The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Facebook Just Can’t Seem to Beat the Russians

Social media companies' defenses are routinely bypassed by an entire manipulation industry, largely based in Russia.

By Leonid Bershidsky

December 06, 2019

PA Images / TASS

Social media companies insist they’re making progress in fighting the manipulation of their platforms. But two researchers, working on an extremely modest budget, have just shown that their defenses are routinely bypassed by an entire manipulation industry, largely based in Russia.

In a report for NATO’s Strategic Communications Center of Excellence, Sebastian Bay and Rolf Fredheim described an experiment they ran between May and August. In the first two months, during and just after the European Parliament election campaign, they hired 11 Russian and five European “manipulation service providers,” who they found simply by searching the

web. The companies then delivered 3,530 comments, 25,750 likes, 20,000 views and 5,100 followers on Facebook, Twitter, Instagram and YouTube — all fake.

Given how serious the social media platforms claim to be about purging inauthentic activity, the experiment's success rate was stunning. Four weeks after they were posted, a vast majority of the fake engagements were still live; even reporting them to the platforms didn't get most removed.

Related article: Russian Media Ordered to Delete Protest Videos Over 'Extremist' YouTube Comments

The study reveals a major weakness in the way the social media giants report their anti-fraud efforts. Facebook has a lot to say about how much content it removes, for instance, but that's like the mayor of a town reporting that 50% of its roads are now pothole-free: You never know which 50%. The important metric is how much manipulative content gets through. Bay and Fredheim found that, once professionals get involved, most of their work sticks, to the extent that they often deliver more engagements than promised for the money. Defenses only work on the most basic level. The pros are always a step ahead.

NATO, of course, is mostly interested in political manipulation, and the researchers found that some of the same accounts that helped carry out their study "had been used to buy engagement on 721 political pages and 52 government pages, including the official accounts of two presidents, the official page of a European political party, and a number of junior and local politicians in Europe and the United States."

An important question is whether such efforts actually work. One recent paper tried to determine what effect the Russian troll farm known as the Internet Research Agency has had on U.S. political attitudes. The IRA, whose employees and owner were indicted in special counsel Robert Mueller's investigation into meddling in the 2016 election, used some of the same techniques as the NATO Stratcom researchers. But, the paper said, their fake accounts were effectively preaching to the converted. Even for users who directly interacted with the IRA accounts, the researchers found "no substantial effects" on their political opinions, engagement with politics or attitudes toward members of the opposing party.

This doesn't mean social-network manipulation is ineffective for political purposes; much more research would be needed to draw any sweeping conclusions. What's clear now, though, is that the manipulation industry isn't primarily geared toward political uses. Bay and Fredheim found that "more than 90% of purchased engagements on social media are used for commercial purposes." Even though it's Russian-based, this industry isn't about evil Kremlin masterminds trying to turn technology against American democracy. Rather, it's about talented Russian engineers, stuck in the wrong country for launching grand commercial ventures like Facebook or YouTube, trying to make money by milking the existing platforms.

Related article: Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels, Researchers Say

What that usually amounts to is helping online "influencers" cheat advertisers. The

abysmally low removal rates for fake video views in the Stratcom experiment show the platforms aren't fighting such abuses hard enough. They don't have to: They're still essentially black boxes from an advertising client's point of view. As a result, perhaps billions of dollars (estimates vary wildly) are lost to such fraud each year.

Platforms have spent enough time trying, and failing, to prove that self-regulation can work for them. Governments should act to protect not so much voters as advertisers from the manipulation industry, penalizing social-media companies for their inability to prevent fraud and demanding more transparency. Now, as Bay and Fredheim wrote, "data is becoming scarcer and our opportunities to research this field is constantly shrinking. This effectively transfers the ability to understand what is happening on the platforms to social media companies. Independent and well-resourced oversight is needed."

Policy makers need to realize that the platform-manipulation industry doesn't thrive because it's a Kremlin weapon. Political weaponization is only a side effect of a parasitic industry built on the flaws of the social media business model. It's the model that needs to be regulated.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2019/12/06/facebook-just-cant-seem-to-beat-the-russians-a68512