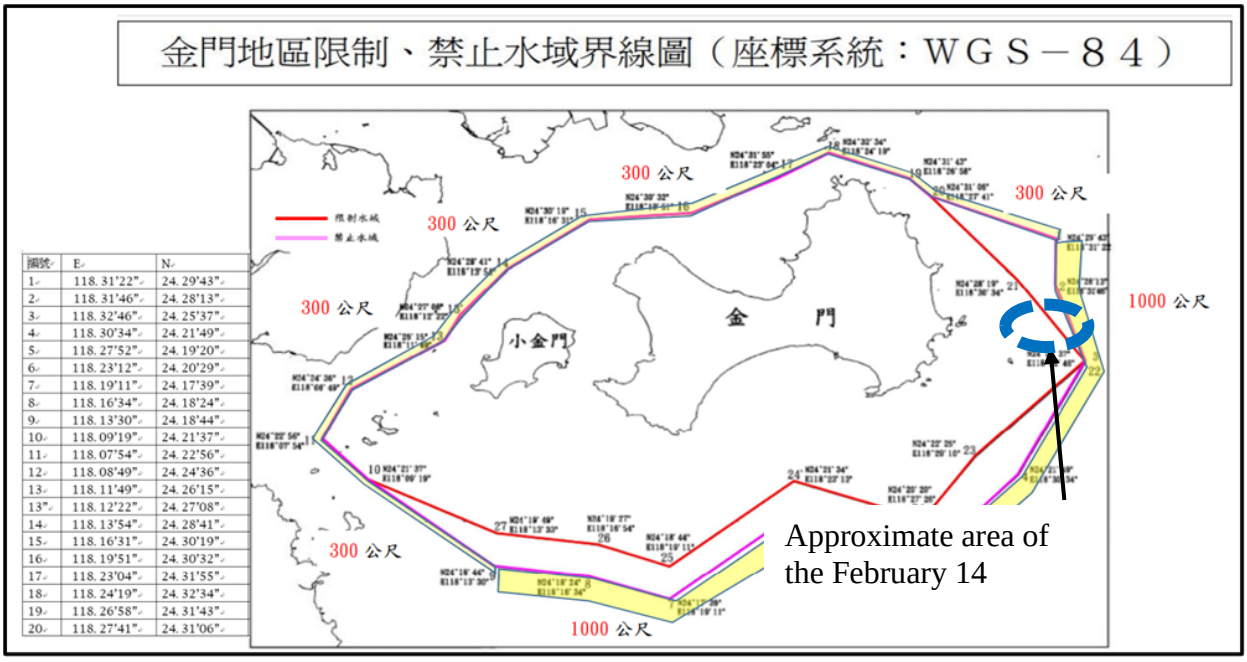
On February 14, an incident occurred near Taiwan's Kinmen Island (金門島) group that illustrated ongoing tensions between Taiwan and the People's Republic of China (PRC) over issues of maritime administration. It also illuminated patterns in the PRC's sustained and ongoing efforts to erode Taiwan's sovereignty. According to the Republic of China (ROC) Coast Guard Administration, around 1:45PM local time the vessel CP-1051 confronted a "three no's boat" (三無船舶)—meaning no name, no registration certificate, no registered homeport—at a point 1.1 nautical miles to the east of Jinmen's Bei-ding Island (北碇島), and .86 nautical miles inside waters declared restricted by Taiwan's government. In the ensuing chase, the boat capsized, resulting in the deaths of two of the four-man crew (ROC Coast Guard, February 14, February 20).

Taiwan's Mainland Affairs Council (MAC, 大陸委員會) explained the ROC Coast Guard's actions by stating that the PRC boat had resisted inspection and capsized while attempting to flee the area. Describing the background to the incident, MAC stated that:

> *[O]ver the past years, a small number of people from mainland China have trespassed in Taiwan's waters to dredge sand, fish with explosives and poisons, dump trash at sea, and engage in other actions harmful to the marine ecosystem. However, Taiwan's calls for mainland China to strengthen governance have not resulted in any improvement … Taiwanese people have repeatedly reported these incidents and called on the competent authorities to expel the vessels in accordance with the law, making the coast guard officers duty-bound to step up law enforcement to protect the people's rights* (MAC, February 15).

Three days later, on February 17, PRC Taiwan Affairs Office spokesperson Zhu Fenglian (朱鳳蓮) issued a statement to provide an official PRC response of the incident. The statement opened with a standard declaration that "[b]oth sides of the Straits belong to one and the same China, and Taiwan is an inalienable part of China's territory." She then went on to declare that the fatal capsizing incident had "sparked widespread outrage on the mainland, and severely hurt the feelings of compatriots on both sides of the Taiwan Straits." Zhu further issued a vague threat that "the mainland reserves the right to take further measures, the consequences of which shall be borne by the Taiwan side" (CGTN, February 18).

In the wake of the incident, there has been a steady continuation of minor incidents involving efforts by the ROC Coast Guard to chase PRC-based fishing boats out of waters that Taiwan has declared off-limits (TaiwanPlus, March 26). There has also been a significant uptick in terms of both PRC presence and "law enforcement" activity around Taiwan's outlying islands, as well as in the escalation of PRC rhetoric directed at Taiwan. Such PRC actions serve to illustrate patterns in the "gray zone (灰色地帶)" operations undertaken by PRC government-directed assets to erode Taiwan's sovereignty and buttress the narratives that the Chinese Communist Party (CCP) propaganda system directs toward both Taiwanese and international audiences.



編號	E	N
1	118. 31'22"	24. 29'43"
2	118. 31'46"	24. 28'13"
3	118. 32'46"	24. 25'37"
4	118. 30'34"	24. 21'49"
5	118. 27'52"	24. 19'20"
6	118. 23'12"	24. 20'29"
7	118. 19'11"	24. 17'39"
8	118. 16'34"	24. 18'24"
9	118. 13'30"	24. 18'44"
10	118. 09'19"	24. 21'37"
11	118. 07'54"	24. 22'56"
12	118. 08'49"	24. 24'36"
13	118. 11'49"	24. 26'15"
13"	118. 12'22"	24. 27'08"
14	118. 13'54"	24. 28'41"
15	118. 16'31"	24. 30'19"
16	118. 19'51"	24. 30'32"
17	118. 23'04"	24. 31'55"
18	118. 24'19"	24. 32'34"
19	118. 26'58"	24. 31'43"
20	118. 27'41"	24. 31'06"

A graphic depicting the “restricted waters (限制水域)” (red lines) and “prohibited waters (禁止水域)” (pink lines) around the Kinmen Islands Group, as declared by Taiwan’s government. The shaded yellow area depicts a “buffer (緩衝)” zone of 1,000 meters (south/east) and 300 meters (north/west) outside these zones. The approximate area of the February 14 incident near Bei-ding Island is depicted in the dotted blue lines, on the eastern side of the map (author’s annotation). (Source: Kinmen County Harbor Bureau)

PRC Actions Following the Incident

PRC government reaction was predictable in the aftermath of the incident. PRC agencies and spokespeople sought to leverage the incident to further denigrate Taiwan’s sovereignty and to deny it any legitimate right of administration over its offshore islands. The PRC Coast Guard—which has fallen under military, rather than civilian, jurisdiction since 2018—has stepped up its presence and patrols in the area in the wake of the incident (Nikkei Asia, March 22, 2018).

In an apparent tit-for-tat intended to assert the PRC’s jurisdictional claims over Taiwan-administered waters, on February 19 two PRC Coast Guard vessels surrounded a Taiwanese tourist boat near Kinmen and boarded the vessel, demanding to inspect the ship’s documents and identity documents of the passengers (VOA, February 19). Various reports from late February indicated that five PRC Coast Guard ships had assumed patrols around Kinmen and that these vessels entered Taiwan-administered waters on or about February 26. On these occasions, confrontational actions were not reported and the vessels reportedly withdrew from Taiwan’s sea space when directed to do so by the ROC Coast Guard (Maritime Executive, February 27).

The PRC Coast Guard has also stepped up its presence and actions around the island of Matsu (媽祖島). Not all such actions are necessarily hostile. For example, in mid-March Taiwan press reported on incidents

near both Kinmen and Matsu involving cooperative search-and-rescue operations for missing fishermen conducted by coast guard vessels from both sides (Taipei Times, March 15, March 16). However, such cooperation is not representative of the PRC's broader approach to Taiwan's maritime claims, as the PRC denies Taiwan any rights to sovereignty or administration over these territories.

PRC Narrative Framing Following the Incident

Both the PRC's actions and its heated rhetoric have served to further raise tensions in the Taiwan Strait. In the wake of the February 14 incident, three major narrative themes have emerged from PRC government outlets.

The Normalization of Greater PRC Presence

In a brief statement issued four days after the incident, the PRC Coast Guard announced that coast guard units based in Fujian Province would initiate "normalized enforcement patrol operations (常態化執法巡查行動)" in the "Xiamen-Jinmen sea area (厦金海域)." The statement claimed that this would "advance the safeguarding of maritime-related work and operations, [and] protect the security of fishermen's livelihoods and property" (PRC Coast Guard, February 18). PRC press has referred to these as "law enforcement patrols and inspections" in the Kinmen area, conducted to "safeguard the legitimate rights and safety of life and property for Chinese fishermen, including those from Taiwan region" (Global Times, March 17). **[1]** This is consistent with an ongoing PRC effort to "normalize (常態化)" its military presence, in multiple domains, encroaching ever-further into Taiwan's maritime periphery.

Taiwan's Malicious Actions—and the Culpability of Taiwan's DPP-Led Government

The PRC government has accused the Taiwan authorities of active malice in the February incident, consistently referring to the matter as the "2-14 Vicious Boat Collision Incident (2.14 惡性撞船事件)" (China News, February 27). One of the clearest examples of such messaging was presented on March 13 by PRC Taiwan Affairs Office spokesman Chen Binhua (陳斌華), who accused—without providing any specifics or evidence—Taiwan's Democratic Progressive Party (DPP)-led government of covering up details of the incident. Chen spoke of "the Taiwan side's rough treatment toward mainland fishermen, resulting in the fishing boat capsizing," and declared that Taiwan's authorities "are the real 'three no's': no compassion, no justice, no reason (無情, 無義, 無理)." Chen hinted at retaliatory measures by the PRC, but stated that, before proceeding with further actions, "we must see what sort of attitude the DPP authorities take in dealing with the incident, [and] what sort of explanation they give to the victims' families and cross-Strait compatriots" (Xinhua, March 13). This language is largely consistent with narratives from the CCP propaganda system that preceded the incident. For instance, on January 31 a state media editorial attacked Taiwan's government for its "impenitent stance on making provocations to pursue independence and stoking up confrontation across the Strait" (Xinhua, January 31).

PRC Taiwan Affairs Office spokesman Chen Binhua (陈斌华) speaking at a March 13 press conference. He accused Taiwan's government of maliciously provoking the February 14 incident near Kinmen and asserted that both Taiwan and the Taiwan Strait represent sovereign PRC territory. (Source: Xinhua, March 13)

Denying Taiwan's Sovereignty and the International Status of the Taiwan Strait

Beijing has also predictably taken the opportunity to leverage the events around the Kinmen Islands to deny any legitimate independent existence for Taiwan once again. It has also used the incident to assert PRC sovereignty over the area—not only over Taiwan itself, but also over the entirety of the Taiwan Strait. Chen Binhua's March 13 statement asserted that "both sides of the Taiwan Straits are China's territory, China enjoys sovereignty, sovereign rights, and jurisdictional rights over the Taiwan Strait (海峡两岸都是中国的领土，中国对台湾海峡享有主权、主权权利和管辖权)." Chen accordingly denied any international status for the sea space of the strait, asserting that "the waters of the Taiwan Strait are divided into China's internal waters, territorial waters, contiguous zone, and exclusive economic zone. So-called 'international waters' do not exist (台湾海峡水域分别为中国内水、领海、毗连区和专属经济区，不存在所谓的"国际水域")" (Xinhua, March 13). This is consistent with a narrative pushed by Beijing since at least summer 2022, which muddles together all generally recognized delineations of maritime space into a de facto single category over which the PRC claims sovereignty and administrative rights tantamount to territorial waters. **[2]**

Conclusion

Some aspects of the February 14 incident near Kinmen Island remain unclear. Whether or not the unidentified vessel was actually a fishing boat, or whether it was instead engaged in other activities, is not known. Similarly, there has been no announcement concerning the exact cause of the small craft's fatal capsizing. However, it appears that the PRC has seized upon the opportunity presented by this incident—one of a constant series of minor incidents prompted by the efforts of Taiwan's coast guard to exercise maritime enforcement rights overfishing and other activities near Taiwan's outlying islands—to provoke an "opportunistic crisis." Such minor crises provide pretexts for the PRC to further advance and "normalize" its gradual encroachments into Taiwan's territorial space. This is similar to the fashion in which the PRC used the August 2022 visit to Taiwan by then-US Speaker of the House Nancy Pelosi as a pretext to ramp up coercive military activity around Taiwan (Global Taiwan Brief, August 24, 2022). Opportunistic crises also provide the CCP propaganda system with a more prominent position from which to assert its narratives about Taiwan—particularly, denying Taiwan's legitimacy and asserting PRC sovereignty—and to further normalize such messages by repetition.

The February 14 incident, and its immediate aftermath, are unlikely to produce a larger crisis. There are subtle indications that the PRC is likely seeking to manage the escalation of these incidents for example, the reportedly cooperative coast guard search-and-rescue efforts near Matsu, or the statements that the PRC will further monitor DPP actions before deciding upon further responses. Such actions could actually represent subtle signals of short-term de-escalation. However, we should expect the PRC's "law enforcement" gray zone actions to continue in tandem with more overt acts of military intimidation as a component of its ongoing psychological warfare directed against Taiwan's population, and its efforts to claim sovereignty over Taiwan and the international waters surrounding it.

John Dotson is the deputy director of the Global Taiwan Institute in Washington, D.C. He was a previous Editor of The Jamestown Foundation's China Brief.

Notes

[1] This follows a consistent pattern observed in recent years in which Beijing has either eroded or outright broken pre-existing norms that offered limited de facto, if not de jure, regard for Taiwan's territorial space—such as observing the Taiwan Strait centerline for military aviation flights, or Taiwan's declared Air Defense Identification Zone (ADIZ). See: Thomas Shattuck, "The PLA Air Force Erases the Taiwan Strait Centerline," *Global Taiwan Brief* (September 7, 2022). https://globaltaiwan.org/2022/09/the-pla-air-force-erases-the-taiwan-strait-centerline/.

[2] For a fuller discussion of this point, see: John Dotson, "Beijing Ramps Up Its Rhetoric over Taiwan and Maritime Sovereignty," *Global Taiwan Brief* (June 29, 2022). https://globaltaiwan.org/2022/06/beijing-ramps-up-its-rhetoric-over-taiwan-and-maritime-sovereignty/.

Deepfakes with Chinese Characteristics: PRC Influence Operations in 2024

by Sze-Fung Lee

Tencent Cloud's product "Digital Intelligence Human," based on the new generation of multimodal human-computer interaction technology, covering industries such as anchors and customer service. (Source: HKSilicon)

Executive Summary:

- The PRC's potential to interfere in elections with deepfakes has been noted, with strategies including creating false narratives around candidates and misleading information on electoral processes. Advanced AI tools could further sophisticate these interference efforts, impacting democratic processes worldwide.
- Beijing appears to have a dual stance on deepfakes—strict regulation domestically due to potential socio-economic and security threats, coupled with an ambition to leverage them for international influence operations.
- Beijing is likely to integrate deepfakes with AI to conduct smear campaigns against critics, amplify PRC propaganda by creating fake personae, and interfere in elections, exacerbating the spread of disinformation.

On March 27, PRC social media platform Douyin announced a ban on the use of artificial intelligence generated content (AIGC) to create and post content that "goes against science, fabricates information, or spreads rumors" (Douyin, March 27). This latest development offers a glimpse into how Beijing perceives deepfakes. As one of the first countries in the world that implement thorough regulations on deepfakes, the PRC sees them as a threat, wary of their being leveraged to disrupt socio-economic stability and threaten national security. However, Beijing appears to be torn between these concerns and its ambition to utilize deepfake technology for influence operations overseas.

The Cyberspace Administration of China (CAC; 国家互联网信息办公室) released regulations on network audio and video information services (网络音视频信息服务管理规定) in November 2019. At the time, officials noted that deepfakes magnify the risk for the dissemination and amplification of "illegal and harmful information" and may be exploited to endanger national security and disrupt social stability and order (China News Service, November 30, 2019). A paper published by the PRC's Journal of International Security Studies in 2022 titled "Deepfakes and National Security: Perspectives Based on the Overall National Security Concept" offered some insights into the fears (Liu, March 31, 2022). These ranged from impersonating government officials for cyber fraud to manipulating the stock market to fabricating false emergencies. Such uses of deepfakes drove the initiative to pre-emptively "drawing the redlines in advance (提前划红线)," and implement these "*ex ante* regulations (事前规制)" (Xinhua, March 19, 2021). In parallel with these concerns is the alacrity with which Beijing leverages deepfakes for influence operations. Recently, attempts were made to reduce public support for the Democratic Progressive Party (DPP) with altered video footage during Taiwan's election.

The challenges posed by emerging technologies when it comes to projecting trends on how the PRC could weaponize deepfakes to amplify their influence operations are understudied. An analysis of current trends, disinformation patterns, and case studies suggests three specific ways Beijing is likely to integrate past strategies with artificial intelligence (AI) in attempts to reinforce transnational repression, influence public opinion, and conduct electoral interference in liberal democracies. First, the PRC could leverage deepfakes to manifest smear campaigns. Second, AIGC could be used to strengthen PRC propaganda narrative, leveraging deepfake personas—from witnesses to news anchors—to support and disseminate its preferred narratives to influence public perception. Third, Beijing is likely to integrate higher quality and a higher quantity of deepfakes to conduct electoral interference worldwide.

Smear Campaigns: The '50 Cent Army' and Spamouflage [1]

Creating accusations out of thin air has long been a strategy for PRC influence operations aiming to defame politicians, regime critics, and human rights activists. For instance, Taiwan President Tsai Ing-wen has been accused of "academic fraud," suggesting that her Ph.D. in law from LSE is fake; former US House Speaker Nancy Pelosi has been called a "wicked witch (妖婆子)"; and Hong Kong democracy activists have been portrayed as rioters (Global Times, September 10, 2021; Huanqiu, April 22, 2020; WaPo, June 8, 2023).

PRC smear campaigns often involve sexual assault and misconduct allegations. Previously, posts were often accompanied by memes or poorly edited photos (The Guardian, February 9, 2023). Deepfakes, however, allow accusations to be supported by persuasive "evidence," disseminated and amplified in large-scale influence operations. This can occur via nationalist trolls such as the "50 Cents Army (五毛党)," the "little pink (小粉红)" cybernationalists, and state-controlled cross-platform political spam networks such as Spamouflage. Given the difficulty of debunking fake news in real-time and the acute virality of negative content, reputational damage and psychological harm to the targeted individual is most likely done before any countermeasures can be deployed (MIT News, March 8, 2018). **[2] [3]**

Beijing has tended to harass women of Asian descent who have "public platforms, opinions, and expertise on China" (ASPI, June 3, 2022). Statistics indicate that women accounted for the targets of 99 percent of deepfake pornography in 2023 (Home Security Heroes, 2023). A recent example involved deepfakes of the artist Taylor Swift appearing on Twitter/ X. However, she is almost uniquely positioned to mobilize actions such as hashjacking (flooding the original hashtag with positive messages and drown out the original image in X's search function) to protect her from such defamation campaigns (NBC, January 27). The PRC could easily create and amplify harmful deepfakes to discredit and silence its opposition, particularly its female opposition, with little recourse for the victims.

To state the obvious, the US Department of Justice's latest indictment on seven hackers affiliated with the PRC Ministry of State Security revealed how their operations could target numerous government and political officials worldwide via sending "thousands of malicious tracking email messages to personal and professional email accounts" in attempts to gain personal information of the receipts such as their location data and contacts since at least 2015 (DOJ, March 25). While the incident demonstrated Beijing's evolving capabilities to target its adversaries, these cyberattack tactics will likely intertwine with deepfakes technologies for a more far-reaching dissemination during its influence operations.

Under the PRC's established legal framework, dissemination and amplification of deepfakes is strictly restricted. However, those regulations do not appear to apply to operations conducted by the PRC-affiliated entities. According to Article 3 of the Regulations on the Management of Online Deep Synthesis Image Services (互联网信息服务深度合成管理规定) enacted in January 2023, despite the CAC is responsible for coordinating and managing the nation's comprehensive synthesis services, the Ministry of Public Safety (MPS) will also manage these services according to its "respective responsibilities" (Government of the People's Republic of China, November 25, 2022).

And Spamouflage campaigns are directly linked to Beijing's MPS. In other words, the PRC could produce deepfakes and amplify them via the cross-platform spam network as they see fit.

Additionally, Spamouflage's tactics are also constantly evolving. Methods include innovations in AIGC and manipulated media, links to fake news sites, hashjacking, and directly replying to targets' posts. Despite efforts from social media platforms such as Meta (which removed thousands of fake Facebook accounts as a

part of its investigation from 2022 to 2023) and US authorities (which have pressed charges on PRC police officers operating the troll farm that attacked Chinese dissidents and disseminated propaganda) (Meta, February 14; DOJ, April 17, 2023), such tactics have enabled them to slowly garner more real-life user engagement (Graphika, February 2023).

These campaigns often have achieved sizeable impact. In many cases, such as the targeting of Hong Kong protestors during the 2019 pro-democracy movement, the enforcement of transnational repression within the Chinese diaspora, and the harassment of Canadian MPs, there has been little pushback (Graphika, September 2019; Bloomberg, December 15, 2023; Government of Canada, October 23, 2023). While there are some current weaknesses over specific language used, images, and issues of cultural sensitivity, these could be eliminated through the use of better AIGC. Some improvements are already apparent: Tweets are becoming more fluent in multiple languages, avatars posing as real-life users are more lifelike, and with the right timing and dissemination methods deepfakes could sow division in target societies. Interference in elections worldwide will undermine the core structures of liberal democracies.

Deepfakes for "Telling China's Story Well"

In 2013, Xi Jinping began to emphasize that the PRC's international communications must "tell China's story well (讲好中国故事)" (Xinhua, August 21, 2013). The goal of this external propaganda strategy is to enhance China's "international discourse power (国际话语权)" (Xinhua, June 1, 2021). In past influence operations, PRC state media, gray media,**[4]** and private actors have worked together to amplify Beijing's preferred narrative. One example is the "happy Uyghurs" meme—videos featuring an airbrushed version of Uyghurs' lives, focusing on traditional dances and innocuous cultural phenomena, giving the false impression that Uyghurs are living "happy lives," and ignoring the hardship and persecution many face (X/@XinjiangChannel, May 13, 2021; X/@D[iscover]Xinjiang, February 1).

Specifically, article 4 of the Regulations on the Management of Online Deep Synthesis Images noted that the provision of comprehensive synthesis services shall "adhere to the correct political orientation, public opinion orientation, and value orientation" and "promote deep synthesis services to be positive and upward" (Government of the People's Republic of China, November 25, 2022). The use of deepfakes to "tell China's story well" conceivably falls into the category of "correct" political and public opinion.

AIGC could easily help Beijing create large quantities of propaganda portraying how "peaceful" Xinjiang is while "debunking" Western countries' allegations about extensive human rights violations. For instance, PRC state media outlet the Global Times published an "investigation of 30,000 Xinjiang-related stories exposing how certain Western media fabricate, hype up 'forced labor' smear" (Global Times, October 15, 2023). Beijing's media, which does not observe the West's journalistic standards, could fabricate testimonies to lend a veneer of authenticity to their narrative. This is not where the greatest potential lies, however.

The real threat of deepfakes for influence operations is beyond the mainland, in Hong Kong. Deepfakes could fabricate scenes of peace and harmony, portraying the city in a positive light. Instead of foregrounding

"riots" and the aftermath of the national security law and now Article 23, Hong Kong could be perceived as "advancing to prosperity (由治及興)," as the city's Chief Executive John Lee claimed (WenWeiPo, October 25, 2023). Hong Kong authorities have less control of the information ecosystem than in the PRC proper, so leveraging deepfakes to depict "happy Hongkongers" to "tell the Hong Kong story well" would be more cost-effective than getting dozens of local interviews and filming shots equivalent to Uyghurs dancing in the streets.

Beijing's influence operations frequently use first-person accounts to "tell the story." **[5]** Cases include fake news about the Kansai Evacuation in 2018 **[6]** and the instance of a Chinese blogger who pretended to be in Israel during the early days of the Israel-Palestine conflict. Both of these emphasized the PRC's effective protection of overseas citizens, something which did not accurately reflect realities on the ground (Taipei Times, September 9, 2023; CDT, October 17, 2023; 404 Beifen, October 17, 2023). Such disinformation could be amplified via deepfake technology to influence public perception of China.

In the past year, Beijing has unveiled deepfake news anchors and websites posing as local news outlets have spread disinformation and *ad hominem* attacks worldwide (Graphika, February 2023; Citizen Lab, February 7). AI-generated witnesses, anchors, and news sites could conceivably merge into one formidable influence operation.

The aim of deepfake content is not to convince everyone exposed to it that the disinformation is true. Rather, the goal is simply to create an alternative narrative for the international audience, and especially for those who have no prior contextual knowledge and for whom repeated exposure through saturating the information space could increase their receptivity. At the very least, malign state actors could sow confusion or erode trust in more accurate narratives.

Leveraging deepfakes to falsify the testimonies of political prisoners constitutes one logical future use case. Televised forced confessions could be reimagined by creating videos of prominent activists (since public figures would likely have enough visual data to train the algorithms) confessing to conspiracy theories or falsely depicting them in good health (as opposed to suffering from torture).

Deepfakes for Electoral Interference

2024 is an unprecedented year in the number of national elections. Beijing thus has numerous opportunities to experiment with and conduct electoral interference (ODNI, March 11). Previous operations have not made a measurable impact, but the potential ramifications of AIGC, especially given the enormous advances in the last eighteen months, indicate a new toolkit (Misinformation Review, October 18, 2023). Beijing's suspected interference in Taiwan's presidential and legislative elections exemplifies its strategies (see China Brief, February 16).

Deepfake content was rampant in the disinformation campaign targeting Democratic Progressive Party (DPP) presidential candidate Lai Ching-Te (賴清德). Altered video footage with Lai's synthesized voice

portrayed him as supporting a coalition between the Kuomintang (KMT) and Taiwan People's Party (TPP) and falsely depicted him commenting on DPP scandals (Taiwan FactCheck Center, December 29, 2023; Taiwan FactCheck Center, November, 2023). While cross-platform posting is a common phenomenon in influence operations, Beijing's ability to manipulate the information environment, especially on PRC-based social, evolves as the data it collects increases—fueling its ability to curate disinformation to target users with specific value-orientations. Based on current trends, two key manifestations of deepfake technology in the near future include content to mislead on electoral laws and regulations, and content inciting chaos.

In early January, there was a widely circulated disinformation campaign on social media platforms that falsely stated, "Taiwan's Central Election prohibits the circulation of political propaganda ten days prior to the election" (Taiwan FactCheck Center, January 4). **[7]** This narrative blends half-truths (real legal references) and half-lies (laws do prohibit the dissemination of poll data close to election day but not general political discussion, and only on election day does the Taiwan law prohibit electioneering) (MyGoPen, January 3). **[8]** It thus exploits the general public's unfamiliarity with the nuances of election laws. It also leverages the psychological insight that people who recognize part of the information conveyed as true are more inclined to accept additional false claims—in this case, discouraging political discussion in the most decisive part of the election cycle (RAND, July 11, 2016). Integrating this tactic with deepfake videos of politicians or reputable experts would further spread confusion and suppress political discourse. The tactic has already been used in the United States, though by a US-based individual. A fake robocall—deepfake audio of President Joe Biden urging voters to skip the primary election in New Hampshire—could be a sign of what to expect later this year (Taiwan FactCheck Center, January 5; Bloomberg, January 22; BBC, January 22; DOJ.NH, February 6).

Deepfake videos depicting chaotic scenes may amplify rumors. The PRC used such tactics during the Taiwan election. On election day, a disinformation campaign alleged the existence of "multiple stabbing incidents across various polling stations" in Tainan, the southern part of the island (Taiwan FactCheck Center, January 13). The rumor was accompanied by an edited photo featuring a victim covered in blood to "prove" its authenticity. The photo originated from PRC-affiliated media *Haixia Net (海峡网),* which is owned by *Fujian Daily Newspaper Press Group (福建日报报业集团*) and controlled by the Fujian Provincial Committee of the Communist Party of China (中国共产党福建省委员会). Beijing could have used the power of deepfakes to craft even more compelling videos to incite chaos and dissuade voters from participating in the democratic process. Text-to-video technology, which could conceivably turn manually typed prompts into powerful weapons of information warfare, already exist. Sora, a recent tool developed by Open AI (although not yet publicly available), is one such tool. In the hands of malign actors, such powerful tools could wreak havoc on electoral processes.

Conclusion

The PRC has already used an array of tactics to create and spread disinformation as part of influence operations to affect democratic elections and undermine liberal democracies. Some of the most advanced deepfake technology currently originates in the country. There is a clear and obvious potential for deepfake technology to be deployed and intertwined with older techniques to maximize their impact. From weaponizing

deepfakes for smear campaigns, and electoral interference to fabricating testimonies for manipulating global narratives, it is only a matter of time until Beijing figures out the best way to integrate these new and evolving tools into its influence operation playbook.

Sze-Fung Lee is an independent researcher specializing in Chinese hybrid warfare, including Foreign Information Manipulation and Interference (FIMI), Grand Strategy, Nuclear Proliferation, Gray Zone Tactics, and Cognitive Warfare. Zir research also focuses on Indo-Pacific security policy, challenges posed by emerging technologies, and the politics of Hong Kong.

Find ze on X (formerly Twitter) @imleeszefung

Notes

[1] Spamouflage is a cross-platform political spam network that hijacked or faked accounts on social media platform to amplify PRC narratives while disguising the spam messages as legitimate. The campaign has been attributed to the PRC Ministry of Public Security (MPS). It was first exposed by social media analytics business Graphika, of which the campaign was used on the Hong Kong protesters during the pro-democracy movement in 2019.

For more details, see Nimmo, B., Shawn Eib, C. and Tamora, L. (2019). 'Cross-Platform Spam Network Targeted Hong Kong Protest'. Graphika. Available at: https://graphika.com/reports/spamouflage

Martin, A. (2023). "Chinese law enforcement linked to largest covert influence operation ever discovered." The Record. Available at: https://therecord.media/spamouflage-china-accused-largest-covert-influence-operation-meta

[2] Schöne JP, Garcia D, Parkinson B, Goldenberg A. Negative expressions are shared more on Twitter for public figures than for ordinary users. PNAS Nexus. 2023 Jul 6;2(7):pgad219. doi: 10.1093/pnasnexus/pgad219. PMID: 37457891; PMCID: PMC10338895.

[3] Rainer Greifeneder et al., eds. *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation.* Routledge, 2020

[4] Gray media are pro-nationalistic media outlets that have alleged ties with the PRC state entities, such as being financed by China-linked corporations, acknowledged by PRC officials for their work and/ or having members that hold positions in the CCP or other government bodies.

[5]洪浩唐. *戰狼來了: 關西機場事件的假新聞、資訊戰.*. 新自然主義, 2021

[6] In the 2018 Kansai Evacuation incident, fake news circulated online claiming that the PRC embassy helped evacuate its citizens from Kansai Airport after a Typhoon while defaming the Taiwan administration's "inaction."

[7] Also data scraped by the author during the election period.

[8] According to the "Presidential and Vice-Presidential Election and Recall Act" and the "Public Officials Election and Recall Act," it is prohibited to publish, report, distribute, comment on, or quote any polling data within the ten days leading up to an election. However, these laws do not restrict individuals from discussing their political preferences or supporting a particular party or candidate, which the disinformation falsely claims. https://www.mygopen.com/2024/01/500k.html

The PRC's Continued Outsized Role in the Cryptocurrency Industry

by Matthew Fulco

Drones fly overhead, carrying small digital billboards advertising the latest crypto exchange platforms in China. (Source: AI-generated)

Executive Summary:

- Despite the Chinese Communist Party's restrictions on decentralized virtual currencies, the PRC has maintained a significant underground cryptocurrency industry, with investors posting $1.15 billion in gains in 2023.
- PRC investors are driven to digital assets by practical considerations amid limited traditional investment opportunities and a weakening economy. The ease of bypassing restrictions, such as using VPNs and financial tech platforms for transactions, has facilitated continued investment in cryptocurrencies by retail investors.
- While the PRC has imposed restrictions to preserve financial stability and address environmental concerns, the decentralized nature of cryptocurrencies challenges comprehensive enforcement. However, an increase in cryptocurrency-related crime could prompt more stringent measures from Beijing.
- Cryptocurrency transactions are not illegal in the PRC. However, a rise in digital asset crimes, including money laundering and scams, poses potential risks that could lead to further regulatory actions to combat illicit activities in the burgeoning sector.

The People's Republic of China (PRC) has developed a thriving underground cryptocurrency industry. This has occurred despite the Chinese Communist Party (CCP) restricting many activities involving decentralized virtual currencies. In 2023, investors in the PRC posted significant crypto investment gains totaling $1.15 billion. This puts them at fourth in the world after their counterparts in the United States, United Kingdom, and Vietnam (SCMP, March 17). While this figure was a significant decrease from the $5 billion that PRC investors made from digital assets in 2021 (the previous iteration of this survey), the numbers are consistent with broader fluctuations in the mercurial crypto market.

Data compiled by blockchain research firm Chainalysis show that the PRC's crypto market recorded an estimated $86.4 billion in raw transaction volume between July 2022 and June 2023. Within this figure, the proportion of large retail transactions (defined as those within the range $10,000-$1 million) is 3.6 percent—nearly twice the global average (MoneyDJ, January 26).

PRC retail investors have flocked to digital assets for practical reasons rather than out of an underlying affinity for the concept of decentralized digital currencies. Traditional investment opportunities in the country have worsened significantly amid a weak economy (Coinlive, January 25), while Beijing's restrictions can be overcome with relative ease—by using a VPN to access crypto websites or apps banned in the PRC, for instance. Additionally, crypto exchanges like OKX and Binance still offer trading services for PRC-based investors and guide them to use fintech platforms such as Ant Group's Alipay and Tencent's WeChat Pay to convert renminbi (RMB) into stablecoins with dealers, so that they can trade cryptocurrencies.

Bans such as those that the PRC government has tried to impose were never likely to work. According to Caroline Malcom, head of public policy at Chainalysis, this is because of "the decentralized nature of cryptocurrencies and the fact that they can be transferred end-to-end and traded on global exchanges makes it difficult for any government to completely eliminate them" (Blockcast.it, May 9, 2023).

However, there is a risk that Beijing's restrictions on the crypto market may become more draconian if it perceives a marked threat to financial stability. The recent uptick in PRC-linked cryptocurrency crime might prompt such a crackdown.

Crackdowns Have Not Precluded New Risks

Previous cryptocurrency crackdowns in the PRC have occurred amid broader turbulence in the global market for digital assets. In 2017, Beijing banned initial coin offerings (ICOs)—a means of fundraising for early-stage crypto projects—amid a global surge in related fraudulent activity. Such fraud at the time was severe. A study published by ICO advisory firm Statis Group in mid-2018 found that more than 80 percent of ICOs that occurred in 2017 were identified as scams (CoinTelegraph, July 13, 2018).

The tough restrictions imposed in 2021 had a different focus. Curbs on domestic exchanges and trading sought to preserve systemic financial stability while a bull market raged. At the same time, Beijing cracked down on crypto mining in part because of the strain it puts on the electrical grid as well as heavy carbon emissions, which could compromise the PRC's environmental goals. A directive issued by the National

Development and Reform Commission (NDRC) in September 2021 offers some insight into Beijing's related thinking about mining. The document called for the "orderly exit of existing mining projects," which it said would "promote the optimization of industrial structure, and help achieve carbon peak and carbon neutrality goals as scheduled" (NDRC, September 3, 2021).

Since 2021, the PRC has not initiated a substantial new crackdown on digital assets. If anything, Beijing's attitude toward cryptocurrency could be interpreted as moderating slightly given its quiet acquiescence of Hong Kong's push to become a leading hub for digital assets. In January 2023, Huang Yiping, a former adviser to the People's Bank of China, said in a commentary that "banning cryptocurrencies may be practical in the short term, but whether it is sustainable in the long term deserves in-depth analysis," adding that long-term restrictions on digital assets could cause China to miss out on "opportunities for the development of some important digital technologies." (Sina.cn, January 29, 2023).

Crypto Seen as a Safe Investment

Demand for cryptocurrency in the PRC has risen because other investment opportunities are lacking. With uncertainty about the country's economic prospects growing, PRC investors are eager to invest offshore and some see Bitcoin as a safe haven like gold (TechNews.tw, January 26). Investment opportunities that were previously reliable are failing to deliver attractive returns. For instance, despite steady IPO activity, the PRC's stock exchanges in Shanghai, Shenzhen, and Beijing have all been struggling. In January, Shenzhen's ChiNext Composite Index fell 20 percent, while the Shanghai Composite Index hit its lowest point since 2018 (VOA Chinese, February 9). Furthermore, the blue-chip CSI Index fell 35 percent in the 36 months to December 2023. According to Morgan Stanley, earnings at listed companies are likely to miss forecasts for a tenth straight quarter, pushing down valuations (Bloomberg, January 24). Though Beijing is reportedly preparing to inject about RMB 2 trillion into the market in an effort to stabilize the situation, that may not be enough to lift investor sentiment. The property market has also been experiencing a slump. Once seen as a safe asset that would appreciate significantly, especially in the PRC's first tier cities, that is no longer the case. Consequently, property investment declined about 9.6 percent in both 2023 and 2022 (Reuters, January 16).

In contrast, the crypto bear market that characterized 2022 and most of last year has ended, with major cryptocurrencies surging in value over the past six months. As of March 27, Bitcoin has jumped 160 percent to $68,509 while Ethereum has risen 118 percent to $3,477.

Meanwhile, Hong Kong, the traditional offshore financial center for the PRC, is vying to become a cryptocurrency hub just as investor interest in the mainland is surging (Lexology, November 13, 2023). It is unclear to what extent, if any, Beijing intends to use the city as a testing ground for an eventual relaxation of restriction on digital assets in the mainland, but mainland investors will naturally be a big focus for Hong Kong in the crypto sector, just as they are in other segments of the financial services industry.

Restricted But Not Illegal

The PRC has imposed many restrictions on cryptocurrency transactions but they are not illegal in the country. Instead, plucky retail investors operate in a gray area. A Fujian Province court explained this issue in an analysis published in September 2023:

> *"Virtual currency transactions that do not involve illegal financial activities are not administratively illegal. Although the civil act of buying and selling virtual currency can be deemed invalid because it harms the country's financial order, the virtual currency itself is not an illegal item," the court said, adding that based on various Supreme People's Court civil judgements since 2022, "under the current legal policy framework, virtual currencies held by relevant entities in China are still legal property and are protected by law*" (Sina.cn, September 1, 2023).

The Xiamen City court further explained how the PRC sees decentralized digital currencies, emphasizing that it has not recognized them as legal tender or allowed them to be used for payments due to "considerations such as protecting the renminbi's status as legal tender and combating crime." However, the exchange value of cryptocurrencies "objectively exists due to legal recognition and legal circulation in overseas markets and cannot be eliminated." (Sina.cn, September 1, 2023).

Binance, the world's largest cryptocurrency exchange in terms of daily trading volume, provides an additional perspective on Beijing's digital asset policies. In a June 2023 Chinese-language post on its official website, Binance notes that Beijing in 2013 prohibited financial institutions from conducting Bitcoin-related business and ordered them not to circulate the mercurial digital asset as currency. Then in 2017, it banned ICOs and in 2021 enacted its toughest crypto controls to date, shutting down domestic exchanges, banning trading by residents, and restricting mining (the process by which cryptocurrency is created). "The purpose of these regulatory measures is to maintain financial order, prevent financial risks and protect the interests of investors," Binance said (Binance.com, June 25, 2023). If cryptocurrency and its technology are not illegal in the PRC, related transactions and business activities are nevertheless "subject to strict regulatory restrictions." With that in mind, PRC citizens and companies "should abide by relevant laws and regulatory policies" to avoid landing themselves in trouble with the authorities, Binance said (Binance.com, June 25, 2023).

New Risks

Crime involving digital assets appears to be on the rise. In February, the Supreme People's Procuratorate (SPP) cited a jump in cybercrime involving blockchain, the paramount technology underlying cryptocurrency. Ge Xiaoyan (葛晓燕), Deputy Prosecutor-General of the SPP, said that from January to November 2023, the Procuratorate pressed charges against 280,000 individuals in cybercrime cases, an annual increase of 36 percent. Additionally, Zhang Xiaojin (张晓津), the director of the Fourth Procuratorate of the SPP, warned of investment scams involving cryptocurrency (Supreme People's Procuratorate, February 23). This

is despite the global cryptocurrency market seeming to have recovered from the bearish sentiment that characterized 2022–2023.

While the alleged criminal activity occurred between 2014 and 2017, an overseas Chinese woman residing in the United Kingdom, Wen Jian (雯簡), was recently implicated in a $6.3 billion fraud case in which Bitcoin was converted into cash and property to conceal the cryptocurrency's origins. Though Wen was not involved in the underlying scam, which allegedly defrauded 130,000 Chinese investors, a London court on March 20 found her guilty of one count of money laundering. Prosecutors say the scheme's mastermind is a Chinese woman named Qian Zhimin, who uses the alias of Zhang Yadi (張雅迪) (HK01, March 21).

Meanwhile, Chinese gangs are reportedly using cryptocurrency to launder profits from drug dealing – fentanyl in particular – and illicit gambling and often have been able to evade authorities thanks to the decentralized nature of digital assets. In October 2023, the U.S. Department of the Treasury's Office of Foreign Assets Control sanctioned a network of individuals and firms based in China that were involved in the production and distribution of fentanyl and ingredients used in other drugs. Some of them used cryptocurrency wallets to send and receive funds. For their part, Chinese police said in January that they had investigated more than 800 cases of suspected cryptocurrency crime, shut down five underground banks involved in processing payments, and discovered about $4 billion in funds based on blockchain data (RFI, February 3, 2024).

The scale of this uptick in crime involving digital assets means that Beijing is likely to respond with more than just police investigations. Money laundering related to the use of digital assets is currently the "most urgent and most necessary" issue for the PRC to tackle at a legal level, Yan Lixin, executive director at the China Center for Anti-Money-Laundering Studies at Fudan University in Shanghai (The South China Morning Post, February 15). The question is whether measures will involve further restrictions on digital assets in the mainland.

Conclusion

Cryptocurrency is becoming an increasingly popular choice for retail investors in the PRC amid a prolonged economic slowdown and a loss of confidence in traditional investments like the stock market and residential property. Despite significant restrictions on certain related activities, holding cryptocurrency is not banned in China, and investing in it is not illegal—an important distinction that is often overlooked when Beijing's so-called "crypto ban" is discussed.

That said, rising cryptocurrency crime involving Chinese citizens poses a threat to social stability and could prompt a third major crackdown on digital assets in the PRC if it continues unabated. For now, Beijing is moving to address gaps in its Anti-Money Laundering Law to better tackle illicit crypto flows. The current law dates to 2006, well before cryptocurrency existed. The revised law, which does not yet have an expected passage date, should provide additional insight into whether a third crypto crackdown is likely (NPC Observer, accessed March 26).

Matthew Fulco is a journalist and geopolitical analyst who worked in Taipei from 2014-2022 and Shanghai from 2009-2014, and is now based in the United States. He is a regular contributor to The Japan Times, The Economist Intelligence Unit and AmCham Taiwan's Taiwan Business Topics magazine.