Foreign Disinformation in 2022: A Review

- Foreign disinformation played an ancillary role to homegrown disinformation in the US in 2022, but this was not necessarily an indication of reduced activity.
- State actors have begun to take steps to circumvent mitigation measures by governments and tech companies, and are learning from each other.
- Frameworks for addressing foreign disinformation have developed around the world 2022, but measures remain largely disjointed, leaving several gaps that can be exploited.

In October 2022, shortly before the US midterm elections, the FBI and the CISA (Cybersecurity and Infrastructure Security Agency) issued a joint public service announce to raise awareness of the potential threat of disinformation by foreign actors during the midterms. Foreign influence operations were linked to two areas of concern being monitored by the FBI and CISA prior to the 2022 elections, threats from state-sponsored actors (including those related to cybersecurity) and disinformation. Together with insider threats and physical threats, these made up the 'big four' areas of concern for the FBI and CISA during the elections, and the agencies emphasised that they were 'interconnected' and should not be viewed individually, particularly in the case of foreign actors.

The agencies specified that they believed false claims of malicious cyberactivity on election infrastructure and other electoral issues would be amplified to undermine voter confidence and the legitimacy of the elections. They indicated that the actors would use a variety of vectors to achieve this, including 'publicly available and dark web media channels, online journals, messaging applications, spoofed websites, emails, text messages, and fake online personas on U.S. and foreign social media platforms'.

The FBI and CISA are likely to have been specifically referencing disinformation by Russia, China and Iran, the state actors with the most developed and pervasive disinformation networks. Reviewing the elections, it appears that foreign disinformation may have played a more ancillary role on this occasion to the stream of falsehoods that emanated from the election candidates themselves. Organisations researching influence operations in the US, such as Recorded Future, Graphika and Mandiant, found for example that Russian disinformation campaigns in the US were much smaller than those in the 2016 elections.

This is at least in part a result of the changes introduced—both in governments and among private corporations—since 2016 to counter disinformation as a result of heightened awareness of its impact. There is now far greater interest and funding for researching disinformation, and the US State Department has also created the Global Engagement Centre, a government body specifically set up to 'proactively [address] foreign adversaries' attempts to undermine U.S. interests using disinformation and propaganda'.

Countries around the world have also introduced legislative and other policy initiatives to combat disinformation, ranging from outright laws to the promotion of media literacy, and even brute force internet shutdowns. The EU, for instance, refined their self-regulatory legislative Code of Practice on Disinformation for tech companies in 2022 by introducing specific commitments and measures that signatories will have to adhere to. This complemented the bloc's Digital Services Act, which entered into force in November and imposed obligations on large social media platforms to introduce assessable mitigation measures against disinformation. Under the threat of regulatory penalties, tech companies running social media platforms have hastened efforts to proactively remove disinformation and de-platform the state media accounts responsible, as was observed in the removal of RT and Sputnik from Facebook, Twitter and YouTube.

Russia

Though these developments have coincided with shifts in patterns of foreign influence operations, changes in the scale and scope of the campaigns do not necessarily indicate their diminished presence or success in combatting them. Rather, it reflects the tactics adopted by foreign state actors to evolve their networks to counter mitigation efforts and respond to the changing needs of disinformation campaigns. Russia's influence operations, which have been the most active in the US, have undoubtedly been shaped by Russia's invasion of Ukraine in 2022. These have not only limited the operating space of the networks caused by the de-platforming of Russian state media content, but also induced a need for pro-Russian narratives and criticism of US support for Ukraine, which may have diluted the campaign's previous focus on US domestic issues.

Russian disinformation networks have begun to relocate onto alt-tech platforms such as Gab, Parler, Gettr and the patriots.win forum. Here, fake personas from the network have found a sympathetic audience to messages critical of the Biden administration on issues popular with the far-right, such as vaccine mandates, gun control, racial injustice and allegations of child sexual abuse. In addition, the Russian disinformation campaign has leveraged on alt-right meme culture by disseminating political cartoons, including some that caricatured Democratic candidates running in tight electoral races during the midterm elections. While the content on alt-tech platforms has limited reach and lower engagement, this expansion strategy may allow Russian influence operations to achieve a higher level of persistence and allow them to become more deeply embedded by piggybacking on existing sympathies among American far-right communities.

Iran

The need by state actors to address local priorities also finds parallels in Iranian influence operations. Iranian operations appear to be less targeted at US voters in order to influence the outcome of the elections, but instead seem to be concentrated on utilising the elections

to share broader propaganda themes such as an impending US civil war, economic collapse and a decline of US international stature. Iran's disinformation campaigns have broadly dovetailed with state media narratives connecting the issue of the Iran nuclear deal (JCPOA) with the US midterms. Accordingly, Iranian campaigns aimed at increasing US domestic polarisation may grow or diminish in scale along with perceptions at home of the prospects of JCPOA negotiations leading to a satisfactory outcome.

China

Signs of evolution were also evident in Chinese influence operations in 2022. Disinformation originating from China has traditionally been the purview of combative 'wolf warrior' government officials and state media personalities. These have been supported by conventional high-level influence campaigns that rely on the political and media machinery. Sympathetic voices—sometimes paid—have been nurtured among local politicians in the target country and in the media, including both local Chinese-language media owned by pro-Beijing businesspeople and paid inserts included in publications otherwise considered to be reputable.

These tactics have continued both in the US and in beyond, including in geographic regions of Chinese interest such as Australia, New Zealand, Taiwan and parts of Southeast Asia. A significant development in Chinese influence operations appears to be the adoption of social media platforms to target audiences with divisive political content, an approach that has generally been more typical of Russian campaigns. Some of these campaigns have adopted the impersonation of cyber personalities and altered news articles to create fabricated narratives that have a falsified veneer of credibility, such as allegations that the US was responsible for the bombing of the Nord Stream gas pipelines.

A major uptick in Chinese influence operations on digital platforms was observed after former US Speaker of the House Nancy Pelosi's visit to Taiwan in August, again emphasising the linkages between disinformation and state actors' local political considerations. New methods of digital disinformation were employed that appeared to prioritise the resilience and longevity of the network. For example, a Chinese essay titled 'Urging (Taiwanese President) Tsai Ing-wen and her military and political leaders to surrender' was circulated by fake accounts across multiple platforms owned by different tech companies, rather than relying on prominent Chinese 'wolf warrior' officials as has been previously observed.

While the efficacy of the new digital disinformation campaigns is questionable, these new tactics are likely to be utilised further in the future if they prove capable of allowing networks to circumvent single 'points of failure' vulnerable to mitigation measures. Moreover, state actors, and in particular Russia and China, learn from each other's perceived propaganda successes, such as Russia's hacking of the Democratic National Committee during the 2016 US presidential elections. The 'comprehensive strategic

partnership' announced between Russia and China and the cleavages in the global political landscape resulting from the war in Ukraine offer additional opportunities for cooperation between state actors in the field of disinformation. Taiwan and other Pacific societies with large Chinese populations are likely to face the brunt of Chinese digital disinformation campaigns and serve as the primary test beds as China seeks to refine its messages and tactics.

Lessons to Learn

While local motivations have differentiated influence operations between each state actor, there are broad strokes across the campaigns that remain similar. Russia, Iran and China have all consistently disseminated messages that seek to broaden distrust in democratic institutions and heighten political divisions over sensitive issues. The US continues to be a major target for these campaigns, but it is possible for many of the messages used in the US to be transplanted to other democratic societies, especially as the state actors expand and share their capabilities. While the heightened attention to the threat of disinformation may help ward off large-scale vulnerabilities to disinformation like that seen in 2016, the continuing expansion of the digital environment, its suitability for propaganda and rising political competition suggest digitally enabled foreign influence operations are only likely to intensify in the future.

A suitable response in facing these threats would be an international framework for addressing disinformation that encompasses governments, tech companies and civil society. Despite the progress made in 2022, it does not appear that such a comprehensive response is forthcoming as yet. In the US, much of the new institutions and initiatives lack authority and are implemented in an ad-hoc fashion and civil society groups are often overlooked. Globally, a veritable patchwork of disinformation countermeasures has been created by the varying responses from different countries, not all of which have proven to be effective.

There are concerns that restrictions on the media could have negative consequences for the freedom of expression. In Singapore, the Foreign Interference (Countermeasures) Bill (FICA) has been criticised for disproportionately impacting members of civil society and sanctioning disproportionate penalties. In the absence of legal necessity, self-interested tech companies have also hindered the ability of civil society groups in researching disinformation on their platforms, and non-anglophone countries have been hamstrung by the lack of linguistic capability within tech giants in order to moderate content on their platforms.

A 2022 poll from the Pearson Institute and the Associated Press-NORC Center for Public Affairs Research found that 91% of American adults said misinformation is a problem, and 74% calling it a major problem. Disinformation is no longer a surprising phenomenon, and state actors, who often are the biggest beneficiaries of its existence, will continue to

perpetuate disinformation campaigns as vehicles for propaganda and tools for seeding instability. The diffusion of disinformation to the less visible backrooms of the internet must not be considered a moment of respite, and growing capabilities among state actors must be matched by reinvested efforts in developing a multilateral, holistic approach to the evolving threat.