European Parliament
2019-2024

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

17.12.2020

WORKING DOCUMENT

on the state of the foreign interference in the European Union, including disinformation

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

Rapporteur: Sandra Kalniete

Introduction

The Parliament set up the special committee on foreign interference in all democratic processes in the European Union, including disinformation, in June 2020. Its goal is to define an approach to addressing evidence of foreign interference in the democratic institutions and processes of the EU and its Member States. Since the first meeting in September, the committee has investigated foreign interference in the public and political domains through a series of hearings with experts.

Regarding preparation against foreign interference, Europe has long acted as if it had no reason to fear and nothing to protect. Our investigations in the INGE committee have already shown loopholes, lack of coordination, lack of sufficient resources, lack of legislation, and even a certain lack of imagination. In addition, the spread of COVID-19-related disinformation affirms the need for a more robust and better-coordinated EU effort to counter disinformation broadly conceived.

One of the reasons is obviously the lack of hard evidence.

It is very difficult to prove exactly how foreign actors try to interfere in our democratic processes and how successful they are. What has emerged at the surface is only the tip of the iceberg.

As we have seen, however, it is not difficult to spot far too many vulnerabilities in our society - vulnerabilities that could be exploited to disrupt, disturb, and manipulate by those willing to do so. It is also not very difficult to see that EU and national legislators have yet to properly do our work protecting the fundamental rights of the citizens of our union.

We have let too many loopholes develop in our regulations. We were too naive with regard to new technology, trade, and investment opportunities. In addition, we failed to set up that safety net, fire alarm, first aid course or supporting structure that is so necessary to protect the core values of our Union: the respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.

Democracy is built on trust. To ensure that all citizens trust our democratic processes, we need to make sure that citizens feel that they can debate, vote and in other ways take part in democracy undisturbed from undue interference.

In this working document, I will take up some main threats in the foreign interference spectrum and point towards possible solutions. I will also start a discussion about terminology and end with my conclusions on how to continue our work.

Foreign interference and hybrid warfare

All forms and vectors of disinformation, especially health-related misinformation amidst a global pandemic, potentially present significant risks to human lives, demanding a robust policy response.

There are many reasons for foreign actors to interfere in democratic processes in the EU: gaining an overall geopolitical advantage, win smaller-scale benefits, for instance in trade or

economy, use political development in the EU for domestic points or help get political allies elected. For authoritarian regimes, there could also be a general motivation either to portray open democracies as worse options than authoritarian systems or to blur the differences between the two systems. Foreign interference in democratic processes often comes together with more general hybrid threats.

Several state actors have been particularly active in this field, such as China, Russia, and Iran.

While they each may have different aims, strategies, tactics, and means to do so, their overall general objective may be to weaken, divide, or discredit the EU.

Overall, the disinformation ecosystem is expanding, and consequently, so should the Union's resources allocated to dealing with it.

Hybrid warfare is creative, spontaneous, opportunistic, unexpected, and confusing. It is hard to properly define and identify because of its covert tactics, its ever-changing methods and its trial-and-error-nature. Moreover, technological developments are happening at an ever-growing pace, often restricting our capabilities to only post factum identification of malicious practices. It could be a mix of disinformation, political funding, strategic advertisement, buying up of critical infrastructure, cyber-attacks, pressure on researchers, setup of new NGOs, and using troll networks to whip up a destructive debate where it needs to be solution-oriented.

Therefore, the development of the EEAS's analytical capabilities and communications capabilities is crucial to effectively tackling foreign interference. Importantly, these steps should be taken in parallel with, and not at the expense of the already existing and successful lines of work, such as the three Stratcom task forces within the EEAS.

The Rapid Alert System should be further developed to realise its full potential, since it is particularly useful as a platform for sharing information, best practices, further EU-wide analysis, policy measures, and strategic communication, whilst serving as a bridge to external cooperation partners. In this regard, closer cooperation with likeminded countries and international organisations remains integral.

Defence involving many disciplines and transcending borders

To discover these attacks, one first needs to connect what seems to be isolated and unrelated incidents. To do this, it is necessary to build networks with participants from many different disciplines. For the same reason, cooperation between the Member States and with international partners is essential.

The same spirit is true for the defence; it needs to replicate the same kind of small-scale multifaceted pattern. A bit of legislation, a bit of education, an alert system, improved IT security and technical independence. Some actions might seem, at first glance, completely unrelated, but might end up being the most effective ones. This is, for instance, the case when it comes to empowering certain vulnerable groups, which could otherwise be tricked into believing or even spreading disinformation.

Journalism vs disinformation

Actors spreading disinformation are in an especially favourable position at the moment. One reason is that one of the best medicines against disinformation, journalism, is experiencing a deep crisis. Media suffers already from significant financial strain, as their readers, viewers and listeners are less and less motivated to pay for journalistic content and many ad revenues go to the platforms instead.

Economic support to journalists is a much more sensitive issue than, for instance, EU aid to farmers or filmmakers. Neither journalists nor the governments can afford to do anything that would compromise journalistic integrity and independence. Some ideas were mentioned during our hearings, including EU-sponsored training. They and others should be examined in cooperation with journalists' organisations.

Adding to the difficult economic situation, individual journalists or media also experience threats, hack-and-leak operations, and other cyber-attacks. The EU needs to find ways to help journalists, activists, and researchers who are under attack after reporting about the truth.

Another challenge for citizens trying to inform themselves is the information overload we are all exposed to. In this attention economy, each of us has less and less time to dedicate to quality journalism. A quick black and white message, even if incorrect or misleading might be easier to digest for today's busy people. This is, even more, the case if the message is tailored to confirm our personal biases or spread via channels that seem trustworthy.

This leads to the challenges linked to developing media literacy skills. That many schools include media literacy and critical thinking in their curricula is important and should be encouraged. This does not, however, remedy the lack of media literacy skills among people who already left school. There are, of course, great initiatives to raise awareness and empower citizens in all social groups and ages. A key challenge remains that most people have very little time, and possibly even less appetite, for learning these skills or even do fact-checking themselves. And very few of us want to fact-check stories that fit too well with our own opinions.

A part of the solution is to make unbiased information more accessible, thus supporting journalism, libraries, teachers, and other sources of information.

EU and national institutions should also communicate strategically against malicious influence operations aiming at manipulating the free political debate or making it harder to reach common positions.

The work done by the EEAS StratCom to uncover disinformation targeting the EU or EU citizens is an important first step to increase the cost for actors engaging in these activities. EU needs to have the means and independence to ensure continued monitoring of foreign disinformation in the EU and to raise awareness about this and continue training in the topic.

This appears to call for a broadening of the mandate and resources of the EEAS StratCom.

To make sure the EU should also consider sanctions when it is proven who is behind foreign disinformation activities. Deterrence activities could include naming and shaming, blacklisting staff from disinformation outlets to press events or media accreditation.

Building societal resilience against disinformation should take a more central role on the EU's agenda for its neighbourhood. Support for independent media, media literacy, and civil society actors in these countries is now more necessary than ever.

The role of platforms

Social media platforms are becoming a dominant arena of public life and debate in our societies. Indeed, for many these platforms represent the main sources of news and trustful opinions. Therefore, these platforms must be held to standards of social responsibility regarding the effects that their algorithms have on the shape and direction of public debate.

At the same time, micro-targeting, the setup of algorithms, the use of sockpuppets and dark ads to manipulate **interest communities** and **even very precisely targeted individual users** already starts to become yesterday's news since Artificial intelligence methods provide new and increasingly sophisticated ways to access unlimited outreach.

Those who want to manipulate us are constantly experimenting with new techniques and narratives. In contrast, the resources and attention platforms spend on spotting and combatting these methods seem to be adapted to the situation and degree of complexity at the time when social platforms and search engines were first invented. **For disinformation in smaller languages, or even most other languages than English, the situation is even worse.** When it comes to legislation protecting citizens and the public debate from interference and manipulation, current practices and tools, unfortunately, reminds of ancient codes of chivalry.

In addition, we should take into account that the business model of social platforms is often harmful due to its deliberate prioritisation and monetisation of controversial, divisive information.

There are, of course, some positive developments. The Code of Practise did lead to improvements. Many NGOs, teachers, journalists, and governments work hard to warn for disinformation online and empower citizens to better tell the difference between manipulation and information.

However, dealing with a range of online threats on a sectorial or ad hoc basis and relying on the goodwill of online platforms to tackle vaguely defined issues is no longer viable. The current lack of an effective EU-wide approach also risks engendering a patchwork of discordant national regulatory regimes. Therefore, the EU should move toward an integrated, EU-wide set of norms that will assert the future of the internet as a both free and safe place for public discourse.

The recently proposed European Democracy Action Plan, the Digital Service Act (DSA) and the Digital Markets Act (DMA) are welcome and important steps forward to make digital environment more transparent, safe and actors like social media companies more accountable. They include concrete proposals against platforms who fail to act.

We now should closely follow the legislative process in the Parliament and avoid fwatering down the ambitious goals.

Also, bearing in mind that harmful content is not directly covered by the DSA, we should consider linking up with other possible initiatives, like DPA, in order to make these proposals strong enough to counter properly the problems linked to interference, in all languages, lack of transparency or misuse of personal data, algorithms and advertising while defending the freedom of expression.

Financing of political actors

A delicate kind of foreign interference is covert funding of political activities by foreign donors.

For many years, the focus has been only put on cyber-attacks and disinformation and not on political funding because this raises political sensibilities.

However, there are many examples of domestic political organisations receiving support from foreign actors. Such supports pursue at least two distinct objectives: undermine European unity (like during the Brexit referendum during which the parties campaigning to leave the EU received substantial foreign funding), or build a group of allied parties supporting the views of a foreign State-actor (campaigning against the Russia sanctions for instance).

According to findings shared with our committee, over the past decade, Russia, China, and other authoritarian regimes have funnelled more than $300 million into 33 countries to interfere democratic processes more than 100 times, and this trend is clearly accelerating. Half of these cases concern Russia actions in Europe.

In addition, third-party organisations, jointly founded by American and Russian ultra-conservatives, are also very active in Europe in financing and coordinating European far-right movements on the basis of an ultra-conservative agenda.

The foreign actors behind these activities seek to take advantage of countries that have perceived loopholes in laws preventing foreign campaign assistance, which is particularly problematic in the EU, where rules on foreign funding of political activities differ substantially amongst Member States.

The seven most exploited loopholes for covert foreign money are: in-kind (a broad definition is needed ranging from loans to intangible assistance), straw donors (intermediaries covering the real sources of funding), shell companies, non-profits conduits like foundations (in almost all EU member states third parties' financing political campaigns is unregulated), funding on-line political ads, funding of media outlets, or even emerging tech (crypto donations).

Bearing all of this in mind, a reflection should be conducted about the need for EU Member States to agree on basic common standards in order to close the existing loopholes allowing foreign actors to interfere in the political activities within the EU.

Cyber security and critical entities

The need to ensure the protection of European critical infrastructures and services against foreign cyber-attacks is also one of the key points of our mandate.

The Commission and the European External Action Service have recently put forward an ambitious set of proposals towards a new cybersecurity strategy for the EU. The aim of the strategy is to bolster Europe's resilience against cyber threats and set standards of cybersecurity for essential services and critical infrastructure, such as hospitals, energy grids railways and the ever-increasing number of connected objects and services. The cornerstone of the strategy is the need for the EU to become technologically sovereign.

As part of the strategy, the Commission has made two legislative proposals to address both

cyber and physical protection of critical entities and networks. First, a Directive on measures for high common level of cybersecurity across the Union (NIS 2) that will help increase sharing and cooperation on cyber crisis management at national and EU level. Second, a new Directive on the resilience of critical entities (CER), which expands the scope of the previous 2008 European Critical Infrastructure directive with ten sectors now covered.

This strategy and legislative proposals are timely and therefore welcome. They need now to be thoroughly assessed by respective parliamentary committees, in order to assess their real added value and whether they are ambitious enough to tackle current challenges.

In addition to the recent initiatives taken by the Commission in these fields, we are also satisfied to see that the new ability of the EU to put in place sanctions against individuals involved in cyber-attacks against critical infrastructures has been implemented at least at two occasions during the last months.

During our hearings, we also found that an important element of the sound functioning of our democracies stems from the security of the digital systems used during electoral campaigns and elections. A number of cyber-attacks, including hack and leak of personal emails, malign communications, or even attacks against public infrastructure on election day, have been brought up to the attention of our committee. These hybrid threats could also be included in the reflection regarding protection of critical infrastructure.

With regard to 5G mobile networks, an indispensable infrastructure prerequisite for achieving a competitive level of digitalisation, the EU and its Member States must strive for autonomy and independence from third country equipment.

Definitions

To have the tools to properly engage foreign interference, the EU also needs to agree on several definitions. This would have many advantages. Firstly, in the planning stage, everybody must understand the same thing when using the same words.

This is, for instance, the case in the dialogue with social media platforms and their work against disinformation. Experience has shown that different platforms act use different kinds of behaviour to trigger an action, which makes it difficult to understand threats cross-platforms and also makes it easy for malicious actors to tailor their manipulative actions so that they can pass through each platform’s respective loopholes. To communicate the EU's expectations successfully, this basic agreement needs to be there.

When it comes to designing counter-tactics, it is important to identify the type of problematic actions before choosing the counter-action. Taking the dis/misinformation sphere as an example, actions against misinformation innocently spread by people who believe they are informing their networks must be fundamentally different to actions against disinformation created and spread deliberately to mislead and harm. In the first case, an answer needs to be gentle, for instance, focusing on education and information, whereas the other case might lead to sanctions or condemnation.

Also on the answer-side, it could be interesting to discuss possible definitions, such as democratic deterrence, debunking, sanctions etc.

Within the scope of the INGE report, we must strive to define the list of terms, building on the work already done by the EC, EEAS, and others.

Conclusion

It deserves to be repeated: The European Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

As stated in its mandate, the INGE committee ultimately aims to protect these values and democracy itself. In the centre of our work is our commitment to protect the right of all citizens to fully participate in all democratic processes, undisturbed from actors trying to interfere and manipulate.

To be perfectly clear, when I talk about citizens, I mean those who have opinions I share completely but also those I deeply disagree with, I mean political animals like myself but also everybody whose daily life is too busy to leave time and energy for political discussions, I mean both the more and less privileged, the young and the old and everybody else in between.

We are not alone in this fight. During our committee meetings and outside of Parliament, we have met an impressive range of activists, researchers, journalists, educators, civil servants and sensible fellow citizens who all contribute in their daily lives to the defence of democracy.

In the next months, we join forces and analyse these challenges, one by one, and look for solutions. My priorities include:

- Development of a clear set of *shared* definitions, acknowledging that distinctions should be drawn between the various types of challenges currently described as “disinformation”, “malinformation”, “misinformation”, “influence operations”, etc.
- Looking at ways to make political funding more transparent and consider caps on foreign funding.
- Enhancing support to vulnerable groups like activists, journalists, researchers, minorities and those targeted to be recruited as domestic proxies.
- Strengthening strategic communication.
- Raise awareness, within public administrations, to key stakeholders and working with partner organisations.
- Create a list of red and orange critical infrastructure that should under no circumstances, or respectively, not fully, be owned by foreign actors. Ensure the independence of supply in a series of critical infrastructure areas.
- Develop stricter rules for regulating platforms with regard to transparency, sanctions, the duty to provide linguistic expertise and cooperate across platforms, as well as clear boundaries to prevent abuse of users’ data.
- Development of implementation criteria and oversight mechanisms for social platforms.

- Establishment of EU-wide general standards for social responsibility in algorithmic design.
- Addressing the challenge of closed messaging groups that increasingly replace open public debate.
- Investigate hybrid threats, support and enhance multidisciplinary networks - involving different branches of society to spot influence operations quickly.
- Support researchers in relevant spheres, such as disinformation, media literacy, covert foreign funding, etc.
- The EU should give support to media literacy initiatives, especially targeting vulnerable groups, and facilitate the exchange of best practices.
- The EU needs to enter into a close dialogue with journalist federations and publishers on appropriate ways to support free media without jeopardising their independence, and helping them secure their fair share of advertisement.
- The EU should increase its investigations in foreign interference, including but not limited to disinformation, to publicly expose and, if possible, sanction those behind it.
- The EU needs to facilitate closer cooperation with likeminded countries and international organisations, such as relevant NATO divisions and research capabilities, the G7's Rapid Response Mechanism (RRM), and the UN (especially UNESCO), among others.
- Ensure effective EU institutional responses to disinformation at times of crisis, drawing lessons from the COVID-19 pandemic.