College of Europe
Collège d'Europe
Brugge
Natolin

The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle?

Mélanie Scheidt

DEPARTMENT OF EU INTERNATIONAL
RELATIONS AND DIPLOMACY STUDIES

EU Diplomacy Paper 01 / 2019

College of Europe
Collège d'Europe
Brugge
Natolin

Department of EU International
Relations and Diplomacy Studies

EU Diplomacy Papers
1 / 2019

The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle?

Mélanie Scheidt

About the Author

Mélanie Scheidt holds an MA in EU International Relations and Diplomacy Studies from the College of Europe in Bruges. Previously, she obtained an MA in European Studies from the University of Aix-Marseille and a BA in Applied Foreign Languages from the University of Strasbourg. She also spent two semesters abroad in Nottingham and Maastricht. She previously worked as a trainee at the Council of Europe and at a French regional representation in Brussels. This paper is based on her Master's thesis at the College of Europe (Manuel Marín Promotion).

Dijver 11 | BE-8000 Bruges, Belgium | Tel. +32 (0)50 477 251 | Fax +32 (0)50 477 250 | E-mail ird.info@coleurope.eu | www.coleurope.eu/ird

Views expressed in the *EU Diplomacy Papers* are those of the authors only and do not necessarily reflect positions of either the series editors or the College of Europe.

Abstract

As a result of increased globalisation and digitalisation, new security challenges emerge such as the rise of online disinformation which undermines democracy and people's trust in mainstream media and public authorities. The 2016 United States presidential elections, the Brexit referendum in the United Kingdom and the 2017 French presidential elections have all been disturbed by external interference coming from Russia, including massive disinformation campaigns which were disseminated on social media to influence citizens' opinion. This paper studies the European Union's (EU) strategy to counter external disinformation campaigns in cyberspace, i.e. the campaigns that are diffused online by foreign actors, such as Russia, within the EU's territory. To what extent is the EU strategically prepared to counter external disinformation campaigns in cyberspace?

The EU has adopted a defensive strategy to deal with disinformation. It has delivered several strategic documents, including an Action Plan in December 2018, that provides a promising basis for action. The work done by the East StratCom Task Force, which detects and debunks Russian narratives, is a strong asset for the EU. The major online platforms are currently trying to implement a Code of Practice that the European Commission has set up with the aim of curbing disinformation spreading on social networks. Having a long-term perspective in mind, the EU rightly implements measures to enhance societal resilience and improve media literacy among its citizens. However, the financial resources dedicated to counter disinformation are not commensurate with the threat it represents. Furthermore, the EU's approach is not focusing enough on artificial intelligence tools that can significantly influence how disinformation is carried out and disseminated but can, on the other hand, also help fact-checking activities. Hence, the EU is not entirely prepared to counter external disinformation campaigns in cyberspace. Moreover, disinformation should be looked at in the wider framework of hybrid warfare and should therefore be considered as a cybersecurity matter.

Introduction: the EU and the new information warfare

According to a recent study, "the majority of people in advanced economies will see more false than true information"[1] by 2022, a worrying prediction that gives us pause for thought about the information society we are living in. Laptops, smartphones, tablets give us the opportunity to be aware at any time of what is happening around the globe. Social media allow us to communicate freely with people all over the world. We are thus constantly surrounded by a flow of information. The technological progress that we are witnessing in the 21st century highlights a paradox: our societies are becoming more interconnected, but are at the same time confronted with a number of challenges, disinformation being one of them.

Disinformation is not a new phenomenon. It is at least "as old as the printing press".[2] However, technological development and social media have tremendously accelerated the speed at which news, and in this case, false news, are diffused and have expanded their reach. Disinformation is a virulent trend that concerns all citizens and all sectors of democratic societies.

Moreover, external interference in national elections or referendums, involving massive disinformation campaigns, seems to have become the 'new normal'. The 2016 Brexit referendum, the 2016 US presidential elections and the 2017 French presidential elections have something in common: they all have been disturbed to a certain extent by the meddling of Russia in the political debates. Indeed, Russia uses disinformation as a weapon in its hybrid warfare strategy to an extent that some would argue amounts to a "weaponisation of information"[3] and of social media. Before the European elections in May 2019, the fear of disinformation and external interference disrupting the ballot was bigger than ever, raising the question whether the EU is ready to fight a battle in the so-called 'information warfare'.

Even though disinformation is not a new phenomenon, governments and international organisations as well as the European Union have only recently started to deal with the issue. Landau argues that "if there is anything we have learned from the Russian cyber activity during the Brexit referendum campaign and the 2016 United States (US) and 2017 French presidential election campaigns, it is that our cybersecurity

[1] K. Panetta, "Gartner top strategic predictions for 2018 and beyond", 3 October 2017.
[2] European Parliament, *Online disinformation and the EU's response*, 24 April 2018.
[3] F. Spildsboel Hansen, *Russian hybrid warfare: a study of disinformation*, Zürich, Centre for Security Studies, 2017.

protections are completely unprepared to cope with a disinformation campaign".[4] This raises the question whether the defensive measures undertaken by the EU so far to deal with disinformation are sufficient, or more offensive measures should be taken. In other words, to what extent is the EU strategically prepared to counter external disinformation campaigns in cyberspace?

Fearing foreign interference in the 2019 European elections, the EU decided to accelerate the pace and take more measures to counter external disinformation threats. The new EU Action Plan against disinformation unveiled in December 2018 provides a strong basis. However, there is currently a multiplicity of actors dealing with disinformation and the EU is lacking an overarching and comprehensive body dealing solely with this issue. Moreover, the EU is not ready to cope with the latest developments made in the field of artificial intelligence (AI) that will significantly impact the way disinformation is done and diffused. Overall, the EU is not entirely prepared to counter external disinformation campaigns in cyberspace.

This paper is structured as follows. First, the features of disinformation and the reasons why it is a security challenge will be presented. It will be shown how cyberspace, social media and AI change the way disinformation is spread and perceived; followed by an explanation why it should be considered as a cybersecurity matter. The subsequent section will be dedicated to Russian disinformation and the EU's tools and mechanisms to deal with it. The last part of the paper will assess the EU's actions so far and their limits. Finally, the future challenges posed by disinformation and some policy recommendations will be presented.

Disinformation: a security threat in cyberspace

Before analysing the EU's actions regarding disinformation, it is important to understand what disinformation is, its features and its consequences. The European Commission conceives of disinformation as "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[5] This definition is appropriate for this paper because it is rather narrow and specifically underlines the negative intentions of disinformation.

[4] S. Landau, "Cybersecurity: time for a new definition", *Lawfare*, 12 January 2018.
[5] European Commission & High Representative, *Action Plan against disinformation*, JOIN(2018) 36 final, Brussels, 5 December 2018.

Online disinformation: an emerging security challenge

As a first step, disinformation needs to be placed in the broader context of hybrid warfare. The European Commission defines 'hybrid war' as a mix of "coercive and subversive activities, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), [that] can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare".[6] Online disinformation is considered as a hybrid threat and a tool in hybrid warfare. Other tools can be cyberattacks, cyberespionage, foreign asset acquisitions, disruption of critical infrastructures (such as transport, energy or banking infrastructures), interference in election processes, strategic leaks, disruption of communications networks, terrorist acts, etc.

Disinformation is a complex phenomenon which has numerous harmful consequences on individuals and on societies. First of all, disinformation disrupts the trust of citizens in traditional media. It "undermines the very fundamentals of information and credibility that informed debates are supposed to rest upon".[7] People face different false narratives which destabilise their sense of certainty about what is happening in world affairs. Moreover, disinformation undermines the trust in public authorities and institutions. It confuses citizens as to what and whom to believe. It therefore undermines democracy, the rule of law and good governance. Bayer *et al.* argue that disinformation violates fundamental human rights: automated dissemination mechanisms and the concealed usage of bots violate privacy and human dignity by misleading the users.[8] It is thus a clear threat to European values which the Union tries to promote internally and externally.

Disinformation usually fosters fear, enhances polarisation (i.e. public opinion moving to extreme political parties), social divisions and tensions.[9] It thus threatens social cohesion and in a larger perspective, European unity. Disinformation campaigns often implicitly support extremist ideas and carry an EU-critical tone. As a consequence, disinformation is also a threat to the EU's perceived political legitimacy and contributes

[6] European Commission & High Representative, *Joint Framework on countering hybrid threats: a European Union response*, JOIN(2016) 18 final, Brussels, 6 April 2016.

[7] K. Giles, *The next phase of Russian information warfare,* NATO: Strategic Communications Centre of Excellence, Riga, 2016, p. 7.

[8] J. Bayer *et al.*, *Disinformation and propaganda – Impact on the functioning of the rule of law in the EU and its Member States*, Directorate General for Internal Policies of the Union of the European Parliament, PE 608.864, Brussels, February 2019, p. 78.

[9] Panel for the Future of Science and Technology, *Automated tackling of disinformation, European Science-Media Hub*, European Parliamentary Research Service, PE 624.278, Brussels, March 2019, p. 7.

to Euroscepticism. All in all, it can be said that disinformation has serious consequences that are threatening the security of the EU and its citizens.

Cyberspace, technological innovations and disinformation

Cyberspace has completely changed the way disinformation is designed, diffused and perceived. Before the creation of the Internet, disinformation used to be limited to written and printed forms through the press, leaflets, posters, etc. With cyberspace, disinformation can be spread anywhere: on the Internet, social media, via smartphones, tablets, computers, and so on. Also, disinformation is not just limited to written texts anymore but concerns also pictures and videos which can easily be modified and falsified. This section will reflect on the changes induced by cyberspace and new technologies such as AI.

Since cyberspace has no geographical borders, disinformation campaigns can easily spread on the web, from one country to another, and reach a large audience. Cyberspace has "low buy-in costs".[10] It means that a person only needs a few instruments and resources to create a wide-ranging disinformation campaign online, with low risk for the author given that anonymity prevails in cyberspace. Today, social media platforms and web search engines have become the major source of information for many citizens.[11] As a consequence, "billions of users worldwide have become targets of online disinformation and propaganda campaigns through these online platforms and technology".[12] In cyberspace, the dissemination of disinformation is more widespread and its outreach is amplified.

In addition, social networks play a key role in online disinformation. Social media platforms are guided by specific algorithms that will display content according to the users' preferences, comforting them in their opinions and beliefs. This is commonly called the 'filter bubble': social media filter the information that users will see, confirming the users' pre-existing beliefs and stances and trapping them in a sort of 'bubble'. This 'filter bubble' effect combined with the speed at which information is diffused online creates a breeding ground for disinformation campaigns. Also, social media and algorithmic dissemination of content "make disinformation spread faster,

[10] D. Betz, "Cyberpower in strategic affairs: neither unthinkable nor blessed", *Journal of Strategic Studies*, vol. 35, no. 5, 2012, p. 694.

[11] K.E. Matsa, L. Silver, E. Shearer & M. Walker, *Western Europeans under 30 view news media less positively, rely more on digital platforms than older adults*, Washington, DC, Pew Research Center, 2018.

[12] Panel for the Future of Science and Technology, *op cit*.

reach deeper and be more emotionally charged".[13] Therefore, it can be said that social media which were long praised for their power to democratise online conversations, may in reality be undermining democracy.

The relationship between cybersecurity and disinformation is not straightforward. Indeed, some argue that "cybersecurity is confined to issues of network security, cybercrime and hacking, that is to say, problems that can be solved by technological means alone".[14] However, this paper argues that cybersecurity and disinformation go hand in hand since disinformation is more and more combined with hacking of networks or cyberattacks. These attacks "may include targeted intrusions to collect sensitive information as a precursor to leaks or tainted leaks, take-over of social media accounts, [or] disruption of information technology systems".[15]

Hacking can be a means in itself to spread disinformation. As Tucker explains, hacking sensitive information is a strategy for disseminating disinformation. The information can subsequently be leaked "in either its real form or following manipulation of the hacked materials, so as to damage the targets of disinformation campaigns".[16] This technique was used in the case of Hillary Clinton's leaked emails or the so-called Macron Leaks. In the first example, the email account of the chairman of Hillary Clinton's 2016 US presidential campaign was hacked, releasing confidential emails of the Democratic candidate. In the Macron Leaks, the email accounts of five collaborators of Emmanuel Macron were hacked during the 2017 French presidential campaign, releasing tens of thousands campaign documents and emails online. A lot of the documents leaked were modified or fake, including emails from and to people who did not exist. In both cases, researchers have linked the attacks with 'Fancy Bear', an entity related to the Russian military intelligence agency (GRU).[17] These two instances demonstrate that disinformation is a cybersecurity problem.

In addition, the development of AI leads to a paradox: on the one hand, AI brings enormous opportunities for progress in a wide range of sectors. But on the other hand, AI has a significant impact on online disinformation and poses serious risks. Indeed, AI

[13] C. Bjola, "Propaganda in the digital age", *Global Affairs*, vol. 3, no. 3, 2017, pp. 189-191.
[14] T. Stark, "The interplay between Russian disinformation and hacking", *Politico*, 18 December 2018.
[15] European Commission, *Action Plan against disinformation*, *op. cit.*, p. 3.
[16] J.A. Tucker *et al.*, *Social media, political polarization, and political disinformation: A review of the scientific literature*, New York, Hewlett Foundation, 2018, p. 31.
[17] N. Popescu & S. Secrieru (eds.), *Hacks, leaks and disruptions - Russian cyber strategies*, Paris, European Union Institute for Security Studies, October 2018, p. 87.

can be used for the purpose of disinformation in several ways: it can help target specific audiences notably through algorithms; it can create false narratives and digital content of any kind (e.g. video, sound); it amplifies the diffusion of disinformation campaigns through bots and trolls. These methods are part of a so-called "computational propaganda",[18] which refers to the use of algorithms and bots to diffuse false information over social networks.

The algorithms used on search platforms and on social media can be a driver for spreading disinformation. AI can manipulate the algorithms used for ranking research requests so that websites or news articles containing disinformation will appear first. The algorithms directing the searches are rarely transparent which makes it very difficult to understand how the search ranking has been done. Furthermore, algorithms on social media will personalise the social feed of users so that they see what they prefer. These algorithms will also facilitate "the sharing of personalised content among like-minded users, [which] indirectly heighten[s] polarisation and strengthen[s] the effects of disinformation".[19] The same algorithms can also display targeted advertising that can be used to promote and monetise online disinformation.

Moreover, AI enables the creation of so-called 'deep fakes' through an "AI-based technique that combines and superimposes existing images and videos to fake what a person is doing or saying".[20] Although manipulation of digital content on computers is nothing new, "in the past that manipulation has almost always been detectable".[21] However, current AI technology allows to create fake videos which seem very authentic, making it difficult for the human eye to detect the fraud. Thanks to deep learning, "the algorithms that generate the fakes continuously learn how to more effectively replicate the appearance of reality, [therefore] deep fakes cannot easily be detected by other algorithms".[22] Deep fakes represent a considerable threat since they look very credible and are very hard to verify. They can, for instance, give the impression that a politician has said or done something that he/she did not do or say. It becomes difficult to distinguish between what is real and what is fake, plunging people into a 'science-fiction world'.

[18] Tucker *et al., op. cit*., p. 23.

[19] European Commission, *Tackling online disinformation: a European approach*, COM(2018) 236 final, Brussels, 26 April 2018, p. 5.

[20] M. Ciobanu, "The challenges and opportunities of using artificial intelligence to tackle misinformation", *Journalism.co.uk*, 14 April 2018.

[21] C. Meserole & A. Polyakova, "Disinformation wars", *Foreign Policy*, 25 May 2018.

[22] *Ibid.*

This section has showed that cyberspace and social media are a game-changer for disinformation campaigns, which can circulate more easily and reach a larger audience than before. It has also been argued that disinformation should be considered as a cybersecurity issue. Moreover, continuous progress in AI is likely to affect the way disinformation is created and diffused. The proliferation of AI technologies raises serious concerns about their applicability and whether they are always used for a good purpose.

Information warfare: Russian disinformation campaigns in the EU

Russia is not the only player in the disinformation realm but it is by far the most active in Europe and frequently uses hybrid warfare tools to destabilise Western countries. Barbière speaks of a "war of disinformation waged by the Kremlin".[23] This section will present Russia's strategies, its goals and the particular characteristics of its disinformation campaigns.

Russia actively uses digital media (such as social media, Youtube) and modern technology to diffuse false narratives, which are cheap tools to reach a large audience regardless of geographical borders.[24] Today, "the Russian political leadership is highly conscious of the power of information as a tool in the sphere of security" and hybrid warfare.[25] The Russian Defence Minister, Sergey Shoigu, acknowledged in 2017 "that a dedicated information warfare force had been established in 2013 within the Ministry of Defence".[26] Disinformation is part of the official military doctrine of Russia and is an accepted tool of its foreign policy. The country invests more than a billion euros per year in its information warfare capabilities.[27]

While Russia's disinformation was initially targeting its 'near abroad', i.e. former Soviet republics like Ukraine or Georgia, Russia has now expanded its outreach beyond the former borders of the Soviet Union. Russia primarily targets EU member states and the US, and appears to be more and more active in Latin America and Africa as well.[28] The campaigns are addressed to "ordinary citizens, politicians and other public

[23] C. Barbière, "Russia: Master of information manipulation", *EurActiv*, 11 September 2018.
[24] Interview with EEAS official 2, Brussels, 15 March 2019.
[25] M. Hellman & C. Wagnsson, "How can European states respond to Russian information warfare? An analytical framework*", European Security*, vol. 26, no. 2, 2017, p. 155.
[26] N. Bentzen, *Disinformation, 'fake news' and the EU's response*, European Parliamentary Research Service, PE 614.584, Brussels, November 2017.
[27] L. Andrikiene, "We still need East StratCom against Kremlin trolls", *EUObserver*, 7 June 2018.
[28] Interview with EEAS official 1, Brussels, 28 February 2019.

figures".[29] A relevant point is that Russia targets audiences on both sides of political and social debates. For instance, in the context of the 2016 US elections, Russian disinformation was aimed at politicians and supporters of both sides of the political spectrum (Republicans and Democrats).[30]

Russia deploys an orchestrated strategy of information manipulation, that is characterised by "the absence of any moral or ethical constraints".[31] The Canadian Security Intelligence Service described Russian disinformation as "universal, flexible, smart and borderless".[32] One key technique is the so-called "4D-approach": "dismiss any negative reporting, distort the facts, distract by launching accusations elsewhere, and spread dismay".[33]

Two main entities that convey Russian narratives and disinformation are the media channel RT (formerly known as Russia Today) and the news agency Sputnik. Taken together, RT and Sputnik operate in almost 40 languages[34] and use a wide range of digital tools (websites, social media, videos, etc.). Both present themselves as "independent, alternative voices"[35] but in reality that means "pro-Russian, conspiracy theoretical and anti-Western". [36] None of them publish articles critical of Putin's regime. Furthermore, many Russian-sourced stories that are first published by RT or Sputnik are then amplified by bots and trolls on Twitter and Facebook "causing algorithms to trend misleading or false reports that then could be picked up by mainstream news coverage".[37] Russia uses trolls on a massive scale, in so-called 'troll farms' or 'troll factories'. One example is the 'Internet Research Agency (IRA)', a troll factory in Saint-Petersburg financed by the Kremlin.[38] It employs hundreds of people creating fake

[29] J. Aro, "The cyberspace war: propaganda and trolling as warfare tools", *European View*, no. 15, 2016, p. 124.

[30] Interview with GMF official, Brussels, 15 March 2019.

[31] *Who said what? The security challenges of modern disinformation*, Ottawa, Canadian Security Intelligence Service, 2018, p. 26.

[32] *Ibid.*, p. 33.

[33] G.H. Karlsen, "Tools of Russian influence: information and propaganda", in J.H. Matlary & T. Heier (eds.), *Ukraine and beyond: Russia's strategic security challenge to Europe*, Basingstoke, Palgrave Macmillan, 2016, p. 185.

[34] *Ibid*., p. 199.

[35] N. MacFarquhar, "A powerful Russian weapon: the spread of false stories", *The New York Times*, 28 August 2016.

[36] Aro, *op. cit.,* p. 125.

[37] G.F. Treverton *et al.*, *Addressing hybrid threats*, Stockholm, Swedish Defence University, 2018, p. 47.

[38] J.-B. Jeangene Vilmer, A. Escorcia, M. Guillaume & J. Herrera, "Information manipulation, a challenge for our democracies", *Policy Planning Staff (French Ministry of Europe and Foreign Affairs) & the Institute for Strategic Research (French Ministry for the Armed Forces)*, Paris, 2018, p. 84.

accounts, writing posts, commenting on them to amplify the narratives on social media and influence conversations on political issues around the world.

Contrary to what one could think, Russian disinformation is not always about fake information. It is often built around an "element of truth",[39] but the information is manipulated in a way, often using biased rhetorical questions, that will disturb the reader and make him or her doubt the facts. This characteristic makes Russian disinformation even more difficult to defeat.

Furthermore, the so-called 'decoy flare' technique is distinctive of Russian disinformation. The expression comes from the military: in order to confuse approaching heat-seeking missiles, military planes will release a lot of false heat targets. When applied to disinformation, this method implies that not only one alternative truth will be diffused but a large variety of different messages will be spread. So many different narratives will be sent out that it will eventually confuse people. Finally, Russia views disinformation in the broader picture of information or hybrid warfare. It will therefore combine disinformation campaigns with more aggressive tools such as cyberattacks or hacking of networks, as was the case for the Macron Leaks.

The EU's strategy to counter external disinformation campaigns

The 2019 European elections were an important driver for the EU to act as quickly and as efficiently as possible to counter external disinformation campaigns. This section will focus on the EU's action tools to deal with and counter the disinformation campaigns from abroad. To this end, it will first introduce the EU's general approach and then look at three strands of its action: debunking disinformation, working with online platforms and improving cyber capabilities.

The EU's general approach to fight disinformation

While Russian disinformation has been going on for several decades,[40] the EU has only started to take measures in 2015 with the creation of the East StratCom Task Force (ESTF). But even at that time, disinformation was not on top of the political agenda.[41]

[39] Interview with EEAS official 2, Brussels, 15 March 2019.

[40] H. Romerstein, "Disinformation as a KGB weapon in the Cold War", *Journal of Intelligence History*, vol. 1, no. 1, 2001, p. 54.

[41] A. Bernstein, *Not Russian to do anything? The EU response to strategic narratives and disinformation in the wake of the Russia-Ukraine crisis,* Master's thesis, Bruges, College of Europe, 2017, p. 25.

There was not much enthusiasm to deal with this issue within the EU institutions. Bernstein argues that, at that time, disinformation was not perceived as a threat and was not taken as seriously as it should have been: "the EU's perception of this threat is not commensurate with the scale of the problem it is facing".[42] An official interviewed at the European External Action Service (EEAS) also had a similar argument saying that "there was not much political support from within the EEAS and from the High Representative to deal with disinformation".[43] Most of the people working at the ESTF were seconded national experts. Nevertheless, one can really witness the change of will within the EU institutions since the end of 2016, beginning of 2017. All the people interviewed for this paper agreed on the fact that the 2016 US elections was a wake-up call for the EU and a turning point in its course of action to tackle disinformation. Moreover, the prospect of having the same scenario (i.e. external interference and hacking) happening during the European elections was frightening enough that the EU institutions were rushing to implement measures during the first semester of 2019. This change of vision is reflected in the choice of words used by the European Commission in its official publications. While the word 'urgent' has not been employed once in the conclusions of the European Council establishing the ESTF in 2015,[44] it was used five times in the Action Plan published in December 2018,[45] for example: "It is *urgent* to step up efforts to secure free and fair democratic processes";[46] or "This calls for *urgent* and immediate action to protect the Union, its institutions and its citizens against disinformation".[47]

The overall approach of the EU to counter disinformation is rather defensive than offensive, meaning that the EU is mostly responding to disinformation campaigns rather than preventing them. More precisely, the EU is developing its capacities for sense-making and meaning-making. Sense-making means making sense of a situation, "sifting through relevant information, building an accurate picture of what is happening, and communicating that analysis to political decision-makers".[48] Meaning-making is linked to communicating about the crisis to the public. Indeed, the EU tries to make sense of disinformation campaigns, analyse them and explain them

[42] *Ibid.*, p. 11.

[43] Interview with EEAS official 1, Brussels, 28 February 2019.

[44] European Council, *European Council meeting (19 and 20 March 2015) – Conclusions*, EUCO 11/15, Brussels, 20 March 2015.

[45] European Commission, *Action Plan against disinformation*, *op. cit*., pp. 2, 3, 4, 8, 12.

[46] *Ibid.*, p. 2.

[47] *Ibid.*, p. 4 [emphasis added].

[48] A. Boin *et al.*, *Making sense of sense-making: the EU's role in collecting, analysing, and disseminating information in times of crisis*, Stockholm, The Swedish National Defence College, 2014, p. 5.

to the public. A large part of the EU's work turns around debunking disinformation and issuing positive strategic communication. The latter means that the EU tries to better communicate within the Union, i.e. to create "persuasive messaging [...] allowing citizens to easily understand that political and economic reforms promoted by the EU can, over time, have a positive impact on their daily lives",[49] but also better communicate in the EU's neighbourhood, including Russia. Bjola argues that "there is therefore a clear ideological dimension to countering Russian influence: the goal is to contain the threat by developing resilience through the soft power of values and ideals".[50] A multiplicity of entities is currently dealing with this issue at the EU level, namely: the EEAS, the Strategic Communication Task Forces (including the ESTF), the EU Intelligence Centre (INTCEN), the EU Hybrid Fusion Cell (located within INTCEN), or the Commission's Directorate-Generals Connect, Near, Home and Just.

The Action Plan published in December 2018 outlines the EU's strategy and the path it needs to take to tackle disinformation. The EU proposes multidimensional and long-term measures. However, when reading the document thoroughly, one can see that a lot of measures are taken with the short-term perspective of the European elections. The Plan draws particular attention to the fact that "exposing disinformation in countries neighbouring the Union is complementary to tackling the problem within the Union".[51] The EU wants to foster cooperation in the Eastern and Southern neighbourhood and in the Western Balkans. As for financial resources, the European Commission pledged to increase its budget dedicated to fight disinformation from 1,9 million to 5 million euros in 2019, compared to Russia's 1,1 billion euros per year. The Action Plan also commits to increase the staff and resources of the ESTF.

Based on the arguments presented in this section, it can be concluded that, so far, the EU has responded with a defensive strategy against a very offensive and aggressive Russian rhetoric.

Debunking Russian disinformation

Among the EU's tools to deal with Russian narratives, the East StratCom Task Force is one of the most efficient and promising. Complementary to the efforts of the ESTF, the EU tries to promote societal resilience and media literacy.

[49] C. Bjola & J. Pamment, "Digital containment: Revisiting containment strategy in the digital age", *Global Affairs*, vol. 2, no. 2, 2016, p. 133.
[50] *Ibid*.
[51] European Commission, *Action Plan against disinformation*, *op. cit*., p. 4.

The ESTF is located within the EEAS and is currently composed of fifteen people. The work of the task force is based on the Council mandate of March 2015, limiting its work to the Kremlin's disinformation. It operates with a small budget of 1,1 million euros since January 2018. Its motto is "Don't be deceived: question even more" in reference to RT's own motto "Question more". The work of the task force is divided into three main tasks: debunking disinformation, providing positive strategic communication in the countries of the Eastern Partnership, and communicating in Russian language.[52] Debunking disinformation consists of fact-checking (i.e. verifying the trustworthiness of an information) and analysing and translating Russian pieces of information. The ESTF maintains a database of false narratives disseminated by Russia which currently contains 5000 cases registered since 2015. The work of the task force can be accessed through its Internet website 'EU vs Disinfo', updated daily, and its weekly 'Disinformation Review'.[53] The latter highlights the latest cases of Russian disinformation, in an easy-to-understand manner and a light tone in order to reach a vast range of people. As for the strategic communication part, the ESTF tries to convey positive messages about the EU in the Eastern neighbouring countries, including Russia. For instance, the task force did a campaign in Russian language about the benefits of Erasmus+.[54]

In parallel to teams of professionals checking disinformation stories, it is equally important to give the keys to citizens to debunk false information themselves. Bjola calls it "digital containment".[55] For that purpose, the 2018 Action Plan rightly focuses on 'societal resilience', i.e. giving citizens the means to be able to sort out true and false information, to encourage them to question what they read and see, and to strengthen their critical spirit. It is interesting to note that the precise term 'societal resilience' is used for the first time in the Action Plan while the communication of April 2018 only refers to 'resilience'. Why this focus on societal resilience at this point in time? The citizens that are reading disinformation online are also the ones that were voting in the European elections in May 2019. It was thus crucial from the perspective of the EU institutions to give them the keys to distinguish between real and fake information.

[52] Interview with EEAS official 2, Brussels, 15 March 2019.
[53] https://euvsdisinfo.eu
[54] EEAS, *New opportunities for Russian students and academic staff to study, teach and train in Europe*, 24 October 2018.
[55] Bjola & Pamment, *op. cit.*

Combatting disinformation with the help of online platforms and cyber tools

With the rise of online disinformation especially on social media, the EU understood that it needs to include platforms in the fight against disinformation. This is easier said than done, knowing the platforms' reluctance to open their private data and the financial benefits they get from advertisement, including political and biased advertisement that can promote false information. Moreover, since disinformation is more and more combined with cyberattacks of all kinds, tackling disinformation means also strengthening cyber tools. This section thus analyses the EU's policies in the realm of online platforms and cyber issues together.

As already mentioned, social media and web search platforms play a key role in transmitting and amplifying disinformation. Therefore, fighting disinformation requires close cooperation with them. To this end, a working group of the multi-stakeholder forum on online disinformation drafted a Code of Practice on disinformation.[56] This Code of Practice was signed by Google, Mozilla, Facebook, Twitter, as well as eight trade associations (e.g. European Association of Communication Agencies, European Digital Media Association) in September 2018. The Code of Practice is non-binding and is part of a self-regulating approach. The signatories are required to submit a regular report assessing their progress in implementing the Code. The first implementation report was published in January 2019 by the four Internet giants. Until May 2019, the platforms had to publish an intermediate monitoring report every month to see how they implemented the actions that are "the most relevant and urgent to ensure the integrity of elections, namely: scrutiny of ad placements; political and issue-based advertising; and integrity of services".[57] Despite some encouraging advancements, the Commission laments the fact that the platforms struggle to transmit enough data and metrics to clearly measure the results of the activities undertaken, especially with the scrutiny of ad placements.[58] A general assessment of the implementation of the Code of Practice will be undertaken at the end of 2019. If not enough progress will have been made, the Commission may move towards a more assertive approach and propose regulation.

[56] European Commission, *EU Code of Practice on disinformation*, Brussels, 26 September 2018.
[57] European Commission, *Statement on the Code of Practice against disinformation: Commission asks online platforms to provide more details on progress made*, STATEMENT/19/1379, Brussels, 28 February 2019.
[58] *Ibid*.

The EU has been criticised for its decision to privilege a self-regulating approach.[59] There are no incentives for the platforms to apply the measures. A report done at the request of the Panel for the Future of Science and Technology of the European Parliament outlined that "social platforms may prioritise addressing certain issues which may not necessarily be the most important ones from disinformation containment perspective".[60] There is a discrepancy between the platforms' actions and the EU's expectations. The EU urged the platforms to act before May 2019 but one might wonder whether it is not too much to ask for in such a short period of time.

Taking measures to counter disinformation goes hand in hand with improving cybersecurity protection. The EU's actions in cyber are, as in the case of disinformation, defensive rather than offensive. Two strands can be distinguished: measures to prepare actors and infrastructures for possible cyberattacks (i.e. prevention and deterrence), coupled with measures to improve resilience and 'punish' the perpetrators of cyberattacks (i.e. sanctions). The document guiding the EU's actions in cyber is the 2013 "EU cyber security strategy: an open, safe and secure cyberspace".[61] The first EU-wide legislation on cybersecurity is the Directive on the Security of Network and Information Systems (NIS) adopted in 2016 (member states should have transposed it in their national legislation by now).[62] Its aim is to achieve "evenly high level of security of network and information systems across the EU".[63] More recently, the European Parliament adopted the Cybersecurity Act in March 2019 that will give a permanent mandate and more resources to the European Union Agency for Network and Information Security (ENISA) and will issue an EU-wide certification framework for information and communication technologies in order to harmonise cybersecurity standards for products and services. This is a step in the right direction.[64]

[59] "Google et Facebook s'engagent à suivre un code de bonnes pratiques", *EurActiv*, 27 September 2018.

[60] Panel for the Future of Science and Technology, *op. cit*., p. 41.

[61] European Commission & High Representative, *Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace*, JOIN(2013) 1 final, Brussels, 7 February 2013.

[62] European Commission, *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, COM(2017) 476 final/2, Brussels, 4 October 2017.

[63] European Commission, *Questions and Answers - Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity*, MEMO/18/3651, Brussels, 4 May 2018.

[64] Agence nationale de la sécurité des systèmes d'information, *Adoption définitive du Cybersecurity Act : un succès pour l'autonomie stratégique européenne*, Paris, 11 June 2019.

During the European Council of October 2018, restrictive measures (i.e. cyber sanctions) to respond to and deter cyberattacks were discussed.[65] They would be part of a so-called 'cyber diplomacy toolbox' and would target "individual hackers as well as state-linked groups with commercial bans and financial restrictions".[66] These sanctions are currently being discussed within the EU institutions. Yet, some questions remain open: how severe should a cyberattack be to merit sanctions? How to apply sanctions given the difficulty to identify the perpetrators of cyberattacks? Many countries lack capabilities for cyber forensics to identify state-sponsored hacker groups and "others lack the political will to call out their sponsors".[67]

In addition, the EU is trying to help member states improve their cyber resilience. In this field, ENISA is a key actor. The agency has set up the 'Partnership for Resilience' in 2011, which provides the guidelines for public-private sector cooperation and encourages member states to collaborate with the private sector. Cyber resilience, like the concept of societal resilience discussed previously, is linked to the concept of cyber hygiene. The latter implies teaching citizens safe behaviour in cyberspace. To this end, ENISA released a "Review of cyber hygiene practices" in 2016.[68]

This section gave an oversight of the different tools that the EU is using to combat online disinformation. The Union is developing its capabilities to debunk disinformation, improving cybersecurity and attempting to cooperate with online platforms. It has stepped up its efforts in view of the European elections 2019. Most of the measures are still at an embryonic stage, the ESFT being one of the most developed and well-functioning ones. How successful has the EU been so far in strategically countering external disinformation campaigns in cyberspace?

Assessment of the EU's actions and reflection on the future of disinformation

This section will first address the limits of the EU's actions to fight disinformation. Then, the future challenges posed by disinformation will be scrutinised, before finishing with some recommendations on how the EU can improve its policy in this field.

[65] European Council, *European Council meeting (18 October 2018) – Conclusions*, EUCO 13/18, Brussels, 18 October 2018.
[66] L. Cerulus, "Europe hopes to fend off election hackers with 'cyber sanctions'", *Politico EU*, 11 February 2019*.*
[67] *Ibid*.
[68] ENISA, *Review of cyber hygiene practices*, December 2016.

The limits of the EU's actions

Despite good initiatives, the EU's strategy is facing some pitfalls. One major criticism that was highlighted by an EEAS official is that the EU is acting too late and "too little in comparison to the means deployed by Russia".[69] Some observers like Bendiek and Schulze are considering the strategic task forces and the Action Plan as mere short-term solutions.[70]

The European elections of May 2019 prompted the EU to treat the fight against disinformation as a top priority. Yet, this was not the case among all member states. An EEAS official admitted that "the political will among member states to do something about disinformation is here, but the will to do a lot is not here since there is no common vision of disinformation being a threat".[71] Indeed, all 28 member states do not equally perceive false information as being a menace. This is particularly relevant when talking about Russian disinformation. Some member states, because of their past relations with the Soviet Union, are much more aware of the threat and much more willing to deal with it. This lack of a common vision has been acknowledged by the European Parliament which has expressed its concerns about "the limited awareness amongst some of [the EU's] member states that they are audiences and arenas of propaganda and disinformation".[72] Some member states also think that the EU is not the best forum to tackle disinformation.[73]

The think tank European Values ranked the EU member states according to their perception of Russian disinformation and the measures they implemented to counter it.[74] This study shows that the countries that have already been victims of Russian interference are keener to act, for instance France (Macron Leaks), the Baltic states (past history with Russia) or the United Kingdom (interference in Brexit referendum, Skripal case).[75] In short, the member states' approach to disinformation depends on the national context, their capabilities and, most importantly, their willingness to deal

[69] Interview with EEAS official 1, Brussels, 28 February 2019.

[70] A. Bendiek & M. Schulze, "Desinformation und die Wahlen zum Europäischen Parlament", *SWP Aktuell*, no. 10, Berlin, Stiftung Wissenschaft und Politik, 2019.

[71] Interview with EEAS official 2, Brussels, 15 March 2019.

[72] European Parliament, Committee on Foreign Affairs, Anna Elżbieta Fotyga (rapporteur), *Report on EU strategic communication to counteract propaganda against it by third parties*, 2016/2030(INI), Brussels, 14 October 2016.

[73] Interview with EEAS official 2, Brussels, 15 March 2019.

[74] European Values, *Ranking of countermeasures by the EU28 to the Kremlin's subversion operation*, Prague, 2018.

[75] On 4 March 2018, the former Russian spy Sergeï Skripal and his daughter Yulia Skripal have been the victim of a poisoning with a chemical weapon (Novichok) in Salisbury, UK. Two Russian nationals, Alexander Petrov and Ruslan Boshirov, are suspects in the attempted murder.

with it. Because there is such a variation in the member states' engagement, the EU is lacking strong political support to act.

Furthermore, there is an important discrepancy between the level of threat posed by disinformation and the EU's allocated resources to fight it. The budget does not represent accurately the scale of the problem, all the more when compared to the resources deployed by Russia. RT, Sputnik and other sources invest more than 1,1 billion euros a year to support pro-Kremlin propaganda. The Russian troll factory in Saint-Petersburg counts around 1000 full-time employees.[76] These numbers compared to the five million euros that the EU plans to allocate to disinformation still "leaves the EU on the weaker side [of this] asymmetric information warfare".[77] The small team of the ESTF will hardly have sufficient capabilities (in terms of human resources and technical material) to analyse big data. The task force is also "too dependent on the goodwill and financial contributions of member states".[78] It therefore needs stronger political commitment from the member states and more investments. The financial resources allocated to cyber are also poor when compared to other big actors: ENISA has an annual budget of 11 million euros while the US plans to spend 17,4 billion dollars for cybersecurity in 2020.[79]

Moreover, the fact that there are so many different entities at the EU level dealing with disinformation can also be a major drawback because it reduces efficiency. Non-governmental organisations (NGOs) have troubles knowing whom to talk to: which DG? Which person in the EEAS? A representative from a civil society organisation interviewed for this study explained that this problem of fragmentation also exists at the member states' level and that it is difficult to know whom to contact (who deals with disinformation at a national level: Ministry of Justice? Ministry of Foreign Affairs?).[80] Nevertheless, an interviewee from the EEAS thinks that this fragmentation can also have a positive side as all the different entities have different points of view that can complement each other.[81]

[76] S. Solton, "EU Commission takes aim at disinformation, admits funding deficit", *EurActiv*, 6 December 2018.
[77] E. Chivot, *The fight against online disinformation calls for concerted approaches to European policymaking*, Brussels, Centre For Data Innovation, 18 February 2019.
[78] C. Mortera-Martinez, "What is Europe doing to fight disinformation?", *CER Bulletin*, no. 123, London, Centre for European Reform, January 2019.
[79] The White House, "Cybersecurity Funding" in *A budget for a better America: Fiscal year 2020 - Budget of the U.S. government*, Washington, DC, 2019, pp. 305-310.
[80] Interview with a representative from a civil society organisation, Brussels, 20 February 2019.
[81] Interview with EEAS official 1, Brussels, 28 February 2019.

In addition, the current EU approach to deal with disinformation is focusing too little on AI and cyber capabilities. The development of AI will produce more performant and innovative bots to create and diffuse disinformation campaigns online. The possibilities that technology offers to generate more real and difficult-to-detect deep fakes seem endless. The EU is ill-prepared for this new wave of technology: Meserole and Polyakova argue that "the EU's measures are still designed to target the disinformation of yesterday rather than that of tomorrow".[82]

In addition, most of the current and upcoming Horizon 2020 projects on disinformation are dealing with fact-checking and only a few with AI and other new technologies. The future programme Horizon Europe allocates an important part of its resources to AI for the health, agriculture and transportation sectors but not directly to AI related to disinformation. Another problem is that technology advances far more quickly than regulation and policies. By the time the EU will have effectively implemented all its measures on disinformation, another wave of technological development will have brought new ways of artificially-created false information and will have made legislation obsolete in no time.

Lastly, the EU does not have a strategy that clearly associates cybersecurity and disinformation. It is also difficult for the EU to act in this field for the simple reason that it has few legal competences: cybersecurity governance remains the responsibility of the member states. As in the case of disinformation, AI will also impact cybersecurity: cyberattacks will be more powerful and more disruptive thanks to increasingly innovative and powerful tools. Some authors argue that a digital Geneva convention on cybersecurity is necessary as "the transnational nature of the web renders all unilateral attempts of protection illusory".[83] A global digital governance would give a common definition of what is truly a cyberattack and would also state how severe a cyberattack should be to merit sanctions. In the case of the EU and its 'cyber diplomacy toolbox', a global digital governance would facilitate the adoption of cyber sanctions. An EEAS official agreed that "a Geneva digital convention would certainly help and would ease the adoption of EU measures but the lack of it does not prevent the EU to act".[84]

[82] Meserole & Polyakova, *op. cit.*

[83] J.-H., Migeon, "Are we prepared for the next cyberwarfare?", *EU Logos*, 18 May 2018.

[84] Interview with EEAS official 1, Brussels, 28 February 2019.

Disinformation never sleeps: future challenges

Disinformation is a moving phenomenon. This paper has already underlined how AI will impact disinformation and will represent an enormous challenge for the EU if it does not take the right measures to adapt its strategy to technological innovations. This section outlines other challenges that the EU is likely to meet in the future.

Decentralised applications are still at a nascent stage but are likely to increase in the future. Decentralised applications store data on a decentralised blockchain and are not controlled by a single authority. Because they are decentralised, it is very difficult to track the accounts on these applications back to real-life individuals or organisations. Moreover, once information is submitted to a decentralised application, it is nearly impossible to take down. Therefore, these applications present an unprecedented challenge as content is impossible to remove. If governments and civil society can currently appeal to online platforms to “block or remove a malicious user or problematic content on social networks”, with decentralised applications, this will be almost impossible since “there will not always be someone to turn to”.[85]

Recently, two additional strategic task forces have been set up alongside the ESTF: the Western Balkans StratCom Task Force (to counter Russian disinformation in the region) and the South StratCom Task Force (to counter Islamic State terrorist organisation propaganda in North Africa and the Middle East). Yet, none of these task forces focuses on the emerging actors that might disrupt Western democracies through disinformation and cyberattacks even more than Russia. China and Iran are indeed two examples of countries whose strategies are becoming more and more offensive with regard to meddling in Western societies. China is known to use disinformation, cyberattacks and espionage to further its interests in Europe.[86] Similar to Russia, China uses a bot-driven computational propaganda, but disseminates positive and non-threatening narratives rather than aggressive ones like Russia. China usually diffuses “biased stories to promote the ‘Chinese dream’ as unfailingly positive and advantageous for the world at large”.[87] What is more, China has a huge potential in the realm of AI technologies, which makes it even more threatening for Europe. Some experts argue that China is “now ahead of Russia as the most prolific nation-state mounting attacks on firms, universities, government departments, think tanks and

[85] Interview with EEAS official 1, Brussels, 28 February 2019.

[86] C. Hymas, “China is ahead of Russia as 'biggest state sponsor of cyber-attacks on the West'”, *The Guardian*, 9 October 2018.

[87] “Beyond hybrid war: how China exploits social media to sway American opinion”, *Recorded Future*, 2019.

NGOs" in the West.[88] Alongside China, Iran is also very active in disseminating disinformation campaigns in the EU. The narratives diffused by Iran mostly deal with current European governments which are depicted as "failures, depraved and undeserving".[89] Its main objective is to influence people's opinion and "turn them against governments that do not support Iran or the Iranian regime".[90]

Underneath Russia's disinformation campaigns within the EU lies an even more complex problem: the links between the Russian Federation and European far-right movements. An EEAS official admitted that "the damage is already done"[91] through the long-standing relationship Russia has forged with some extreme right-wing parties in the EU. In line with its aim to destabilise the West, Russia tries to support political forces in Europe that have the same objective of disrupting Western unity. In some cases, Russia finances these parties. One of the most blatant examples is Russia's link with the French far-right party the 'Rassemblement National' led by Marine Le Pen. In 2014, the party received a loan of nine million euros from the First Czech-Russian Bank in Moscow.[92] More recently, Matteo Salvini, Deputy Prime Minister of Italy and Minister of the Interior, has been accused to have received three million euros from the Kremlin to finance the campaign of his party for the European elections.[93] It can be said that the Russian Federation has secured "a predominantly loyal political structure at the heart of European democracy".[94] Having this in mind, disinformation and cyberattacks do not seem as the most worrying issues right now.

Moreover, there is a growing number of European politicians (especially from the extreme right) that bring up false information during political debates, interviews or speeches.[95] Some use disinformation as a "means of political campaign".[96] Therefore, internal disinformation campaigns can to a certain extent be even more dangerous than the external ones.

[88] Hymas, *op. cit.*
[89] "Global Iranian disinformation operation - Large-scale fake news infrastructure promoting Iranian interests", *Clear Sky Cybersecurity*, October 2018.
[90] *Ibid*.
[91] Interview with EEAS official 1, Brussels, 28 February 2019.
[92] Popescu & Secrieru, *op. cit.,* p. 78.
[93] "Matteo Salvini accusé d'avoir profité de financements russes", *Courrier International*, 6 March 2019.
[94] A. Shekhovtsov, *Russia and the Western Far Right: Tango Noir*, Abingdon, Routledge, 2017.
[95] "Les politiques, relais des fake news", *LCI*, 19 January 2019.
[96] Interview with representative from a civil society organisation, Brussels, 20 February 2019.

At this point in time, no foreign interference in the 2019 European elections has been detected. The European Commission reports that "available evidence has not allowed to identify a distinct cross-border disinformation campaign from external sources specifically targeting the European elections. However, the evidence collected revealed a continued and sustained disinformation activity by Russian sources aiming to suppress turnout and influence voter preferences".[97] Based on these findings, some policy recommendations for the EU can be proposed.

Ways forward: policy recommendations

All the following suggestions have a common point: they call for a 'whole-of-government', a 'whole-of-society' and a 'whole-of-EU' approach. Indeed, the fight against disinformation requires a variety of actors to work together: policy-makers, social media platforms, journalists, the educational community, cybersecurity specialists, data scientists, AI researchers, political and social scientists, NGOs, etc.

AI has a darker and a brighter side. On the one hand, AI tools can act as amplifiers for disinformation but on the other hand, they can also help to detect and analyse false narratives. With the massive flow of information that circulates online on a daily basis, it becomes almost impossible for small teams of fact-checkers like the ESTF to detect false information all by themselves. Therefore, AI can be very helpful in identifying hostile narratives and analysing big data. AI can be used to detect and flag narratives: it can find "words or even patterns of words that can throw light on fake stories [...] [since] AI makes it easy to learn behaviours, possible through pattern recognition".[98] AI can suggest to users media outlets and reporting "outside of their echo chambers, thus opening their eyes to a broader range of viewpoints".[99] AI can also be used to determine the authenticity of a website by creating a machine-learning model. Nevertheless, it is important to underline that AI tools need to be combined with human verification. For instance, algorithms can make mistakes (i.e. censoring accurate and true information). Human oversight is therefore needed to contextualise information and to verify algorithms. It was suggested that the best way forward is to

[97] European Commission & High Representative, *Report on the implementation of the Action Plan Against Disinformation*, JOIN(2019) 12 final, Brussels, 14 June 2019.

[98] ENISA, *Strengthening network and information security and protecting against online disinformation*, April 2018, p. 4.

[99] Y. Benkler, R. Faris, H. Roberts & N. Bourassa, "Understanding media and information quality in an age of artificial intelligence, automation, algorithms and machine learning", Cambridge, Massachusetts, *Berkman Klein Center for Internet and Society at Harvard University*, 12 July 2018.

"implement human-in-the-loop solutions, where people are assisted by machine learning and AI methods, but not replaced".[100]

A key recommendation for the EU is to dedicate significant financial resources to research and development at the intersection of disinformation and AI. Most of the projects funded by the EU are either related to disinformation or to AI but very few combine both issues. The next Horizon Europe and Digital Europe programmes should therefore have calls for projects directly combining disinformation and AI. The research should focus on automated methods for detection of false information, detection of bots and improving algorithms on searching and social media platforms. Research efforts should also be dedicated to better understand decentralised applications and their role and impact on disinformation. Also, it is fundamental for researchers to have access to data and algorithms to analyse them, understand the patterns of disinformation and to find adequate solutions. The EU should find incentives for platforms to open their data and make their algorithms completely transparent.

It is essential to continue cataloguing and analysing the tools, techniques and intentions of disinformation campaigns. The EU should continue its support for quality journalism and fact-checking. It should support national fact-checking initiatives and encourage all mainstream media outlets to have specific fact-checking teams. The study done at the request of the Panel for the Future of Science and Technology of the European Parliament also suggested fact-checking to "be crowd-sourced with citizens flagging suspicious information which is then checked independently".[101]

Moreover, the EU needs to dedicate more financial resources to the fight against disinformation. Five million euros is not enough to deal with the complex issue of disinformation. An upgraded budget should first benefit the ESTF in order to hire more people and to upgrade their AI tools to help them deal with the abundance of information and disinformation sources. With the help of a larger team, the 'Disinformation Review' could be diffused on a larger scale and could be translated in all EU languages.

In a long-term perspective, raising public awareness on disinformation, promoting media literacy and critical thinking among citizens are key measures. The EU Action Plan rightly puts the focus on societal resilience beyond elections. The EU should put

[100] Panel for the Future of Science and Technology, *op. cit*., p. 40.

[101] *Ibid*., p. 76.

further efforts in promoting media literacy all over Europe and reach out to citizens that are the most vulnerable to disinformation. To this end, collaborating with non-state actors such as NGOs running projects on disinformation and local governments is essential. It is also important to promote the different tools and resources available to help citizens verify pieces of information. Education to media and training to recognise true and false information should be mandatory at schools all over the EU. Critical thinking should be included in every curriculum.

The EU needs therefore to have a strategy that combines cybersecurity and disinformation. While there is a tendency to think in silos and separate cyber issues and disinformation, the Macron Leaks showed that Russia has a global vision linking cyberattacks, disinformation and election interference. As a first step, Landau advocates a new definition of cybersecurity that takes into account disinformation.[102] Likewise, ENISA suggests classifying election systems and infrastructures as critical infrastructures. It would oblige "the responsible stakeholders to take the appropriate and necessary measures to safeguard their network and information systems to ensure a high level of cybersecurity".[103] Furthermore, the EU should dedicate additional financial resources to cyber and improve its capabilities in this domain. Collaboration with the private sector is key. The EU should develop public-private partnerships on cybersecurity: the more communication and coordination between the EU, national governments and the private sector, the better.

Lastly, the EU's efforts to tackle disinformation need to be combined with those of the member states. Since cyber governance remains a national competence, it is equally important that the member states improve their own cyber capabilities including by introducing legislation to tackle the challenges associated with online disinformation.

Conclusion: preparing for the battle

Disinformation is a multifaceted problem, "it does not have one single root cause, and thus does not have one single solution".[104] By focusing on Russian disinformation, this paper tried to answer the following question: to what extent is the EU strategically prepared to counter external disinformation campaigns in cyberspace? In the run up to the European elections in May 2019, the EU was taken by a sense of urgency and

[102] Landau, *op. cit.*

[103] ENISA, *Strengthening network and information security and protecting against online disinformation*, *op. cit.*, p. 5.

[104] European Commission, *Report of the independent High-level group on fake news and online disinformation: a multi-dimensional approach to disinformation*, Brussels, March 2018, p. 11.

accelerated its course of action in order to secure the ballot. The EU Action Plan against disinformation published in December 2018 provides a strong basis for action. The ESTF is a key asset to detect and debunk false Russian narratives. Measures such as the Code of Practice, if well implemented by the platforms, as well as the Cybersecurity Act and the prospect of cyber sanctions are promising steps in the right direction. However, to be fully prepared to counter external disinformation campaigns in cyberspace, substantial additional resources need to be deployed to try to reduce the strategic asymmetric gap between the EU and Russia. Also, the Union needs to focus more on the latest developments made in the field of AI that will tremendously impact the creation and dissemination of disinformation.

Overall, this paper has shown that technological development and social media have greatly accelerated the speed at which (false) news are diffused and have expanded their reach. It has also demonstrated how social media and AI tools such as algorithms and bots affect the way people inform themselves and create their own reality ('filter bubble' effect). Therefore, it is as important to have experts debunking disinformation than to educate citizens to think critically. This paper could serve as a basis for future research on Iranian or Chinese disinformation campaigns within the EU or to compare Russian disinformation campaigns diffused in the EU with the ones addressed to African or Latin American countries.

Bibliography

Aro, Jessikka, "The cyberspace war: propaganda and trolling as warfare tools", *European View*, no. 15, 2016, pp. 121-132.

Bendiek, Annegret & Matthias Schulze, "Desinformation und die Wahlen zum Europäischen Parlament", *SWP Aktuell*, no. 10, Berlin, Stiftung Wissenschaft und Politik, 2019.

Bernstein, Adam, *Not Russian to do anything? The EU response to strategic narratives and disinformation in the wake of the Russia-Ukraine crisis*, Master's thesis, Bruges, College of Europe, 2017.

Betz, David, "Cyberpower in strategic affairs: neither unthinkable nor blessed", *Journal of Strategic Studies*, vol. 35, no. 5, 2012, pp. 689-711.

Bjola, Corneliu, "Propaganda in the digital age", *Global Affairs*, vol. 3, no. 3, 2017, pp. 189-191.

Bjola, Corneliu & James Pamment, "Digital containment: Revisiting containment strategy in the digital age", *Global Affairs*, vol. 2, no. 2, 2016, pp. 131-142.

Boin, Arjen, Magnus Ekengren & Mark Rhinard, *Making sense of sense-making: The EU's role in collecting, analysing, and disseminating information in times of crisis*, Stockholm, The Swedish National Defence College, 2014.

European Values, *Ranking of countermeasures by the EU28 to the Kremlin's subversion operation,* Prague, 2018.

Hellman, Maria & Charlotte Wagnsson, "How can European states respond to Russian information warfare? An analytical framework", *European Security*, vol. 26, no. 2, 2017, pp. 153-170.

Jeangene Vilmer, Jean-Baptiste, Alexandre Escorcia, Marine Guillaume & Janaina Herrera, "Information manipulation, a challenge for our democracies", *Policy Planning Staff (French Ministry of Europe and Foreign Affairs) & the Institute for Strategic Research (French Ministry for the Armed Forces)*, Paris, 2018.

Karlsen, Geir Hågen, "Tools of Russian influence: information and propaganda", in Haaland Matlary, Janne & Tormod Heier (eds.), *Ukraine and beyond: Russia's strategic security challenge to Europe*, Basingstoke, Palgrave Macmillan, 2016, pp. 181-208.

Matsa, Katerina Eva, Laura Silver, Elisa Shearer & Mason Walker, *Western Europeans Under 30 View News Media Less Positively, Rely More on Digital Platforms Than Older Adults*, Washington, DC, Pew Research Center, 2018.

Mortera-Martinez, Camino, "What is Europe doing to fight disinformation?", *CER Bulletin*, no. 123, London, Centre for European Reform, January 2019.

Romerstein, Herbert, "Disinformation as a KGB weapon in the Cold War", *Journal of Intelligence History*, vol. 1, no. 1, 2001, pp. 54-67.

Shekhovtsov, Anton, *Russia and the Western Far Right: Tango Noir*, Abingdon, Routledge, 2017.

Spildsboel Hansen, Flemming, *Russian hybrid warfare: a study of disinformation*, Zürich, Centre for Security Studies, 2017.

Treverton, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee & Madeline McCue, "Addressing hybrid threats", Stockholm, *Swedish Defence University*, 2018.

Tucker, Joshua A., Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal & Brendan Nyhan, *Social media, political polarization, and political disinformation: A review of the scientific literature*, New York, Hewlett Foundation, 2018.

Who said what? The security challenges of modern disinformation, Ottawa, Canadian Security Intelligence Service, 2018.

Newspaper articles

Andrikiene, Laima, "We still need East StratCom against Kremlin trolls", *EUObserver*, 7 June 2018, retrieved 22 April 2019, https://euobserver.com/opinion/142022

Barbière, Cécile, "Russia: Master of information manipulation", *EurActiv*, 11 September 2018, retrieved 22 April 2019, https://www.euractiv.com/section/future-eu/news/la-russie-championne-de-la-manipulation-de-linformation/?utm_term=Autofeed&utm_campaign= Echobox&utm_medium=social&utm_source=Facebook#Echobox=1536702850

Cerulus, Laurens, "Europe hopes to fend off election hackers with 'cyber sanctions'", *Politico EU*, 11 February 2019, retrieved 22 April 2019, https://www.politico.eu/article/europe-cyber-sanctions-hoped-to-fend-off-election-hackers

"Google et Facebook s'engagent à suivre un code de bonnes pratiques", *EurActiv,* 27 September 2018, https://www.euractiv.fr/section/economie/news/google-et-facebook-sengagent-a-suivre-un-code-de-bonnes-pratiques/

Hymas, Charles, "China is ahead of Russia as 'biggest state sponsor of cyber-attacks on the West'", *The Guardian*, 9 October 2018, retrieved 22 April 2019, https://www.telegraph.co.uk/technology/2018/10/09/china-ahead-russia-biggest-state-sponsor-cyber-attacks-west

"Les politiques, relais des fake news", *LCI*, 19 January 2019, retrieved 22 April 2019, https://www.lci.fr/insolite/les-politiques-relais-des-fake-news-2110583.html

MacFarquhar, Neil, "A powerful Russian weapon: the spread of false stories", *The New York Times*, 28 August 2016, retrieved 22 April 2019, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html

"Matteo Salvini accusé d'avoir profité de financements russes", *Courrier International*, 6 March 2019, retrieved 20 April 2019, https://www.courrierinternational.com/article/enquete-matteo-salvini-accuse-davoir-profite-de-financements-russes

Meserole, Chris & Alina Polyakova, "Disinformation wars", *Foreign Policy*, 25 May 2018, retrieved 20 April 2019, https://foreignpolicy.com/2018/05/25/disinformation-wars

Stark, Tim, "The interplay between Russian disinformation and hacking", *Politico*, 18 December 2018, retrieved 22 April 2019, https://www.politico.com/newsletters/morning-cybersecurity/2018/12/18/the-interplay-between-russian-disinformation-and-hacking-459226

Solton, Samuel, "EU Commission takes aim at disinformation, admits funding deficit", *EurActiv*, 6 December 2018, retrieved 22 April 2019, https://www.euractiv.com/section/digital/news/eu-commission-takes-aim-at-disinformation-admits-funding-deficit/

Official documents

Agence nationale de la sécurité des systèmes d'information, *Adoption définitive du Cybersecurity Act : un succès pour l'autonomie stratégique européenne*, Paris, 11 June 2019.

Bayer, Judit, Natalija Bitiukova, Petra Bárd, Judit Szakács, Alberto Alemanno & Erik Uszkiewicz, *Disinformation and propaganda – Impact on the functioning of the rule of law in the EU and its Member State*s, Directorate General for Internal Policies of the Union of the European Parliament, PE 608.864, Brussels, February 2019.

Bentzen, Naja, *Disinformation, 'fake news' and the EU's response*, European Parliamentary Research Service, PE 614.584, Brussels, November 2017.

European Commission & High Representative, *Cybersecurity Strategy of the European Union: an open, safe and secure cyberspace*, JOIN(2013) 1 final, Brussels, 7 February 2013.

European Commission & High Representative, *Joint Framework on countering hybrid threats: a European Union response*, JOIN(2016) 18 final, Brussels, 6 April 2016.

European Commission & High Representative, *Action Plan against disinformation*, JOIN(2018) 36 final, Brussels, 5 December 2018.

European Commission & High Representative, *Report on the implementation of the Action Plan Against Disinformation*, JOIN(2019) 12 final, Brussels, 14 June 2019.

European Commission, *EU Code of Practice on disinformation*, Brussels, 26 September 2018.

European Commission, *Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*, COM(2017) 476 final/2, Brussels, 4 October 2017.

European Commission, *Questions and Answers - Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity*, MEMO/18/3651, Brussels, 4 May 2018.

European Commission, *Report of the independent High-level group on fake news and online disinformation: a multi-dimensional approach to disinformation*, Brussels, March 2018.

European Commission, *Statement on the Code of Practice against disinformation: Commission asks online platforms to provide more details on progress made*, STATEMENT/19/1379, Brussels, 28 February 2019.

European Commission, *Tackling online disinformation: a European approach,* COM(2018) 236 final, Brussels, 26 April 2018.

European Council, *European Council meeting (19 and 20 March 2015) – Conclusions,* EUCO 11/15, Brussels, 20 March 2015.

European Council, *European Council meeting (18 October 2018) – Conclusions*, EUCO 13/18, Brussels, 18 October 2018.

European Parliament, Committee on Foreign Affairs, Anna Elżbieta Fotyga (rapporteur), *Report on EU strategic communication to counteract propaganda against it by third parties*, 2016/2030(INI), Brussels, 14 October 2016.

European Parliament, *Online Disinformation and the EU's response*, 24 April 2018, retrieved 20 April 2019, https://epthinktank.eu/2018/04/24/online-disinformation-and-the-eus-response

European Union Agency for Network and Information Security, *Review of cyber hygiene practices*, Athens, December 2016.

European Union Agency for Network and Information Security, *Strengthening network and information security and protecting against online disinformation*, Athens, April 2018.

Giles, Keir, *The next phase of Russian information warfare*, NATO: Strategic Communications Centre of Excellence, Riga, 2016.

Panel for the Future of Science and Technology, *Automated tackling of disinformation*, European Science-Media Hub, European Parliamentary Research Service, PE 624.278, Brussels, March 2019.

Popescu, Nicu & Stanislav Secrieru (eds.), *Hacks, leaks and disruptions - Russian cyber strategies*, Paris, European Union Institute for Security Studies, October 2018.

The White House, "Cybersecurity Funding", in *A budget for a better America: Fiscal year 2020 - Budget of the U.S. government*, Washington, DC, 2019, pp. 305-310.

Websites

Benkler, Yochai, Rob Faris, Hal Roberts & Nikki Bourassa, "Understanding media and information quality in an age of artificial intelligence, automation, algorithms and machine learning", Cambridge, Massachusetts, *Berkman Klein Center for Internet and Society at Harvard University*, 12 July 2018, retrieved 20 April 2019, https://cyber.harvard.edu/story/2018-07/understanding-media-and-information-quality-age-artificial-intelligence-automation

"Beyond hybrid war: how China exploits social media to sway American opinion", *Recorded Future*, 6 March 2019, retrieved 20 April 2019, https://www.recordedfuture.com/china-social-media-operations

Chivot, Eline, *The fight against online disinformation calls for concerted approaches to European policymaking*, Brussels, Centre For Data Innovation, 18 February 2019, retrieved 20 April 2019, https://www.datainnovation.org/2019/02/the-fight-against-online-disinformation-calls-for-concerted-approaches-to-european-policymaking

Ciobanu, Mădălina, "The challenges and opportunities of using artificial intelligence to tackle misinformation", *Journalism.co.uk*, 14 April 2018, retrieved 20 April 2019, https://www.journalism.co.uk/news/the-challenges-and-opportunities-of-using-artificial-intelligence-to-tackle-misinformation/s2/a720411

European External Action Service, *New opportunities for Russian students and academic staff to study, teach and train in Europe*, Brussels, 24 October 2018, retrieved 20 April 2019, https://eeas.europa.eu/headquarters/headquarters-homepage/52419/new-opportunities-russian-students-and-academic-staff-study-teach-and-train-europe_en

"Global Iranian disinformation operation - Large-scale fake news infrastructure promoting Iranian interests", *Clear Sky Cybersecurity*, October 2018, retrieved 20 April 2019, https://www.clearskysec.com/wp-content/uploads/2018/11/Global-Iranian-Disinformation-Operation-Clearsky-Cyber-Security.pdf

Landau, Susan, "Cybersecurity: time for a new definition", *Lawfare*, 12 January 2018, retrieved 20 April 2019, https://www.lawfareblog.com/cybersecurity-time-new-definition

Migeon, Jean-Hugues, "Are we prepared for the next cyberwarfare?", *EU Logos*, 18 May 2018, retrieved 20 April 2019, https://eulogos.blogactiv.eu/2018/05/16/are-we-prepared-for-the-next-cyberwarfare

Panetta, Kasey, "Gartner top strategic predictions for 2018 and beyond"*, Gartner.com*, 3 October 2017, retrieved 20 April 2019, https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond

Interviews

Interview with EEAS official 1, Brussels, 28 February 2019.

Interview with EEAS official 2, Brussels, 15 March 2019.

Interview with GMF official, Brussels, 15 March 2019.

Interview with representative from a civil society organisation, Brussels, 20 February 2019.

List of recent EU Diplomacy Papers

For the full list of papers and free download, please visit ***www.coleurope.eu/EUDP***

1/2018
Elise Cuny, *The EU's New Migration Partnership with Mali: Shifting towards a Risky Security-Migration-Development Nexus*

2/2018
Sara Canali, *The Thin Veil of Change: The EU's Promotion of Gender Equality in Egypt and Tunisia*

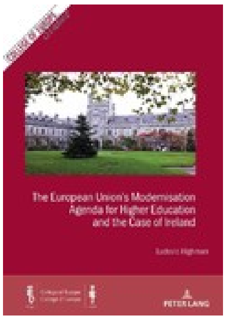
3/2018
Bram De Botselier, Sofía López Piqueres & Simon Schunz, *Addressing the 'Arctic Paradox': Environmental Policy Integration in the European Union's Emerging Arctic Policy*

4/2018
Valentin Steinhauer, *Leaving the Paris Agreement: The United States' Disengagement from the Global Climate Regime and its Impact on EU Climate Diplomacy*

5/2018
Esther Kestemont, *What Role(s) for the European Union in National Dialogues? Lessons Learned from Yemen*

6/2018
Melanie Bonnici Bennett, *The Refugee Crisis and the EU's Externalisation of Integrated Border Management to Libya and Turkey*

1/2019
Mélanie Scheidt, *The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle?*


The European Union's Modernisation Agenda for Higher Education and the Case of Ireland
Ludovic Highman
PETER LANG

College of Europe Studies

Order online at www.peterlang.com

PIE - Peter Lang Bruxelles

vol. 20 Highman, Ludovic, *The European Union's Modernisation Agenda for Higher Education and the Case of Ireland*, 2017 (272 p.) ISBN 978-2-8076-0616-6 pb.

vol. 19 Bourgeois, Jacques H.J. / Marco Bronckers / Reinhard Quick (eds.), *WTO Dispute Settlement: a Check-up: Time to Take Stock*, 2017 (167 p.) ISBN 978-2-80760-377-6 pb.

vol. 18 Schunz, Simon, *European Union Foreign Policy and the Global Climate Regime*, 2014 (371 p.), ISBN 978-2-87574-134-9 pb.

vol. 17 Govaere, Inge / Hanf, Dominik (eds.), *Scrutinizing Internal and External Dimensions of European Law: Les dimensions internes et externes du droit européen à l'épreuve,* Liber Amicorum Paul Demaret, Vol. I and II, 2013 (880 p.), ISBN 978-2-87574-085-4 pb.

vol. 16 Chang, Michele / Monar, Jörg (eds.), *The European Commission in the Post-Lisbon Era of Crises: Between Political Leadership and Policy Management (With a Foreword by Commission Vice President Maros Sefcovic)*, 2013 (298 p.), ISBN 978-2-87574-028-1 pb.

vol. 15 Mahncke, Dieter / Gstöhl, Sieglinde (eds.), *European Union Diplomacy: Coherence, Unity and Effectiveness (with a Foreword by Herman Van Rompuy)*, 2012 (273 p.), ISBN 978-90-5201-/842-3 pb.

vol. 14 Lannon, Erwan (ed.), *The European Neighbourhood Policy's Challenges / Les défis de la politique européenne de voisinage,* 2012 (491 p.), ISBN 978-90-5201-779-2 pb.

vol. 13 Cremona, Marise / Monar, Jörg / Poli, Sara (eds.), *The External Dimension of the European Union's Area of Freedom, Security and Justice*, 2011 (434 p.), ISBN 978-90-5201-728-0 pb.

vol. 12 Men, Jing / Balducci, Giuseppe (eds.), *Prospects and Challenges for EU-China Relations in the 21st Century: The Partnership and Cooperation Agreement*, 2010 (262 p.), ISBN 978-90-5201-641-2 pb.

vol. 11 Monar, Jörg (ed.), *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*, 2010 (268 p.), ISBN 978-90-5201-615-3 pb.

vol. 10 Hanf, Dominik / Malacek, Klaus / Muir Elise (dir.), *Langues et construction européenne,* 2010 (286 p.), ISBN 978-90-5201-594-1 br.

vol. 9 Pelkmans, Jacques / Hanf, Dominik / Chang, Michele (eds.), *The EU Internal Market in Comparative Perspective: Economic, Political and Legal Analyses*, 2008 (314 p.), ISBN 978-90-5201-424-1 pb.

vol. 8 Govaere, Inge / Ullrich, Hans (eds.), *Intellectual Property, Market Power and the Public Interest*, 2008 (315 p.), ISBN 978-90-5201-422-7 pb.

vol. 7 Inotai, András, *The European Union and Southeastern Europe: Troubled Waters Ahead?*, 2007 (414 p.), ISBN 978-90-5201-071-7 pb.

vol. 6 Govaere, Inge / Ullrich, Hanns (eds.), *Intellectual Property, Public Policy, and International Trade*, 2007 (232 p.), ISBN 978-90-5201-064-9 pb.