Securing US Elections from Nation-State Adversaries

Written Testimony of Brad Smith
Vice Chair and President, Microsoft Corporation

U.S. Senate Select Committee on Intelligence

September 18, 2024

Chairman Warner, Vice Chairman Rubio, Members of the Committee, I appreciate the opportunity to join you and other technology leaders today to discuss the timely and critical issue of protecting US elections from nation-state interference.

Today we are 48 days away from the general election; in some states like Pennsylvania, voters have already begun casting ballots, and three days from now all 50 states will send ballots to military and overseas voters. The election is here, and our adversaries have wasted no time in attempting to interfere. Earlier this week, Microsoft's Threat Analysis Center (MTAC) reported efforts by our adversaries to interfere in our elections leveraging both old and new tactics. Earlier this month the United States Government sanctioned[1] Russian actors for their attempts to influence the election.[2]

The threats to our democracy from abroad are sophisticated and persistent. We must stand together as a tech community, as leaders, and as a nation to protect the integrity of our elections. We pursue this work guided by two key principles:

1. We must uphold the foundational principle of free expression for our citizens.
2. We must protect the American electorate from foreign nation-state cyber interference.

Our adversaries target our democracy in part because they fear the open and free expression it promotes and the success it has brought our country.

Current State of Nation-State Interference

Among Microsoft's vast team of security professionals, dozens are part of Microsoft's Threat Analysis Center (MTAC), a team whose mission is to detect, assess, and disrupt cyber influence threats to Microsoft, its customers, and democracies worldwide. Part of MTAC's mission is protecting elections from nation-state adversaries who seek to use online operations to distort the information going to voters, change the outcome of an election, or interfere in electoral processes.

As MTAC has observed and reported, foreign adversaries are using cyber influence operations to target both political parties in the 2024 U.S. presidential election. In the last two years, Microsoft has detected and analyzed cyber-attacks and cyber-enabled influence operations stemming from Russia, Iran, and China, many of which pertain to elections and elections infrastructure.

---

[1] Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations | U.S. Department of the Treasury

[2] Office of Public Affairs | Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere | United States Department of Justice

This follows similar activity Microsoft has observed in several other countries that recently have held national elections. This includes the 2023 elections in the Netherlands and Slovakia and, in 2024, the Taiwanese, EU, UK and French elections (as well as the 2024 Paris Summer Olympics). Since the beginning of this year, we have been working directly with elected government officials and often with the public to combat these threats. We have used our findings to better understand adversarial behavior and intentions leading into the upcoming 2024 U.S. election, including with respect to nation states' malicious employment of generative AI, of which we have detected and analyzed many such instances.

Today, we see Iran, Russia, and China using cyber operations to target the U.S. election in November. Iranian operations have targeted candidates of both parties but are inclined to denigrate former President Trump's campaign, which indicates a preference for a Harris victory. Russian operations, meanwhile, are inclined to denigrate Vice President Harris's campaign, indicating a preference for a Trump victory. China, for its part, has aimed to collect intelligence and to stoke discord, while to date not showing a clear preference for a specific candidate.

Let me share more about the details in what we have detected so far this year:

Iran

So far in 2024, Iranian election interference mirrors what we observed from Iran in 2020 in tempo, timing, and targets. As we reported in an August 8 report,[3] an Iranian actor we track as Sefid Flood, known for impersonating social and political activist groups, started in March to lay the groundwork for U.S. election cyber-enabled operations. Additionally, Iranian-linked covert propaganda sites and social media networks began and have continued to aim to amplify divisions among Americans across ethnic and religious lines.

In June 2024, Microsoft observed an Iranian actor tracked as Mint Sandstorm compromised a personal account linked to a U.S. political operative. Mint Sandstorm used this access to the political operative's account to conduct a spear phishing attack on a staff member at a U.S. presidential campaign. Microsoft products automatically detected and blocked this phishing email. Microsoft took additional steps to notify the political operative and the campaign of this activity. Last month, Microsoft detected that Mint Sandstorm compromised additional personal accounts belonging to individuals linked to a U.S. presidential candidate. Microsoft quickly took action to notify these users and assist them in securing their accounts. We expect the pace and persistence of Iran's cyberattacks and social media provocations will quicken as Election Day approaches in November.

Iran has a history of targeting voters in U.S. swing states. In 2020, an IRGC-directed group, Cotton Sandstorm, posed as the right-wing "Proud Boys" to stoke discord in the U.S. over purportedly fake votes. Using a Proud Boys-named email, Cotton Sandstorm sent emails to Florida residents warning them to "vote for Trump or else!"[1] Cotton Sandstorm's cyber activity ahead of the operation included scanning of at least one government organization in Florida.

In 2022, ahead of the midterm elections, Microsoft detected Mint Sandstorm targeting county-level government organizations in a few states, a pair of which were tightly contested states in 2020. Similarly, in 2024, we've observed another group operating on the IRGC's behalf, Peach Sandstorm, successfully access an account at a county government in a tightly contested swing state.

[3] Iran Targeting 2024 US Election - Microsoft On the Issues

We do not know if the IRGC's targeting of swing states in 2022 or 2024 was election related; in fact, Peach Sandstorm's targeting was part of a large-scale password spray operation. That said, Iran appears to have demonstrated an interest in U.S. swing states for potential follow-on operations similar to the one ahead of the 2020 elections that sought to sow discord on our electoral process.

Russia

Russian threat actors, the most notable adversary in previous U.S. election cycles, currently are spoofing reputable media outlets and distributing staged videos to spread the Kremlin's preferred messages to U.S. voters online. In some cases, these campaigns gain a significant number of views and sizeable reach among U.S. and international audiences.

For example, in early May, Microsoft observed a Russia-affiliated influence actor we track as Storm-1516 disseminate a staged video that claimed to show Ukrainian soldiers burning an effigy of former President Trump. The fake video received some international press, which inaccurately covered the video as genuinely originating from Ukraine. The video was reposted across social media and received several million impressions.

Later, after Vice President Harris joined the presidential race, our team saw Storm-1516 pivot its campaigns. In a second video staged in a Storm-1516 operation in late August, several people who are depicted as Harris supporters are shown assaulting an alleged supporter of former President Trump. This video received at least five million impressions. In a third staged video released earlier this month, Storm-1516 falsely claimed that Harris was involved in a hit-and-run incident. This video similarly gained significant engagement, the original video reportedly receiving more than two million views in the week following its release.[4]

We also anticipate that Russian cyber proxies, which disrupted U.S. election websites during the 2022 midterms,[5] may seek to use similar tactics on Election Day in November 2024. In addition to the Russian cyber proxy "RaHDit," which the U.S. State Department recently revealed as led by Russian intelligence,[6] Microsoft tracks nearly a dozen Russian cyber proxies that regularly use rudimentary cyberattacks to stoke fear in election and government security on social media.

In our August 9 elections report, we revealed a Russian actor that we track as Volga Flood (also known as Rybar) and their efforts to infiltrate U.S. audiences by posing as local activists.[7] Volga Flood created multiple social media accounts called "TexasvsUSA." The accounts post inflammatory content about immigration at the Southern border and call for mobilization and violence. This month, we've seen Volga Flood shift its focus to the Harris-Walz campaign, posting two deceptively edited videos of Vice President Harris on social media.

Volga Flood is publicly positioned as an anonymous military blogger covering the war in Ukraine. In reality, however, Volga Flood is a media enterprise employing dozens of people and headed by EU-sanctioned Russian national Mikhail Zvinchuk. Volga Flood's media enterprise is divided across multiple teams that include monitoring, regional analytics, illustration, video, foreign languages,

---

[4] https://uk.news.yahoo.com/russia-spread-fake-rumour-kamala-153333198.html

[5] https://www.usatoday.com/story/news/politics/elections/2022/11/08/2022-midterm-websites-mississippi-hit-cyber-attack/8308615001/

[6] https://www.state.gov/u-s-department-of-state-takes-actions-to-counter-russian-influence-and-interference-in-u-s-elections

[7] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf

and geospatial mapping—all to fulfill its mission statement of waging information warfare on behalf of the Kremlin. Volga Flood publishes analyses through dozens of social media brands and establishes and runs covert social media accounts.

Two additional Russian actors MTAC tracks have largely focused on European audiences but at times shift to U.S. electoral influence. Since March 2022, we have seen the Russian threat actor we track as Ruza Flood, known internationally as "Doppelganger," attempt to undermine U.S. politics. Ruza Flood receives significant resourcing and direction from the Russian Presidential Administration.[8] The U.S. Justice Department, in its September 4 announcements, revealed Ruza Flood's efforts to influence the U.S. citizenry through projects like the "Good Old USA Project," "The Guerilla Media Campaign," and the "U.S. Social Media Influencers Network Project."[9]

Finally, Storm-1679, a Russian influence actor previously focused on malign influence operations targeting the 2024 Paris Olympic Games, has recently shifted its focus to the U.S. presidential election.[10] Storm-1679 routinely creates videos masquerading as reputable news services or impersonating international intelligence agencies, including France's DGSI and the U.S.'s CIA. Storm-1679 recently pivoted to creating videos sowing conspiracies about Vice President Harris, which the actor distributes across a range of social media platforms.

Microsoft's current tracking of current Russian influence operations targeting elections extends beyond the U.S. presidential election. We are also seeing efforts to influence the upcoming Moldovan presidential election and EU referendum on October 20, 2024. In Moldova, a longstanding target of Russian strategic influence campaigns, we currently observe pro-Kremlin proxy activity aimed at achieving Moscow's goal of destabilizing democratic institutions and undermining pro-EU sentiment. We and others expect Russia will leverage an array of techniques in Moldova: political influence, electoral interference, cyberattacks, sabotage, and cyber-enabled influence campaigns that promote pro-Kremlin political parties and denigrate the current Moldovan leadership.

Microsoft is working in collaboration with the Moldovan government and others to assist in identifying and defending against Russian cyber and influence operations seeking to influence the outcome of these two elections.

China

Chinese actors' election efforts are more extensive in 2024 than in previous U.S. election cycles. We observe Chinese influence actors spreading politically charged content over covert social media networks, pretending to be U.S. voters and polling Americans on divisive social issues. Chinese actors have also posed as student protestors online, seeking to stoke division over conflict in the Middle East. These fake accounts—masquerading largely as U.S. conservative voters but also a handful of progressive personas as well—frequently ask their followers whether they agree with a political topic or political candidate. This tactic may be for reconnaissance purposes to better understand how Americans view nuanced political issues.

This messaging style may also be part of a broader engagement strategy: Over the past year, these China-linked personas have conducted more tailored audience engagement than observed

[8] https://www.justice.gov/opa/media/1366261/dl

[9] https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

[10] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

previously, replying to comments, tagging politicians and political commentators, and creating online groups with likeminded voters. Their content strategy has shifted as well. Rather than producing original infographics and memes that largely failed to resonate with U.S. voters in the past cycle, these personas are creating simple short-form videos taken and edited from mainstream news media. Clips denigrating the Biden administration have successfully reached hundreds of thousands of views.

In July 2024, Microsoft responded to a cyberattack on an organization supporting the upcoming U.S. presidential election. Microsoft worked to remediate and secure the organization's infrastructure. Subsequent investigation and analysis has attributed this attack to a state affiliated actor based in China.

These examples, as well as others, underscore the ways in which Iranian, Russian, and Chinese influence actors may seek in the next two months to use social divisions and digital technology to further divide Americans and sow discord ahead of this November's election. We also need to be vigilant in combatting the risk that nation-state adversaries will seek to conduct cyberattacks directly on key American entities that play critical roles in these elections. More information on these actors can be found in our most recent MTAC report.

Deceptive use of synthetic media (deepfakes)

AI is a tool among many tools that adversaries may opt to leverage as part of a broader cyber influence campaign. As we have navigated through the numerous global elections this year, the emergence of AI as a means for interference has presented itself so far this year as less impactful than many had feared. We recognize, however, that determined and advanced actors will continue to explore new tactics and techniques to target democratic countries, which will include additional and improved use of AI over time.

Though we have not, to date, seen impactful use of AI to influence or interfere in the U.S. election cycle, we do not know what is planned for the coming 48 days, and therefore we will continue to be vigilant in our protections and mitigations, against threats both traditional and novel.

As a leading technology company heavily invested in AI, we recognize our important responsibility to implement proactive measures to counter these risks. This includes developing robust frameworks for detecting and responding to deceptive AI election content, enhancing transparency within AI applications, and fostering international collaboration to protect the democratic process. The future of our elections depends on our collective ability to utilize AI responsibly and ethically.

In response to these challenges, we have taken significant steps, including joining together with twenty-seven of the world's largest technology companies this year to sign the Tech Accord to Combat Deceptive Use of AI in 2024 Elections.[11] This accord addresses abusive AI-generated content through eight specific commitments, categorized into three pillars: Addressing Deepfake Creation, Detecting and Responding to Deepfakes, and Transparency and Resilience. It represents one of the important steps the tech sector has taken this year to protect our elections, and we appreciate the encouragement and support of this Committee to be more proactive, including through Chairman Warner's presence and voice at the launch of this accord at the Munich Security Conference in February.

[11] AI Elections accord - A Tech accord to Combat Deceptive Use of AI in 2024 Elections

Here are some updates on how Microsoft is directly responding to these threats and upholding our joint commitments:

Addressing Deepfake Creation

We recognize that companies whose products are used to create AI generated content have a responsibility to ensure images and videos generated from their systems include indicators of their origin. One way to accomplish this is through content provenance, enabled by an open standard created by the Coalition for Content Provenance and Authenticity (C2PA).[12] Microsoft is a founding member of C2PA and has leveraged this standard ("content credentials") across several of our products, ensuring that AI generated content is marked and readable.

Specifically, Microsoft has added content credentials to all images created with our most popular consumer facing AI image generation tools, including Bing Image Creator, Microsoft Designer, Copilot, and in our enterprise API image generation tools via Azure OpenAI. We recently started testing a content credentials display in Word. When images with content credentials are inserted into Word documents, future viewers will be able to right click and see the credits and author information of these images. In addition, C2PA tagged content is starting to be automatically labeled on LinkedIn.[13] The first place you'll see the content credentials icon is on the LinkedIn feed, and we'll work to expand our coverage to additional surfaces.

As important as it is to mark content as AI generated, a healthy information ecosystem relies on other indicators of authenticity as well. This is why in April we announced[14] the creation of a pilot program that allows political campaigns in the U.S. and the EU, as well as elections authorities and select news media organizations globally, to access a tool that enables them to easily apply content provenance standards to their own authentic images and videos.

We also joined forces with fellow Tech Accord signatory, TruePic[15] to release an app that simplifies the process for participants in the pilot. This app has now launched for both Android and Apple devices and can be used by those enrolled in Content Credentials program.

Detecting and Responding to Deepfakes

Microsoft is harnessing the data science and technical capabilities of our AI for Good Lab and MTAC teams to better assess whether abusive content—including that created and disseminated by foreign actors—is synthetic or not. Microsoft's AI for Good lab has developed and is using detection models (image, video) to assess whether media was generated or manipulated by AI. The model is trained on approximately 200,000 examples of AI and real content. The Lab continues to invest in creating sample datasets representing the latest generative AI technology. When appropriate, we call on the expertise of Microsoft's Digital Crimes Unit to operationalize the early detection of AI-powered criminal activity and respond fittingly, including through the filing of affirmative civil actions to disrupt and deter that activity and through threat intelligence programs and data sharing with customers and governments.

[12] Overview - C2PA
[13] (1) LinkedIn Adopts C2PA Standard | LinkedIn
[14] Expanding our Content Integrity tools to support global elections - Microsoft On the Issues
[15] Truepic's Secure Camera Enhances Microsoft's Content Integrity Tools - Truepic

To build on the work of our AI for Good lab, in April we announced[16] that we were joining up with AI researcher, Oren Etzioni[17] and his new non-profit, True Media.[18] True Media provides governments, civil society and journalists with access to free tools that enable them to check whether an image or video was AI generated and/or manipulated. Microsoft's contribution includes providing True Media with access to Microsoft classifiers, tools, personnel, and data. These contributions will enable True Media to train AI detection models, share relevant data, evaluate and refine new detection models as well as provide feedback on quality and classification methodologies.

We are also empowering candidates, campaigns and election authorities to help us detect and respond to deceptive AI that is targeting elections. In February we launched the Microsoft-2024 Elections site[19] where candidates in a national or federal election can directly report deceptive AI election content on Microsoft consumer services. This reporting tool allows for 24/7 reporting by impacted election entities who have been targeted by deceptive AI found on Microsoft platforms.

Transparency and Resilience

In advance of the EU elections this summer, we kicked off a global effort to engage campaigns and elections authorities. This enabled us to deepen understanding of the possible risks of deceptive AI in elections and empower those campaigns and election officials to speak directly to their voters about these risks and the steps they can take to build resilience and increase confidence in the election. So far this year we have conducted more than 150 training sessions for political stakeholders in 23 countries, reaching more than 4,700 participants. This included training and public educations sessions at the Republican and Democratic National Conventions, as well as with state party chairpersons for both major political parties in the United States.

Building on this training, Microsoft also ran public awareness campaigns in the EU ahead of the EU Parliamentary elections,[20] as well as in France[21] and the UK[22] ahead of their national elections. We are now pursuing similar work in the United States ahead of the November general election. This campaign, which is entitled "Check, Recheck, Vote," educates voters of the possible risks posed by deepfakes and empowers them to take steps to identify trusted sources of election information, look for indicators of trust like content provenance, and pause before they link to or share election content. This includes our 'Real or Not?' Quiz, developed by our AI for Good lab to expose users to the challenges of detecting a possible deepfake. So far, individuals from 177 countries have taken the quiz.

Overall, our public awareness campaigns outside the United States have reached more than 350 million people, driving almost three million engagements worldwide. Our U.S. Public Awareness campaign[23] has just begun and already has reached over six million people with over 30,000 engagements.

---

[16] TrueMedia.org to Enhance Deepfake Detection Capabilities · TrueMedia
[17] An A.I. Researcher Takes On Election Deepfakes - The New York Times (nytimes.com)
[18] TrueMedia.org
[19] Microsoft-2024 Elections
[20] Addressing the deepfake challenge ahead of the European elections - EU Policy Blog (microsoft.com)
[21] Microsoft s'engage dans la préservation de la sincérité des élections législatives en France – News Centre
[22] Combating the deceptive use of AI in elections (microsoft.com)
[23] Combating the deceptive use of AI in US elections (microsoft.com)

In May, we announced a series of societal resilience grants in partnership with OpenAI.[24] Grants delivered from the partnership have equipped several organizations, including Older Adults Technology Services (OATS) from AARP, International Institute for Democracy and Electoral Assistance (International IDEA), C2PA, and Partnership on AI (PAI) to deliver AI education and trainings that illuminate the potential of AI while also teaching how to use AI safely and mitigate against the harms of deceptive AI-content.

Protecting Campaign and Election Infrastructure

Since the 2016 election, adversaries have regularly targeted essential systems that support elections and campaigns in the U.S. to advance their cyber enabled influence operations. As mentioned earlier, recent Iranian hacking incidents involved attempts by these actors to provide stolen or allegedly stolen material to the media to propagate narratives of dissent and distrust. This underscores why we continue to invest in efforts that focus on safeguarding the critical infrastructure that underpins our elections.

Our efforts include several initiatives designed to support election officials and political organizations. First, we offer AccountGuard, a no-cost cybersecurity service available to our cloud email customers in 35 countries. This service provides advanced threat detection and notifications against nation-state adversaries for high-risk customers, including those involved in elections. AccountGuard extends beyond commercial customers to individuals at election organizations, their affiliates, and immediate family members who may use personal Microsoft accounts for email. We have observed that sophisticated adversaries often target both professional and personal accounts, amplifying the need for comprehensive protection. More than 5.4 million mailboxes of high-risk users are now protected by AccountGuard globally.

Additionally, our Election Security Advisors program provides federal political campaigns and state election departments with expert security consultation. This includes proactive security assessments or forensic investigations in the event of a cyber incident. Our goal is to ensure that these entities have the necessary support to maintain the integrity of their operations.

For critical election-adjacent systems, such as voter registration databases and voter information portals, we provide our Azure for Election service. This service provides proactive security reviews, resilience assessments, and load analysis. During the election week, we offer our highest tier of reactive support to address any security or availability issues that may arise. Since offering this service from 2018 to today, we have assisted more than half of U.S. states, including many counties and cities, in reviewing their election IT infrastructure.

In preparation for the election this November, we are also establishing a situation room staffed by our team to provide constant management and triage of any election-sensitive issues and maintain real-time communications with other situations rooms across our industry partners. This ensures that any incidents receive the highest level of priority and executive support.

While we continue to provide robust security services, we recognize that collaboration is essential. Public-private partnerships are crucial in strengthening the entire ecosystem. Our Democracy Forward team actively participates in tabletop cybersecurity training exercises with U.S. election officials at both national and state/county levels.

[24] Microsoft and OpenAI launch Societal Resilience Fund - Microsoft On the Issues

Microsoft remains steadfast in its commitment to supporting the security and integrity of democratic processes. Through our comprehensive programs and collaborative efforts, we aim to protect democracy from the evolving threats posed by nation-state actors.

Policy Recommendations

Finally, we find ourselves at a moment in history when anyone with access to the Internet can use AI tools to create a highly realistic piece of synthetic media that can be used to deceive: a voice clone of a family member, a deepfake image of a political candidate, or even a doctored government document. AI has made manipulating media significantly easier, quicker, more accessible, and requiring little skill. As swiftly as AI technology has become a tool, it has become a weapon.

I want to acknowledge and thank this Committee for its longstanding leadership on these important issues. We particularly commend the efforts reflected in section 511 of the SSCI FY 25 Intelligence Authorization Act (IAA), which focuses on protecting technological measures designed to verify the authenticity and provenance of machine-manipulated media. These protections are essential as technology companies strive to provide users with reliable information about the origins of AI generated content.

We are also encouraged and supportive of the recent agreement by the Federal Election Commission (FEC)[25] applying existing restrictions regarding fraudulent misrepresentation to campaigns use of AI technology. Existing robocall provisions are another means of addressing the fraudulent use of synthetic content. These provisions have historically restricted the use of artificial or prerecorded voices and allow for enforcement actions when these rules are violated.

Along those lines, it is worth mentioning three ideas that may have an outsized impact in the future fights against deceptive and abusive AI-generated content.

- First, Congress should enact a new federal "deepfake fraud statute." We need to give law enforcement officials, including state attorneys general, a standalone legal framework to prosecute AI-generated fraud and scams as they proliferate in speed and complexity.
- Second, Congress should require AI system providers to use state-of-the-art provenance tooling to label synthetic content. This is essential to build trust in the information ecosystem and will help the public better understand whether content is AI-generated or manipulated.
- Third, Congress should pass the bipartisan Protect Elections from Deceptive AI Act, sponsored by Senators Klobuchar, Hawley, Coons, and Collins. This important piece of legislation prohibits the use of AI to generate materially deceptive content falsely depicting federal candidates in political ads to influence federal elections, with important exceptions for parody, satire, and the use of AI-generated content by newsrooms. Such legislation is needed to ensure that bad actors cannot exploit ambiguities in current law to create and distribute deceptive content, and to ensure that candidates for federal office have meaningful recourse if they are the victim of such attacks. Several states have proposed or passed legislation similar to this federal proposal. While the language in these bills varies, we recommend states adopt prohibitions or disclosure requirements on "materially deceptive" AI-generated ads or something akin to that language and that the bills contain exceptions for First Amendment purposes.

[25] showpdf.htm (fec.gov)

Conclusion

In conclusion, we recognize that the protection of electoral integrity and public trust is a shared responsibility and a common good that transcends partisan interests and national borders.

This must be our guiding principle.

Looking ahead, we believe that new forms of multistakeholder action are essential. Initiatives like the Paris Call and Christchurch Call have demonstrated positive global impacts by uniting representatives from governments, the tech sector, and civil society. In addressing the challenges posed by deepfakes and other technological issues, it is evident that no single sector of society can solve these complex problems in isolation. Collaboration is crucial to preserving our timeless values and democratic principles amidst rapid technological change.

Thank you for your time and consideration. I look forward to answering any questions you may have.