PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 128 (2436), 2 SEPTEMBER 2024 © PISM

BULLETIN

Russia and Iran Interfering in U.S. Presidential Election

Filip Bryjka

Russia and Iran are conducting social media influence operations to shape Americans' voting attitudes in the upcoming presidential election. Russian interference poses the greatest threat. Iran's growing activity in this area poses an additional challenge to the U.S. security services. While the authoritarian regimes' goal in common is to undermine the credibility of democratic institutions and deepen political polarisation in the U.S., they differ on their preferred candidates. While Russia supports Donald Trump, Iran's goal is to prevent his re-election.

Representatives of the intelligence services and the U.S. administration warn that both Russia and Iran are attempting to influence the outcome of the November presidential election. The authoritarian regimes are using, among other things, hacking groups and a specially prepared internet infrastructure to do so. To influence audiences more effectively, they use artificial intelligence (AI) and the services of specialised political marketing, communications, and public relations companies. To date, China's involvement is minor, limited to undermining U.S. democracy and international standing.

Objectives and Methods of Russian interference—Trump 2.0. Just as it did during the 2016 and 2020 elections, Russia is supporting Trump's candidacy, hoping that his unpredictability and transactional approach to international politics will allow Russia to impose peace on Ukraine on Russia's preferred terms. Trump's controversial statements about the cost of supporting Ukraine, his boast that he can ensure peace within 48 hours of becoming president, and his questioning NATO's existence lead to such calculations. His re-election is therefore considered more favourable to Russian interests than a victory for Kamala Harris, who announced continued support for Ukraine.

To promote its specific narratives and spread conspiracy theories, Russia is increasingly using artificial intelligence (AI), hacking groups (including Ruza Flood/Doppelganger, Storm-1516, Storm-1841/Rybar), and infrastructure prepared for influence operations. The disinformation detection and analysis company Newsguard has identified 170 fake websites impersonating (or completely faking) local U.S. newspapers, some with names that seem real (e.g., *Houston Post*, *Chicago Crier*, *Boston Times*, *DC Weekly*, etc.). They are created by Russian operatives employing "information laundering" to attribute false information to a source that seems credible. The authors of the texts are rarely real journalists but who sometimes use photographs of real people. To increase the credibility of such manipulated content, YouTube videos are created in which alleged informants or whistleblowers reassure viewers of the credibility of the sensational information. Fake documents are also created, such as an invoice purporting to show that the Ukrainian president's wife bought a luxury car with U.S. military aid. In this way, Russia seeks to influence both the electoral attitudes of Americans and to undermine their support for U.S. support for Ukraine.

At the same time, real events or stories are manipulated using AI-based tools that present them with a particular (conservative) position. They are also often based on conspiracy theories, which are prevalent among about 25% of the Republican electorate (PRRI study 2022). Examples include various interpretations of the Trump assassination attempt or false information about the FBI wiretapping his Florida residence. These fit with the narratives promulgated by the former president himself, who consistently attempts to undermine the integrity of the U.S. justice system with claims there is a conspiracy to prevent his re-election.

So far, there have been no major cyberattacks on the parties or process (e.g., on Democratic staff) or hack-and-leak operations (which involve stealing and making public correspondence or documents denigrating an individual or political party) such as those used by Russian intelligence services in previous years. These activities helped Trump win the 2016 election, as revealed by the special prosecutor's investigation (Muller report). That information led the U.S. Department of Justice to indict 12 individuals working for the 85th Special Communications Centre (Unit 26165) and cyber unit No 74455 of the Russian military intelligence service GRU.

Objectives and Methods of Iranian Interference—No to Trump. Iran, like Russia, is fuelling internal divisions in the U.S. and undermining Americans' trust in public institutions. Unlike Russia, however, Iran's goal is to prevent Trump's re-election. The balance of his term (2016-2020) is viewed negatively by the Iranians. During this period, the U.S. withdrew from the nuclear agreement with Iran (JCPOA), provocatively recognised Jerusalem as the official capital of Israel, and killed in Iraq the Iranian Gen. Qasem Soleimani, the commander of the Islamic Revolutionary Guards Corps (IRGC). Trump's victory in November could mean support for Benjamin Natanyahu's policies against Iran and the armed groups it supports (Hamas, Hezbollah, Houthi, and others). Harris, on the other hand, as a more left-wing politician than even President Joe Biden, may seek to balance the U.S. approach to Israel and the war against Hamas, which is in Iran's interest.

Iran's methods of interfering in the U.S. electoral process have not changed since 2020 when it launched a number of cyber-influence operations to sow discord in society and incite violence against U.S. government officials. Two Iranian hackers were convicted in 2021 for spreading the content of the far-right group the Proud Boys and sending email threats against politicians in the U.S.

As part of its ongoing influence operations, Iran uses hacking groups (e.g., Sefid Flood, APT-42/Mint Sandstorm, APT-33/Peach Sandstorm). Using the "phishing" method, they attempt to access the email inboxes and social media accounts of politicians to steal and then make public sensitive information (hack-and-leak). These groups are also involved in spreading manipulated and false information through the Storm-2035 network of fake websites (e.g., Nio Thinker, *Savannah Time*), "troll" farms, and bots. Like Russia, Iran uses AI to manipulate information, transforming real articles into content with specific theses and narratives to influence the target audience. AI tools are also used to create fake images and videos ("deep fakes") that are increasingly difficult for ordinary audiences to detect, increasing the effectiveness of the manipulation and attempts to misinform. These activities are conducted around issues that polarise American society, such as LGBTQ+ rights, racial tensions, and the Israeli-Palestinian conflict, among others. According to a Microsoft Threat Analysis Center (MTAC) investigation, through fake activist profiles and covert funding, Iran (with the help of Chinese hacking groups) helped stoke the pro-Palestinian protests at U.S. universities that erupted against Israel's military operation in Gaza. In mid-August in a joint statement, the Federal Bureau of Investigation (FBI), the Office of the Director of National Intelligence (ODNI), and the Cybersecurity and Infrastructure Security Agency (CISA) accused Iran of sowing discord.

Conclusions and Outlook. Although Russia and Iran have conflicting candidate preferences, and Russian interference in the election is much more extensive and sophisticated, the effect of both countries' actions is to deepen internal divisions in the U.S., spread chaos, and undermine trust in U.S. state institutions. We should expect Russian and Iranian information operations to intensify in the coming weeks as they spread false stories and try to impose a narrative designed to support or denigrate their preferred candidate. In doing so, Russia may put pressure on Iran to cease or limit activities that could damage Trump's image. In the run-up to the vote, hackers may launch cyberattacks on electoral infrastructure (e.g., voter registries). In the event of their preferred candidate is defeated, Russia or Iran may launch a disinformation campaign aimed at undermining the legitimacy of the election, with the aim of sowing chaos (including pressure for riots along the lines of the 2020 Capitol Hill attack).

Effectiveness in countering foreign information manipulation and interference (FIMI) could be enhanced by closer cooperation between the U.S. and the EU, as well as in a bilateral format between the U.S. and EU countries. Information-sharing broadens situational awareness (e.g., in identifying infrastructure used for influence operations), which would allow for a more rapid response. U.S. government agencies could also play an important role in pressuring (mostly U.S.) online platforms to detect and remove harmful content, as well as in responding to reported incidents.