The evolution of computational propaganda: Bots, influencers, and platform responsibility

By Samuel C. Wooley

When my colleagues and I began studying "computational propaganda" at the University of Washington in the fall of 2013, we were primarily concerned with the political use of social media bots. We'd seen evidence during the Arab Spring that political groups such as the Syrian Electronic Army were using automated Twitter and Facebook profiles to artificially amplify support for embattled regimes while also suppressing the digital communication of opposition. Research from computer and network scientists demonstrated that bot-driven astroturfing was also happening in western democracies, with early examples occurring during the 2010 U.S. midterms.

We argued then that social media firms needed to do something about their political bot problem. More broadly, they needed to confront inorganic manipulation campaigns — including those that used sock puppets and tools — in order to prevent these informational spaces from being co-opted for control — for disinformation, influence operations, and politically-motivated harassment. What has changed since then? How is computational propaganda different in 2020? What have platforms done to deal with this issue? How have opinions about their responsibility shifted?

As the principal investigator of the <u>Propaganda Research Team</u> at the University of Texas at Austin, my focus has shifted away from political bots and towards emerging means of sowing biased and misleading political content online. Automated profiles still have utility in online information campaigns, with scholars detailing their use during the <u>2020 U.S. elections</u>, but such impersonal, brutish manipulation efforts are beginning to be replaced by more relationally focused, subtle influence campaigns. The use of these new tools and strategies present new challenges for regulation of online political communication. They also present new threats to civic conversation on social media.

In 2020, our team's research has focused on four topics related to the evolution of propaganda over the internet: 1) the use of paid political <u>nano- and micro-influencers</u>, 2) marked changes in campaigns' <u>peer-to-peer (P2P)</u> text messaging tactics, 3) the spread of misinformation and disinformation on <u>encrypted and private messaging services</u>, and 4) efforts to recreate Facebook Graph API-style demographic microtargeting via the use of network data extracted directly from users' phones, <u>location data</u>, <u>and tools like geofencing</u>.

Over the last year we have conducted more than 80 interviews with data brokers, political consultants, digital marketing experts, and party IT professionals. Together, they form the sundry combination of actors referred to as "advanced persistent manipulators." They are, in other words, computational propagandists. The majority of these interviews have been with individuals or teams based in the United States, though we have also formally spoken to several people in Brazil, India, and Mexico.

Our conversations have revealed several shifts in how political groups are currently using social media and other digital communication tools to manipulate public opinion.

First, our interviewees consistently speak about combining more heavy-handed social media bot campaigns — aimed at manufacturing consensus, or creating the illusion of popularity or dissent for particular politicians or ideas — with "relational organizing" tactics. Specifically, propagandists across all four countries discussed leveraging small, more intimate, digital communication spaces in order to more effectively coerce and cajole. The psychological literature shows that people are more likely to alter their political opinions if influence efforts prey upon their sense of belonging or identity. Political bots may be useful at laundering information or, say, getting social media trending algorithms to re-curate content because they mistake sheer amounts of (automated) political engagement for popularity. But recruiting a combination of paid human proponents and zealous volunteers to seed and fertilize propaganda, disinformation, or political attacks among smaller, more homogenous, groups on platforms like WhatsApp, Telegram, Parler, Gab, and Discord is seen as more efficacious at actually changing minds and actions. Our current research points to the smaller, heavily politically motivated, groups on these platforms sharing content and using a diversity of tactics to achieve outsized influence in the public forums of Twitter and Facebook. Propagandists are utilizing new technological means for generating data sets on individuals and small groups within important voting constituencies and in pivotal electoral locations. After the Cambridge Analytica scandal in 2016, Facebook battened down the hatches on the Graph API — which advertisers used to access and exploit people's sociopolitical information. But digital political communication consultants have told us that they've worked to piece together similarly intimate data sets by garnering access to people's cell phone contact lists through political apps. They use them to spread manipulative messaging.

Second, and closely tied to the first due to a similar focus on relational organizing, political groups are beginning to compensate <u>social media influencers</u> for spreading particular political messages. Many of our interviewees, particularly in the U.S., tell us that they are paying micro- (under 25,000 followers) and nano- (under 10,000 followers) influencers to spread highly partisan content — including, at times, disinformation — to

their followers. One group claimed to be managing a roster of over three million small-scale political influencers during the 2020 U.S. election. The ranks included an assortment of local movers and shakers: teachers, religious leaders, small business owners, and, yes, young people aspiring to become social media famous. Crucially, those employing these minor influencers explained that because they were well known in their communities, and because they were often speaking to hyperlocal audiences (many in swing states), they were more likely to have a tangible impact on people's political opinions. But, and herein lies a serious problem for platforms and regulators, many of these political influencers do not clearly state that they are being compensated by political groups when they spread paid content online. There should also be stricter disclosure laws around political peer-to-peer texting, which simultaneously makes use of communication via close relational ties and mass messaging. Relationally focused P2P, facilitated by various apps like outvote.io, is turning family members and friends into political propagandists on a small scale — and often preys upon an oversight in the law about automated various human texting. In short, although people are clicking the "send" button on these texts, the rest of the process looks automated.

Third, U.S. political groups on both the left and right are collecting as much location-oriented information as they can on what they see as particularly moldable voting groups — including Latinos, African Americans, Catholics, suburban women, and issue-specific voters — in order to target them with highly specific, and often misleading, messaging and advertising via various digital platforms. They use tools like geofencing and Bluetooth beacons to track group and individual movement: Are people at church? Which church? How often? Did they attend a political rally? If so, are they registered to vote for the party who hosted it? Propagandists then work with data brokers to combine this data with other behavioral information from credit agencies, voter rolls, and, yes, social media, in efforts to persuade voters for one cause or another. We call this phenomenon "geo-propaganda": the use of location data by campaigns, lobbyists, and other political groups to influence political discussions and decisions. Importantly, many of the data-gathering tactics of geo-propaganda are facilitated by the relational organizing.

These emerging propaganda tactics pose several challenges to platforms and regulators:

 First, what can encrypted messaging platforms do to curb intimate influence operations on their closed ecosystems? How can governments protect citizens and civic discourse on these apps without dismantling encryption, which certainly has democratic utility — particularly in countries with repressive and restricted media systems?

- Second, how can platforms hold influencers accountable for spreading paid political messages when they are paid off-platform? When influencers aren't paid to spread political content — perhaps they are compensated through swag or face time with a candidate — are they still part of coordinated inorganic behavior?
- Third, what role does a platform like Facebook which has worked to restrict access to the type of behavioral data they used to make available to political advertisers via the Graph API have in stopping political groups from using similar race-religion-belief-location information to reverse engineer a similar method of targeting their users with highly manipulative political messaging? What can (or will) the U.S. government do to curb widespread, predatory, location- and social-graph gathering practices aimed at political ends?

People around the world still communicate about politics in digital spaces marred by automated amplification campaigns, anonymous disinformation peddlers, and feckless trending algorithms. But computational propaganda is evolving. In some ways it's becoming more human — with political actors recognizing that it is not just the right message that matters, but the right messenger. In others, it's becoming more technical. What is clear, regardless, is that it's still a serious problem. With a Biden win in 2020, but with a Trump refusal to concede and the corresponding cascade of disinformation following his intransigence, how will platforms' regulation of this issue shift? Will the federal government in the U.S. actually begin to regulate the social media space? What will the people think?

Samuel C. Woolley is an assistant professor of journalism and the project director for propaganda research at the Center for Media Engagement at the University of Texas at Austin.