JACQUES DELORS INSTITUTE
BERLIN
Centre for European Affairs at the Hertie School of Governance

POLICY POSITION 13.11.2018

EP19: The Shadow of Disinformation

Paul-Jasper Dittrich Policy Fellow at the Jacques Delors Institute Berlin

Computational propaganda and online election interference pose a threat to the conduct of free and fair elections and to the legitimacy of the democratic process itself. Since the last EP elections in 2014 a string of votes worldwide were marked by disinformation campaigns, manipulation of social media algorithms and other attempts of online interference, among them the Brexit referendum as well as elections in the Philippines, the US, Italy and Brazil. Both domestic and foreign actors make use of online propaganda. Against this background it is of little surprise that the European Commission and national governments are increasingly worried about the safety, integrity and legitimacy of the European Parliament elections of May 2019 (EP19).

"FAKE NEWS" IS A MISLEADING TERM

The problem is however more complicated than "Fake News", which is an imprecise, often inaccurate and academically discharged term to analyse computational propaganda and election interference. To identify possible threats in the context of the EP19 elections, we should instead look at four tactics and tools that have been deployed before:

1.) Disinformation: Deliberate spread of misleading, enraging, conspiracy-laden and hateful content out of financial or political motives on a massive scale; often targeted and "customized"
2.) Inauthentic amplification: Massive use of inauthentic accounts (spam bots, multiple accounts operated by one person, paid "Super Posters") to artificially increase the reach and "virality" of political messages and trick algorithms, often in combination with 1.)
3.) Information Operations: In the context of elections, organized online propaganda campaigns by foreign state or non-state actors, using 1.) and 2.) , but also tactics such as strategic hacking and subsequent leaking of compromising material
4.) Infrastructure attacks: Cyber-attacks on election infrastructure such as registration databases, voting machines or counting software

Which of these threats will the EU exactly be up against in the coming months? The degree and kind of interference is hard to predict. Malevolent actors, domestic and foreign, adapt to technological innovations, new user patterns and attempts of online platforms to curb the spread of disinformation. They constantly change and update their tactics and distribution channels. Services like WhatsApp or Instagram for example have gained in popularity for political communication and the spread of disinformation (end-to-end encrypted in the case of WhatsApp) and have taken over Facebook in recent years. The EP19 also consist of 27 national elections, each with their individual threat scenario. Some member states have a very high proliferation rate of social networks and high levels of news consumption on social media, others don't. Countries with "exotic" languages like Lithuanian or Basque might be more exposed to disinformation as

there are less native-speaking content moderators. A country like Latvia, with a large minority of ethnic Russians, is exposed very differently to Russian information campaigns than Italy where online manipulation tactics appear to be mostly applied by domestic actors such as League or Five Star Movement supporters. Estonia, where up to 25% of the population vote online, faces a different danger of election infrastructure hacking than Germany where the act of voting is still done with pen and paper.

A "EUROPEAN ELECTION CRISIS CENTRE"

The Commission has started to take action against online disinformation in recent months. It agreed a Self-regulatory Code on Disinformation with the largest social media platforms and recommended further measures to national governments such as transparency for political online advertisement. The General Data Protection Regulation (GDPR) provides more legal instruments to deal with parties or organizations, which violate data protection regulation to amass voter profile data. The five most important platforms – Facebook, Instagram, WhatsApp, Twitter and YouTube – have themselves continuously stepped up their efforts. Facebook alone deleted 583 million fake accounts and 865 million posts, mostly spam, in the first three months of 2018. The platforms are now employing tens of thousands of content moderators worldwide and improve their detection algorithms.

These steps are relevant, but cannot guarantee an effective curbing of disinformation. The presidential election in Brazil has shown that the large platforms are seemingly overwhelmed with the amount of content generated by its users (100 billion messages daily on all Facebook services alone, in hundreds of languages) and ever-changing tactics to trick their algorithms and filters. The EU should do more to follow through on its proposal to support member states in ensuring the resilience of their elections. The difficulty to predict exact threat levels for each member state should not hamper the EU's ability to react if a crisis erupts. The EU institutions are in the best position to identify and monitor transnational disinformation campaigns and narratives, even if they only occur in a handful of member states. The EU is also the best level to coordinate help for smaller countries. Finally, the Commission is the most important interlocutor for global online platforms since it oversees the Single Market. It can put much more pressure on them than single governments, which might prove crucial in the critical weeks before the elections.

To help secure the EP19 elections, the EU should thus create a "European Election Crisis Centre" to combat disinformation during the campaign. This centre should build on the experience made with the EU's East StratCom Task Force on Russian disinformation. It could be established as an inter-institutional task force bringing together experts from the EP, the Commission and the External Action Service. It would compile evidence of disinformation from member states by receiving input from national governments, NGOs, researchers and journalists. It should be able to swiftly identify and compare conspiracy theories and narratives as they spread across member states, develop counter-narratives and coordinate national responses. It could support member states with fewer capacities to react and serve as a central communication node with the online platforms. Immediate naming and shaming might force them to react faster to rapidly evolving tactics of disinformation. The centre could even become a permanent after the campaign and inform policy makers with regards to future regulatory steps.