EUROPEAN INTEGRATION 08.02.2019 | Moritz Wiesenthal

Time for an update

This May's European elections are vulnerable to cyber-attacks from the right – and the EU's defences are too weak

Read this article in German.

There can be no doubt about it: the elections for the European Parliament this May will be the target of hacker assaults, disinformation campaigns, and attempts to manipulate the outcome using social media. In hindsight, it has become clear that, since the US presidential election of 2016, all major political events in Europe have been subject to cyber-attacks: be it the Brexit Referendum, the French presidential elections, or the controversial plebiscite on Catalonian secession, think-tanks, NGOs, and state actors have been able, *post facto*, to document attempts to sow disinformation or launch direct assaults from cyberspace.

In December of last year, for instance, the Belgian coalition government split over a controversy regarding the United Nations' Global Compact for Migration which was in no small part driven by far-right movements using social media to fan the flames. In this context, it's no wonder that, according to a recent Eurobarometer survey, three quarters of Europeans are concerned by the prevalence of misleading information on the internet.

As a reaction to this threat from cyberspace, in their European Council statement of October 2018, the member states' heads of state and government accorded no small deal of importance to the issue; the European Commission quickly followed up with a plan of action against disinformation which proposed a range of specific measures to ensure the proper conduct of elections.

Yet the actions taken (and indeed not taken) until now are dangerously negligent: they don't really respond to the challenges facing the European elections and instead, leave them acutely vulnerable to assaults launched from the shrouded extents of cyberspace. When compared to national-level votes, three factors make the potential effects of cyber-attacks on European Elections especially powerful and add particular urgency to

discussion of the downsides of digital democracy in the context of the EU.

The threats to Europe

It's enough to simply look at the party-political situation of the continent as a whole: there's an increasing number of Eurosceptic right-of-centre formations whose stated aim is to weaken the EU. These parties are already using social media during national elections and referendum campaigns as a key element in their attempts to rabble-rouse – and do not hesitate to launch campaigns of disinformation and circulate fake news. The German elections of 2017 can serve as an example: the Alternative for Germany (*Alternative für Deutschland*) spread all kinds of unsubstantiated rumours and false claims in the campaign (some are documented here in German).

In addition to domestic forces, the European elections are also likely to be affected by an external player with a serious cyberspace presence: Russia.

The media-savvy Eurosceptics becomes even more dangerous in view of current initiatives in the continent's right-wing, led by Italian right-wing populist Matteo Salvini, to create an international alliance of Eurosceptic parties. Should he be successful, then it would open a new pan-European front in the digital sphere. And, in contrast to the plethora of piecemeal country-level election outcomes, come late May, the results of various nationalist cyber campaigns in the European elections will all meld into one single Eurosceptic result which will, in turn, give anti-European parties a substantial boost in the European Parliament.

In addition to domestic forces, the European elections are also likely to be affected by an external player with a serious cyberspace presence: Russia. The EU's neighbour has already made multiple attempts to use both fake news and targeted bot-attacks in the social media space, launched from the notorious St. Petersburg troll factory, to manipulate the outcome of various elections in Europe. What is most worrying about this is the overlap of the Kremlin's aims with those of anti-European parties: both seek to destabilise the European Union as a whole, and as such, Moscow is also more than happy to provide Eurosceptic parties across the continent with financial support.

Why the European elections are so vulnerable

The essential difference between country-level ballots and the European elections is that key players in the digital space will be looking to instrumentalise the results of the elections in May 2019 not just to bolster or counter a particular political agenda (i.e. for or against a higher minimum wage in one member state), but rather as a plebiscite over the EU as a whole. This would be unthinkable in elections at the level of single member states.

What's more, in the European elections, this looming threat hangs over a flank which has been neglected and is weakly defended – that's the second important difference between these and national elections. It's about the way the elections themselves are carried out: rather than being held in on single, continent-wide ballot, the elections are held from 23rd to 26th May across 27 (maybe even 28...) member states. This puts the responsibility for ensuring the protection of electoral process from cyber-attacks in the remit of member states – states' whose level of readiness differs wildly. Combined with the lengthy voting period, this fragmented structure offers a range of attractive weak-spots for digital forces.

Even if an attack on the electoral process in just one of the member states should be successful, this would lead to an open question with regard to the result of the election and the legitimacy of the European Parliament.

It's therefore no surprise that the European Commissioner for Justice, Consumers, and Gender Equality referred to the measures thus far taken by member states as 'patchwork preparations'; the fact that hackers were able to crack the core software for transmitting results to the German electoral authority in the run-up to the German elections in 2017 should be enough to raise serious concern.

A third, and perhaps decisive factor is the effect of the elections themselves. In the event that campaigns of disinformation or the automated diffusion of fake news on social media have their intended effect, this could deliver Eurosceptic parties a huge increase in the number of seats they hold in the European Parliament and thus compromise the EU's ability to act to a considerable extent. Even if an attack on the electoral process in just one of the member states should be successful, this would lead to an open question with regard to the result of the election and the legitimacy of the European Parliament. In either case, the effect on necessary attempts to strengthen the European Parliament and on plans to make the EU more democratic would be

severe.

Overall, what the discussion about how to deal with digital threats reveals is a dangerous imbalance: if member states do not discharge their responsibility to ensure the proper conduct of elections, it's the European Union as a whole which will be left with the bill for the damage. Considering the current situation in Europe – a situation in which a discussion about the Union's political orientation is increasingly becoming a polemical argument about its very existence – this bill may turn out to be unconscionably high.



Moritz Wiesenthal
Berlin

Moritz Wiesenthal works at the Department of International and European Politics of the European University Viadrina in Frankfurt (Oder), where he also finished his PhD. Previously, he worked in the German Parliament, among others. He studied European Studies and International Relations in Magdeburg, Berlin and Nizhny Novgorod.