The Chinese Communist Party's Internet Trolls Are the World's Largest Cyber Army

The Epoch Times Commentary by Gu Feng
March 25, 2021

In the online world, a group of people endangers the safety and health of the internet, and Chinese netizens call them the "cyber triad." Among the groups are the Chinese regime's internet trolls, known as "wumao dang" in Chinese or "50 cent army."

These internet trolls pose a threat to personal data and national security. They carried out the Chinese Communist Party (CCP)'s disinformation campaigns with regards to the COVID-19 pandemic, Hong Kong's anti-extradition bill protests, Taiwan's 2020 election, and the U.S. 2020 election, and other major international events.

The History of the CCP's Internet Trolls

The CCP's internet trolls, described in a study (pdf) as "for-hire astroturfers working for and advancing the interests of companies and other actors willing to

pay their fees," are one of the largest criminal organizations. Based on the historical data of major search engines, commercial trolls have been emerging on the internet since 2004.

Through an analysis of online data, the CCP's internet trolls can be divided into three stages of development.

The first stage was from 2004 to 2009, during which the CCP's trolls mainly focused on the deletion of posts, sales and promotion, and advocacy of rights on behalf of others.

The second stage was from 2010 to 2013, which was the business development stage of the CCP's trolls. In this stage, its business scope began to expand. Major internet troll companies began to act as public relations agents for individuals, enterprises, local CCP parties, government agencies, and the CCP's non-governmental institutions to deal with online crises. During this stage, the 50 cent army, civilian internet trolls hired by the CCP, started to appear on the internet to participate in public events.

The third stage was from 2014 to 2021, when the business transformed for the CCP's trolls. In February 2014, the CCP officially established the Central Leading Group for Cyberspace Affairs, under which is the Cyberspace Administration of China (CAC), or Office of the Central Cyberspace Affairs Commission.

Five business sectors were established to work under the CAC: the Internet Commentary Work Bureau, the Internet Social Work Bureau, the Mobile Network Administration Bureau, the Internet Security Coordination Bureau, and the International Cooperation Bureau. Their responsibilities include internet opinion monitoring, management, control of the CCP's internet trolls, public relations related with internet issues, overseas propaganda, and the CCP's United Front Work Department.

After the establishment of the CAC, it launched a cyber campaign to consolidate various independent civilian hackers and troll companies under its control. At the same time, the Communist Youth League of China (CYLC) recruited tens of millions of university students to work as part-time internet trolls in major universities across China, and the

Central Committee of Political and Legal Affairs recruited millions of detainees in major prisons as full-time cyber trolls. In this way, cyber hackers and trolls have changed from a “guerrilla army” into a “regular army” controlled by the CCP.

The Organizational Structure of the CCP’s Internet Trolls

According to CCP insiders, the CCP attaches great importance to the formation and management of its internet trolls. The CCP has set up special organizations of cyber army governance at all levels of government. Personnel recruitment, training, task assignment, payment, and meetings are all conducted online.

The CCP’s internet trolls are composed of the following six categories of personnel: cadres of CYLC, social media influencers, university students, employees of internet companies, prison inmates, and the unemployed. Their payment is based on different job categories and is calculated on the number of posts they have submitted. There are many types of job roles, and the major roles include conveners, technical staff (hackers), writers, online

commentators, and public opinion supervisors. The trolls themselves are divided into two major categories: domestic and overseas.

The CCP's Internet Trolls Are Anathema to Chinese Netizens

The Chinese people dare not voice their anger at the CCP for spending huge sums of public money to pay tens of millions of 50 cent army members every year.

In China, major internet portals, at the behest of the CCP, allow the 50 cent army to suppress criticism and stigmatize CCP dissidents, create false public opinion, cover up various crimes committed by the CCP, undermine social order and morality, create the illusion of national prosperity, incite racial and ethnic hatred, maliciously create rumors about other countries, falsify historical truths, and spread messages to fool the public.

Whenever articles by major CCP leaders appear on the internet, the comments are almost always filled with adulation written by the internet trolls. The Chinese netizens despise the 50 cent army, but the

Chinese regime regards their comments as public opinion.

The **CCP's Cyber Army Has Become a Malignant Tumor to the Whole World**

Today, with the globalization of the internet, the CCP's cyber army has long been endangering the social security of countries around the world. In the cyber world, the CCP's online trolls are like an infectious disease, attacking countries all over the world. For example, online hackers attack the websites of key government departments, scientific research institutions, large enterprises, and universities to steal their information. The 50 cent army maliciously attacks and abuses government leaders and anti-communists in other countries. The Chinese regime's social media influencers implement cultural aggression on the internet. In short, the CCP's cyber army is taking advantage of the freedom of speech in democratic countries to attack other countries.

As early as a decade ago, the United States had included the CCP's cyber attacks as an important

issue in U.S.-China diplomacy, but the situation is getting worse.

On March 18, the Biden administration held its first high-level dialogue with the Chinese regime in Alaska, where Secretary of State Anthony Blinken met with Yang Jiechi, a senior CCP foreign policy diplomat, and Chinese Foreign Minister Wang Yi. Blinken said that the United States would "discuss our deep concerns with actions by China, including in Xinjiang, Hong Kong, Taiwan, cyber attacks on the United States, economic coercion of our allies."

Instead of including the South China Sea and U.S.-China trade issues on the agenda, the United States made cyberattacks an important topic of the talks, which shows the extent of harm the CCP's cyber army has done to the United States.

The CCP's cyber army has also launched fierce attacks on U.S. social media.

Twitter announced on June 12, 2020, the "disclosure" of the Chinese regime's "23,750 accounts" that Twitter said as being involved "in a range of manipulative and coordinated activities,"

and that they tweeted “predominantly in Chinese languages” to spread “geopolitical narratives favorable to the Communist Party of China (CCP) while continuing to push deceptive narratives about the political dynamics in Hong Kong.”

On Sept. 22, 2020, Facebook also removed a network of fake accounts from China that “coordinated inauthentic behavior” in political discussions through “155 accounts, 11 Pages, 9 Groups, and 6 Instagram accounts.” According to Facebook, their activities “originated in China and focused primarily on the Philippines and Southeast Asia more broadly, and also on the United States.”

Gu Feng is a former media veteran from mainland China now living in the United States.

https://www.theepochtimes.com/the-chinese-communist-partys-internet-trolls-are-the-worlds-largest-cyber-army_3748483.html