Computational propaganda techniques

The techniques used by anti-democratic state and non-state actors to disrupt or influence democratic processes are constantly evolving. The use of algorithms, automation and artificial intelligence is boosting the scope and the efficiency of disinformation campaigns and related cyber-activities. In response, the EU is stepping up its efforts to protect its democratic processes from manipulation ahead of the European elections in May 2019.

Background: evolving information influence techniques

Computational propaganda has been defined as 'the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks'. These activities can feed into influence campaigns: coordinated, illegitimate efforts of a third state or non-state agent to affect democratic processes and political decision-making, including (but not limited to) election interference. Experts assert that disinformation (deliberately deceptive information) turns one of democracy's greatest assets – free and open debate – into a vulnerability. This affects us all: by 2020, virtually everyone in the world will be online. Two-thirds of US adults and over half of Europeans get their news on social media, despite concerns over inaccuracy. Social media are key for young people to develop their political identities.

Algorithms, bots, trolls and artificial intelligence

Algorithms on social media and search engines

Algorithms are processes in (computational) calculations or operations. Online platforms such as Google, Facebook and Twitter use various algorithms to predict what users are interested in seeing, spark engagement and maximise revenues. Based on a user's habits and history of clicks, shares and likes, algorithms filter and prioritise the content that the user receives. As users tend to engage more with content that sparks an emotional reaction and/or confirms already existing biases, this type of content is prioritised. This can isolate different user groups within echo chambers: social spaces that reinforce beliefs among like-minded users, contributing to political polarisation. When data from 87 million Facebook users (including that of 2.7 million EU citizens) were improperly shared with the political consultancy company Cambridge Analytica, data about sexual orientation, race and intelligence were gathered by algorithms and used to micro-target and mobilise voters in the US presidential election and the UK referendum on EU membership. Calls for greater algorithmic accountability and transparency keep mounting.

Bots: automated accounts

A bot (short for robot) is an automated account programmed to interact like a user, in particular on social media. For disinformation purposes, illegitimate bots can be used to push certain narratives, amplify misleading messaging and distort online discourse. Some of the bots used to spread disinformation in the context of the 2017 French presidential election had previously been used in the US election to spread pro-Trump content, indicating that there is a black market for reusable disinformation bot networks. Responding to growing concern about the impact of disinformation bots, Twitter suspended up to 70 million accounts between May and June 2018. Facebook removed 583 million fake accounts in the first quarter of 2018 in an attempt to combat false news. Experts predict that the next generation of bots will use natural language processing, making it harder to identify them as bots.

Trolls: online bullies

Trolls are human online agents, sometimes sponsored by state actors to harass other users or post divisive content to spark controversies. However, ordinary citizens can also engage in trolling activities. One prominent example of coordinated, state-sponsored trolling is the Russian Internet Research Agency IRA), based in St Petersburg and run by Yevgeny Prigozhin, a close aide of Russian President Vladimir Putin. In February 2018, US Special Counsel Robert Mueller indicted Prigozhin and 12 other individuals for their roles in the 2016 US presidential election. On 17 October 2018, Twitter disclosed data on millions of tweets, images and videos linked to troll farms in Russia and Iran, shedding light on their activities from 2013 to 2018.

Author: Naja Bentzen, Members' Research Service

Artificial intelligence, MADCOMs and deep fakes

Machine-driven communications (MADCOMs) marry artificial intelligence (AI) with machine learning to generate text, audio and video content, making it easier to tailor messages to individual users' personalities and backgrounds. For example, MADCOM can use chatbots using natural language processing to engage users in online discussions, or even to troll and threaten people. As deep-learning algorithms evolve, it is becoming easier to manipulate sound, image and video for impersonation, or to make it appear that a person did or said something they did not ('deep fakes'). This will make it increasingly difficult to distinguish between real and (highly realistic) fake audiovisual content, further hampering trust online.

Related cyber-activities

Disinformation activities are often combined with cyber-attacks, such as hacks, during which information is collected and selectively leaked to undermine the adversary. The main state actors involved in cyber-attacks on foreign adversaries are China, Russia, Iran and North Korea. A number of techniques are described below.

Spear phishing

In spear phishing (targeted phishing), emails with infected attachments or links are sent to individuals or organisations in order to access confidential information. When opening the link or attachment, malware is released, or the recipient is led to a website with malware that infects the recipient's computer. During the 2016 US presidential campaign, Fancy Bear – a hacker group affiliated with Russian military intelligence – used spear phishing to steal emails from individuals and organisations associated with the US Democratic Party. The online entities DCLeaks and Guccifer 2.0 leaked the data via media outlets and WikiLeaks to damage Hillary Clinton's campaign. In July 2018, Special Counsel Robert Mueller indicted 12 Russian intelligence officers alleged to be behind the attack. Another state-sponsored Russian hacker group, Cozy Bear, has used spear phishing to target Norwegian and Dutch authorities. This prompted the decision to count the votes for the 2017 Dutch general election by hand.

Distributed denial of service (DDoS)

In DDoS attacks, massive amounts of information are sent to targeted websites, overloading and freezing them. In the first known coordinated cyberwar against a country, the removal of a Soviet war memorial in Estonia sparked street protests, followed by cyber-attacks, including DDoS attacks that paralysed the government, banks, telecommunications companies, internet service providers and media outlets for weeks. Estonia blamed Russia for the attacks. The Kremlin denied any involvement. In July 2018, hackers used DDoS to disrupt Democratic campaign websites during the US primary election campaign.

Brute force attacks on internet of things (IoT) devices

Ahead of the July 2018 summit between US President Donald Trump and Russian President Vladimir Putin in Helsinki, China-based hackers launched a wave of attacks on IoT devices in Finland, aiming to take control of the devices to collect audio or visual information. IoT devices are often poorly secured, thus vulnerable to brute force attacks – trial-and-error attempts to crack a password – on remote management ports.

Related EU policy responses: defending democratic elections in a digital age

In his 12 September 2018 state of the Union address, President Jean-Claude Juncker announced the Commission's proposed new rules to protect Europe's democratic processes from manipulation by third countries or private interests. These measures, as laid out in the Commission's September 2018 communication on securing free and fair European elections, include recommendations on election cooperation networks, online transparency, protection against cybersecurity incidents and steps to counter disinformation campaigns in the context of the European elections. As election periods are a strategic target of hybrid threats, the Commission and the High Representative identified steps in June 2018 to boost resilience and capabilities. Increased EU-NATO cooperation on hybrid threats has materialised in the European Centre of Excellence for Countering Hybrid Threats, established in Finland in 2017. Following Parliament's call to look into the problem of fake news, in its 26 April 2018 communication on online disinformation the Commission issued an action plan and proposed tools to counter online disinformation, including a code of practice for online platforms to increase clarity about algorithms and close down bots and fake accounts. The Facebook/Cambridge Analytica revelations highlighted the relevance of the EU's General Data Protection Regulation, which took effect on 25 May 2018 and gives the EU tools to address the unlawful use of personal data, including during elections.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.