BRENNAN CENTER FOR JUSTICE – 24 OTTOBRE 2023

Tech Titans Must Step Up to Protect Elections

di Lawrence Norden e David Evan Harris

"We interfered, we interfere, and we will interfere," said late Russian oligarch and mercenary leader Yevgeny Prigozhin in an **admission** last year that we can expect more Kremlin interference in American elections. While Prigozhin since died in a **plane "crash,"** it's safe to assume that his successors will continue receiving orders to attack U.S. elections from every possible angle, but this time they'll have a new and formidable ally: artificial intelligence.

In 2024, we can expect an AI-amplified assault on our election systems. The Department of Homeland Security has already **warned** that China, Russia, and Iran are likely to use generative AI to target U.S. "election infrastructure, processes, and personnel." Microsoft says it **caught China in the act**. And on September 27, federal lawmakers took up the topic for **discussion** in a hearing of the U.S. Senate Committee on Rules and Administration.

With AI, attacks on our elections can be personalized in powerful new ways. Drawing on publicly available information about an election office's chain of command, contact information, and its employees' personal lives, generative AI can be used to send election **workers phishing emails or cloned voice messages** that seem like communications from a colleague or manager seeking confidential information. Many Americans have **fallen victim** to AI's talent for mimicry, duped into sending money to hackers disguised as loved ones. The stakes are even higher for attacks against our election systems — and this is only one of the myriad ways AI threatens our democracy.

The need to regulate AI is clear. Even billionaire AI developers, who stand to profit most from the widespread adoption of AI technology, **agreed** on this in a private meeting with U.S. senators last month. But necessary as it may be, federal regulation

won't come in time for the next election. Given the billions of dollars they will make from this new technology, tech firms must act now to protect the 2024 elections from AI-related threats, even without congressional mandates.

For starters, they can provide resources to nonprofits and programs such as the **Election Technology Initiative**, which is focused on maintaining, supporting, and delivering technologies to help election administrators increase confidence, access, and transparency in elections. And when asked for help from state officials, they can provide free resources and low-cost support. In the case of protecting against the phishing attacks described above, that could mean helping election offices remove online information that provides fodder for email scams and securing personal social media accounts to shield critical information.

A commonly cited danger of generative AI is its potential to distort reality. Political campaigns have produced realistic deepfakes of public officials doing controversial things, such as an AI-generated Donald Trump embracing Dr. Anthony Fauci. Its ability to imitate **authoritative voices** is especially concerning on social media, as election officials have depended on these platforms to share critical information with voters. A well-timed deepfake, deployed in the hours or days before voting begins, can **spread** much more quickly than a debunk, and the damage can be irreversible.

The change in X's (formerly Twitter) verification policies this year inspired a **rash of imposter accounts** posing as government agencies. Similar efforts could threaten the thousands of local election officials who have limited resources and staff available to debunk deepfakes or push to deplatform imposters. Left unaddressed, AI-generated fake accounts can fuel bogus claims of fraud or disseminate incorrect information about voting.

Again, tech companies can help mitigate these risks. Platforms such as X can provide distinct verification to election officials — a process X has begun, but **far too slowly** — and amplify their authentic content. Social media platforms should publish clear guidelines for verification programs, proactively reach out to election officials, process verifications quickly, and, better yet, collaborate to make it easier for election officials to share content across platforms. They should also double down on early efforts from **TikTok** and **Google** to prominently label AI-generated content.

AI "**hallucinations**" pose a separate set of dangers. As people increasingly use chatbots rather than traditional search engines to answer their questions, they may seek out AI-generated information about how to vote, as well as about the legitimacy of election-related conspiracy theories. AI is not equipped to accurately answer these questions. Chatbots should make clear their limitations and redirect users to official, authoritative sources of election information.

Of course, AI threatens more than just our election offices. Generative AI can amplify efforts to suppress votes, libel candidates with deepfakes, incite violence, and pollute the information environment. These threats may disproportionately impact populations that are historically more vulnerable to misinformation because of issues with language proficiency, knowledge of American elections, and digital literacy. Here, too, AI developers and social media companies must work with civil society to invest in new defenses and expose **synthetic media** used to deceive the public.

As the ones responsible for unleashing and enabling these unprecedented threats to our democracy, tech companies — especially AI developers and social media platforms — must step up and play a leading role in keeping our elections secure.

David Evan Harris is chancellor's public scholar at UC Berkeley, senior research fellow at the International Computer Science Institute, visiting fellow at the Integrity Institute, senior advisor for AI ethics at the Psychology of Technology Institute, an affiliated scholar at the CITRIS Policy Lab, and a fellow at the Centre for International Governance Innovation. Lawrence Norden is senior director of the Brennan Center's Elections & Government Program.