

Chinese nationalist groups are launching cyber-attacks—often against the wishes of the government

May 15 2024, by Lewis Eves



Credit: Pixabay/CC0 Public Domain

The UK's national security agency, MI5, [warned](#) in April that British universities participating in military research are targets for cyber-

attacks by foreign states. More recently, news broke of a [cyber-attack](#) against the UK's Ministry of Defense, which exposed the personal details of 270,000 armed forces personnel. China is the main suspect behind these attacks.

China is often presented as a monolithic entity, entirely at the whim of the Chinese Communist Party (CCP). However, the reality is more complex. Many Chinese cyber-attacks and other kinds of digital interference are conducted by Chinese nationalist groups.

Some of these groups are funded by and act under the direction of the CCP. The 50 Cent Army (五毛党), for example, is a group who post pro-CCP messages on social media. Its name is derived from reports that the CCP pays recruits [0.5 yuan \(US\\$0.69\)](#) per post.

But many of these groups operate independently. There are even cases of Chinese nationalist groups engaging in online warfare [against the wishes](#) of the CCP.

The fact that cyber-attacks are being launched independently of the CCP and against its directives suggests that China's nationalist movement is escaping the government's societal controls. This could become a headache for China's president, Xi Jinping, as the number of cyber-attacks grows.

China's nationalist movement is very sensitive to what it considers insults to the Chinese nation. This is due to the careful construction of Chinese nationalism through stories like the ["century of humiliation"](#), a period from roughly 1839 to 1949 in which China was exploited and victimized by foreign imperialist powers.

Chinese nationalists now act against what they perceive to be renewed attempts by foreign powers to again humiliate China. They take action

through "online wars" against those who they believe pose a threat to China's interests.

In 2016, Taiwan elected Tsai Ing-wen, an anti-Beijing candidate, as president. During and after the election, a group of predominately young, female cyber-nationalists known as the Little Pinks (小粉) waged a "[meme war](#)" against Taiwan.

This involved thousands of Little Pinks posting a deluge of pro-Beijing memes on the social media profiles of President Tsai and numerous Taiwanese news outlets. The memes emphasized China's claim that Taiwan is a Chinese province and not an independent nation state.

Some cyber-nationalist groups have gone a step further by engaging in hacktivism. This involves targeting institutions and organizations through cyber-attacks to pursue the nationalist agenda.

In 2008, an informal group of hacktivists called the Red Hacker Alliance (红黑客联盟) attempted a [denial-of-service attack](#) against US media company CNN. The attack was in response to CNN's reporting on anti-Beijing protests in Tibet, which has been occupied by China since 1950. It caused the company's website to be briefly unavailable in some parts of Asia.

In another example, a group called the Honker Union (轰客联盟) launched cyber-attacks against the Philippines in 2014. Triggered by the attempted arrest of Chinese fishermen in a disputed area of the South China Sea, the Honker Union [hacked](#) into the website of the University of the Philippines. Hackers posted pro-Chinese slogans and a map showing China's territorial claims on the university's homepage.

The CCP's societal control

The CCP leans into nationalist sentiment to legitimize its regime, presenting itself as the vanguard of the Chinese nation. But this reliance on nationalism has given China's nationalist movement considerable influence. The CCP cannot be seen to contradict its nationalist credentials by constraining nationalist activity too heavily.

As a result, cyber-nationalists have escaped the CCP's societal controls, such as its ability to direct China's nationalist movement through propaganda. In doing so, cyber-nationalists undermine the CCP's authority and occasionally contradict its foreign policy.

In 2020, the CCP [called for restraint](#) among nationalist groups following foreign criticism of China's crackdown on Hong Kong. However, cyber-nationalists still undertook an anti-foreign smear campaign on social media. Even the Communist Youth League, a nationalist organization with formal links to the CCP, [took part](#) against the CCP's instruction.

As part of this campaign, hacktivists also launched cyber-attacks such as [hijacking](#) the Twitter account of the Chinese embassy in Paris. The hacktivists [posted a picture](#) of the US as the personification of death visiting Hong Kong.

The embassy quickly deleted the image and apologized to France and the US. But the incident speaks to a CCP that is struggling to control cyber-nationalists who are evading its societal controls and are willing to hijack state propaganda infrastructure to pursue their goals.

There have also been hacktivist cyber-attacks directed against the Chinese state, usually coinciding with periods of discontent with the CCP. In 2014, one group [briefly seized control](#) of a television network in the eastern city of Wenzhou and broadcast nationalistic and anti-CCP messages. This cyber-attack was made in protest of the detention of [Wang Bingzhang](#), a nationalist activist and political dissident.

Another group [hacked](#) into a Shanghai police database in 2022, leaking 23 terabytes of personal information that the state had collected on the Chinese people as part of its program of mass domestic surveillance. The information was later made available for sale on online forums from an anonymous hacker referred to as "[ChinaDan](#)."

In the west, we assume that Chinese cyber-attacks reflect a malicious Chinese state. The reality is more complex. As cyber-nationalists continue to take matters into their own hands, increasing numbers of [cyber-attacks](#) also reflects a major domestic problem for the CCP—one that showcases the limits of its societal controls.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Chinese nationalist groups are launching cyber-attacks—often against the wishes of the government (2024, May 15) retrieved 17 July 2024 from <https://techxplore.com/news/2024-05-chinese-nationalist-groups-cyber.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--