How an Iranian Influence Operation Used ChatGPT to Target the U.S. Presidential Election

October 27, 2025 • vajiramandravi.com

What's in today's article?

- Why in News?
- What is Storm-2035?
- Use of ChatGPT to influence U.S. presidential election
- Steps taken by OpenAI to safeguard its tech

Why in News?

Recently, OpenAI announced that it had banned ChatGPT accounts connected to an Iranian influence operation that aimed to generate content to sway the U.S. presidential election.

The Microsoft-backed company reported that it had identified and removed a "cluster of ChatGPT accounts" and is actively monitoring the situation.

What is Storm-2035?

- OpenAI identified a group involved in an Iranian influence operation, dubbed “Storm-2035,” which operated through four websites posing as news organizations.
- These sites, including EvenPolitics, Nio Thinker, Westland Sun, Teorator, and Savannah Time, exploited divisive issues such as LGBTQ rights and the Israel-Hamas conflict to influence U.S. voters.
- According to a Microsoft Threat Analysis Center (MTAC) report, the sites used AI tools to plagiarize content and drive web traffic. The operation targeted both liberal and conservative voters in the U.S.

Use of ChatGPT to influence U.S. presidential election

- **Use**
  - OpenAI revealed that operatives from the Storm-2035 group used ChatGPT to generate long-form articles and social media comments, which were then posted on X and Instagram accounts.
  - These AI-generated posts mimicked American language patterns, rehashed existing comments or propaganda, and significantly reduced the time needed to produce and distribute plagiarized content aimed at influencing voters.
  - The operation not only targeted the upcoming U.S. presidential election but also covered global issues such as Venezuelan politics, Latin rights in the U.S., the situation in Palestine, Scottish independence, and Israel’s participation in the Olympic Games.
  - It also exploited popular topics like fashion and beauty.
- **Impact**
  - OpenAI has downplayed the severity of the Storm-2035 incident, noting that the content generated by the operation received minimal engagement on social media.
  - Using Brookings’ BreakoutScale, which rates the impact of covert operations from 1 to 6, the report classified this operation as low-end Category 2.
- This means the content was posted on multiple platforms but failed to gain traction among real users.
  - Despite this, OpenAI emphasized that it had shared the threat information with relevant government, campaign, and industry stakeholders.
  - While OpenAI viewed the disruption of this Iran-linked influence operation as a positive outcome, it also acknowledged the serious implications of foreign operatives using generative AI tools to target U.S. voters.
  - The incident underscores multiple vulnerabilities across OpenAI, social media platforms like X and Instagram, and the search engines that ranked the sites involved.
- **Other similar issues OpenAI faced in the past**
  - In May, OpenAI disclosed that it had spent over three months dismantling covert influence operations using its AI tools to generate social media comments, articles in various languages, fake profiles, and to translate or proofread content.
  - One Russian group, dubbed “Bad Grammar,” used Telegram to target Ukraine, Moldova, the Baltic States, and the U.S.
  - Other operations included “Doppelganger” from Russia, “Zeno Zeno” from Israel, “Spamouflage” from China, and “International Union of Virtual Media” (IUVM) from Iran.
- These groups used ChatGPT to write social media comments and articles on platforms like X and 9GAG.

- They focused on topics like Russia's invasion of Ukraine, the Gaza conflict, elections in India and Europe, and criticism of the Chinese government.
    - OpenAI also uncovered instances of state-backed actors using AI for malicious purposes.
    - In July, it revealed that a hacker had accessed its internal messaging systems the previous year, stealing information related to its AI technologies.
- Although the hacker was an individual, the breach raised concerns about potential threats from Chinese adversaries.

Steps taken by OpenAI to safeguard its tech

- OpenAI found that its **AI tools successfully refused to generate certain text or images** due to built-in safeguards during its investigation into influence operations.
- The company also developed **AI-powered security tools** that can now detect threat actors within days instead of weeks.
- Although not widely discussed, OpenAI has deepened its ties with U.S. federal agencies.
- In June, OpenAI appointed cybersecurity expert and retired U.S. Army General Paul M. Nakasone to its Board of Directors.
    - Nakasone, who previously led the U.S. National Security Agency, has extensive experience in cyber units across the U.S., Korea, Iraq, and Afghanistan.
- Recently, OpenAI also announced a partnership with the U.S. AI Safety Institute, allowing the institute to preview and test its upcoming foundational model, GPT-5.

Q.1. What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) refers to systems or machines that simulate human intelligence to perform tasks and improve over time through learning. It encompasses technologies like machine learning and natural language processing, enabling computers to analyze data, recognize patterns, and make decisions with minimal human intervention.

Q.2. What is ChatGPT?

ChatGPT is an AI language model developed by OpenAI that generates human-like text based on input. It can understand and respond to a wide range of topics, engage in conversations, and assist with various tasks. It leverages machine learning to continually improve its language and interaction capabilities.

Source: How an Iranian group used ChatGPT to influence U.S. presidential election | Times of India

Source: https://vajiramandravi.com/current-affairs/how-an-iranian-influence-operation-used-chatgpt-to-target-the-u-s-presidential-election/
© Vajiram & Ravi. For personal use only.