## THE ABSOLUTE WRONG TIME TO HAMSTRING EFFORTS TO COUNTER FOREIGN ELECTION INTERFERENCE

Last week, Naomi Nix and Cat Zakrzewski, writing in the Washington Post ("U.S. stops helping Big Tech spot foreign meddling amid GOP legal threats"), reported that the US government, reversing concerted efforts over the past few years to prevent Russian and other malign actors from interfering in US elections, has stopped alerting key social media companies, including Meta, about foreign disinformation campaigns deployed on their platforms.  At the same time, Meta, Microsoft and others have warned of increased foreign influence operations on their platforms aimed at the elections.

The curtailment of government efforts highlights the pernicious impact of legal campaign being waged by conservatives to undermine content moderation and other programs intended to combat election disinformation and other online threats.  The legal campaigns are part of a muti-pronged effort, framed as efforts to counter the "suppression of conservative free speech," that includes litigation, House-led investigations and online attacks targeting government, academic and civil society disinformation researchers.

At a time when we could face a plethora of threats to free and fair elections next year – from legislative and practical efforts to restrict voter access and undermine election administration, to the potential for chaos and political violence, to potential blatant subversion of election results (for example, through a tsunami of election litigation that overwhelms the courts at a critical time and ahead of critical constitutional deadlines), not to mention the wildcard impact of the 91 felony charges that Trump will be navigating, we seriously need to question the motives of those intent on derailing efforts to counter election-related disinformation.

### Assault on Content Moderation

Perhaps it was the allegations of Russian interference in the 2016 election that conservatives found highly inconvenient or the culture wars that erupted over mask mandates and other pandemic-related mitigation efforts that morphed into accusations that public awareness campaigns against public health disinformation was in reality intended to suppress conversative free speech.  By 2021, the ultimate disinformation operation – the Big Lie – and related election denial became Republican Party orthodoxy.

Not surprisingly, academic and civil society efforts to quantify and track misinformation and disinformation, prompted largely by the revelations of Russian online influence in 2016, became proxies in the eyes of conservatives for a Democratic plot, and the resulting assault on disinformation research has been unrelenting.  It is ironic that research has found little evidence of anti-conservative bias at social media companies, with studies not surprisingly showing that the algorithms typically amplify right-wing content.  As set out in a report by the NYU Center for Business and Human Rights, "False Accusation: The Unfounded Claims that Social Media Company Censor Conservatives," "the claim of anti-conservative animus is itself a form of disinformation: a falsehood with no reliable evidence to support it. No trustworthy largescale studies have determined that conservative content is being removed for ideological reasons or that searches are being manipulated to favor liberal interests."

### *The DHS Disinformation Governance Board*

The weaponization of this backlash took an ugly turn in the spring of 2022, when a DHS initiative called the Disinformation Governance Board (admittedly a poor name from the

perspective of any student of Orwell) and its designated Executive Director Nina Jankowicz came under a barrage of harassment and abuse from Republican lawmakers and right-wing media and, in Jankowicz's case, highly personal attacks and death threats. The Board was intended to coordinate efforts to identify disinformation; it had no operational authority or capability, yet it became a tempting target. From the early days of the new administration, DHS had witnessed malign online activity as whipping up many of the problems DHS was tasked with addressing. The working group that ultimately became the short-lived Board was intended to fill a significant gap in coordination of government efforts, including between components that have different legal authorities (that is, for example, some components can work undercover and while others cannot).

The effort was described by conservatives as a Ministry of Truth, dystopian in design. The Board was scrapped (at the time the announcement said it was "paused") three weeks after it was announced, and Jankowicz resigned (*see, e.g.,* NPR coverage, Washington Post coverage and POLITICO coverage). In August 2022, the Board was disbanded. A poorly named and poorly communicated effort fell victim to the very tactics a well-intentioned working group was intended to combat. The online playbook was easy to see: get influencers to whip up a frenzy against an individual target, repeat misstatements and lies across social media about the individual over and over again, attack anyone who presents a counter narrative and count on the likely failure of the institution under attack to respond effectively.

It is easy to see this as the opening salvo of a war on civil servants, academics and other researchers, all designed to rein in content moderation and other efforts to mitigate disinformation. In the process, conservatives lost sight of the fact that ultimately we all suffer when we lose our democracy.

### *Biden v. Missouri*

The efforts picked up further steam, and gained national attention, in July when a federal judge sitting in Louisiana (in *Missouri v. Biden*) imposed a nationwide preliminary injunction prohibiting Biden administration discussions with social media platforms regarding content moderation. Incidentally, the injunction exempted communications about national security threats as well as "foreign attempts to influence elections," and was first pared back and then lifted pending review of the merits by the Supreme Court. But, the damage had been done. (I reported on the injunction in July and again in October.)

### *House Attacks*

The House Judiciary Committee's Select Subcommittee on the Weaponization of the Federal Government, led by Congressman Jim Jordan, is undertaking its own investigations into alleged collusion between the Biden administration and the platforms to curb conservative political speech. Jordan is using the Subcommittee's subpoena power to target federal agencies, academic institutions and civil society researchers through demands for correspondence, documents and testimony.

In June, the Subcommittee turned its sights on academic researchers, including University of Washington professor Kate Starbird (who co-founded the University's Center for an Informed Public ("CIP")) and Stanford University's Stanford Internet Observatory ("SIO"). According to Naomi Nix and Joseph Menn writing in the Washington Post ("These academics studied falsehoods spread by Trump. Now the GOP wants answers"), other groups

targeted by the Subcommittee include the National Conference on Citizenship, the Center for Cybersecurity at the NYU Tandon School of Engineering and NYU's Center for Social Media and Politics. A particular target of the Subcommittee is the Election Integrity Partnership ("EIP"), a joint effort of the CIP, SIO, Graphika and The Atlantic Council's Digital Forensic Research Lab. The consortium and Starbird personally also were named in the *Missouri v. Biden* complaint.

The Committee and the Subcommittee published an [interim staff report](#) on November 6, which describes at length what the authors characterize as a newly emerging "censorship-industrial complex" and the Biden administration's efforts to suppress conservative free speech. Interestingly, while the authors recognize that "foreign states do attempt to conduct influence operations," the report gives short shrift to that threat and instead the overarching message is that disinformation research quickly mutated to target domestic (that is, American) speech and needs to be stopped. The EIP, which figures prominently in the report (with 360 references before you get to the appendices), is accused of providing a "way for the federal government to launder its censorship activities in hopes of bypassing both the First Amendment and public scrutiny."

### *Self-censorship*

The legal challenges quickly prompted concerns that, at a time when the platforms were cutting back on content moderation, those efforts would suffer further due essentially to self-censorship – the uncertainty and the growing hostile environment were such that there were few assurances that interactions involving the government would not be attacked, challenged and potentially sanctioned.

The Washington Post [reporting](#) underscores that those concerns were not misplaced, and could not have come at a more vulnerable time. As the [authors](#) note, the government's retreat "erodes a partnership considered crucial to the integrity of elections around the world – just months before voters head to the polls in Taiwan, the European Union, India and the United States." An [estimated](#) two billion will head to the polls next year in over [50 elections](#). US elections present both Russia and China, as well as other actors, with a target rich environment to sow discord and distrust in election outcomes, and they and countless other actors will have at their disposal generative AI tools to amplify disinformation at scale.

The value of the interactions with government should not be underestimated. As the head of security policy at Meta, Nathaniel Gleicher, noted (as [reported](#) by the Washington Post), while Meta has resources to detect coordinated disinformation attacks, the government is better placed to track campaigns that originate offline. It is bad enough that government has scaled back its effort. But it is equally concerning that academic researchers and civil society researchers have also reduced their footprint in this space.

Self-censorship extends beyond academic researchers. As recounted in a November 10 NPR report ("[Why the fight to counter false election claims may be harder in 2024](#)") and just one of no doubt countless examples, a Republican election supervisor in Florida stopped using the term "misinformation" because "others in his party see the term as code for censorship of conservatives." An election partnership that the supervisor helps lead stopped advertising a service that allows local officials to report false voting information for fear of a conservative backlash. A combination of legal and political pressures portraying efforts to counter rumors

and conspiracy theories has resulted in the scaling back or dismantling of tools to flag and mitigate election-related falsehoods.

**And as for that threat…**

While the 2016 election provided Russia in particular with the ideal opportunity to sow distrust and discord, little did the Kremlin imagine how tilting the election outcome in its favor could result in tangible geopolitical benefit.  There is now no mystery how much is at stake, not only for the protection of democracy within our borders, but also from a geopolitical perspective.  And while it is a long-held view that very few US elections turn on the views of the electorate on foreign policy issues (though some posit 2024 may be different), that does not mean that elections have no foreign policy consequences.  In 2024, each of Russia, China and Iran has the potential to gain significantly if the Democrats lose the White House.

As Microsoft's Threat Assessment Center ("MTAC") set out in its November 8 report on foreign malign influence on the 2024 election, for these countries in particular, "the next US president will define the direction of conflict – whether wars might occur, or peace might prevail."  MTAC expects that these actors "are unlikely to sit out next year's contest – the stakes are simply too high."  And, in contrast to 2016 and despite protestations to the contrary from conservative elements, there is no question that malign foreign influence will be pronounced.

Last week, Meta announced in its Third Quarter Adversarial Threat Report that it had taken down 4,789 Facebook accounts intended to look like accounts created by ordinary Americans commenting on political issues.  The accounts reshared posts from X created by politicians, news outlets and others.  A smaller but more sophisticated set of accounts targeting India and Tibet were made to look like they were journalists, lawyers and human rights activists.  Meta reported that these "coordinated inauthentic behavior" (CIB) campaigns, which it defines as "coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation," are based in China.  The report also covered Russian CIB networks disrupted in the third quarter.

Meta reported that China is now the third most common source of foreign CIB campaigns, behind Russia and Iran, and cautions that while these networks struggle to build audiences and shift to smaller platforms (with less scrutiny), they serves as a warning that foreign actors will seek to reach domestic audiences ahead of upcoming elections.  Much of the content is copy-pasted from mainstream US media outlets (sometime conservative, and some time from both sides of the aisle) and, in yet other cases, altered to question US democracy and promote conspiracy themes.  Copy-pasting authentic content ("copypasta") may be designed to amplify partisan tensions, build audiences among existing supporters or make the fake accounts seem genuine.

Similarly, MTAC has concluded that, while the 2022 midterms were relatively free of foreign influence operations, "US election defenders should not believe that the trends of 2022 will extend to 2024."  Unsurprisingly, the report notes that "for authoritarian nation states – principally Russia, Iran, and China – next year's presidential contest will be critical for each of these countries seeking to advance their strategic goals.  Election 2024 may be the first presidential election during which multiple authoritarian actors simultaneously attempt to interfere with and influence an election outcome."

- For Russia, the outcome of the 2024 election could determine the outcome of the war in Ukraine. MTAC sees Russia's influence ecosystem accelerating "operations mimicking current news trends with political narratives. Overt Russian media outlets and covert Russia-affiliated social media networks have aligned, focusing their propaganda and disinformation on Western military aid to Ukraine and messaging against candidates committed to it." MTAC sees a three-prong assault: Kremlin-aligned actors redeploying existing assets to infiltrate and influence voters; Wagner-affiliated assets remain active and Russian-affiliated actors will likely leverage generative AI tools.

- Iran is likely to deploy operations closer to election day, particularly if tensions in the Middle East remain high.

- China has grown more provocative, with efforts aimed at the 2022 midterms and the Canadian federal elections. These are likely to continue.

## Concluding Thoughts

Since February, one Republican Senator has posed a greater threat to our national security than myriad foreign forces arrayed against us. That one Senator, Tommy Tuberville, has wreaked havoc on our national security command structure by placing holds on military appointments. Notwithstanding support last week from 20 conservative House members, the holds (or at least some of them) may be coming to an end. But, the fact remains that conservative elements have been prepared to sacrifice our national security for purely domestic political ends.

Similarly, legislative efforts originating in the House to curb content moderation efforts are undermining this country's ability to protect upcoming elections from foreign influence and interference. And once again, DHS's Cybersecurity and Infrastructure Security Agency (CISA) is a particular target among many Republicans in Congress.

As Meta itself noted,

> "Sharing information between tech companies, governments and law enforcement has also proven critical to identifying and disrupting foreign interference early, ahead of elections. This type of information sharing can be particularly critical in disrupting malicious foreign campaigns by sophisticated threat actors who coordinate their operations outside of our platforms. While we've continued to strengthen our internal capacity to detect and enforce against malicious activity since 2017, external insights from counterparts in government, as well as researchers and investigative journalists, can be particularly important in detecting and disrupting threat activity early in its planning taking place off-platform. While information exchange continues with experts across our industry and civil society, threat sharing by the federal government in the US related to foreign election interference has been paused since July."

The Heritage Foundation's Project 2025, the potential blueprint for the next Republican administration, calls for ending the counter-misinformation/disinformation mission of CISA, which it describes as a DHS component that "the Left has weaponized to censor speech and affect elections." To support its criticisms of CISA, it points to the over-hyped Twitter Files (which, in fact, largely show executives and employees at Twitter grappling with tough content moderation questions, and yes mistakes were made, but

while more details emerged the overall picture did not change). Project 2025 urges limiting CISA's election security role to helping states and localities assess whether they have good cyber hygiene in their hardware and software, and nothing more. Apparently, only the Department of Defense and National Security Agency should counter foreign actors, and apparently the "alleged Russian misinformation in the 2016 election … in fact turned out to be a Clinton campaign 'dirty trick.'"

In an op-ed published in November 2020 the same day Trump fired CISA-head Chris Krebs for rebutting Trump's accusations of "massive fraud and improprieties" in the election, David Ignatius wrote that "[w]hen the history books about this election are written, Krebs will be one of the heroes."

As MSNBC contributor Steve Benen noted in August (as did POLITICO in an October piece detailing efforts to slash CISA funding), Trump and his acolytes are still trying to derail CISA's work (which incidentally also is tasked with protecting the nation's critical infrastructure against cyberattacks). The key elements of the multi-pronged attacks all are tracked above, and Benen rightly questions – is the effort despite CISA's successes, or because of it.

This is a question that applies across the entire disinformation research ecosystem.

<div align="center">*     *     *</div>

**Mark S. Bergman**
**7Pillars Global Insights, LLC**
**Washington, D.C.**
**December 4, 2023**