

# [***US and UK go after Chinese hackers accused of state-backed operation against politicians, dissidents***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:6BMS-4CS1-DYMD-654Y-00000-00&context=1516831)

The Associated Press

March 25, 2024 Monday 9:52 PM GMT

Copyright 2024 Associated Press All Rights Reserved

**Section:** BUSINESS NEWS; WASHINGTON DATELINE

**Length:** 1068 words

**Byline:** SYLVIA HUI and ERIC TUCKER, Associated Press

**Dateline:** WASHINGTON

**Body**

WASHINGTON — Hackers linked to the Chinese government launched a sweeping, state-backed operation that targeted U.S. officials, journalists, corporations, pro-democracy activists and the U.K.'s election watchdog, American and British authorities said Monday in announcing a set of criminal charges and sanctions.

The intention of the campaign, which officials say began in 2010, was to harass critics of the Chinese government, steal trade secrets of American corporations and to spy on and track high-level political figures. Western officials disclosed the operation, carried out by a hacking group known as APT31, while sounding a fresh, election-year alarm about a country long seen as having advanced espionage capabilities.

The U.S. Justice Department charged seven hackers, all believed to be living in China. The British government, in a related announcement, imposed sanctions on two of the defendants in connection with a breach that may have given the Chinese access to information on tens of millions of U.K. voters held by the Electoral Commission.

“The Justice Department will not tolerate efforts by the Chinese government to intimidate Americans who serve the public, silence the dissidents who are protected by American laws, or steal from American businesses,” Attorney General Merrick Garland said in a statement, adding that the “case serves as a reminder of the ends to which the Chinese government is willing to go to target and intimidate its critics.”

As part of the cyber-intrusion campaign, prosecutors said, the hackers sent more than 10,000 emails to targets all over the world that purported to be from prominent journalists but that actually contained malicious code. Once opened, the emails installed tracking software that allowed the hackers to know the victims’ location, IP addresses and even the devices they used to get email.

The hackers further leveraged that tracking to target home routers and other devices, “including those of high-ranking U.S. government officials and politicians and election campaign staff from both major U.S. political parties,” the indictment says.

Targets included officials at the White House and multiple government agencies, including the Treasury and Commerce departments, senators from both parties, the spouse of a senior Justice Department official, political strategists, and political figures from around the world who were critical of the Chinese government, including members of a pro-democracy advocacy group.

The Justice Department said the hackers also began targeting email accounts belonging to senior staffers of a presidential campaign in May 2020, several months before the general election.

Also, the cybersecurity firm Proofpoint [*later noted in a blog*](https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists), the hackers heavily focused their phishing on Washington-based journalists, including White House correspondents, just prior to the Jan. 6, 2021, attack on the Capitol.

Britain's sanctions follow an announcement [*last August*](https://apnews.com/article/britain-election-commission-hacked-90427209cae68bbe5cc7b0476ce17cca) that “hostile actors” had gained access to its servers from around 2021 to 2022.

At the time, the watchdog said the data included the names and addresses of registered voters. But it said much of the information was already in the public domain.

The Foreign Office said Monday the hack of the election registers “has not had an impact on electoral processes, has not affected the rights or access to the democratic process of any individual, nor has it affected electoral registration.”

British cybersecurity officials also said that APT31 hackers “conducted reconnaissance activity” against British parliamentarians who were critical of Beijing in 2021. They said no parliamentary accounts were successfully compromised.

Three lawmakers, including former Conservative Party leader Iain Duncan Smith, told reporters Monday they have been “subjected to harassment, impersonation and attempted hacking from China for some time.” Smith said in one example, hackers impersonating him used fake email addresses to write to his contacts.

APT31 has previously been accused of [*targeting U.S. presidential campaigns*](https://apnews.com/article/1b877badbd3ba454be2aac9fca8d7643) and the information systems of [*Finland’s parliament*](https://apnews.com/article/legislature-beijing-finland-china-hacking-f9879cd03785aefda6c631e1c5c46fb5), among others.

Britain’s Deputy Prime Minister Oliver Dowden said his government will summon China’s ambassador to account for its actions.

China’s Ministry of Foreign Affairs said before the announcement that countries should base their claims on evidence rather than “smear” others without factual basis.

“Cybersecurity issues should not be politicized,” ministry spokesperson Lin Jian said. “We hope all parties will stop spreading false information, take a responsible attitude, and work together to maintain peace and security in cyberspace.”

British Prime Minister Rishi Sunak reiterated that China is “behaving in an increasingly assertive way abroad” and is “the greatest state-based threat to our economic security.”

“It’s right that we take measures to protect ourselves, which is what we are doing,” he said, without providing details.

U.S. officials over the years have brought a broad array of criminal cases against hackers affiliated with the Chinese government. They have also expressed concern about Chinese government influence operations and the potential that Beijing could meddle in presidential ***politics***.

A [*2021 intelligence assessment*](https://apnews.com/article/joe-biden-donald-trump-iran-moscow-elections-c640ed02202c9d44f0ad186ebd0b3396) found that China ultimately did not interfere on either side during the 2020 election and “considered but did not deploy” influence operations intended to affect the outcome. U.S. officials say they believe Beijing prioritized a stable relationship with the U.S. and did not consider either election outcome as advantageous enough for it to risk the “blowback” that would ensue if it got caught with interfering.

The Justice Department said the indictment unsealed Monday does not alter that conclusion, noting that there's no allegation that the hacking was designed to further a Chinese government influence operation against the U.S.

Even so, Assistant Attorney General Matthew Olsen, the Justice Department's top national security official, said in a statement that, “Today’s announcements underscore the need to remain vigilant to cybersecurity threats and the potential for cyber-enabled foreign malign influence efforts, especially as we approach the 2024 election cycle."

\_\_\_\_\_

Hui reported from London. Associated Press writers Frank Bajak in Boston, Didi Tang in Washington and Dave Collins in Hartford, Connecticut, contributed to this report.

**Load-Date:** March 25, 2024

**End of Document**