China tests US voter fault lines and ramps AI content to boost its geopolitical interests

Apr 4, 2024 | Clint Watts - General Manager, Microsoft Threat Analysis Center

China is using fake social media accounts to poll voters on what divides them most to sow division and possibly influence the outcome of the U.S. presidential election in its favor. China has also increased its use of AI-generated content to further its goals around the world. North Korea has increased its cryptocurrency heists and supply chain attacks to fund and further its military goals and intelligence collection. It has also begun to use AI to make its operations more effective and efficient.

These are among the Microsoft Threat Intelligence insights in the latest East Asia report published today by the Microsoft Threat Analysis Center (MTAC) – *Same targets, new playbooks: East Asia threat actors employ unique methods*.

Three key findings emerge in the report:

Related Stories

Feb 13, 2024 | Brad Smith

Combating abusive AI-generated content: a comprehensive approach >

Feb 6, 2024 | Clint Watts

Iran accelerates cyber ops against Israel from chaotic start >

Feb 16, 2024 | Brad Smith

Meeting the moment: combating AI deepfakes in elections through today's new tech accord >

Related Blogs

Mar 28, 2024 | Julie Brill

Protecting the data of our commercial and public sector customers in the AI era >

- Deceptive social media accounts by Chinese Communist Party (CCP)-affiliated actors have started to pose contentious questions on controversial U.S. domestic issues to better understand the key issues that divide U.S. voters. This could be to gather intelligence and precision on key voting demographics ahead of the U.S. presidential election.
- There has been an increased use of Chinese AI-generated content in recent months, attempting to influence and sow division in the U.S. and elsewhere on a range of topics including: the train derailment in Kentucky in November 2023, the Maui wildfires in August 2023, the disposal of Japanese nuclear wastewater, drug use in the U.S. as well as immigration policies and racial tensions in the country. There is little evidence these efforts have been successful in swaying opinion.
- China's geopolitical priorities remain unchanged but it has doubled down on its targets and increased the sophistication of its influence operations (IO) attacks. These priorities are:
  - The South Pacific islands
  - The South China Sea region
  - The U.S. defense industrial base

Inauthentic Chinese social media accounts try to learn more on what divides US voters

Figure 12: Chinese sockpuppets solicit opinions on political topics from other users on X.

MTAC previously reported in September 2023 how CCP-affiliated social media accounts had begun to impersonate U.S. voters in an effort to influence the 2022 U.S. midterm elections.

Mar 20, 2024 | Tania Cosentino

AI in Brazil: Exploring opportunities >

Feb 26, 2024 | Brad Smith

Microsoft's AI Access Principles: Our commitments to promote innovation and competition in the new AI economy >

More Cybersecurity Stories

Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries >

April 11, 2023

Digital Crimes Unit: Leading the fight against cybercrime >

May 3, 2022

This activity has continued and these accounts nearly exclusively post about divisive U.S. domestic issues such as global warming, U.S. border policies, drug use, immigration, and racial tensions. They use original videos, memes, and infographics as well as recycled content from other high-profile political accounts. In recent months, there has been an increase in, effectively, polling questions. This indicates 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 main phase of the U.S. presidential election.

China increases use of AI in influence campaigns

Chinese IO operations in the U.S. continued to opportunistically jump on events which could serve their strategic interests – such as portraying the U.S. in an unfavorable light. These operations, attributed to Storm 1376, included:

- Claiming that the Maui wildfires of August 2023 were deliberately set by the U.S. government to test a military-grade "weather weapon"

Figure 8: Storm-1376 posts conspiratorial content within days of the outbreak of the wildfires, alleging the fires were the result of US government testing of a "meteorological weapon." These posts were frequently accompanied with AI-generated photos of massive fires.

- Urging audiences to consider whether the derailment of a train carrying molten sulfur in Kentucky in November 2023 was deliberately caused by the U.S. government and whether it is "deliberately hiding something". Some messages even likened the derailment to 9/11 and Pearl Harbor cover-up theories.

- Accusing the U.S. of purposefully poisoning other countries' water supplies to maintain "water hegemony". This was part

Keeping your vote safe and secure: A story from inside the 2020 election ›

June 22, 2021

of a wider multilingual campaign, principally focused on Japan and its government's decision to dispose of treated radioactive wastewater into the Pacific Ocean. Storm-1376 tried to cast doubt on the International Atomic Energy Agency's (IAEA) scientific assessment that the disposal was safe.

Figure 9: AI-generated memes and images critical of the Fukushima wastewater disposal from covert Chinese IO assets (left) and Chinese government officials (center). Influencers affiliated with Chinese state-owned media also amplified government-aligned messaging critical of the disposal (right).

The Taiwanese presidential election in January 2024 saw a surge in the use of AI-generated content to augment IO operations by CCP-affiliated actors. This was the first time that Microsoft Threat Intelligence has witnessed a nation-state actor using AI content in attempts to influence a foreign election.

The group we call Storm-1376, also known as Spamouflage and Dragonbridge, was the most prolific. For example, on election day, it posted suspected AI-generated fake audio of Foxconn owner and election candidate Terry Gou (who had bowed out of the contest in November 2023) endorsing another candidate in the presidential race. Gou had made no such statement. YouTube quickly removed this content before it reached a wider audience.

Figure 3: Videos published by Storm-1376 used AI-generated voice recordings of Terry Gou to make him appear as though he endorsed another candidate.

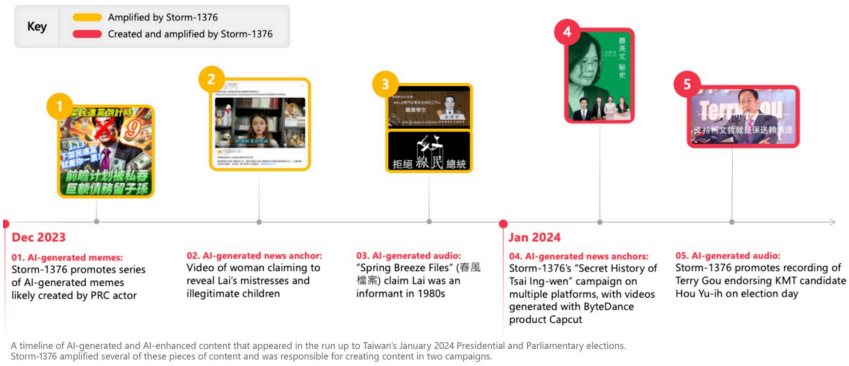
Figure 6: AI-generated memes accuse DPP presidential candidate William Lai of embezzling funds from Taiwan's Forward-looking Infrastructure Development Program. These memes featured simplified characters (used in the PRC but not in Taiwan) and were part of a series that showed a daily "countdown to take the DPP out of power."

Storm-1376 has promoted a series of AI-generated memes of Taiwan's then-Democratic Progressive Party (DPP) presidential

candidate William Lai, and other Taiwanese officials as well as Chinese dissidents around the world. These have included an increasing use of AI-generated TV news anchors that Storm-1376 has deployed since at least February 2023.

Figure 7 Microsoft Threat Intelligence

Timeline of AI influence in Taiwan elections



A timeline of AI-generated and AI-enhanced content that appeared in the run up to Taiwan's January 2024 Presidential and Parliamentary elections. Storm-1376 amplified several of these pieces of content and was responsible for creating content in two campaigns.

North Korean cyber operations

North Korea continued to prioritize the theft of cryptocurrency funds, conducting software supply-chain attacks and targeting their perceived national security adversaries. This is likely to generate revenue, principally for its weapons program, in addition to collecting intelligence on the United States, South Korea, and Japan.

The United Nations estimates that North Korean cyber actors have stolen over $3 billion in cryptocurrency since 2017. Heists totaling between $600 million and $1 billion occurred in 2023 alone.

Our report catalogs multiple instances of cryptocurrency heists, spear-phishing, and software supply-chain attacks and efforts to undermine the trilateral alliance between the U.S., Japan, and South Korea.

Notably, Microsoft and OpenAI have observed the North Korean actor we call Emerald Sleet using tools powered by AI large-language models (LLMs) to make their operations more effective and efficient. Microsoft partnered with OpenAI to disable accounts and assets associated with Emerald Sleet.

Looking forward

With major elections taking place around the world this year, particularly in India, South Korea and the United States, we assess that China will, at a minimum, create and amplify AI-generated content to benefit its interests. Despite the chances of such content in affecting election results remaining low, China's increasing experimentation in augmenting memes, videos, and audio will likely continue – and may prove more effective down the line. We can expect to see North Korea continue to steal cryptocurrency to fund space, missile, and nuclear programs as well as launch supply-chain attacks on the defense sector.

Tags: AI, China, cyber influence, elections, influence operations, MTAC, North Korea, open ai