

Analysis of Recent Disinformation Campaigns Linked to Russian IRA Successors

Summary:

This report provides an analysis of emerging disinformation campaigns, particularly focusing on websites such as the Miami Chronicle (miamichron.com) and Chicago Chronicle (chicagochron.com), which have been identified as platforms for disseminating misleading narratives and Kremlin-aligned propaganda in the United States. Initial investigations have revealed connections to Russian operatives, suggesting a strategic attempt to influence U.S. public discourse and political events. This assessment incorporates a technical examination of the websites involved, revealing insights into the operation's structure and potential affiliations with known Russian entities.

Key Findings:

There Are Numerous Other Domains Created: The actors have a constellation of sites out on the internet today that are functional and likely more domains in the wings waiting to be activated, however, since the reporting in the news, and this report, these domains and sites have started to be taken down by domain registrars and are thereby burned assets. The group will have to change their operations and tempo to re-constitute their campaigns.

Origin and Operation of Disinformation Sites: Investigations have identified several fake news sites, including the Miami Chronicle and Chicago Chronicle, which blend authentic content with fabricated narratives. These sites are part of a broader disinformation effort, with ties traced back to Russia, aiming to impact U.S. political dynamics. Notably, these platforms utilize basic web design elements and lack distinctive authorship, suggesting a low-budget operation aimed at broad dissemination of disinformation.

Connection to Russian Entities: The operation is assessed with medium to high certainty to be an offshoot of the Internet Research Agency (IRA), historically linked to Yevgeny Prigozhin. Ownership is attributed to **Alexander Sergeevich Frolov**, a figure noted in the Panama Papers and associated with the Russian oligarchy. Daily operations are managed by **Mikhail Leonidovich Burchik**, a sanctioned individual with a history of involvement in IRA activities.

Bios:

Frolov:

Aleksandr Vladimirovich Frolov, born May 17, 1964, served as the CEO of Evraz from 2007 to 2021, making significant contributions to the steel industry and leading the company to become Russia's largest producer of coking coal. His educational background includes graduating with honors from the Department of Molecular and Chemical Physics at the Moscow Institute of Physics and Technology in 1987 and earning a Ph.D. in physics and mathematics. Frolov has faced UK government sanctions in 2022 related to the Russo-Ukrainian War. Forbes listed his net worth at \$2.6 billion as of August 2022.

Burchik:

Mikhail Leonidovich Burchik, born on June 7, 1986, in Saint Petersburg, Russia, is associated with the Internet Research Agency (IRA), a group involved in online propaganda and influence operations. He has been under sanctions by various entities, including the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury, for his role in activities aimed at interfering in the U.S. 2016 elections and conducting malicious cyber-attacks. Burchik's involvement with the IRA highlights his significant position within the organization, which has been implicated in widespread efforts to manipulate public opinion and political processes.

Technical Analysis and Tradecraft Failures: A notable tradecraft failure was identified in the misuse of a common email address across multiple disinformation sites (@thezeeworldnews.com). This oversight facilitated the linkage of these sites to a broader network operated by Technologies LLC Business Media, a company owned by Frolov, with Burchik serving as the CEO. This connection underscores the continued involvement of Russian operatives in disinformation campaigns targeting the U.S.

Financial Overview: Technologies LLC Business Media, the entity behind these operations, reported a revenue of 32.1 million rubles for 2022, with a profit of 1.4 million rubles. The findings indicate a modest financial base for the disinformation efforts, suggesting a focus on operational efficiency and impact.

Conclusion:

The analysis confirms the existence of a coordinated disinformation campaign linked to Russian entities, aimed at influencing U.S. public opinion and political processes. The identified websites serve as platforms for spreading fabricated narratives, with technical and operational strategies designed to obfuscate their origins. This operation reflects an evolution in digital disinformation tactics, leveraging online platforms to reach targeted audiences. The involvement of figures with known connections to Russian oligarchies and previous disinformation efforts highlights the persistent threat posed by state-aligned actors in the cyber domain. Further monitoring and analysis of related sites and activities are recommended to understand the full scope and impact of these campaigns.