Exposure, Enforcement, and Then What? How Information Operations Actors Use Persistence Mechanisms to Adapt After Campaign Exposure

Sam Riddell, Ron Graf, and Lee Foster

Exposure, attribution, and enforcement are often thought of as the final steps in the chain of defense against disinformation and information operations (IO). This ignores the fact that IO actors, diverse in their resourcing, sophistication, and motivations, have a say in what happens next. After public exposure, IO actors react in vastly different ways. Some immediately close up shop or ignore exposure entirely, while others adopt persistence mechanisms to circumvent the enforcement actions taken against them and continue operating. In this paper we recommend anchoring enforcement policy in the study of how and when various actors leverage persistence mechanisms to circumvent social media bans, evade monitoring, revive networks, build audiences while under scrutiny, and otherwise react to exposure, attribution, and enforcement. Our analysis explores three reported state-backed information operations in which the responsible actors adapted persistence mechanisms to continue their campaigns after public exposure and is informed by tactical observations gleaned through tracking nation-state and commercial IO actors as part of FireEye's Mandiant's Information Operations Analysis team. Our analysis suggests that current enforcement policies are insufficient at deterring and permanently disrupting IO campaigns.

Persistence Mechanisms in the Information Operations Context

In traditional cyber threat parlance, persistence mechanisms typically refer to actions taken by a threat actor to maintain access to a victim's systems, either pre-emptively, or after the victim has tried to remove the attacker's malware or expel them from a network. Here, we use the concept of persistence mechanisms in the disinformation context to describe steps taken by IO actors to avoid detection, circumvent social media platform and government enforcement measures, and to continue to reach their target audiences despite public exposure. Examples of persistence mechanisms include changing domain infrastructure, switching social media platforms, and implementation of account-level obfuscation. Public messaging from actors can also be considered a persistence mechanism. For instance, actors may issue statements denying attribution or providing alternate explanations for their behavior to their target audiences. Our analysis here explores three case studies in which suspected state-backed IO actors used different persistence mechanisms to continue pushing disinformation to target audiences following their public exposure.

Case Study #1: Enemies of the People (Reported Iran-backed Actors)

In December 2020, multiple domains and social media assets using the moniker "Enemies of the People" disseminated personally identifiable information (PII) belonging to U.S. government officials and other individuals involved in the administration of the 2020 presidential election. In a press release, the FBI attributed this coordinated effort to discredit the election results and threaten election officials to "Iranian cyber actors." Following this attribution and the suspension of EOTP websites[1] and related social media assets on multiple social media platforms, we believe this activity set, which we refer to here as Enemies of the People 1 (EOTP 1), adapted and reappeared in January 2021 with new assets, dissemination tactics, and infrastructure.

Persistence Strategy: Denial, Obfuscation, and Audience Building from the Shadows

In January, a new "Enemies of the People" website emerged explicitly claiming to be a reincarnation of the previous, then-removed website. We subsequently identified new inauthentic social media assets that we assess with moderate confidence comprised an effort centered around this new website to revive the original campaign. We refer to this activity set as Enemies of the People 2 (EOTP 2).

Through a statement published on the home page of the EOTP 2 website, the actors directly rejected the FBI's Iran attribution, claiming to be "American patriots". The actors made several changes between EOTP 1 and EOTP 2, seemingly to maintain persistence in anticipation of further U.S. government and private sector enforcement. The EOTP 2 site featured solicitations for donations to a bitcoin wallet, possibly a false flag attempt at posing as a financially motivated actor rather than a state-backed one. Unlike EOTP 1, the EOTP 2 webpage was not hosted directly on a domain. Instead, the operators primarily used coordinated, inauthentic social media assets to disseminate short links to the website, which was hosted directly on two actor-controlled IPs and a Tor web proxy rather than linked to a domain name. EOTP 2 actors reportedly[2] also threatened "the lives of US federal, state, and private sector officials using direct email and text messaging".

[1] https://www.ic3.gov/Media/Y2021/PSA210115
[2] https://www.ic3.gov/Media/Y2021/PSA210115

The actors' social media dissemination strategy appears to have shifted from overt promotion by self-affiliating social media assets to masked promotion via short links using covert, inauthentic accounts posing as real individuals. EOTP 1 social media assets explicitly listed their affiliations to the EOTP 1 website and linked to the domain. In contrast, the actors behind EOTP 2 did not create any overtly affiliated social media accounts and instead relied on inauthentic personas on various platforms to disseminate links to the new site. EOTP 2 assets used more abstract handles than those leveraged in EOTP 1, avoiding direct mention of EOTP, perhaps to evade automated detection.

Case Study #2: News Front (Reported Russian Federal Security Service)

News Front is a prolific pro-Russian media outlet based in Crimea. Since its founding in 2014, the site has leveraged a multitude of domains and social media accounts to disseminate pro-Russian-interest narratives to global audiences in several languages. On May 5, 2020, Facebook removed[3] a total of 140 assets they linked to News Front and the FSB-linked[4] disinformation site South Front, claiming the actors behind the sites used "fake accounts to post their content and manage Groups and Pages posing as independent news entities in the regions they targeted." Also on May 5, researchers at the Atlantic Council's DFRLab wrote a report[5] accompanying Facebook's takedown which detailed specific instances of inauthentic promotion of News Front content by those social media assets. Dozens of News Front-related accounts and pages have been suspended by other social media platforms as well. A report[6] on Russian disinformation tactics published by the US State Department's Global Engagement Center (GEC) in August 2020 profiled News Front, labeling it a "proxy site…with reported ties to the Russian security services and Kremlin funding." Most recently, sanctions announced by the U.S. Department of Treasury on April 15, 2021, officially alleged coordination between News Front and the Russian Federal Security Service (FSB)[7].

Persistence Strategy: Cloaking Domains, Covert Promotion

[3] https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf
[4] https://home.treasury.gov/news/press-releases/jy0126
[5] https://medium.com/dfrlab/facebook-removes-propaganda-outlets-linked-to-russian-security-services-51fbe2f6b841
[6] https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
[7] https://home.treasury.gov/news/press-releases/jy0126

By the Fall of 2020, the United States government had publicly accused News Front of being a Russian proxy site, several major U.S. social media platforms had removed News Front accounts on their respective platforms, likely also restricting the sharing of links to News Front domains, and researchers had publicly written about portions of News Front's inauthentic activity on social media. Undeterred, News Front employed persistence measures to continue its operations. To circumvent platform enforcement and public exposure, News Front created what the German Marshall Fund's Alliance for Securing Democracy (ASD) first referred[8] to as eight "mirror sites" – domains which hosted News Front content on separate URLs that did not disclose their ties to News Front. The Institute for Strategic Dialogue reported[9] on two of those sites in February 2021, referring to them as "cloaking domains". In March of 2021, we identified and reported on nine additional cloaking domains presenting as independent news sites but serving as mirror websites for News Front domains. Each website corresponded to a different language edition of News Front, featuring simple black-and-white home pages with no mention of News Front, but which exclusively published identical copies of News Front articles in the nine languages. These sites redirected visitors to pages resembling identical versions of News Front, featuring News Front logos and branding, but which maintained URLs on the cloaking domains. We judged that these nine websites, along with the eight then-inactive sites identified by ASD, comprised part of the same coordinated network based on technical and behavioral indicators.

A mix of social media assets and accounts we assessed with low confidence to be inauthentic, as well as accounts we believe belonged to genuine News Front employees, systematically disseminated links to the News Front articles hosted on the cloaking domains to various social media audiences. For instance, links to the French-language News Front mirror domain FrenchNews[.]info were published at high volume by multiple suspected inauthentic social media assets. We observed similar activity for several of the other mirror sites in various languages. The participation of real individuals, including those with identifiable ties to News Front, suggests News Front had direct knowledge of and participated in the dissemination of News Front content via these "cloaking" domains.

[8] https://securingdemocracy.gmfus.org/russias-affront-on-the-news-how-newsfronts-persistence-past-social-media-bans-demonstrates-the-need-for-vigilance/

[9] https://www.isdglobal.org/wp-content/uploads/2021/02/20210202-ISD-US-Crimean-Connection-V3.pdf

Case Study #3: Newsroom for American and European Based Citizens (Reported Russian Internet Research Agency-Linked)

In June 2020, an inauthentic politically right-leaning outlet referring to itself as the "Newsroom for American and European Based Citizens" (NAEBC) began publishing controversial articles on U.S. politics. In the months leading up to the 2020 presidential election, social media accounts officially affiliated with NAEBC and at least five social media personas posing as editors, authors, and contributors of NAEBC published and shared divisive content related to U.S. politics, and successfully recruited unwitting Americans to write opinion pieces for the outlet.

On October 1, 2020, *Reuters*[10] and Graphika[11] reported that, according to the Federal Bureau of Investigation (FBI), NAEBC was run by individuals associated with the Russian Internet Research Agency (IRA)- the infamous state-linked[12] troll farm which engaged in interference efforts targeting the 2016 U.S. election. By that time, Facebook, Twitter, and LinkedIn had reportedly already removed assets linked to NAEBC's operation.[13] The platforms Gab and Parler did not take action against NAEBC assets. Gab CEO Andrew Torba stated, "It's irrelevant to us who runs it or why."

Persistence Strategy: Ignore and Press On

We have continued to monitor NAEBC's activity since its public exposure. While we have not observed further attempts from the actors to re-establish a presence on the platforms from which NAEBC assets had been removed, we have observed that NAEBC assets have remained active on Gab and Parler. These accounts largely ignored their public attribution and have continued attempts to drive Gab and Parler users to articles published on the NAEBC domain. These personas did take limited steps to mask their inauthenticity; for instance, the profile photos of some of accounts were changed, and references to NAEBC in the accounts' bios were mostly removed. One identified persona and purported editor of the NAEBC site, "Nora Berka", responded to a Reuters request for comment on the alleged ties between NAEBC and Russia saying, "I have no idea what does NAEBC have to do with it."

[10] https://www.reuters.com/article/us-usa-election-russia-disinformation-ex-idUSKBN26M5ND
[11] https://graphika.com/reports/step-into-my-parler/)
[12] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf
[13] https://www.reuters.com/article/us-usa-election-russia-disinformation-ex-idUSKBN26M5ND

In the two weeks following the Oct. 1 exposure, over 30 additional articles were published to the NAEBC domain - the vast majority of which pertained to U.S. politics and promoted far-right viewpoints. On Oct. 7, the site published an original article from author "Kris Stark" that defended NAEBC and its left-leaning counterpart, a site called Peace Data that was also similarly exposed[14] as being tied to individuals associated with Russia's Internet Research Agency, against allegations that the two outlets were Russian operations – the closest NAEBC came to directly acknowledging their exposure. In the article, "Stark" claimed they were paid $75 USD to write for NAEBC, stating, "Besides, even if I'm writing for a 'St. Petersburg-based Internet Research Agency,' so what? I'm having my voice, facts and opinions heard by thousands of other American Patriots. So, thank you to Russia for paying me $75 to have my logical and rational views heard…"

Lessons Learned:

In all three case studies, the reported state-backed actors behind these high-profile disinformation campaigns adopted varying persistence mechanisms to continue their activity after public exposure and platform enforcement, demonstrating that the deterrent and disruptive efficacy of exposure, attribution, and enforcement can be limited in the disinformation domain. The persistence mechanisms detailed here are by no means comprehensive and we hope that this conceptualization can provide a useful framework for categorizing existing and new mechanisms as they are observed. During our analysis, we identified several research questions for further study: Do a target audience's political leanings or perceived receptivity to continued operational activity after a campaign's public exposure play a role in an actor's decision to continue their campaign? How much explanatory power do the motivations, resources, adherence to democratic norms, and risk tolerance of a state actor have on the adoption of persistence mechanisms? How much and what type of cost must defenders inflict on an actor's assets and infrastructure to make it prohibitive for them to maintain operations? How much do bureaucratic realities such as top-down tasking and quotas dictate if and how state disinformation actors adapt? We believe that answers to these questions could help inform future research and subsequent enforcement actions and policies.

[14] https://www.reuters.com/article/usa-election-facebook-russia/facebook-says-russian-influence-campaign-targeted-left-wing-voters-in-u-s-uk-idUSKBN25S5UC