British American Business

Securing The Vote
Threats to Anglo-American Democracy

Author: Akshat Dhankher

This piece serves as a follow-on to a roundtable event of the same name, 'Securing the Vote: Cyberthreats to Anglo-American Democracy', run by BritishAmerican Business in London on December 2, 2019.

General Background

The constantly changing complexity of data, online information, and social networks has rendered modern democracies greatly vulnerable to illegitimate influence. Malicious actors have developed several techniques of interfering in elections, ranging from information manipulation and dissemination through legitimate channels, to cyberattacks that access personal information or disrupt infrastructure.[1]

Failure to act on addressing these threats is leading to a loss of trust in democratic institutions, carrying long-term impacts that shape the environment in which governments and businesses operate. Ultimately, businesses need a reliable political environment to ensure that operations remain smooth and employees can enjoy the benefits of job security and stable income. To best preserve this necessary trust, it is essential that business and government put resources behind understanding the nature of contemporary disinformation and cyber threats and develop proactive responses to them.

Widespread Incidents

Elections are primarily an interaction between candidates and voters, facilitated by media and content providers. When malicious actors enter as a tertiary force, they violate the sanctity of democratic processes. The instances of such interference are widespread and can be highly effective, as seen in Europe in 2018 when far-right activists used a coordinated misinformation campaign to derail support for a UN Migration Pact, and ultimately caused the collapse of Belgium's government over the issue.[2]

The situation is currently worsening, with effective attacks increasingly occurring across election cycles in the past five years alone. These situations are made especially dangerous by the combination of disinformation operations with cyberattacks, forming an unprecedented hybrid threat to modern democracies. For example, prior to 2017 elections in Germany, a Kremlin-linked group infiltrated and monitored computers in German parliament undetected for weeks, leading to public tensions over the extent to which the electoral outcome may have been influenced by this attack. France also experienced this form of attack when hackers used a phishing scam to access and release nine gigabytes of emails from the En Marche party prior to a second round of presidential voting.[3]

Also important to consider is the growing challenge around 'deepfakes' — an emerging technology that trains artificial intelligence to create videos in which faces are swapped or digitally altered with convincing results.[4] The use of this technology, typically featuring celebrities or politicians, aims to paint public figures as making statements that the individual never actually made. While the technology around deepfakes

is still primitive, the continued developments ahead of major elections like the US 2020 race pose challenges for media providers and the democracies impacted by misinformation.

Impacts on Transatlantic Democracy

The US and UK have not been spared by this phenomenon and are facing unprecedented threats which erode institutional and democratic trust. In the UK, the 2016 referendum to exit the European Union was targeted by Russian-based disinformation operations. The UK Parliament's February 2019 report on "Disinformation and 'fake news'" found evidence of over 150,000 Russian-language social media accounts posting pro-Brexit material prior to the vote, a form of message amplification, as well as several hundred accounts linked to the Russian Internet Research Agency (IRA) spreading disinformation.[5] The efficacy of this attack is difficult to determine, but its presence in the democratic process should be deeply troubling for all sides.

Similarly, there is bipartisan consensus that Russian actors executed and intricate, multi-faceted influence campaign in the 2016 US elections. This included many of the same tactics seen elsewhere, — such as mobilizing false social media accounts to amplify politically polarized views — but also hacking into networks of the Democratic National Committee and the Democratic Congressional Campaign Committee in order to leak information that would damage Democrat Hillary Clinton's candidacy at strategic points in the campaign, as identified by the US Department of Justice.[6] As always, it is difficult to quantify the direct impact on the votes, but these revelations have reverberated throughout US political system and the world, intensifying national divides and undermining public faith in the democratic process entirely.

Current State of Play

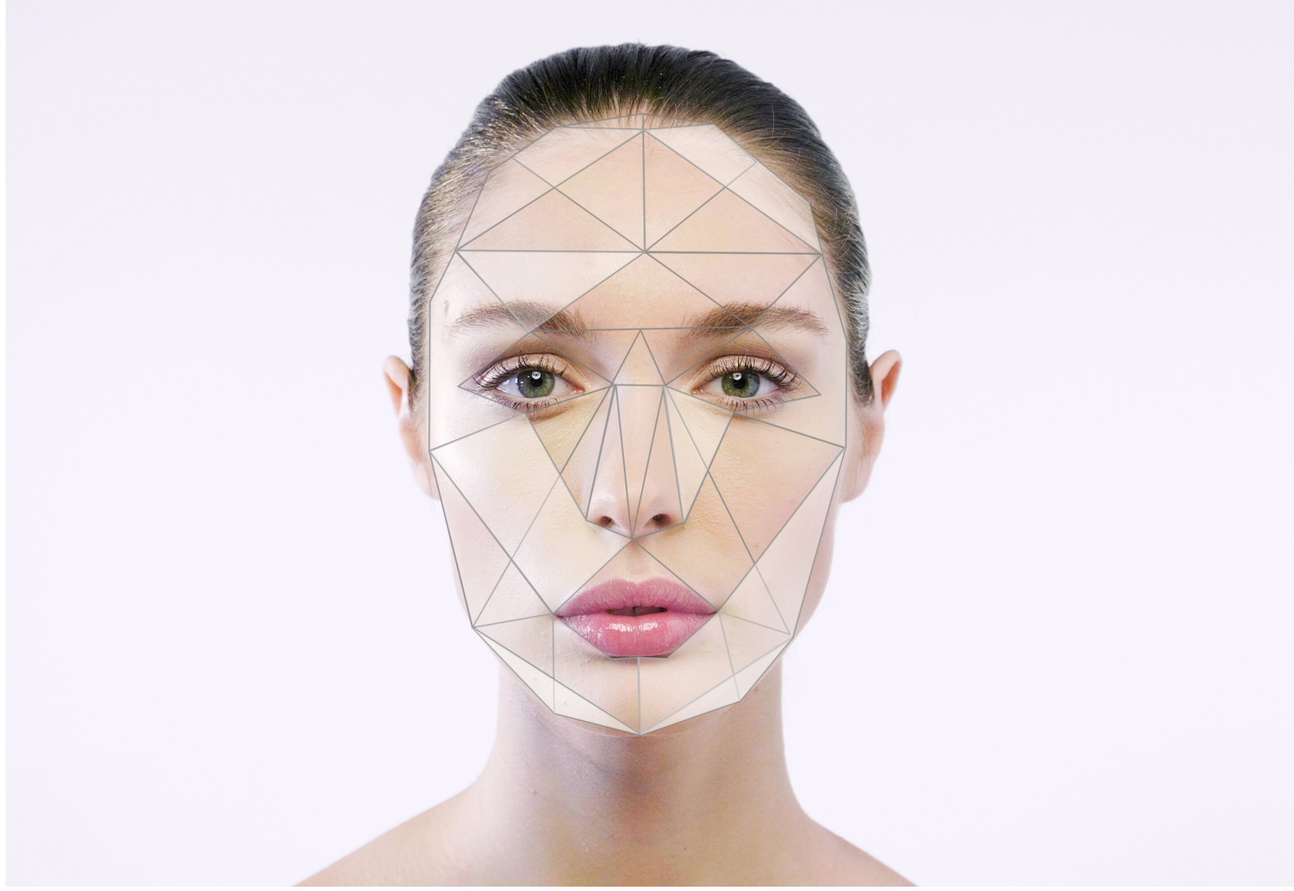
With elections once more dominating the discourse in both the US and UK, concerns over the security from election interference return. Ahead of the US 2020 election, Facebook has already detected and removed dozens of disinformation campaigns perpetrated by foreign state actors, some of which targeted specific Democratic Presidential candidates, and others which aimed to amplify social divides in the political discourse by posing as genuine users.[7]

While in the UK there have yet to be any fully-verified instances of foreign interference in the December 2019 national elections, the current set of electoral laws is already antiquated for the digital age. The UK Electoral Commission has highlighted several vulnerabilities that current regulations fail to address, chiefly the lacking transparency in digital campaign advertising and where materials come from, online intimidation of public candidates, and limited protection of voters from undue influence.[8] Even regulations as simple as the imprints rule — which requires all physical election materials to contain an imprint denoting who published the material — have not been extended to apply to digital elections.

Additionally, since the Parliament Intelligence & Security Committee's report on the extent of Russian interference in UK elections was not released in time for the December elections, there was neither preparation for nor certainty about the integrity of the electoral process — another area with the potential to undermine confidence in the outcome of this election after the fact.

Finding a Solution: Past, Present, and Future

Nonetheless, the overt and consistent use of media platforms by both domestic and foreign actors interfering in elections underlines the need to better protect user data, crack down on microtargeting, better ensure the veracity of political content, and increase transparency over the source of posted political information.



The dangerous potential of new technology has led companies to establish the Deepfake Detection Challenge in order to advance deepfake detection technology.

While regulatory action is lagging on election security, businesses have been acting on the issue. In response to public concern over the political targeting and disinformation online, Twitter made a sweeping decision regarding its advertisements policy by globally prohibiting the promotion of all political content on its platform, and further banning political action committees from posting any kind of advertisements.[9] Google has also followed suit by banning political advertising that is microtargeted based in users' demographic information, and further enhanced transparency by creating a political advertising report that details advertising spending by region, campaign, and even as granular as individual advertisements.[10] [11]

When it comes to approaches that content providers take to limit foreign interference, it ultimately depends on the business model of each company.

Microsoft, for example, have established a whole new suite of products for elections to provide enhanced security to political campaigns that use them.[12] The company is also combating deepfakes, partnering with Facebook to create a "Deepfake Detection Challenge" to advance deepfake detection technology.[13]

Additionally, journalists and the news media have a responsibility to proliferate fair, accurate, and comprehensive news on contemporary political issues. What often happens — as was the case in the discourse surrounding the UN Migration Pact — is that a vacuum of authentic information on public issues can easily be filled by malicious actors.[14]

If instead the news media provides critical, well-researched information to the public, it in turn builds the capacity for public resilience to disinformation. The BBC, for example, has taken up this responsibility in its 'Beyond Fake News' initiative, in which it researches and publishes findings regarding the nature of disinformation itself, thus building public media literacy on how to recognize and rely on more

accurate and credible information.[15] Such media literacy initiatives can even be extended to the business community, allowing employers to build resilience to external malpractices among employees.

Ultimately, action by both the UK and US governments is needed to engage with the business community and promote a regulatory environment that better preserves and protects the integrity of elections. UK electoral law reforms are long overdue; in fact, the Electoral Commission has already recommended effective measures like extending the imprints rule to digital content, requiring greater detail and transparency on digital spending by campaigns, and imposing large electoral sanctions against actors who aim to intimidate or misinform participants in the electoral process.[16]

The US — by virtue of hosting the companies whose platforms greatly influence dialogue in democracies around the world — is central to efforts combating election interference. Naturally, different jurisdictions will require different regulations as per regional specificities, but US-led cooperation remains paramount for securing elections. The 2018 G7 meeting showed signs of progress in this area, as the leaders committed to strengthened cooperation in defending democracy from foreign threats, sharing lessons and best practices across governments and private sectors, requiring greater transparency around advertising and the treatment of personal data, and promoting civic awareness around online security and safety.[17]

More broadly, global cooperation on the cybersecurity environment must take place. The Paris Call for Trust and Security in Cyberspace serves as a good framework for such cooperation, bringing together stakeholders from government, business, and civil society to promote such change. The Paris Call is a step in the right direction to improve digital cooperation, increase capacity-building efforts, and building user awareness and resilience.[18] Multi-stakeholder efforts in which government moves forward with business input, as in the fashion of the Paris Call, will continue to be important for the most effective progress on cybersecurity and anti-disinformation.

The US and UK government must take action to combat hybrid threats to electoral security. Even if regulators delay change, aggressors to democracy do not. Digital technology and the nature of how people receive information will continue to change, so government and business in the US and UK must keep up. The transatlantic economy is built on the strength of our democratic institutions, so the erosion of trust in these spells trouble for Anglo-American democracy and business. This is an area where we cannot afford complacency.

About the Author

Akshat Dhankher is a student from Northeastern University in Boston, where he studies Computer Science, Economics, and International Affairs. Joining BAB London's Policy Team in 2019 as part of Northeastern University's Co-op programme, Akshat has played a key role in BAB's policy engagements and content production.

1 Methods of Foreign Election Interference, 02 April 2019, EUvsDisinfo: https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/
2 ISD research featured in POLITICO about the trolling of the UN Migration Pact, April 2019, ISD: https://www.isdglobal.org/isd-research-featured-in-politico-surrounding-the-trolling-of-the-un-migration-pact/
3 Cybersecurity of Voting Machines, 29 November 2017, Brookings: https://www.brookings.edu/testimonies/cybersecurity-of-voting-machines/
4 Deepfakes: What are they and why would I make one?, 2019, BBC: https://www.bbc.co.uk/bitesize/articles/zfkwcqt
5 Disinformation and 'fake news': Final Report, 14 February 2019, House of Commons: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
6 Report on the Investigation into Russian Interference in 2016 Presidential Election, March 2019, U.S. Department of Justice: https://www.justice.gov/storage/report.pdf
7 Facebook Finds New Disinformation Campaigns and Braces for 2020 Torrent, 21 October 2019, NY Times: https://www.nytimes.com/2019/10/21/technology/facebook-disinformation-russia-iran.html
8 Response to the UK Government policy consultation: Protecting the Debate, 16 August 2019, UK Electoral Commission: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/response-uk-government-policy-consultation-protecting-debate
9 Political Content, 2019, Twitter: https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html
10 An update on our political ads policy, 20 November 2019, Google: https://blog.google/technology/ads/update-our-political-ads-policy/
11 Google Transparency Report, 2019, Google: https://transparencyreport.google.com/political-ads/region/US?hl=en
12 Microsoft 365 for Campaigns, 2019, Microsoft: https://m365forcampaigns.microsoft.com/en-us/
13 Facebook, Microsoft launch contest to detect deepfake photos, 05 September 2019, Reuters: https://uk.reuters.com/article/us-facebook-microsoft-deepfakes/facebook-microsoft-launch-contest-to-detect-deepfake-videos-idUKKCN1VQ2T5
14 ISD research featured in POLITICO about the trolling of the UN Migration Pact, April 2019, ISD: https://www.isdglobal.org/isd-research-featured-in-politico-surrounding-the-trolling-of-the-un-migration-pact/
15 BBC launches huge new international anti-disinformation initiative, 09 November 2018, BBC: https://www.bbc.co.uk/mediacentre/latestnews/2018/beyond-fake-news
16 Response to the UK Government policy consultation: Protecting the Debate, 16 August 2019, UK Electoral Commission: https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/response-uk-government-policy-consultation-protecting-debate
17 Charlevoix Commitment on Defending Democracy from Foreign Threats, 2018, Group of Seven: https://www.mofa.go.jp/files/000373846.pdf
18 Paris Call for Trust and Security in Cyberspace, 2019, Paris Call: https://pariscall.international/en/