Middle East Disinformation: 2020 Prospects & Solutions

Social media has transformed the information landscape in the Middle East over the past decade. The 2009 Green Revolution and the 2011 Arab Spring demonstrated the enormous power of platforms like Twitter and Facebook for political organizing. Popular perception in the U.S. at the time was that these services would democratize a region notorious for its strongman governments. But it also showed governments and militants in the Middle East how powerful social media campaigns can be, if coopted for their own purposes.

> *"Like any technological innovation, social media initially favored asymmetric actors — a tool of the weak against the strong. In the Middle East, it was democratic activists who first embraced social media, and terrorist groups soon after them. With time, however, national governments have learned how to harness social media to their own ends. By using their vast resources and economies of scale, these governments can exploit the platforms in ways that loose networks of activists never could."*
> *— Emerson Brooking, Resident Fellow, Digital Forensics Research Lab*

In Israel's 2012 Operation Pillar of Defense against Hamas in Gaza, supporters of both the Israel Defense Forces (IDF) and Hamas took to Twitter to support their own sides. Official IDF Twitter accounts would share videos of civilians fleeing to bomb shelters and warn of Israel's determination to bring terrorists to justice, while accounts aligned with Hamas would share gruesome images of civilian casualties and threats of righteous retaliation. When ISIS rose to power in 2014, it unleashed the most sophisticated and disturbing terrorist propaganda campaign in history, driving Americans' fear of terrorism higher than it was in the immediate aftermath of 9/11.

Today many governments in the Middle East don't just use official social media accounts to spread their messaging — a completely normal practice well within platforms' terms of service — but they also use armies of social media "bots," automated to tweet, retweet, and like certain messages, driving up visibility of specific topics and viewpoints. In the immediate aftermath of the 2017 hack on the Qatar News Agency, bots lit up pro- and anti-Qatar hashtags, cleaving the regional information space and ultimately culminating in the diplomatic and economic blockade that continues to this day. Another technique, used heavily by Iran, is to establish reputable-looking "news" websites and inauthentic "sockpuppet" social media accounts, all to skew information spaces in one direction or another. These were all techniques used effectively by the Russian government to exacerbate tensions within the Democratic Party and drive up support for Donald Trump in 2016.

The dearth of independent news outlets and justifiable distrust of foreign media in the Middle East exacerbate this trend. Al Arabiya, a Dubai-based Saudi news channel that often features reputable scholars from around the world, maintained during the onset of the Qatar crisis that the Qatar News Agency was not hacked even though Qatar released evidence supporting its claim and the CIA concurred. Qatari-owned Al Jazeera, an equally if not more reputable news channel, consistently avoids examining the substance of the accusations made by the four states carrying out the blockade — Saudi Arabia, the UAE, Bahrain, and Egypt — that Qatar has funded terrorism. In an age when people around the world increasingly receive their news via Twitter and Facebook, it is becoming more difficult for the public in the Middle East to reliably fact-check or dispute claims and viewpoints they find trending — artificially or not — on social media.

Several emerging trends are making disinformation more difficult to contain and control. U.S.-based Instagram has censored criticism of Qassem Soleimani's killing in its attempt to comply with the U.S.'s designation of the Islamic Revolutionary Guard Corps as a terrorist organization, while the wildly popular Chinese-owned TikTok has censored content criticizing Chinese mistreatment of Uighurs. Inauthentic social media activity is increasingly being carried out by private companies in the region, and new tools like deepfakes create new potential avenues for malicious deception. The result is a fractured international information space and heightened risk to a globally shared sense of facts and reality.

There are a variety of policies that governments in the Middle East and around the world are taking to deal with disinformation. None is a panacea, and each has different advantages.

LEGAL RESPONSES

An emerging (or reemerging) trend is the regulation of sharing fake news. England first outlawed "the publish[ing] or tell[ing] of any false News or Tales" in the 1275 Statute of Westminster, explicitly to prevent "Discord… between the king and his People[.]" In recent years, Saudi Arabia, Egypt, Pakistan, and Qatar have taken action to either censor or criminalize fake news with the same intent. Even in the United States, President Trump has called to "open up" America's libel laws and Senator Elizabeth Warren has proposed criminalizing sharing disinformation about when and where to vote.

The impulse is reasonable — fake news and conspiracy theories have become a scourge in the internet age. Sweeping bans on fake news, however, functionally give governments the authority to arbitrarily define the truth. The implications for freedom of expression can be dangerous. Circumscribed restrictions, such as the criminalization of Holocaust denial in Germany, can be sustainable. However, centuries of litigation and legislation have moved the boundaries of free speech in the English-speaking world since England's 13th century ban, meaning blanket laws like Saudi Arabia and Qatar's are unlikely to solve the problem conclusively.

OFFENSIVE CYBER OPERATIONS

In at least two cases, the United States has relied on offensive cyber operations to disrupt the sources of disinformation and influence campaigns. First, in 2016, Cyber Command's Operation Glowing Symphony struck the networked resources ISIS was using to promote its notoriously effective propaganda. During the 2018 midterm elections, Cyber Command similarly launched a cyber attack against the Russian Internet Research Agency, the same troll farm that ratcheted up political tensions with fake news and bogus social media profiles in the 2016 election.

Cyber attacks can acutely disrupt disinformation and influence campaigns, but they are not a cure-all. Adversaries can always buy new devices, set up new accounts, and return to business as usual.

These operations can also set a risky precedent. ISIS's propaganda inarguably incited terrorist violence against the U.S., but Israel and the Gulf blockade quartet have accused Al Jazeera of the same thing. Some networks of inauthentic social media behavior, furthermore, are run by America's own allies, where cyber attacks would be unthinkable.

> *"While Operation Glowing Symphony likely had immediate initial impact from the effects of coordinated computer and social media network disruptions, the lasting effect of disruptions on resilient, adaptive media networks is debatable. It is important to remember, however, that OGS occurred in coordination with and provided support to combat operations, Department of State efforts, domestic law enforcement, and Department of Treasury Office of Foreign Assets Control sanctions to apply pressure against the ISIS media network. OGS demonstrated that offensive cyber operations, both disruptive and for intelligence collection, are an effective multiplier for existing whole-of-government counter-disinformation campaigns and can impose sustained 'time and resource costs' on adversaries."*
>
> *— Michael Martelle, Cyber Vault Fellow, National Security Archive*

COUNTER-MESSAGING

States can work to combat disinformation and influence campaigns with counter-messaging through public diplomacy, like the U.S.'s Global Engagement Center. Israel has pioneered this strategy, known in Hebrew as hasbara (, literally "explanation"): government efforts dating back to the 1970s to correct the record on matters it considers construed or misunderstood. To this day, the IDF proactively contextualizes strikes on Gaza in connection to Hamas rocket launches and publicizes Israeli efforts to minimize civilian casualties.

The line distinguishing an influence campaign and a counter-influence campaign, however, is blurry (if it can even be said to exist). Hasbara is often skewered as propaganda, even by Israeli and Jewish news outlets. The countervailing public diplomacy of Qatar and the blockade quartet since 2017 has been cacophonous, with each side accusing the other of supporting terrorism. The U.S. State Department's counter-ISIS Twitter effort, a much more circumspect campaign, has been derided by terrorism expert Rita Katz as "embarrassing" and "ridiculous."

Public diplomacy is an important tool to combat disinformation and influence campaigns, not just for the U.S. but countries in the Middle East and beyond. Like any government tool, however, it can be (and often is) used ineffectually or excessively.

PUBLIC-PRIVATE PARTNERSHIPS

A fourth option to counter disinformation and influence campaigns is through public-private partnerships. American intelligence agencies tracked and documented Russian interference in the 2016 election, including on social media; in response, Facebook developed a threat investigation team to take down such accounts. A partnership between those agencies and Facebook could, at least in theory, have limited the trouble Russia was able to cause. Partnerships between social media and organizations like Graphika and the Digital Forensics Research Lab have produced deeply insightful public reports on inauthentic social media campaigns, not just containing those campaigns but educating the greater public on them.

Public-private partnerships are perhaps the most promising option to combat influence campaigns, especially considering how common it is to consume news via social media. They are not a panacea, however. The Russian state-run news channel RT, for example, has been implicated in reports of Russian interference in the 2016 election — no partnership could have prevented its skewed coverage. Foreign adversaries can also hack and selectively leak damaging information to the press, effectively coopting reputable news outlets to drive a particular narrative.

CONCLUSION

Disinformation is a destabilizing force around the world, but there are many opportunities and avenues to contain and disrupt it. Governments worldwide need to be wary of the threat, especially around politically divisive lightning rods like national elections and ongoing kinetic conflicts in Syria, Yemen, and Libya. Russian interference in the 2016 U.S. presidential election was a black swan event for social media platforms and the U.S. intelligence community; now that its lessons have become clear, governments should be prepared to anticipate and counter similar campaigns now and in the future. Recommendations like these can help reduce that risk.