Taiwan: A battlefield for cyberwar and disinformation

The complicated relationship between Taiwan and China is the most sensitive security issue in the Asia Pacific. The People's Republic of China (China hereafter) claims that Taiwan is a renegade province of China which needs to be reunified, while most people in Taiwan see it as an independent democratic country.

In recent years, China has increased its military pressure against Taiwan. A large-scale joint military exercise was held in 2022 with ballistic missiles fired over Taiwan. There was also a drastic increase in China's fighter jets and naval patrols intruding Taiwan's territory in 2022 with 1,737 flights tracked in Taiwan's Air Defence Identification Zone (ADIZ), which was a 79 percent increase over those tracked in 2021.

China has also been exerting increasing political pressure on Taiwan. The number of countries that recognise Taiwan as a nation has dropped from 22 in 2015 to 12 in 2024 with five nations ceasing diplomatic relations with Taiwan since 2019, including Solomon Islands (2019), Kiribati (2019), Nicaragua (2021), Honduras (2023) and Nauru (2024). Recognition is more than symbolism and it has had consequences for geo-strategic competition evident in China signing a security arrangement with Solomon Islands which allows China to deploy its military and armed police to the Islands. China also partnered with Kiribati to rebuild a runway on Kiribati's Kanton Island which could be used for military purposes. The pro-China groups in Taiwan, including the Kuomintang, manipulated and disseminated messages to make the public believe that the Democratic Progressive Party (DPP) government is incapable of maintaining its alliances and urged that formal dialogue between Taiwan and China needs to resume, despite China's insistence that they will only do this under the condition that Taiwan recognises that there is one China.

While it is unclear if or when China would launch a conventional war against Taiwan, we can see action being taken to cause conflict and fear within Taiwan and among Taiwanese which would help in the future if China were to launch a conventional war. But is it possible that China and Taiwan are already at war, albeit not a conventional one?

Sun Tze, in his 'The Art of War ' (孫子兵法), a Chinese military treatise dated

roughly 500 B.C., said that 'supreme excellence consists in breaking the enemy's resistance without fighting'. In his seminal early 1800s work, Carl von Clausewitz defined war as 'an act of force to compel our enemy to do our will' and 'as merely the continuation of [politik] by other means.' Based on this definition, war does not necessarily cause a serious number of deaths or physical damage; instead, it can be a coercive and deliberate act on an adversary, forcing it to follow their will. Much more recently, academics such as Mary Kaldor, argue that 'new wars' appear to be 'decentralised and fragmented' and emphasise the role that non-state actors can play in the new wars.

Cyberspace is providing a platform for new forms of war that might realise Sun Tze's ideal of winning a war without fighting. While some Clausewitzians might have different views on whether cyberwar can be real, the US Department of Defense's Strategy for Operating in Cyberspace identifies cyberspace as the fifth domain of warfare, not only because the Department relies heavily on cyberspace for its missions but also because disruption and exploitation of critical infrastructure and public opinion can cause societal instability. The Strategy emphasises the importance of strengthening capacity to protect this space. Similarly, the North Atlantic Treaty Organisation (NATO) recognises the importance of enhancing cyber defence capability.

Notwithstanding the great focus on cyber defence capability, we see that cybercrime, cyberattacks and disinformation campaigns are becoming dominant tactics that the Chinese government is using against Taiwan. While there is no universally agreed definition of cybercrime, it is usually understood to include conventional crime facilitated by computers and technology, such as identity and information theft, webpage defacement and dissemination of malicious and damaging messages and/or hate speech. Cybercrime can also be in the form of cyberattacks, such as Distributed Denial of Services (DDoS) and Advanced Persistent Threat (APT) attacks, which can weaken the power of the country targeted and cause physical damage by interrupting the functioning of critical infrastructure such as banking, energy, telecommunications and water systems. In Taiwan, cybercrimes are regulated by the Criminal Code and are usually dealt with by law enforcement agencies. Taiwan's President Tsai Ing-Wen declared 'cyber security is national security ' (資安即國安) in the 2018 National Information and Communication Security Strategic Report and emphasised it again in the 2022 report. The term cybercrime was mentioned in these reports, in relation to the targeting of important government agencies and personnel, and/or mass attacks on critical infrastructure.

However, some of the types of cybercrime listed above, and many more, can damage national security and thus be viewed as a form of cyberwarfare, especially if they are state-sponsored and organised. The line between cybercrime and cyberwar is becoming blurred as cybercrime can contribute not only to the preparation stage of cyberwar but be a critical part of it.

Taiwan tops cyberattacks in the region

Taiwan experiences a disproportionately high number of cyberattacks. Senior government officials, including the Secretary of the National Security Council, have publicly revealed Taiwan receives more than five million cyberattacks per day. Figures from Frontinet, a US-based cyber security firm, indicate that Taiwan is a hotspot for malicious actors, experiencing 55 percent of billions of malware attacks detected in the Asia-Pacific region in the first half of last year.

The visit to Taiwan by the then Speaker of the United States House of Representatives, Nancy Pelosi, on 2 August 2022 was particularly significant in terms of the number and nature of cyberattacks and disinformation campaigns. The Taiwanese Government stated there was a significant number of cyberattacks on public and private institutions and disinformation campaigns during her visit. They also described the disinformation created by the People's Liberation Army and disseminated by the Chinese media as 'cognitive war' or 'wars without gun smoke.' Her visit saw an increase in the number of Distributed Denial of Service attacks (DDoS), that is, sending a significant number of messages or requests to a website at the same time to flood the server to prevent users from accessing the site. Both central and local government websites were targets of DDoS and Audrey Tang, Minister of Taiwan's Ministry of Digital Affairs, reported that during Pelosi's visit, the recorded number of cyberattacks was 23 times more than usual. Centrally, the Office of the President, the Ministry of Foreign Affairs, and the Ministry of National Defense suffered multiple times during Pelosi's visit. For example, the Ministry of Foreign Affairs website received, within a single minute, more than 8.5 million site access requests, which is significantly over the site's capacity. Private organisations, including the Taipei Taoyuan International Airport and Taiwan Power, as well as education institutions, also recorded instances of DDoS. It is clear that these attacks were not only intended to interfere with communication between the government and its people but also to cause chaos more generally.

Website defacement was also observed during Pelosi's visit. Website defacement is a

type of cyber-enabled crime in which attackers hack into a website and replace the content with messages and/or images of their own. For example, an image of China's flag was placed on a page of the website of the Kaohsiung City Government Environmental Protection Bureau; and the words '世界只有一個中國' (There is only one China) were placed on some pages of the National Taiwan University's website.

Information screens at some train stations and convenience stores were targeted, with messages such as '老巫婆竄訪台灣，是對祖國的嚴重挑釁' (The old witch's visit to Taiwan is a serious provocation to the Chinese government) and '戰爭販子裴洛西滾出台灣' (Warmonger Pelosi, get out of Taiwan) posted. This showed that public information messaging services can be easily hacked and replaced with threatening messages that could cause fear and societal anxiety. These types of screens were not previously regarded as critical infrastructure and had not been seen as a priority for cyber security protection, but it has become critical to better protect these broadcasting facilities.

The Taiwanese Government claimed that a significant number of attacks came from Internet Protocols located in Russia and China. But there is no direct evidence showing that the Chinese or other governments were involved; and the attacks could have been the work of Chinese 'hactivists', given they were uncoordinated. On the other hand, late last year Microsoft, Google and cyber security company Fortinet all reported concern about increasing state-sponsored hacking groups based in China which target Taiwan. Some may be isolated cybercrime or cyberattacks, but state-sponsored activities designed to influence or threaten Taiwan should be seen as a concerted strategy of cyberwarfare, rather than cybercrime.

There was also significant disinformation disseminated during Pelosi's visit to Taiwan. One example was the false claim that '台灣桃園機場遭導彈襲擊，台灣防空攔截失敗 (Taipei Taoyuan International Airport had been bombed and Taiwan Airforce failed to intercept) reported in the Chinese Government's Global Times (環球網) and disseminated through social media. This happened on the same day that Taiwan's Ministry of National Defense was subjected to serious DDoS attacks. While there is no evidence showing a connection between the dissemination of disinformation about the airport and the DDoS attacks on the Ministry of National Defense, the coincidence led to suspicion that the two incidents were coordinated to cause widespread fear. There was also a claim on PPT, Taiwan's largest online forum, that Pelosi was paid a significant amount of money to visit Taiwan. This was later fact-checked and found to be incorrect. Taiwan's Ministry of Foreign Affairs issued a

statement to condemn those who intentionally spread false claims designed to undermine the Taiwan Government. The Ministry also said Taiwan was now facing cognitive warfare by foreign hostile forces via cyberattacks and warned the public not to fall for cognitive warfare and not to become a collaborator by disseminating disinformation.

Disinformation can be used to cause strategic, political, economic, or social harm, such as internal conflict or interference in democratic elections. In this year's presidential and legislative elections in Taiwan, extensive disinformation campaigns were circulated with support of Artificial Intelligence (AI), mostly targeting the ruling Democratic Progressive Party (DPP) which has the view that Taiwan is a sovereign country and not part of the People's Republic of China. The most significant was the dissemination of a 300-page e-book called 'The Secret History of Tsai Ing-wen (蔡英文秘史)'. In an attempt to undermine her and the public's trust in DPP, the book claimed that the mother of Taiwan's 14th and 15th President was a prostitute, and that Tsai falsified her doctoral degree. Using Capcut, AI software developed by the ByteDance Ltd (字結跳動), a company owned by Chinese internet technology company Duoyin, short videos featuring the book were created with fake news anchors and AI-generated voiceovers. These videos were then widely and rapidly disseminated on Youtube, X, Tiktok and other platforms and were promptly replaced if deleted by platforms or accounts banned. Doublethink Lab, a Taiwanese civil society organisation that observes disinformation and tracks Chinese influence, believes the campaign was the handiwork of the Chinese Communist Party. There were also unsubstantiated claims circulated that several DPP candidates and government officials were having extra-marital affairs, accompanied by images generated by AI technologies. Fake videos falsely showing the presidential candidates Lai Ching-tei and Ko Wen-je making comments on various issues were also circulated, presumably with the aim of influencing the election outcome.

To sum up, perhaps more than anywhere else, Taiwan is increasingly proving to be a battlefield for cyberwar, which may be a precursor to or an ongoing and less violent option than traditional warfare. Cyber warfare is launched through attacks on defence and critical infrastructure, as well as through cybercrimes such as stealing personal information, webpage defacement on public and private websites and screens, defamation and dissemination of disinformation. However, actions influencing public opinion, encouraging political polarisation, gradually corrupting democracy and creating instability within Taiwan, either state-sponsored or non-state sponsored, should also be seen through a national security lens. These are all

tactics to strengthen pro-China sentiment through foreign interference.

Lennon Yao-Chung Chang, Associate Professor, Centre for Cyber Resilience and Trust, Deakin University, Australia.
President, Australasian Taiwan Studies Association, Australia
Chairperson, Doublethink Lab, Taiwan.

Want more on Taiwan? Click here!

Image: Taipei at night. Credit: Anko Yeh/Flickr.

Related podcast: Ear to Asia: The future of Taiwan-China relations: Is the status quo the best option?