

# [***China Eying Election Disruption Campaigns Including With AI, Microsoft Says***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:6BR9-96Y1-JBCM-F011-00000-00&context=1516831)

Forbes.com

April 5, 2024 Friday

Copyright 2024 Forbes LLC All Rights Reserved

**Length:** 871 words

**Byline:** James Farrell, Forbes Staff

**Highlight:** A new Microsoft report details new tactics used by Chinese-affiliated entities to influence public opinion.

**Body**

**Topline**

Entities affiliated with China are using deceptive social media accounts to probe U.S. opinion on divisive issues in a potential attempt to gather information on how to disrupt elections, while also using AI-generated content to attempt to sway public opinion, according to a new report fromMicrosoft though their success has been limited so far.

<figure>

<figcaption>

FILE - The Microsoft logo is shown at the Mobile World Congress 2023 in Barcelona, Spain, on March 2, 2023. (AP Photo/Joan Mateu Parra, File)

Copyright 2023 The Associated Press. All rights reserved

</figcaption></figure>

**Key Facts**

The analysis from Microsoft s Threat Analysis Center found no change in China s priorities or targets seeking to launch influence operations targeting the South Pacific Islands, the South China Sea region and the U.S defense industrial base but it noted the latest trends represent a change in tactics.

The Microsoft Threat Analysis Center has in thepastnoted how Chinese-affiliated social media accounts were beginning to impersonate U.S. voters, but in this latest report, it notes how these accounts have started to almost exclusively post about divisive U.S. political issues, and in recent months those posts have started to include what Microsoft described as polling questions questions like What do you think about this? And What s your reaction?

Microsoft says it believes this could be a deliberate effort to understand better which U.S. voter demographic supports what issue or position and which topics are the most divisive ahead of the 2024 presidential election.

Chinese influence operations have also increasingly used artificial intelligence to try and sow political divisions in the U.S. and elsewhere, according to the report.

Microsoft says it observed the Chinese-affiliated network known as Spamouflage, which Microsoft refers to as Storm-1376, ramp up AI operations during the Taiwanese presidential election, promoting misleading AI-generated audio clips, memes and other content.

In the U.S., Storm-1376 attempted to use AI-generated content to spread misinformation on a wide variety of issues claiming the Maui wildfires in 2023 were staged by the U.S. government, for instance though Microsoft finds little evidence these efforts have been successful in swaying opinion.

**What Other Threats Did The Report Find?**

Microsoft also flagged concern about North Korea, noting the country has continued its longstanding efforts to steal cryptocurrency that funds its weapons program. North Korean cyber attackers have taken more than $3 billion in cryptocurrency heists since 2017, according to United Nations numbers cited by Microsoft. North Korea is also gearing its cyber operations to gathering intelligence on the U.S., South Korea and Japan. A North Korean entity that Microsoft calls Emerald Sleet has been using AI to improve its operations, and Microsoft said it is working with OpenAI to disable accounts associated with Emerald Sleet.

**Key Background**

Microsoft has previously flagged concern that state-sponsored groups might be using artificial intelligence to improve their hacking operations. In February,Microsoftpublished a report that various groups affiliated with Russia, China and others were regularly using OpenAI s tools to become more productive in their hacking efforts, though Microsoft officials noted they were mostly using them for simple tasks. They re just using it like everyone else is, to try to be more productive in what they re doing, Tom Burt, head of Microsoft s cybersecurity, told the New York Times at the time. U.S. adversaries have long faced accusations of using social media to sway ***politics*** or stoke division most notably in 2016, when Russian government-sponsored entities were linked to a push to back then-candidate Donald Trump.

**Contra**

Chinese Embassy Spokesperson Liu Pengyu told Forbes in an email the report was in itself disinformation as it misrepresents facts and truth. Pengyu maintained that the presidential election is a domestic affair in the U.S., and said China is committed to the principle of non-interference and that claims about China influencing U.S. presidential elections are completely fabricated. He also accused the U.S. of being the true breeding ground of disinformation, often framing Chinese policy negatively.

**Contra**

The report comes as Microsoft responds to its own cybersecurity challenges. The company in January disclosed a Russian-linked group calledMidnight Blizzardaccessed some of its corporate email accounts and later in March noted the group s continued attempts to access the company s systems. Earlier this week, the federal government s Cyber Safety Review Board issued a report criticizing Microsoft for a cascade of avoidable errors that contributed to a breach of the tech giant s systems by Chinese-affiliated groups. The hackers in that cyber attack reportedly accessed email inboxes from dozens of organizations and several U.S. government officials.

**Tangent**

On Thursday, billionaireElon Musksaid he was planning on trying to purge bot accounts on his social media platform X, formerly known as Twitter though the platform has long struggled to control the emergence of fake accounts.

**Further Reading**

**Load-Date:** April 6, 2024

**End of Document**