Taiwan is experiencing millions of cyberattacks every day—the world should be paying attention

May 4 2024, by Lennon Y.C. Chang

Credit: Pixabay/CC0 Public Domain

Taiwan stands out as a beacon of democracy, innovation and resilience in an increasingly autocratic region. But this is under growing threat.

In recent years, China has used a variety of "gray zone" tactics to pressure Taiwan to accept the Communist Party's attempts at unification. This has included an onslaught of cyberattacks, which not only pose a significant threat to Taiwan's national security but also seek to undermine its democratic processes.

These attacks range from phishing attempts to sophisticated malware intrusions. Website defacement attacks and Distributed Denial of Service (DDoS) attacks are often seen during significant events, such as the August 2022 visit of Nancy Pelosi, then-speaker of the US House of Representatives. Government agencies, educational institutions, convenience stores and train stations are among the targets.

So, how is Taiwan defending itself from these attacks? And can it continue to do so as China's tactics become more sophisticated?

Millions of cyberattacks a day

Despite Taiwan's technological prowess and robust cybersecurity measures, it continues to be a major target for malicious actors seeking to sow chaos in the country.

According to senior government officials, Taiwan receives some five million cyberattacks a day. And Frontinet, a US-based cybersecurity firm, has found Taiwan experienced just over half of the billions of malware attacks detected in the Asia-Pacific region in the first half of 2023.

The intensity of cyberattacks reached new heights during Taiwan's January 2024 elections—a critical juncture in its democratic journey. The Ministry of Digital Affairs reported on the widespread use of social engineering tactics to compel people to click on links or download files, which then allowed perpetrators to steal sensitive information.

One particularly alarming incident involved a "threat actor" named Earth Lusca, which targets organizations of interest to the Chinese government.

From December to January, this actor emailed a malicious zip file entitled "China's gray-zone warfare against Taiwan" to selected targets, including government and educational institutions and news media in Taiwan. The file was designed to install malicious software to infiltrate computer systems. It also included documents written by experts in Taiwan–China relations, believed to have been stolen from the authors or agencies that own them.

The timing of these attacks, peaking just 24 hours before the elections, underscored their strategic intent to undermine Taiwan's electoral integrity.

Disinformation and deepfakes

These efforts to destabilize Taiwan are not confined to conventional hacking techniques. Disinformation campaigns are also causing political, economic and social harm to the country.

In the lead-up to the elections, for instance, a deluge of false narratives and fabricated content circulated on social media. These targeted the ruling Democratic Progressive Party (DPP), which advocates for Taiwanese sovereignty.

Among the most egregious examples was the dissemination of a 300-page e-book entitled "The Secret History of Tsai Ing-wen" (□□□□□), laden with baseless allegations about the Taiwanese president aimed at eroding the public's trust in her and her party. It claimed, for example, that Tsai's mother was a prostitute.

It also portrayed Tsai as a vile, morally corrupt dictator who is sexually promiscuous and hungry for power. Taiwanese security officials said the book bore the hallmark of the Chinese Ministry of State Security.

Using AI tools such as Capcut, developed by the Chinese technology giant ByteDance, the book's developers also produced and disseminated fake news videos for social media. Featuring AI-generated voices and fake news anchors, these videos were produced with alarming efficiency and promptly replaced if they were taken down by platforms.

Furthermore, rumors circulated on social media about DPP presidential candidate Lai Ching-te having illegitimate sons, and other candidates having extramarital affairs. The videos used deepfake technologies to make the claims appear more real to deceive the public.

Although these campaigns were not entirely successful—Lai won the presidency—they are still a cause for concern.

Orchestrated disinformation campaigns are becoming more sophisticated and widespread, especially with the support of generative AI and deepfake software. And their potential to influence public opinion or fuel political polarization could gradually weaken Taiwan's democracy and create instability.

And these tactics can also be replicated elsewhere. Other countries worried about the impact of cyberattacks and disinformation campaigns on their elections and democratic institutions should be paying attention.

How Taiwan is responding

In response to these multifaceted threats, Tsai, the outgoing president, has stressed that cybersecurity is synonymous with national security.

However, the country's existing cybersecurity regulations primarily target cybercrime. Because of the blurry line between cybercrime and cyber warfare, Taiwan needs to adopt a more holistic approach. This should encompass preventive measures, rapid response strategies and enhanced public-private and international collaborations.

For example, Taiwan is now developing its own satellite internet service—an alternative to Elon Musk's Starlink—to reduce the potential harm from severed underwater internet cables.

Working with the American Institute In Taiwan, the government is also promoting a US Department of Defense cybersecurity framework for local businesses to make them more resilient to attacks. And in January, Taiwan's Ministry of Justice Investigation Bureau established a new research center aimed at combating the threat of online disinformation.

Non-governmental organizations such as the Doublethink Lab, Cofacts and the Taiwan Factcheck Center are also playing a significant role through real-time monitoring of foreign influence and disinformation campaigns and fact-checking services.

However, with advances in technology, cyberattacks and disinformation will evolve. This is why other components are essential to build a comprehensive cyberdefense strategy. This includes increased investment in cybersecurity infrastructure, fostering digital literacy and promoting responsible online behavior.

Only through collective vigilance and concerted efforts can Taiwan safeguard its democratic values in the face of relentless cyber threats.

Provided by The Conversation