SWP

SWP Comment

NO. 16 MARCH 2019

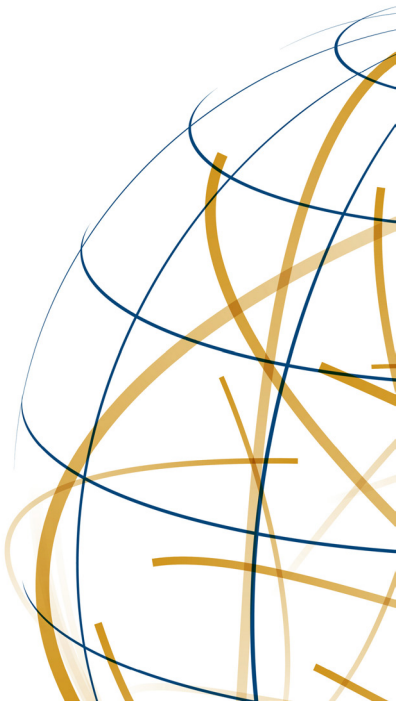
Disinformation and Elections to the European Parliament

Annegret Bendiek and Matthias Schulze

Elections to the European Parliament (EP) will take place in May 2019. Politicians and experts fear that the election process might be disrupted by disinformation campaigns and cyber attacks. In December 2018, the European Commission presented an action plan against disinformation. It provided 5 million euros for raising awareness amongst voters and policymakers about manipulation, and for increasing the cyber security of electoral systems and processes. The strategy relies on voluntary and non-binding approaches by Internet companies to fight disinformation. To protect the integrity of elections in the medium term, independent research into technical, legal and market-regulating reforms must be boosted. The objective should be to preserve the functionality of democracies and elections in the age of digitalisation.

The next European elections will be held in EU member states from 23 to 26 May 2019. Since right-wing nationalist and Euro-sceptic movements have gained in strength, there is already talk of a "defining election" that could decisively influence the future orientation of the EU. Euro-sceptic parties already account for almost one-third of parliamentarians, a proportion that might rise following the elections.

EP elections have thus far been seen as "second-rank elections" and therefore as a good opportunity by the electorate to teach the respective member state's government a lesson. This attitude fails to appreciate the mobilisation potential of the current debate on the pros and cons of European integration, the influence of third parties, and the growing importance of the EP. The elections are extremely significant for the strategic orientation of European integration. A success for EU opponents could push the EU to the very limits of its capacity to act, for example through further exit demands along the lines of Brexit, or a blockade of the complex decision-making process. The elections not only decide the renewal of the EP, but also the inauguration of the new EU Commission for the 2019—2024 parliamentary term. The EP influences the appointment of the Commissioners and can force the entire Commission to resign with a two-thirds majority and realign the Multiannual Financial Framework.



Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Challenges

The EU's structure and functions are not easy to understand. European issues are unfamiliar to many, and it is relatively simple to spread false information about the EU. Considering the upcoming election, the European Commissioner for the Security Union, Sir Julian King, urged member states to "take seriously the threat to democratic processes and institutions posed by cyber attacks and disinformation" and to draw up "national prevention plans" to prevent "state and non-state actors from undermining our democratic systems and using them as weapons against us". This specifically includes disinformation campaigns and cyber attacks on the electronic electoral infrastructure, which can affect the confidentiality, availability and integrity of the electoral process.

Disinformation already appears to have had an impact in Europe: researchers at Edinburgh University identified over 400 false accounts on social networks, operated by so-called trolls based in St Petersburg, which were used to influence the Brexit referendum. Security and defence policy defines disinformation and cyber attacks as elements of hybrid threats, i.e. covert actions by third parties aimed at destabilising Europe or the EU system. The term "hybrid threats" usually refers to a form of warfare that remains below the threshold of using military force. This ambiguity generally complicates a military response according to international humanitarian law.

Disinformation Campaigns

Disinformation is not a new phenomenon. In security research it is regarded as "black" propaganda, since it seeks to influence public opinion from the shadows. It uses the same means as modern public relations (PR) and advertising campaigns.

In contrast to PR, however, disinformation wants to destabilise the pillars of democracy by attacking parties, elected politicians or the EU as a political system. Disinformation does not necessarily mean false information, since even true statements taken out of context can be misused for suggestive conclusions. Disinformation campaigns can be short-term, for example to influence an election result, or long-term, for instance to undermine confidence in the EU. Attempts can thus be made to discredit individual politicians so as to prevent them from being re-elected. For example, "negative campaigning" can uncover alleged scandals or make accusations of corruption. During the last presidential election campaign in the USA, automated computer programmes known as Twitter bots, probably of Russian origin, spread predominantly negative reports about Hillary Clinton and relatively positive reports about Donald Trump. In the medium term, this promotes social division and the polarisation of public discourse.

The negotiation of political interests in social discourses is the key element — but also the Achilles heel — of democracies. Tactics such as disseminating dubious claims ("muddying the waters") or constantly repeating large volumes of false information or conspiracy theories ("firehose of falsehood") are used to undermine political certainties and dissolve a socially shared concept of truth. One example was the reaction to the downing of a Malaysian passenger plane in July 2014: on social networks, there were attempts to discredit the investigation report which found that the Russian armed forces had caused the catastrophe.

IT-Enabled Disinformation

A distinction must be made between digital and IT-enabled disinformation: digital disinformation encompasses the entire range of digital mechanisms for disseminating information. IT-enabled disinformation, on the other hand, includes hacking incidents or cyber attacks that compromise IT security, namely confidentiality, availability and integrity of data or systems. The technical hack is only one of many means by which the confidentiality of information can be violated, for example by stealing sensitive information from the accounts of politi-

cians, parties or officials and then publishing it with harmful intent (doxing). Well-known examples are the publication of e-mails from the US Democratic National Committee (DNC) on the WikiLeaks platform in 2016 and from the Emmanuel Macron campaign team in 2017.

The restriction of the availability of technical systems via cyber attacks can facilitate disinformation campaigns as well. Especially in authoritarian regimes, websites of opposition politicians, parties and services such as Twitter and Facebook are deliberately paralysed shortly before elections by "distributed denial of service" attacks, meaning the deliberate overload of the server concerned. Similarly, the digital voting infrastructure with its voting computers and counting systems can be disrupted and manipulated.

Digital Disinformation

Digital disinformation has the advantage of having low costs while having a high impact: with few resources, a global audience can be reached with customised disinformation through digital technologies. Digital disinformation employs the legitimate means of the advertising industry to target users based on their individual behaviour profiles (so-called "targeted ads" and "micro-targeting").

Social networks such as Facebook were not developed for the purpose of democratic discourse, but to analyse and categorise their users' interests and behaviour, and sell this information to third parties for advertising purposes. According to their behaviour patterns, users will be shown content that other users of the same category or with a similar behaviour profile also prefer. Algorithms thus ensure that users are shown more of the same so as to hold their attention and keep it on the platforms as long as possible. These so-called filter bubbles arise directly from the business model of online platforms to bring advertising to as many users as possible. If the same opinions are grouped together and, simultaneously, differing views are hidden, a self-referential "echo chamber" can develop. In online forums that bring together only like-minded users, the latter's perceptions tend to be strengthened because they do not experience any contradiction.

Disinformation has a particularly polarising effect on already politicised groups with strong ideological stances. These can be deliberately targeted with conspiracy theories that fit their worldview. One example is the campaign against alleged rape by asylum seekers, the so called Lisa case of 2016. During the 2016 US election campaign, there were incidents where supporters of the right-wing Alternative Right movement and left-wing groups were separately invited via Facebook to take part in the same demonstration, in the hope of provoking a violent escalation.

Conspiracy theories and disinformation can quickly be shared worldwide over social networks. This can be accomplished using a mix of automated accounts ("social bots"), hybrid accounts (partly human, partly automated) and so-called troll armies or 50-cent armies. Such "armies" consist of state actors or privately organised commentators who systematically disseminate certain narratives in social media or on news sites. Often volunteers also unknowingly spread disinformation ("unwitting agents"). In the 2016 US election campaign, US citizens spread Kremlin propaganda without knowing its source. But traditional media coverage is also involved, as it increasingly takes up trending topics from social networks. If these contain disinformation, and the media carries them unreflectively, they reinforce the narratives or false reports. Disinformation has a cumulative effect over longer periods of time.

EU Counter-Strategies

Holding EP elections is the responsibility of member states. Although they are doing much to protect the integrity of elections, mostly this is in the form of patchwork measures. There are concerns that the EP

elections will be manipulated, disrupted or unlawfully influenced by opponents of the EU, whether during the election campaign, at the ballot box or during the counting of votes. According to a Eurobarometer survey, 83 percent of Europeans are worried about targeted disinformation on the Internet. The EU expects that targeted disinformation campaigns will be present during election campaigns.

Disinformation Warfare

Since 2015, the European Commission has been attempting to combat disinformation and technical influences using foreign and domestic policy measures. It has, inter alia, increased staffing and funding for the European Network and Information Security Agency (ENISA) and set up an East StratCom Task Force within the European External Action Service (EEAS). The Task Force documents and regularly informs about disinformation campaigns in the north-eastern member states. This was followed in 2016 by a Joint Communication and a Joint EU Framework for Countering Hybrid Threats. The Commission and the EEAS agree that such threats are increasingly causing trouble in the EU.

The EU defines hybrid threats as "a mixture of military and civilian warfare by state and non-state actors such as covert military operations, intense propaganda and economic harassment". These aggressions, it believes, not only cause direct damage and exploit vulnerabilities, but also destabilise societies and promote the division of the EU "through cover-ups". Internal and external security must therefore be even more closely interlinked.

Commission President Jean-Claude Juncker, in his speech on the state of the Union 2018, proposed a series of concrete measures to ensure that the May 2019 elections are free, fair and secure. Among other things, he called for more transparency in (often covert) political advertising on the Internet, and the possibility of sanctions if personal data are used illegally to influence the outcome of the European elections.

Networks such as Facebook, Twitter and YouTube have agreed on a Code of Practice on Disinformation to combat disinformation and fake accounts on their platforms. In October 2018, this Code was signed by Facebook, Google, Twitter and Mozilla, as well as professional associations operating online platforms and the advertising industry.

Two months later, the Commission and the EU High Representative for Foreign Affairs and Security Policy presented an action plan against disinformation. Both launched the creation of an early warning system for information about disinformation. Five million euros and 50 staff positions were approved for it. The system is meant to be able to identify campaigns in real time and raise awareness of the problem.

Since the EU fears being misrepresented beyond its borders as well, other teams are monitoring the spread of misinformation in North Africa, the Middle East and the Balkans. Furthermore, it has set up an electoral network, elaborated a guide to the application of EU data protection law in elections, and given guidance on cyber security. As of February 2019, member states will be running a simulation of what would need to be done in the event of an attack. EU states rely on the exchange of experience. Further meetings are scheduled for spring 2019. In late January 2019, the Commission warned Internet companies that their transparency initiatives against covert advertising were not sufficient to protect the integrity of EP elections.

Cyber Security Measures

What is the EU doing about IT-enabled disinformation? Critical infrastructure protection has long been subject to EU regulation. However, member states were unable to agree on defining voting systems as critical infrastructure as part of the 2016 Network and Information Security (NIS) Directive. The IT security of voting technology was considered a purely national task. However, reports of alleged influence on the Brexit

referendum and elections in France, Catalonia and Belgium, have increased sensitivity to the problem. In September 2017, the EU proposed a whole range of cybersecurity measures, including a pan-European network of cooperation between data protection authorities, to share knowledge on how elections are influenced. Only in December 2018 did EU states agree on a cyber security law that will strengthen the cyber security agency ENISA, and for the first time create a certification framework for the protection of critical infrastructures.

When, that same month, a hacker published explosive data on Twitter under the pseudonym "0rbit", politicians demanded an "emergency plan to be able to react within a short time to the outflow of sensitive data, digital industrial espionage or sabotage". There are also calls for uniform minimum legal standards for the security of information technology equipment, which would mean replacing the voluntary certification framework of the EU by a European regulation. This would apply, for example, to end-user devices such as mobile phones and laptops. Providers of online services and manufacturers of devices connected to the Internet would need to design their products in such a way that users must choose strong passwords and update them regularly.

As well as making technical infrastructures more robust, the EU relies on operational cyber security measures. These include the development of better attribution capabilities for cyber attacks, an exchange of information, and a stronger role for Europol in the fight against cybercrime. If member states become the target of such attacks, they should be able to find out for themselves where the attacker came from, which security gaps were used, and which data was affected or extracted. The discussion will focus on harsher penalties for cybercriminals and new criminal offences, such as the operation of criminal infrastructures. With principles such as "security by design", i.e. the development of hardware and software that seeks to avoid weak points and manipulations from the outset, the General Data Protection Regulation (GDPR) contains a further building block for action against cyber attacks and disinformation. In January 2019, the EU also agreed on a relevant law that allows for fines to be imposed on political parties and foundations that violate data protection rules in the European election campaign in order to influence voters. Parties can even lose all claims to EU party funding. The reason for this regulation was that Facebook had passed on user data to the British company Cambridge Analytica, which evaluated the data records of 220 million American Facebook users to create user profiles for targeted advertising.

Cyber Security in Elections

What measures are being taken to ensure the confidentiality, availability and integrity of electronic voting systems? Following reports alleging that the US elections were unlawfully influenced, the Council of Europe's Venice Commission has been in close contact with the electoral agencies of the 61 Council members. Electronic voting systems in member states vary widely. Electronic voting in the EU has so far only been used in Belgium, Bulgaria, Estonia and France. In Belgium, Flemish municipalities in particular use voting machines. In Bulgaria, such machines will only be used in smaller polling stations in the 2019 EP elections. In France, the use of voting machines was suspended during the 2017 presidential election due to the alleged incidents in the US election. In other countries, such as Germany or Austria, voting is exclusively by ballot paper, with information technology being used to determine the election result. The security of the IT systems is therefore essential when establishing the provisional election results. Estonia is the only country in the world that allows online voting via the Internet.

Overarching assessments of the technical vulnerability of electronic voting systems are not possible, as EU countries use different voting computers and systems. However, since all voting computers can be manipu-

lated, experts recommend a physical paper printout for each individual vote. In July 2018, under Article 11 of the NIS Directive, representatives from 20 member states prepared a compendium on the cyber security of elections. They called on member states to put in place specific security arrangements and contact points for an overarching European cooperation network.

If individual constituencies experience irregularities during the actual voting, or technical problems with the vote count, elections in individual countries could be held again at short notice without the need for the entire European Parliament to be re-elected. A cyber attack on a member state would mean that the allocation of seats in the EP could not be confirmed immediately. Targeted cyber attacks launched by third countries on individual elections can be sanctioned by the EU applying its Joint Diplomatic Response (Bendiek 2018). A comprehensive and serious attack on the EP elections would be seen as an attack on the EU. Under certain conditions this would allow the use of the solidarity clause under Article 222 TFEU or even the mutual assistance clause under Article 42 para 7 TEU.

Promoting Independent Research

The EP elections decide on the new composition of the European Parliament, but election rules are a national responsibility. In many EU countries, local electoral authorities are responsible for conducting the election. Although they are aware of the danger of disinformation and cyber attacks, they are not sufficiently technically prepared for them. The credibility of the EP elections and thus of the EU is at stake. European policy-makers prefer short-term and more technical measures in close cooperation with Internet companies to combat disinformation and hold cyber-security exercises. Research on causes, however, is lacking. The findings of the various independent interdisciplinary research programmes on disinformation, cyber attacks and the conditions of democracy must therefore be taken into account more closely.

Hybrid Threats?

There is competition for responsibilities and resources between security and defence policy on the one hand, and domestic policy on the other. From the perspective of defence policy, the phenomenon of disinformation belongs in the category of hybrid threats. But narrowing the subject in this way is not sufficient. In a 2017 congressional hearing, heads of American secret services rightly stated that disinformation represents a new normal. According to NATO and the European Commission, Russia leads the way in the targeted dissemination of false information, but more than 30 other countries are also involved. Governments mandate think tanks and non-governmental organisations to provide analyses, so there is no shortage of relevant reports. The American Alliance for Securing Democracy, for example, or the Digital Forensic Research Lab, financed by the Atlantic Council and Facebook, concentrate their work primarily on Russia and China. Think tanks and political foundations dealing with disinformation must identify clients and financiers of their projects so as to avoid suspicions of partiality.

However, false information does not only come from countries outside the EU, but is also disseminated within its member states. Political activism, especially from the anti-European spectrum; the pretence of a grassroots movement ("astroturfing"); and the role of the tabloid media are at least as significant as external attempts at influence. Their impact on Brexit, for example, probably outweighed that of Twitter bots, which only has a user adoption of 17 percent of the British population.

The effectiveness of digital disinformation has not been scientifically proven. Recent studies on the relevance of filter bubbles have come to diverging conclusions. Empirical data indicate that users deliberately choose certain formats and contents that differ from those of the estab-

lished media. Filter bubbles of dissent do not seem to arise because users are unaware that information can be one-sided or false. Rather, the explicit interest of users in divergent opinions seems to be the decisive factor, accompanied by a steady loss of trust within democratic societies in political and public institutions. The idea that filter bubbles are deliberately formed and controlled is reinforced by the fact that it seems to be small groups that spread "alternative facts", disinformation and manifestly false reports in a particularly vocal way. The fear that digital algorithms could largely destroy social communication is thus probably exaggerated.

IT-Enabled Disinformation

The EU's technical measures to combat disinformation campaigns and cyber attacks are only a first step. Ideally, they will direct member states to try to improve protection for the EP elections during the election campaigns, the actual voting and the vote count. Constant exchange and regular cyber security exercises are necessary to minimise dangers. However, most member states have so far failed to consider elections as a critical infrastructure for democracy and to secure them at a high level. Manufacturers and suppliers of critical IT products therefore urgently need to be made more accountable. The problem of unsecured IT hardware and software in voting technology is still underestimated. In the long term, the EU must also be enabled to respond strategically, communicatively and with technical effectiveness to attempts at manipulating elections, and must be provided with the necessary financial and human resources. Until this goal has been achieved, emergency teams can be deployed around the clock during the elections.

The Supremacy of Internet Companies

It is questionable, however, whether the weaknesses of European democracies as discussed above can be addressed effectively with short-term task forces and medium-term action plans. Linguistic research shows that mere fact checking is more likely to inadvertently reinforce false information. The effectiveness of automated artificial-intelligence systems in combating disinformation is also overestimated. Obviously, it is unrealistic to hope to eliminate false information completely. Instead of tackling symptoms, it would be useful to promote independent research to analyse proposals for short-term technical and policy measures. These should provide the blueprint for fundamental reforms in the data economy.

Google's global market share of 80 percent of all search queries and Facebook's and YouTube's market share of 70 percent in social networks are an expression of the unprecedented concentration processes within communication infrastructure. Alongside the growing importance of digital audiences, communication in society is shifting towards a market-orientated arena where every "speech act" or announcement has its price. Private companies provide spaces for public digital discourse; access to them is controlled. Only those who enter into a private contractual relationship and make their contribution either financially or in the form of commercially usable data have a say.

These social networks were developed for marketing purposes and do not cater for unconditional democratic participation based only on citizen status. They are comparable to a situation in which the parliament building is owned by a private provider, access to it is regulated according to economic criteria, and the loudspeaker volume and transmission of speeches to the outside world are assessed in line with market conditions. The EU's previous regulatory approaches, for example its insistence on voluntary commitments, do not do justice to this concentration of power. The Council and Commission were right to criticise the code of conduct currently in force. It contained "no common measures, no substantial obligations, no compliance or enforcement measures". When the personal data of numerous German politicians were illegally

published in December 2018, the online platform Twitter dragged its feet despite its voluntary commitment under the code. Large platform providers have hardly any competition to fear in Europe, meaning that a fundamental reform of the antitrust legislation is the last resort. Previous procedures for the evaluation and control of monopolies have often been inadequate.

A key problem is merger control. Large companies buy burgeoning smaller competitor start-ups before they can become a threat to their business model. A striking example of this is Facebook's acquisition of WhatsApp and Instagram, and its merging of user data, against former promises not to do so. Election advertising on television and a stall on the high street are no longer what decides elections, but rather artificial-intelligence technologies such as microtargeting. These are used to specifically address voters who are willing to change their minds and who can often tip the scales. Only the EU, with its economic power as a whole, can fight the power of transnational digital corporations. In this context, the EP elections are a historic turning point: European policy means tackling the major fundamental issues of the European communication order, such as the control of platform monopolies and excessive communicative power. During EP election campaigns, political parties and organisations must commit themselves to bringing transparency to their campaign activities and to preventing the use of social bots.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761
doi: 10.18449/2019C16

Translation by Tom Genrich

(English version of SWP-Aktuell 10/2019)

Dr Annegret Bendiek is Senior Associate in the EU/Europe Division at SWP.
Dr Matthias Schulze is Associate in the International Security Division at SWP.