PSYOPS AND CYBERWAR IN TAIWAN

Lennon Chang

CYBERATTACKS TARGETING Taiwan are nothing new. Every day, there are both attempted and successful attacks targeting government and private sector websites. But during former US House Speaker Nancy Pelosi's visit to the island in August 2022, we saw a drastic increase in cyberattacks and cybercrime generally.

The Taiwanese government recorded twenty-three times more cyberattacks than usual on 2 August. Government websites, including those of the Office of the President and the Ministry of Foreign Affairs, came under especially serious attack. It was reported that a significant number of attacks came from internet protocol (IP) addresses in Russia and China.[1]

One popular type of attack that occurred during Pelosi's visit, but which happens with less intensity in normal times, is the distributed denial-of-service (DDoS). By sending a huge number of messages to a website at the same time, a DDoS attack can be used to disable the website. This happened to the websites of the Office of the President, the Ministry of Foreign Affairs, and the Ministry of National Defence multiple times during this period. For example, the Ministry of Foreign Affairs' website received,

A man stands in front of a projection
Source: Alvan Nee, Unsplash

within a single minute, more than 8.5 million requests for access, which was significantly more than the site's capacity. This sort of attack leaves the government unable to communicate with its citizens through its websites. Website defacement is another popular approach by hackers, and one used intensively during Pelosi's visit. Hackers even replaced the webpages of some government departments and universities[2] and screens at train stations[3] were replaced with messages such as 'There is only one China' 世界只有一個中國 and 'The old witch's visit to Taiwan is a serious provocation to the Chinese government' 老巫婆竄訪台灣，是對祖國的嚴重挑釁. Significantly, screens at convenience stores also came under attack, their content replaced with similar messages. This caused serious concern as cyber-defence for Taiwan's private sector, which is not on the critical infrastructure list, has not previously been considered a priority but now emerges as a worrying vulnerability.

The timing and intensity of these attacks raise concerns that what was previously thought of as 'cybercrime' or isolated 'cyberattacks' should instead be seen as a concerted strategy of 'cyberwarfare'.

The use of DDoS and website defacement as tactics of cyberwarfare can go further than simple disruption of business. These measures can also facilitate the dissemination of fake news and enable extended disinformation campaigns.

War in the digital era can be very different from traditional warfare in that it can be launched without its victims even being aware they are being targeted. Indeed, as outlined in the Australian government's 2022 *Defence Strategic Update*, disinformation campaigns

have already been used to achieve strategic goals without provoking conflict. In Australia and the Indo-Pacific, especially among democratic nations, there is growing concern about disinformation campaigns, especially those believed to originate in China and from the Chinese government.

Some people might associate a disinformation campaign with 'fake news' or 'misinformation', but, these things are better thought of as *mis*information. In a misinformation campaign, people share false or misleading information that they think is true, without intending to mislead others. A disinformation campaign is different. As defined by the Australian Department of Foreign Affairs and Trade, it is

> the intentional creation and dissemination of wholly or partly false and/or manipulated information that is *intended to deceive and mislead* audiences and/or obscure the truth for the purposes of causing strategic, political, economic, social, or personal harm or financial/commercial gain.[4]
>
> (Emphasis in original)

The purpose of disinformation is to deliberately mislead others. The creation and distribution of disinformation can cause great harm to a society or government.

The information distributed in a disinformation campaign may not necessarily be entirely fake. Even verifiable information can be presented in a misleading way to target certain people. An example of a disinformation campaign of this sort involves allegations that the Taiwanese government spent NTD94 million lobbying Pelosi to visit the country. Taiwan's Ministry of Foreign Affairs clarified that money was paid to a lobbying company to expand ties with the US government, not to lobby Pelosi to visit Taiwan, nor to pay for her trip.[5]

We see disinformation disseminated not only through government channels but also in collaboration with individuals, groups, or even criminal organisations. Some examples of such collaboration include the voluntary participation of 'Little Pinks' 小粉紅 — typically young self-identified Chinese patriots, including students; the '50 cents party' 五毛黨, the predecessors of the Little Pinks, who it is alleged receive

a small payment for each post or repost of desired content; and 'content farms', which are organised groups that receive support from companies to disseminate information to the public but also to create content. Disinformation can also be spread through official channels, including official Twitter accounts, Facebook pages, websites, television, and radio.

The crucial lesson is that war might already have appeared in a new guise — one that we do not even recognise as war. Psychological operations ('psyops') are an integral part of the contemporary military strategy of many countries including the United States and Australia. By influencing public opinion, fomenting political polarisation, and otherwise causing conflict within a country, hostile objectives can be accomplished with little effort and no bloodshed. Taiwan has long been a target of psyops over the past decades and has built good countermeasures. However, technologically facilitated psyops are spreading faster and wider than before. While it is important that Taiwan's government continues to improve its measures against psyops, it is also crucial that it adopts new technologies and ideas to provide genuine information in real time. The tactic of 'humour over rumour' used by the Taiwanese government during the COVID-19 pandemic successfully reduced fear and panic-buying of items such as toilet paper among the public.[6] However, there is a risk in times of disaster that the use of humour as a tactic might not be appropriate and careful consideration must be given to ensure its effectiveness. To protect the country, it is important to study how disinformation campaigns are created and disseminated, and how people are influenced by disinformation, with particular attention to the role of culture and language.

Countering cyberattacks and disinformation campaigns must involve the public and private sectors, as well as individual effort — that is, co-production is critical to tackling cyberattacks and disinformation campaigns.

This text is taken from *China Story Yearbook: Chains*, edited by Linda Jaivin, Esther Sunkyung Klein and Annie Luman Ren, published 2023 by ANU Press, The Australian National University, Canberra, Australia.

doi.org/10.22459/CSY.2023.05B