TRT WORLD research centre

Déjà Vu:
Disinformation and the US Presidential Elections

Dr Tarek CHERKAOUI



(Atılgan Özdil - Anadolu Agency)

Disinformation has taken numerous forms in the past decade, particularly in the run-up to contested elections. This policy outlook examines some key disinformation methods, which were heavily utilised in the 2016 US presidential elections and are part of the influence operations surrounding the 2020 presidential elections. Four aspects will be closely examined: Data theft and data mining, trolls and bots, extremist and hate groups, and hack-and-leak operations.

The opinions expressed in this policy outlook represent the views of the author(s) and do not necessarily reflect the views of the TRT World Research Centre.

The 2016 US election cycle was one of the most controversial in recent electoral history. The campaign was characterised by an emotionally charged primary combined with high doses of hype and drama. In defiance of most polls and forecasts, the real estate tycoon and reality tv celebrity Donald Trump won the nomination of the Republican primary. This selection took place amidst vitriolic rhetoric, which revealed deep fractures within the Republican party.

The 2016 elections fused several layers of complexity, including celebrity gossip, identity politics, negative emotional dimensions, and considerable foreign interference, all of which seemed to intensify in the echo chamber of political incivility. One of the aspects that continues to warrant closer scrutiny is disinformation. The year 2016 became known as a turning point of our era, in which the blatant fraudulence and the quantities of falsehoods disseminated as part of political campaigns in the West reached unprecedented levels. It was also no coincidence that the Oxford Dictionaries chose "post-truth" as 2016's Word of the Year. At that juncture, the pollution of the information sphere was in large part instigated by far-right movements seeking to mobilise their bases as well as unaffiliated voters against centrist politicians and the mainstream media that typically conveys their message. The existing divide in US politics was enlarged by Russian meddling. A declassified report, submitted in 2017 by the US Intelligence Community to the Congress, outlined how Russian operations interfered in the months leading up to the 2016 US elections.

The Russian state, which mastered techniques of disinformation over the course of a century, has a long track record in using it both internally and externally. Given that the US devoted significant resources in the past two decades to containing Russia and its policies worldwide, the Kremlin has a vested interest in undermining institutional legitimacy in the US and weakening US political actors that the Russians see as a threat to their global aspirations. One of the shortcuts to do so is by spreading disinformation on a large scale. When applied adeptly, disinformation has the potential to disrupt the democratic order by limiting the amount of credible information people receive. As a RAND report warns, such disinformation operations aim to "achieve policy paralysis by sowing confusion, stoking fears, and eroding trust in Western and democratic institutions." The ultimate goal is to "undermine the fabric of society."

There were very heated campaigns in the past. However, candidates generally played more or less by the book, bending the truth as much as they could while avoiding blatant lies. When caught, they would provide stretched explanations and express regrets. The Trump campaign shifted the goalposts, a posture that became a feature of his presidency.

The levels of deceit and manipulation in the 2020 presidential elections are expected to surpass those of 2016. On September 17, 2020, FBI Director Christopher Wray testified in front of the US Congress and warned about the existence of "very active efforts" by state actors to meddle in the 2020 election, primarily by attempting to harm the image of Democratic presidential nominee Joe Biden. Wray singled out Russia, which has been actively using social media, as well as "proxies, state media, online journals" and other platforms to vilify Biden and what it considers as anti-Russian circles in US politics.

Disinformation is indeed rife and has taken numerous shapes, particularly in the run-up to the presidential elections. This policy outlook examines four key disinformation tools, which were utilised back in 2016 and constitute an integral part in the ongoing attempts to influence the results of the 2020 elections.



Former White House cybersecurity coordinator Michael Daniel (R) and Former US Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland (L) testify during a hearing on Policy Response to Russian Interference in the 2016 US Elections before the Senate Intelligence Committee at Capitol Hill in Washington D.C. on June 20, 2018. (Yasin Öztürk- Anadolu Agency)

Data Theft and Data Mining

In 2016, the Trump campaign foresaw the strategic importance of social media and made better use of this weapon than their opponents. Trump's digital director, Brad Parscale, stated that platforms such as Facebook and Twitter were pivotal in helping the Trump campaign to channel significant support amongst the US population and raise substantial grassroots contributions. There is nothing wrong in using these platforms to spread the campaign's messages. However, there was something more sinister, which led to a scandal about the use of personal data without consent. An investigation by the New York Times found that "the firm harvested private information from the Facebook profiles of more than 50 million users without their permission [...] making it one of the largest data leaks in the social network's history". British data analytics firm Cambridge Analytica was at the centre of the controversy through circulation of a seemingly benign application on Facebook. Initially, some 270,000 people downloaded the application and logged in with their Facebook credentials. The application harvested their data and data about their friends. This data was then passed to British academic, Aleksandr Kogan, who collaborated with Cambridge Analytica to develop psychological profiles of the app's users.[1] It allowed the Trump campaign to pinpoint possible swing voters and craft messages more likely to resonate with them.

Cambridge Analytica was incepted in 2013 with an initial emphasis on US elections. The company was bankrolled with $15 million from billionaire Republican donor Robert Mercer and had in its senior management Steve Bannon, the far-right pundit and (now former) advisor of President Trump. It started as a branch of SCL Group, a government and military contractor, working on a wide span of activities, ranging from food security research and counter-narcotics to political campaigns.

The British data company's key objective was to influence election outcomes[2] in the US and resorted to highly questionable tactics and potentially illegal deeds, such as coordinating between the Trump campaign and outside groups. An investigation conducted by British television Channel 4 exposed some of the firm's actions, revealing facets of the company's murky strategy. For instance, the firm used a secret email system where messages self-destruct and leave no trace. Similarly, the company's social media approach was deceitful. It established proxy organisations to feed negative and untraceable messages about opposition candidates onto the internet and social media. The non-traceability of some of these techniques have helped Cambridge Analytica avoid congressional investigations into their activities.

In short, the 2016 US elections became a textbook example of how citizens' personal data is procured, collected, and sold unbeknownst to the concerned. These data troves eased the job of Cambridge Analytica to use behavioural analytics and digital psychographic tactics on behalf of the Trump campaign to manipulate voters' choices.

Four years later, the situation has not improved arguably because the Trump administration and Republicans in Congress have been disinclined to tackle the issue of election security. Among the reasons behind such insouciance is the White House's concern that focusing on Russian election-meddling might raise questions about Trump's 2016 win. Kirstjen Nielsen, former US secretary of homeland security, was forced to relinquish her position after she tried to put more emphasis on tackling new and different Russian forms of interference in the 2020 election. Mick Mulvaney, President Trump's chief of staff, explained that the president equated any public conversation on harmful Russian election activity with questions about the legitimacy of his victory.

Many signs indicate that disinformation is rife in 2020. Several actors are reportedly trying to undermine election security by targeting election infrastructure. The US Department of Homeland Security defines election infrastructure as "storage facilities, polling places, and centralised vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments." In this context, Senate minority whip Dick Durbin expressed his concerns about the 2020 election outcome: "We have so much meddling going on here," adding that "We have the Russians still at work, the Chinese, perhaps the Iranians and others, we certainly have conspiracy theorists in this country."

In the interim, a wave of ransomware attacks has targeted big cities, small towns, and the contractors who supervise their voting systems. For some observers, these are clear signs that unidentified hackers are attempting to create

1 Aleksandr Kogan, an ex-psychology professor at the University of Cambridge, developed a personality quiz app called thisisyourdigitallife. This app combined individual psychological profiles with personal data scraped from the Facebook pages of quiz-takers and their online friends. That data was then developed to put forward a psychometric profile of the users, which allowed Cambridge Analytica to produce political adverts tailored to their personalities. For example, when the profile indicated that a personality is high in neuroticism, then ads featuring images of immigrants pouring into the country would likely trigger an emotional reaction in favour of Trump's anti-immigration messaging. Another tactic would be to persuade Democrat voters to stay at home.

2 In fact, Cambridge Analytica and its parent company SCL were at the heart of many influence operations around the world. In Nigeria, they were hired in December 2014 by an opulent Nigerian businessman to support the electoral campaign of the incumbent, President Goodluck Jonathan. An ex-employee of Cambridge Analytica explained this involvement. According to him, "it was the kind of campaign that was our bread and butter [...] We were employed by a billionaire who was panicking at the idea of a change of government and who wants to spend big to make sure that doesn't happen."

disorder around the election. This surge in cyberattacks is believed to be connected with Russian criminal groups. The recent targeting of Tyler Technologies, used by election officials to aggregate and report votes in at least 20 locations around the country, was particularly worrying a month before the election. Most of the 15,000 customers of Tyler Technologies are state and local government clients. They use the firm's services to offers solutions for courts, police, EMS, fire department, probation, parking tickets and water bills. According to CNN, "the company bought Socrata, an advanced AI platform in 2018, which extracts information from municipal systems giving decision-makers actionable datasets used in urban planning. A part of that includes data from elections departments, raising the concern that ransomware actors could be attempting to tamper with elections."

The ransomware attack against Tyler Technologies exemplifies a trend, in which Hackers try to log-in into the systems of individuals and organisations that are connected to the elections. Such a tactic is part of a wider disruption campaign against 'soft targets'; the kind of worst-case scenario that the Department of Homeland Security, the FBI and US Cyber Command strive to avert on election night.

Hacking is only the tip of the iceberg. The other part is represented by third-party data brokers that can easily sell[3] data to the foreign governments. It is widely known that social media and tech companies collect huge amounts of private data to enhance user experiences and generate revenue from advertising. However, not many people know that these troves of private information are sold to third-party data brokers, who can re-sell it with no strings attached.

At times, both threats merge as when hackers break into the systems of data brokers. In 2017, the credit brokerage company Equifax was hacked. Equifax later acknowledged that hackers stole the personal information of 147.7 million Americans from its servers. The data that was compromised from the breach was never retrieved, and hackers made immense profits by selling the entire database. It is believed that the Equifax hack was part of a concerted effort from Chinese intelligence services to steal trade and personal information of US nationals. Then, in 2019, 49 million business contacts, hacked from data broker LimeLeads, were put up on sale on a hacking forum. The data troves obtained from security intrusions could contribute to identity theft and phone scams as well.

In the 2020 election, the result of these massive breaches could again be deployed as part of influence campaigns by foreign parties. While the Cambridge Analytica scandal revealed in 2016 that the company created personal profiles on over 240 million Americans by mining personal data, a similar modus operandi could be at play in November 2020. The private data of US citizens has become the new battleground of international influence operations and is a weapon of choice in the 21st century's disinformation campaigns.

Bots and Trolls

Political bots have been defined as "algorithms that operate over social media, written to learn from and mimic real people to manipulate public opinion across a diverse range of social media." During the 2016 US elections, bots pervaded the core of political conversations on Twitter, where they spread disinformation on a massive scale. The influence of bots reached unprecedented levels and became central to channelling flows of information. Given the quest of the Trump campaign to ensure supremacy over the digital realm, independent research reveals that bots conveyed Trump's messaging much more than Clinton's, allowing Trump to steer discussions to his advantage.

2016 was also the year where a massive Russian influence operation took place via bots and trolls. There has been a series of revelations from Facebook and Twitter that Russian nationals used social media and political bots to push content during the elections, playing a considerable role in spreading disinformation during the 2016 contest. One of the key protagonists in this context was the Internet Research Agency (IRA), which was described in the 2017 report form the US intelligence community as a troll farm with "ties to Russian intelligence." According to an investigation by the New York Times, the IRA has become known for having hundreds of Russians on its payroll. The primary task of these individuals is to use fake accounts on social media, spread falsehoods by trolling and operating bots. The IRA's ultimate aim is to subvert US and European politics, exploit discord and division, and influence election outcomes. In 2018, the IRA and 13 Russian nationals were indicted in the US for alleged illegal interference in the 2016 presidential elections, during which they strongly supported the candidacy of Donald Trump.

Despite attempts to curb their activities on American soil, Russian operators seem to have learned from some of their blunders. According to University of Wisconsin researcher Young Mie Kim, "despite the increased transparency measures by top platforms, it looks like the Russians are taking advantage of loopholes to try and circumvent the tech platforms' defences. They have improved their mimicry behaviours, and because of their evolving tactics, it is increasingly more difficult to detect these foreign actors."

[3] For decades, data brokers in the United States have been running a lucrative business worth billions of dollars on consumer information, largely operating without regulation or consumer knowledge. There have been recent attempts in the state of Vermont to regulate the industry by establishing a data broker registry. However, this move was rather limited. Only 121 entities registered, which represents a mere fraction of the data brokerage industry. From the firms registered, only few offered clear answers about what they do with data and whether users may opt out from databases. Furthermore, the Vermont law only covers third-party data firms–those dealing with the data of people with whom they have no relationship–as opposed to 'first-party' data holders like Amazon, Facebook, or Google. Data brokers fundamentally lack transparency regarding their practices.



Facebook co-founder, Chairman and CEO Mark Zuckerberg testifies before the House Energy and Commerce Committee on Capitol Hill April 11, 2018 in Washington, DC. This is the second day of testimony before Congress by Zuckerberg, 33, after it was reported that 87 million Facebook users had their personal information harvested by Cambridge Analytica, a British political consulting firm linked to the Trump campaign. (Yasin Öztürk - Anadolu Agency)

Kim also noted that in 2020, Russian operators have become more fixated on impersonating genuine domestic US organisations or claiming links to them. These info-warriors are keen to find cracks in the societal fabric and discover social, economic, or racial divides that they can exploit to weaken collective trust in institutions and governments. In this context, Kim highlighted some examples such as a post from a racially charged Instagram account called "iowa.patriot," who posted an anti-Elizabeth Warren meme. Another one was named "Bernie.2020_" and used campaign logos to make it appear as if it was connected to Sanders' campaign. These are merely a few examples of dozens that targeted specific communities in crucial swing states like Michigan, Ohio and Iowa with divisive messaging on race relations, gun laws and immigration.

This does not mean that Russian operators were the only ones responsible for bot manipulation. Other protagonists include fringe political forces and rogue campaigners, who copied the Russians' modus operandi and refined their blueprint further. Recently, Twitter suspended several fake accounts posing as black supporters of President Trump. Many have tweeted the same phrase: "Yes I am Black, and I am voting for Trump." In a piece published by the Columbia Journalism Review, Bob Moser warned about the rise of domestic operators in the disinformation campaigns connected to the 2020 elections. He outlined a series of tactics put forward by domestic trolls which were used to undermine Trump's rivals in the road to the 2020 elections.

Massive volumes of manipulation were peddled by trolls, who concocted falsehoods at every turn to smear anti-Trump candidates. For instance, when a mass shooter embarked on a killing spree in Odessa, West Texas, trolls quickly circulated a fake story that the killer had a sticker of the democratic candidate, Beto O'Rourke on his truck. Evidently, by the time journalists investigated the claims and debunked them, the information had circulated widely on social media. The Facebook post amassed more than 15,000 likes and 11,000 retweets. This disinformation scheme took place amidst complete apathy from Facebook and Twitter.

Such lack of responsiveness prompted Siva Vaidhyanathan, a media studies professor at the University of Virginia, to declare: "We will not need Russia in 2020. We will hijack our democracy ourselves. And Facebook is sure to be a major factor in that hijacking – once again." Some observers have hinted that Facebook benefited significantly from the controversies stirred by Trump, as well as his policies. Former CIA officer Yaël Eisenstat, who worked briefly as Facebook's global head of elections integrity operations, business integrity, expressed her concerns. She stated: "I find Mark Zuckerberg's reaction to different politicians to be very telling. I do not want to imply that he is purposely trying to get Donald Trump re-elected. But it is in his best interests to have this administration stay in power rather than to have a new administration that will regulate or break up his company."

Extremist and Hate Groups

One of the seismic shifts caused by social media sites is that they provided a lifeline to extremist views. In the past, extremists from all prisms used to face enormous challenges to get their opinions on mass media. However, in the age of Facebook and Twitter, all shared content looks identical no matter their origin. Whether it is an article written by a prominent investigative journalist after months of diligent work or tabloid-like verbiage produced in less than an hour, both items will be placed in the same space and be subjected to the same aesthetics, thus confusing audiences. Some stories, which operate completely outside the realm of facts, would have never found an audience in the past. However, because of social media, they are enjoying high levels of viewership.

A second facet, which empowers hate groups and extremist view, is the informational cascade phenomenon. As explained by American legal scholar Cass Sunstein, "in an informational cascade, people cease relying, at a certain point, on their private information or opinions. They decide instead on the basis of the signals conveyed by others. Social media provide an obvious breeding ground for cascades. As a result, thousands or even millions of people who consult sources of a particular kind will move in one or another direction, or even believe something that is quite false." When more people start sharing content about particular subjects, others tend to emulate them, creating additional buzz around these articles. These dynamics allow certain extremist views and analysis to get enormous reach and traction, accelerating the mainstreaming of such fringe opinions.

A third feature is the echo chambers and filter bubbles which create even more polarisation. It allows some ideas to spread among like-minded people, creating a herd mindset. This mentality considers opposing arguments as hostile, leading to isolation from other thoughts undercurrents. According to Sunstein, the herd mentality allows the leadership of these groups to dismiss ideas from outside the group easily.

The algorithms of social media sites are generated to pick up cues for high engagement and curate them to keep audiences interacting on these subjects. A New York Times columnist pointed to some of these methods in a piece entitled "YouTube, the Great Radicalizer". The author noticed in the course of her research on Donald Trump's voter base how YouTube started to recommend and "auto-play" videos that featured white supremacist tirades and other extremist subjects. She continued with her experiments and soon reached a conclusion that "YouTube was recommending content that was more and more extreme than the mainstream political fare [she] had started with."

These extended interactions by social media organisations generate the interest of advertisers and allow these platforms to make huge financial returns. In return, social media organisations give little scrutiny to the content of the ads. Despite the recurrent outcry from legislators and civil society organisations about the need to fix these issues to prevent extremist views from gaining traction in the public sphere, such complaints have often fallen on the deaf ears.

There have been some attempts by social media organisations to take action on this issue. For example, in May 2020, Twitter labelled a few of the President's tweets as inaccurate. For years, this social media platform was permissive of Trump's tweets, which often contained falsehoods and threats. However, this fact-checking action by Twitter provoked the ire of the President, who issued an executive order threatening to remove some of the legal protections given to social media platforms that 'censor speech for ideological reasons'. He also incited his followers to organise a smear campaign against Twitter via social media, digital forums and via local legislators.

Nevertheless, action undertaken by social media organisations to deal with these issues were still perceived as inadequate. Yaël Eisenstat expressed her scepticism towards the ability of Facebook me to address the issues at stake. According to her, "they are making all sorts of reactive changes around the margins of the issues, [to suggest] that they are taking things seriously – such as building an ad library [...] – things they should have been doing already. However, they were never going to make the fundamental changes that address the key systemic issues that make Facebook ripe for manipulation, viral misinformation and other ways that the platform can be used to affect democracy."

Similar concerns were further prompted by a memo issued by Andrew Bosworth, a Facebook executive close to Mark Zuckerberg. In this memo, titled "Thoughts for 2020" and posted on the firm's internal network, Bosworth, who oversaw Facebook's advertising efforts during the 2016 election, stated that President Trump's savvy use of Facebook's advertising tools "very well may lead to" his re-election.

These dynamics were already at play in the 2016 elections. Back then, social media played a pivotal role in transforming the likes of Breitbart and other 'alt-right'[4] organisations from fringe players to key mobilising engines for millions of disgruntled voters. According to journalists Michael M. Grynbaum and John Herrman, Breitbart rivalled "news organisations like The Washington Post and Yahoo on Facebook", and "has challenged conservative favourites like Fox News in its influence on the campaign, if not in the size of audience". The alt-right nexus drew its appeal from the anti-immigration and anti-establishment campaign themes of Donald Trump. They used these themes and continuously pushed the boundaries via provocations and sensationalism until many of their views poured into the mainstream.

4 Short for alternative right. This semantical design is an attempt to dress up white supremacy and make it politically acceptable.



"Save Our Children" is a term that has been taken over by the QAnon conspiracists as Right-wing demonstrators, many armed, clash violently with Black Lives Matter and Antifa counter-demonstrators, in Portland, Oregon, United States on August 22, 2020. (John Rudoff - Anadolu Agency)

Breitbart and other alt-right organisations continue their activities in 2020. However, they have been outshined by other fringe players, such as QAnon. The latter is coming with force into the mainstream thanks to social media. In 2019, the FBI cited QAnon as one of the most dangerous conspiracy theories that poses a domestic terrorist threat to the US. With the events of 2020, such as the Covid-19 pandemic and Black Lives Matter, QAnon emerged as "one gigantic mass of suspicion." The movement now has several candidates running for office, and it was reported by Newsweek that at least 44 people with connections to QAnon were running for Congress, state legislatures, and mayoralties. President Trump and his campaign have tacitly embraced QAnon and circulated some of its accounts and memes.

Covid-19 played a leading role in energising QAnon's rhetoric. As millions of people were affected by the pandemic, and many questions were left unanswered, the group offered its absolutist take on coronavirus-related issues. Questions concerning mask-wearing, social distancing, vaccinations, herd immunity, whether the pandemic is a deception, whether Bill Gates is the person responsible for this problem, and so forth, were tackled through a binary approach, leaving no space for nuanced answers and informed commentary.

The combination of conspiracy theories, informational cascades, and echo chambers acts as an effect multiplier for hate and extremist groups. They create a sort of siege mentality, convincing their partisans that unknown forces, often characterised as the deep state or satanic cabals, are allegedly taking over the country. These narratives allow them to pin the blame for the deterioration of their economic and social conditions on these unknown parties while absolving the incumbent president from any wrongdoings.

Thanks to social media, new horizons have opened to their propaganda that aims to increase the racial divide, fuel issues of immigration and religion. Their new goal is to influence the 2020 presidential campaign. This endeavour will represent yet another milestone in their attempt to move from an online cultural force to become a major political player in the country.

Hack-and-Leak Operations (HLO)

Hacktivism, which has been originally defined as a marriage between political activism and computer hacking, has long been the target of law enforcement agencies. In the 2000s, hacktivist collectives, such as Wikileaks and Anonymous, became known to the general public through their Distributed Denial of Service (DDoS) attacks against symbols of US capitalism, shutting down the websites of PayPal, Visa, MasterCard, and the Bank of America.



WikiLeaks founder Julian Assange. (Maurizio Gambarini - Anadolu Agency)

They also gained in popularity by providing platforms to whistle-blowers and exposing state secrets and evidence of war crimes. For instance, WikiLeaks became widely known when it released a video of a US helicopter opening fire on a Baghdad street in 2010, killing many civilians including two journalists from Reuters. They also leaked troves of confidential documents on the US-led wars in Iraq and Afghanistan, which exposed a systematic whitewash of civilian casualties.

Initially, these groups used HLO techniques to cause a stir and disrupt normal operations, but apart from being a nuisance to the US image abroad, these actions did not cause severe damage. Therefore, some academics dubbed them 'cyber-vigilantes,' while others depicted them as extraordinary bandits or 'e-bandits' who typified modern-day Robin Hoods. However, hacktivist collectives have evolved since then. In the prelude to the 2016 US elections, many of these groups became involved in more serious crimes, such as cyberespionage and information warfare campaigns.

The cyberattack on the Democratic National Committee (DNC) in 2016 was a defining moment in the cyber blitzkrieg against the Democrats. Using a seven-month infiltration strategy, via spear-phishing emails, thousands of emails from the top echelons of the Democratic Party were exposed, including Hillary Clinton's campaign chairman, John D. Podesta, whose private email account was also hacked. These leaks harmed the campaign of Hillary Clinton beyond repair and tilted the election in favour of her rival Donald Trump. This operation, which had the fingerprints of Russian operatives all over it, took place simultaneously with a similar covert action. The latter targeted the Democratic Congressional Campaign Committee, causing many Democratic house candidates to lose their seats.

Similar attempts are taking place in 2020. A report issued by Microsoft warned about the interference of foreign states in the US elections. This warning is consistent with the findings of federal agencies, which named Russia, China and Iran as three countries trying to obtain information about the campaigns. The Microsoft assessment concluded that Strontium, a hacker collective operating from Russia, has attacked more than 200 organisations including political campaigns, advocacy groups, parties and political consultants.

Meanwhile, the Microsoft report also indicated that Zirconium, operating from China, launched attacks on the private email accounts of Biden's campaign staff members, along with a range of other academics and think tankers, including institutions such as the Atlantic Council and the Stimson Centre. The hacking attempts also targeted personnel at Washington-based SKDKnickerbocker, a strategic communications firm working with Biden and other Democrats.

The Microsoft report also stated that hackers affiliated with Russian military intelligence – the same unit that spearheaded the HLO efforts in 2016 - are going the extra mile to conceal their activities. Increasingly, they are using services, such as Tor, which help hide the identity and location of the hackers.

Subsequently, the Biden campaign said that it was "aware of reports from Microsoft that a foreign actor has made unsuccessful attempts to access the noncampaign email accounts of individuals affiliated with the campaign," and that it was preparing for the inevitable barrage of hacking attempts in the campaign trail.

Conclusion

The 2020 US elections constitute a very important threshold for the future of democracy in the country as well as the future of political communication. Internet and social media networks have had a profound effect on the political field in the US. Multiple players, both domestic and international, now have the opportunity to influence the mindset of the American population and sway large portions of the public towards particular candidates. US authorities have multiplied their efforts to monitor the cyberspace and try to stop any foreign meddling. However, the successful interference back in 2016, combined with toxic politics, paves the way for computational propaganda to be omnipresent in the upcoming elections.

Echo chambers and filter bubbles further exacerbate the existing polarisation. The fact that the information consumed does not need to align with the dominant discourse or with the truth has created pockets of digital tribalism, further insulating these 'tribes' from the rest of the country. These developments make disinformation a potent weapon capable of mobilising millions of people to take political action and possibly change the course of the elections.