College of Europe
Collège d'Europe

Brugge

Natolin

The EU's Response to Disinformation in the Run-up to the 2019 European Elections: Ideational, Political and Institutional Genesis of a Nascent Policy

Matteo Riceputi

DEPARTMENT OF EUROPEAN POLITICAL AND GOVERNANCE STUDIES

Bruges Political Research Papers 85 / 2021

College of Europe
Collège d'Europe

Brugge

Natolin

European Political and Governance Studies /

Etudes politiques et de gouvernance européennes

Bruges Political Research Papers / Cahiers de recherche politique de Bruges

No 85 / June 2021

The EU's Response to Disinformation in the Run-up to the 2019 European Elections: Ideational, Political and Institutional Genesis of a Nascent Policy

Matteo Riceputi

© Matteo Riceputi

About the author

Matteo Riceputi graduated with an M.A. in European Political and Governance Studies from the College of Europe (Bruges) in 2020. After completing a master's degree in European Politics and Public Affairs from Sciences Po Strasbourg, he joined the General Secretariat of the Council of the European Union in 2019, witnessing first-hand the EU's response to disinformation in the run-up to the European elections. Mr Riceputi now works in a European public affairs consultancy, based in Brussels.

This paper is based on the author's master's thesis at the College of Europe under the supervision of Professor Nathalie Brack.

Acknowledgements

Mme la Professeure Brack ainsi que M. Frederik Mesdag, pour leur encadrement d'une immense qualité, leur grande disponibilité et leurs précieux conseils.
Mme Catherine Dodane et M. Franck Bouillé, pour leur inaltérable soutien, patience et bienveillance.
M. Vincent Riceputi, pour son travail acharné et sans qui je n'aurais jamais passé les portes du Collège.
Mme Berta Carol Galcerán, pour ses grands enseignements et la curiosité professionnelle qu'elle a éveillé.
M. Carlo Didonè, pour son amitié et son hospitalité sans faille.
Le groupe Pyrolyse, pour les rires qui ont égayé cette année.
M. Daniel Böhmer et M. Guillermo Rebollo, pour leur assistance technique bienvenue.
M. Tom Crance, pour ces après-midis faites d'évasion et de conquêtes.
Mlle Claudia Fernández García, pour tout ce qui ne s'explique pas.

Contact details:

matteo.riceputi@coleurope.eu

Editorial Team
Michele Chang, Alexia Fafara, Eva Gerland, Oriane Gilloz, Lorenzo Giulietti, Frederik Mesdag, Pauline Thinus, Thijs Vandenbussche, Pablo Villatoro, and Olivier Costa

Dijver 11, B-8000 Bruges, Belgium | Tel. +32 (0) 50 477 281 | Fax +32 (0) 50 477 280
email michele.chang@coleurope.eu | website www.coleurope.eu/pol

Views expressed in the Bruges Political Research Papers are solely those of the author(s) and do not necessarily reflect positions of either the series editors or the College of Europe. If you would like to be added to the mailing list and be informed of new publications and department events, please email rina.balbaert@coleurope.eu. Or find us on Facebook: www.facebook.com/coepol

Abstract

The run-up to the 2019 European elections has seen an unprecedented effort of EU institutions to address the phenomenon of disinformation. From the mid-2010s frenzy of 'fake news' up to the institutionalisation of a European disinformation policy, this study seeks to identify the main drivers of the EU's response to disinformation in the run-up to the 2019 European elections. We most specifically try to explain why the EU's response to disinformation has been mostly formulated in security-centred terms, as opposed to society-centred terms. This research builds on original empirical material comprising interviews from EU officials that were in charge of the disinformation 'file' in their respective institution. Using the method of explaining-outcome process tracing, we look at the extent to which 'ideas', 'interests' and 'institutions' have respectively shaped the EU's disinformation policy, from its appearance on the European agenda in 2015 up until the climax of its implementation in early 2019. (i) The initial framing of the problem of disinformation as a foreign threat from Russia, (ii) the EU's interest for the preservation of its input legitimacy and the enhancement of its output legitimacy, as well as (iii) the weight of the European Council and the EEAS in inter-institutional competition have all played a significant role in shaping the EU's security-centred response to disinformation.

1. Introduction

Fake news, or rather, political mentions of 'fake news', have invaded public space since the mid-2010s. Embraced by prominent politicians and their supporters, this term has become a formidable weapon, a performative label allowing for the disqualification of political adversaries, be they institutional entities, politicians or media outlets.[1] The frenzy surrounding this magic yet oxymoronic formula certainly reached its highpoint in 2016, in the context of the British EU membership referendum and US presidential election. What is at stake here is nothing less than one of the pivotal features of democratic polities, namely, well-informed citizens. Quite logically, this stake will take decisive importance in electoral periods, just as voters are expected to go to the polls and perform – in all good conscience – the most sacred ritual of contemporary democracies.[2]

However and despite its global resonance, **the term 'fake news' does not enable one to grasp the many motives, uses and consequences of the much wider, systemic and pernicious phenomenon which is that of disinformation**. In addition to being charged politically, the term 'fake news' cannot account for something which is not an "isolated incident of falsehood" but a targeted and intentional endeavour,[3] involves content that is not necessarily 'fake' but rather rigged information mixed with facts, and translates into techniques that have not much to do with the traditional acceptance of 'news'.[4]

Consensus has therefore emerged amongst researchers, and permeated the European Union (EU) decision-making bodies, to prefer the term 'disinformation'. We here retain the definition put forward by the European Commission-mandated "High-Level Group on fake news and online disinformation" (HLEG), which defined disinformation as: "false, inaccurate,

---

[1] Cherilyn Ireton and Julie Posetti (eds.), *Journalism, Fake News & Disinformation*, UNESCO, Paris, 2018, p. 14. High Level Group on fake news and online disinformation, *A multi-dimensional approach to disinformation*, Luxembourg, EU Publications Office, March 2018, p. 10.
[2] Yves Déloye and Olivier Ihl, *L'acte de* vote, Paris, Presses de Sciences Po, 2008.
[3] Lance Bennett and Steven Livingston, "The disinformation order: Disruptive communication and the decline of democratic institutions", *European Journal of Communication*, vol. 33, no. 2, 2018, p. 124.
[4] High Level Group on fake news and online disinformation, *A multi-dimensional approach to disinformation*, Luxembourg, Publications Office of the European Union, March 2018, p. 10.

or misleading information designed, presented and promoted to intentionally cause public harm or for profit".[5] Disinformation thus appears as a *deliberate* and politically or financially *motivated* act. While the EU had sporadically addressed disinformation since 2015 as one of the aspects of the Russia/Ukraine dispute,[6] the Commission's initiative of convening the HLEG attests to its willingness to create a new "*catégorie d'action publique*"[7] and objectify a disinformation "public problem",[8] paving the way towards **a fully-fledged EU disinformation policy**. As the 2019 European elections were approaching and for the first time in history, the EU indeed perceived disinformation as a looming and credible threat.

We preliminarily consider 'the EU's' response to disinformation as a single and relatively homogeneous outcome. However, this study looks into the respective role of the five major EU political institutions – the European Commission, European External Action Service (EEAS), European Council, Council of the EU, and European Parliament – and may therefore subsequently regard the EU's response as pluralistic and fragmented along institutional lines.

While having engendered significant amounts of media coverage and policy recommendations, this topic remains little-studied. Recent research has mostly considered disinformation through the – often US-centred – narrow prism of 'fake news' and social media. In turn, when exploring the EU's legitimacy, EU studies have interestingly identified the information of citizens as a major issue, but have focused on citizens' lack of information rather than on disinformation as such. Finally, research points at the potentially counter-productive effects of direct regulation, advocating for an approach favouring a healthy media ecosystem and empowered citizens.

---

[5] High Level Group, *op. cit.*
[6] European Council, Conclusions (EUCO 11/15), 20 March 2015, p. 5.
[7] Vincent Dubois, "L'action publique", in: Cohen, Lacroix and Riutort (eds.), *Nouveau Manuel de Science Politique*, Paris, La Découverte, 2009, p. 17.
[8] Pierre Lascoumes and Patrick Le Galès, *Sociologie de l'action publique*, Paris, Armand Colin, 2nd edn, 2012, pp. 63-65.

We seek to identify the main drivers of the EU's response to disinformation in the run-up to the 2019 European elections. More specifically, this study aims at explaining **why the EU's response to disinformation has been mostly formulated in security-centred terms**. We indeed regard European institutions as having primarily conceived, designed and implemented what we term a **'security-centred' approach to disinformation**. Such an approach describes disinformation as an *ad hoc*, external and exogenous threat arising from malicious foreign actors aiming to disseminate political confusion; in this perspective, effective responses to disinformation should consist of reactive measures, implying enhanced detection and strategic response capabilities allowing to counter disinformation in a swift and frontal manner. One major alternative to this approach is what we identify as a **'society-centred' approach**. Here, disinformation is regarded as an internal, endogenous and multi-faceted problem which takes advantage of citizens' overall lack of trust in institutions and the media; in this perspective, disinformation would be best addressed through a preventive empowerment of citizens' media and information literacy, as well as the promotion of a plural and sustainable media environment rendering disinformation attempts non-profitable. These two approaches are ideal-typical forms, into which EU actions do not always distinctly fall. Still, our research has evidenced that the most significant of them predominantly relate to the 'security-centred' paradigm.

In order to best account for this outcome and produce a comprehensive investigation of its many potential drivers, we use the '3I' model and **analyse the extent to which 'ideas', 'interests' and 'institutions' have respectively contributed to make the EU's response to disinformation a security-centred one**[9]**.** First, when investigating 'ideas', we put forward the hypothesis that the EU has formulated a security-centred response to disinformation as a result of the initial framing of the problem, namely, as a foreign threat from Russia. Turning

[9] Bruno Palier and Yves Surel, "Les 'trois I' et l'analyse de l'État en action", *Revue française de science politique*, vol. 55, no. 1, 2005, p. 8.

to 'interests', we focus on the legitimation stakes implied by the electoral context of 2018-19 and set the double hypothesis that EU policy-makers have preferred a security-centred response because it would be (i) most protective of the European elections' integrity, hence best securing the EU's input legitimacy, and (ii) most visible for EU citizens, hence most profitable in terms of policy feedbacks and output legitimacy.[10] Finally, we assess the extent to which the EU's security-centred response to disinformation has been influenced by the European Council and the EEAS in inter-institutional competition.

This research builds on original empirical material comprising interviews of the EU officials that were in charge of the disinformation 'file' in their respective institution, namely the European Commission, EEAS, European Council, Council of the EU and European Parliament. Aiming to rigorously account for the main causal mechanisms driving the formulation of this policy, we use the inductive method of "explaining-outcome process tracing".[11]

Starting by introducing the three streams of research this study builds on, we then detail our theoretical approach as well as core research question, before presenting our process tracing methodology and the original empirical data we obtained from interviews. Finally, after exposing the 'security-centred' nature of the EU's response to disinformation, we assess the respective influence of (H1) the initially Russian-focused frame of the problem, (H2a and H2b) the EU's search for input and output legitimacy, and (H3) the weight of the European Council and the EEAS in inter-institutional competition on the formulation of the EU's response to disinformation in the run-up to the 2019 European elections.

[10] Claire Dupuy and Virginie Van Ingelgom. "Comment l'Union européenne fabrique (ou pas) sa propre légitimité", *Politique européenne*, vol. 54, no. 4, 2016, pp. 152-187.
[11] Derek Beach and Rasmus Brun Pedersen, *Process-tracing Methods: Foundations and Guidelines*, Ann Arbor, University of Michigan Press, 2013.

2. Literature Review

Disinformation as such has usually been regarded as a sketchy object of research, considered exclusively in the US context, or studied through the restrictive lenses of 'fake news' and social media. When it comes to EU studies, scholars have extensively documented the growing distrust of citizens in European institutions in terms of *lack* of information, as opposed to disinformation as such. In parallel, the implications of the well-documented democracy/ security tension and its limits have not been sufficiently explored regarding public institutions' approach to disinformation.

Of note, however, is the attempt by a few American scholars to study 'fake news' and social media aspects as mere components of a broader "disinformation order".[12] Rather than framing the problem as "isolated incidents of falsehood and confusion", this approach bypasses the popular but inaccurate concept of 'fake news' to look at disinformation as a systemic and motivated phenomenon.[13] This approach also considers the breakdown of citizens' trust in public institutions and mainstream media as being key, and studies disinformation not in relation to the tool of social media, but rather in relation to the underlying issue of legitimacy in democratic regimes. The focus thus shifts from vectors to root causes – or, one may say, from the wood to the trees. The decline of citizens' confidence in official or mainstream messages, hence generating a demand for alternative discourse, is here identified as the breeding ground of disinformation.[14] To some extent this study falls in line with this approach, which is closer from encompassing the complexity of the origins and implications of disinformation.

[12] Bennett and Livingston, *op. cit*.
[13] *Ibid*., p. 124.
[14] See: Paul Butcher, *Disinformation and democracy: The home front in the information war*, European Policy Centre, European Politics and Institutions Programme, 2019.

By building on the theoretical contributions of the seminal American research on disinformation, the substantive literature on EU legitimacy, and the debate about the security/democracy tension, this research therefore seeks to propose an original analysis of the formulation of the EU's security-centred disinformation policy.

3. Theoretical approach

3.1 Main drivers: a multi-dimensional public policy analysis

As a more general theoretical framework, this study fits into the **sociology of public action**, which provides several crucial theoretical assumptions. First, we break with the idea of a single and monolithic politico-administrative apparatus,[15] to look at inter-service and inter-institutional competition within the field of decision-making. We secondly rely on the key concept of "public problems".[16] The latter allows us to conceive public policy as being preceded by the formulation, configuration and selection of its fields of intervention, that is, the *construction* of 'problems'.[17] So-called "public problems" are not natural, autonomous or pre-existing: public institutions actually play an active part in their shaping and objectification.[18] This process implies the construction of cognitive / interpretative frames of any given phenomenon, with "entrepreneurs" promoting their own definition (frame) of the problem (phenomenon) in order to obtain gains, notably in terms of legitimacy.[19] The 'solutions' chosen by public decision-makers may therefore be closely related to the way in which the 'problem' was framed.[20] In this perspective, public policy is considered as being

[15] Dubois, *op. cit*., p. 6.
[16] Joseph Gusfield, *The Culture of Public Problems*, Chicago, University of Chicago Press, 1981, cited in Dubois, *op. cit*. p. 14.
[17] Lascoumes and Le Galès, *op. cit*., p. 63.
[18] Gusfield, *op. cit.*, cited in Dubois, *op. cit*. p. 14.
[19] Howard Becker, 1985, cited in Dubois, *op. cit*., p. 15.
[20] Dubois, *op. cit*., p. 15.

conditioned by the cognitive frames that have been attached to a 'problem' by certain actors and institutions.

A related operational concept is "path dependency".[21] It shows that once a public policy is formulated in one particular way or settled on one particular path, alternative policy options become more difficult to implement or even consider.[22] In this regard, the early stages of policy-making – such as the formulation of "public problems" – are of critical importance in the subsequent development of a policy, since they generate certain ideational, political and institutional settings in which alteration entails ever-increasing costs.[23] The potential inertia effects generated on the EU's disinformation policy by the initial formulation of the disinformation "problem" will therefore be of particular interest.

The **EU's legitimacy** also plays an important theoretical role in our study. The EU's disinformation policy reached its climax prior to the 2019 European elections. The EU's response to disinformation can logically be considered as an attempt to protect the EU's main source of input legitimacy.[24] Secondly, the EU's disinformation policy also has implications in terms of output legitimacy, defined as the quality of policy outcomes for citizens.[25] Any public policy indeed contributes to determine citizens' attitudes vis-à-vis their institutions, as part of a "policy feedback" process.[26] This is particularly relevant in the case of the EU, which, often described as a "regulatory"[27] or "policy-making"[28] state, has been primarily relying on output legitimacy. In this perspective, the showcase of policy outcomes is of critical importance.[29] More precisely, positive policy-feedbacks are generated if a public policy is both visible and traceable in the eyes of citizens,[30] meaning that citizens should be able to link

[21] Paul Pierson, 2000, cited in Lascoumes and Le Galès, *op. cit*., p. 84.
[22] *Ibid*.
[23] Lascoumes and Le Galès, *Ibid*.
[24] Scharpf, *op. cit*.
[25] *Ibid*.
[26] Dupuy and Van Ingelgom, *op. cit.*
[27] Giandomenico Majone, *Regulating Europe*, London, Routledge, 1996.
[28] Jeremy Richardson, 2012, cited in Dupuy and Van Ingelgom, *op. cit*., p. 154.
[29] See for instance the campaign 'What the EU does for me', launched by the European Parliament in 2018.
[30] Dupuy and Van Ingelgom, *op. cit*., p. 155.

policy outcomes with the action of public authorities.[31] We therefore consider that, as much as citizens' formal 'input' political participation, the outcome of EU public policies play a crucial role in the legitimation of the EU. The EU's disinformation policy will therefore be examined as a legitimation tool for EU institutions, both regarding the protection of its input legitimacy and the enhancement of its output legitimacy.

Finally, in order to undertake the most comprehensive possible analysis of the potential drivers of the EU's response to disinformation, this study makes use of the **'3I' model and evaluates the extent to which 'ideas', 'interests' and 'institutions' have respectively influenced this policy in the run-up to the 2019 European elections**. The concept of 'ideas' relates to a cognitivist approach of public policy analysis, insisting on the intellectual dynamics that contribute to frame policy processes.[32] In this regard, we use the concept of "construction of public problem" as a way to analyse the cognitive frames attached to disinformation in the EU. Second, the concept of 'interests' is linked to a more rational account of public policy analysis, taking into account the cost-benefit calculus made by relevant actors.[33] We associate the notion of 'interests' to the EU's legitimacy since, as the distrust of citizens has become an ever-growing concern for EU decision-makers over the last decades, the EU's disinformation policy involves high legitimation stakes both on the input and output sides.[34] Finally, the concept of 'institutions' refers to the weight of historically constructed structures which constrain the margin of manoeuvre of actors.[35] Consistent with the idea that the EU's politico-administrative apparatus is not a monolithic entity, we here seek to examine the influence of inter-institutional or inter-service relations on the formulation of the EU's disinformation policy.

[31] Paul Pierson,1993, cited in Dupuy and Van Ingelgom, *op. cit*., p. 158.
[32] *Ibid*., p. 16.
[33] Palier and Surel, *op. cit*., p. 11.
[34] Hooghe and Marks, *op. cit.*
[35] *Ibid*., p. 13.

3.2 Research question

Building on the '3I' model as well as the theoretical mechanisms exposed by the study of the EU's legitimacy and public policy analysis, we aim to identify the main drivers of the EU's response to disinformation in the run-up to the 2019 elections. More specifically, this study seeks, from the construction of a disinformation public problem in 2015 to the implementation of a European disinformation policy in 2019, to **explain why the EU's response to disinformation has been mostly formulated in security-centred terms.** This approach envisages disinformation as an *ad hoc*, external and exogenous threat arising from malicious foreign actors, which social media endow with high capabilities for disseminating political confusion. Effective responses to disinformation should consist of reactive measures, implying enhanced strategic and cyber response capabilities allowing to counter disinformation in a swift and frontal manner.[36]

By contrast, what we term a 'society-centred' approach would regard disinformation as an internal, endogenous, and multi-faceted problem whose primary source is citizens' distrust in public institutions and mainstream media, and their consequent demand for alternative narratives. As such, disinformation can possibly be conveyed by domestic actors, including public authorities, media outlets, or civil society actors. This view hence considers disinformation as being best addressed through a preventive empowerment of citizens' media and information literacy, as well as the promotion of a sane (plural, sustainable) media environment rendering disinformation attempts harmless and non-profitable.[37] These two approaches are summarized in Table 1.

[36] See: Butcher, *op. cit.*, pp. 14-16.
[37] See: Butcher, *op. cit.*, pp. 17-20.

Table 1: Security-centred and society-centred approaches to disinformation

	Security-centred approach	Society-centred approach
Main root cause	Malicious political intentions	Citizens' distrust in public institutions and mainstream media
Nature of the phenomenon	Ad hoc, exogenous threat	Endogenous problem
Main conveyers	External actors, especially foreign governments	External and possibly internal actors, including public authorities and media outlets
Main vector	Social media	Citizens' demand for alternative discourses
Nature of the perceived most efficient response	Reactive	Preventive
Aim of the perceived most efficient response	Counter disinformation in a swift and frontal manner	Rendering disinformation attempts harmless and non-profitable
Content of the perceived most efficient response	Enhanced capabilities for strategic communication and cyber defence	Empowerment of citizens' media literacy, promotion of a sane media environment

We hence look at the extent to which 'ideas', 'interests' and 'institutions' have respectively shaped, from its appearance on the European agenda in 2015 up to the climax of its implementation in early 2019, the EU's disinformation policy and contributed to make it a security-centred one.

4. Methodology and data

4.1 Process tracing: exposing the causes of the EU's security-centred disinformation policy

We use the method "explaining-outcome process tracing", which consists in identifying the main drivers of a particular policy outcome.[38] Explaining-outcome process tracing is most helpful for pioneering case-centric studies and allows for an inductive approach.[39] We hence start our analysis from the outcome that we seek to explain, that is, the

[38] Beach and Pedersen, *op. cit*.
[39] *Ibid*., pp. 11-21.

EU's security-centred response to disinformation, and then trace back the process that has led to it.

Explaining-outcome process tracing enables the use of two types of causal mechanisms. It brings into play not only pre-defined causal mechanisms – such as identified by the sociology of public action and policy analysis, organized through the '3I' model – , but also "non-systematic" or "case-specific" mechanisms.[40] This is the case precisely because explaining-outcome process tracing is best fit for case-centric studies and aims to take fully into account particular contextual elements. We therefore start by using pre-existing theoretical mechanisms and, if insufficient, complement them with case-specific mechanisms. This is summarized in Table 2, through the example of our first hypothesis.

Table 2 : Explaining-outcome process tracing

Example based on H1

Variable	**Causal Variable** →	**Causal Mechanism** →	**Outcome Variable**
Synonym	Independent Variable	Intervening Variable	Dependent Variable
Description	Initial framing of the problem, namely, as a foreign threat from Russia	*Path dependency* ? *Case-specific mechanism* ?	Security-centred EU response to disinformation

Structure derived from Kay and Baker, 2015.[41]

In order to define the outcome we seek to account for, that is, the EU's security-centred response to disinformation, we conduct a quali-quantitative textual analysis of the official EU documents that have played a central role the latter's formulation. The most important of these is the Commission-EEAS Action Plan against Disinformation, which synthesized all EU initiatives against disinformation with a view to the 2019 European elections. This analysis

[40] Beach and Pedersen, *op. cit.*, p. 19.
[41] Kay and Baker, *op. cit.*, p. 8.

allows us to 'paint the picture' and account for the security-centred nature of the EU's response. The ten documents we analyse are listed in Table 3.

Table 3: Key documents in the formulation of the EU's response to disinformation

Date	Document	Institution	Service responsible
June 2015	Action Plan on Strategic Communication	EEAS	SG AFFGEN
October 2016	Report on EU strategic communication to counteract propaganda against it by third parties	Parliament	AFET Rapporteur: Anna Fotyga (ECR, PL)
March 2018	Report of the High-Level Group on fake news and online disinformation	Commission	DG CNECT
April 2018	Communication "Tackling online disinformation: a European Approach"	Commission	DG CNECT
September 2018	Communication "Securing free and fair elections"	Commission	DG JUST
September 2018	Recommendation on election cooperation networks, online transparency, protection against cyber security incidents and fighting disinformation campaigns	Commission	DG JUST
December 2018	**Action Plan** against Disinformation	Commission and EEAS	SecGen and SG AFFGEN
February 2019	Conclusions on "Securing free and fair elections"	Council	GIP
March 2019	Recommendation taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties	Parliament	AFET Rapporteur: Anna Fotyga (ECR, PL)
June 2019	Report on the implementation of the Action Plan against Disinformation	Commission and EEAS	SecGen

We base our textual analysis on the two previously defined approaches to disinformation.[42] In order to detect these two approaches in the relevant EU documents, we define eight key words for each ideal-type, as in Table 4.

Table 4: Keywords attached to the security- and society-centred approaches to disinformation

	Security-centred approach keywords	**Society-centred approach keywords**
Main root cause	Russia Foreign	Trust Domestic
Nature of the phenomenon	Interference Threat Hybrid	Media pluralism Independent media Quality journalism
Perceived most efficient measures	Counter Cyber security Strategic communication	Prevent Empower citizens Media literacy

Through a quali-quantitative textual analysis consisting in counting the number of occurrences of these keywords, we construct a 0 to 1 "security-centred vs. society-centred" index, where 0 is a totally society-centred approach, and 1 a totally security-centred approach. We do it through a simple proportional method, as in Table 5.

[42] See Table 1.

Table 5: Security vs. society-centred index construction

Example based on the Report of the High-Level Group on fake news and online disinformation (European Commission, DG CNECT, March 2018)

	Security-centred approach keywords	**Society-centred approach keywords**
Main root cause	Russia : 0 Foreign : 4	Trust : 37 Domestic : 4
Nature of the phenomenon	Interference : 1 Threat : 0 Hybrid : 1	Media pluralism : 32 Independent media : 27 Quality journalism : 24
Perceived most efficient measures	Counter : 12 Cyber security : 0 Strategic communication : 0	Prevent : 3 Empower citizens : 18 Media literacy : 70
Total keywords (100%)	233	
Sub Total	18	215
Relative Percentage	8%	92%
Index Security-centred = 1 Society-centred = 0	**0,08**	

This index's role is to allow for eased comparison between the ten documents, which are then gathered into one single graph.[43] The distribution of dots provides us with a clear overview of the EU's security-centred response to disinformation (with most dots, especially the Action Plan against Disinformation, being closer to 1). The core of our analysis then consists in linking these dots, that is, clarifying the 'grey zones' in between the official documents, so as to identify why the EU's response has been mostly formulated in security-centred terms. We do this thanks to semi-directed interviews.

[43] See section 5.1

4.2 Interviews: The internal logic of the formulation of the EU's disinformation policy

In order to grasp the internal logic specific to the formulation of the EU's disinformation policy, we interviewed the EU officials that were in charge of the disinformation 'file' in their respective service or institution. Overall, four main themes were discussed. Each of them aims at testing one or several of our hypotheses:

I. The interviewee's understanding of the concept of disinformation (H1)
II. His/her reflection on the overall EU's response (H1, H2a, H2b)
III. His/her institution's – and, for the Commission, DG's – work (H2a, H2b)
IV. Inter-institutional – and, for the Commission, inter-service – cooperation (H3)

The interviews' outcomes are analysed through a qualitative method of content analysis. Based on the themes of the interview guide, we undertook a transcription and open coding of the most indicative extracts of the interviews.

In total, we interview seven EU officials who held a key role in the formulation of the EU's response to disinformation. Their institutional affiliations in the run-up to the 2019 European elections are provided in Table 6. We assign each interview a footnote code. Also, for the sake of simplicity and anonymity, when referring to our interviewees we indifferently use 'he', 'him' and 'his' as gender-neutral pronouns for 'interlocutor'.[44] Unfortunately, due to the exceptional sanitary circumstances in which this analysis was conducted, no official from the European Commission's DG CNECT could be interviewed, despite the DG's significant role in the initial formulation of the EU's response.

[44] Amongst our interviewees were four women and three men.

Table 6: Institutional position of interviewees

Institution	Body or Directorate General	Function	Interview footnote code
European Commission	Secretariat General	Administrator	'ComSG'
European Commission	DG HOME	Administrator	'ComHO'
European Commission	DG JUST	Administrator	'ComJU'
European External Action Service	SG AFFGEN	Senior Administrator	'EeasAD'
Council of the EU / European Council	General Secretariat	Senior Administrator	'EucoAD'
Council of the EU	General Secretariat	Administrator	'CounAD'
European Parliament	Secretariat	Administrator	'ParlAD'

5. Analysis

We start by 'painting the picture' of the security-centred nature of the EU's response, through a textual analysis of ten major official documents issued from 2015 to 2019 by the European Commission, EEAS, Council and Parliament.[45] We test each of our four hypotheses – each relating to 'ideas, 'interests', or 'institutions'[46] – through the method of explaining-outcome process tracing, by using original qualitative data obtained from semi-directive interviews with seven EU officials that were in charge of the disinformation 'file' in their respective service or institution.

[45] European Council conclusions are also taken into account, but not subject to the keyword analysis because too short.
[46] See section 3.

5.1 'Painting the picture': the chronological narrative of the EU's security-centred response to disinformation

The embryo of the EU's disinformation policy can traced back to June 2015 and the publication by the EEAS of an Action Plan on Strategic Communication.[47] This document was issued in the context of the Russia/Ukraine dispute in March 2015, after the European Council highlighted the "need to challenge Russia's ongoing disinformation campaigns".[48] As a follow-up, in June 2015, the Action Plan on Strategic Communication announced the creation, within the EEAS, of the East Strategic Communication Task Force. This 'East StratCom Task Force' was the very first EU structure to be expressly and specifically dedicated to addressing disinformation. This sequence shows that the disinformation problem initially appeared on the EU's agenda as the component of an external conflict. It was thus addressed as such, in a perspective which largely corresponds to the security-centred approach we previously defined.

The second main document produced by EU institutions with respect to disinformation was the European Parliament's Report on EU strategic communication to counteract propaganda against it by third parties, adopted in October 2016.[49] This report was developed by the Parliament's committee on Foreign Affairs (AFET), under the leadership of Anna Fotyga, a Polish MEP from the European Conservatives and Reformists (ECR) group. As suggested by the committee and rapporteur responsible, this report is in line with the 2015 sequence and largely frames disinformation as a war-like external threat, with a very strong emphasis on Russia.[50]

[47] European External Action Service, Action Plan on Strategic Communication (Ares(2015)2608242).
[48] European Council, Conclusions (EUCO 11/15), 20 March 2015, p. 5.
[49] European Parliament, Report on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)), Committee on Foreign Affairs, 14 October 2016.
[50] The Polish PiS party, which Ms Fotyga belongs to, has strongly opposed Russian influence in Poland and Europe.

Following the 2015-2016 agenda-setting of disinformation as a foreign affairs issue, no official EU stance on disinformation was taken for some time. The topic only arose again in late 2017 – early 2018, as the European Commission's DG CNECT convened the High Level Group on fake news and online disinformation (HLEG), composed of thirty-nine researchers, journalists, media professionals and stakeholders. This DG CNECT-led initiative contributed to the definition/delineation of the field of disinformation. It was therefore critical in the (re)construction of a disinformation "public problem" and in making disinformation a fully-fledged "*catégorie d'action publique*".[51] The HLEG report was issued in March 2018, [52] marking the creation of a completely different – even, opposed – approach and work stream to the initial one. The HLEG has indeed provided DG CNECT with a very different approach to disinformation than that of the EEAS, much closer from the society-centred ideal type we previously outlined. The HLEG report notably recommended the EU to base its response to disinformation on enhancing the "transparency of online news", promoting "media and information literacy", "empowering users and journalists", or safeguarding the "diversity and sustainability of the European news media ecosystem".[53] This vision is reflected in our fourth document, which is the subsequent DG CNECT-led Commission Communication on "Tackling online disinformation", issued April 2018.[54] This Communication extensively builds on the HLEG's perspective and proposals and also follows a society-centred approach.

As the May 2019 European elections were approaching, the Commission then put forward a set of measures entirely and expressly aimed at them. Designed and implemented primarily by DG JUST,[55] the September 2018 'Elections Package' constitutes a third EU work stream, in addition to the EEAS' and DG CNECT's. The two documents we analyse here are

[51] Dubois, *op. cit*., p. 17.
[52] High level Group, *op. cit.*
[53] *Ibid*., pp. 5-6.
[54] European Commission, Communication "Tackling online disinformation: a European Approach" (COM/2018/236), 26 April 2018.
[55] Interview with a European Commission administrator from the Secretariat General, Brussels, 10 March 2020. (Hereinafter: ComSG)

the most representative of this 'Elections Package': namely, a Communication on securing free and fair elections[56] and a recommendation on election cooperation networks.[57] They can be considered as twin documents, both emphasising the importance of protecting the integrity of the then approaching European elections. They most clearly adopt a security-centred approach.

The EU's 'master' document was issued in December 2018: the joint Commission-EEAS Action Plan against Disinformation (hereinafter, 'Action Plan').[58] It is considered as such for the reason that it centralised and synthesised all past and upcoming EU initiatives against disinformation with a view to the May 2019 European elections.[59] Still, it rather fits into the security-centred approach. Just like the 2015 Action Plan on Strategic Communication, the Action Plan against Disinformation originates from a European Council request from June 2018.[60] This was interestingly done under the conclusions' "Security and Defence" chapter and "in line with the March 2015 European Council conclusions" (the ones requesting the Action Plan on Strategic Communication during the Russia/Ukraine conflict).[61] Overall, although aiming to combine the EEAS', DG CNECT's and DG JUST's previously established work streams, the Action Plan against Disinformation rather fits into the security-centred approach, as evidence by our keyword analysis below.

A somehow parallel initiative to these EEAS- and Commission-driven processes are the February 2019 Council conclusions on securing free and fair elections, describing the Council's position on the matter.[62] As for the European Parliament, it should be noted that, from 2015 to Spring 2019, only two texts directly dealing with disinformation were voted. The

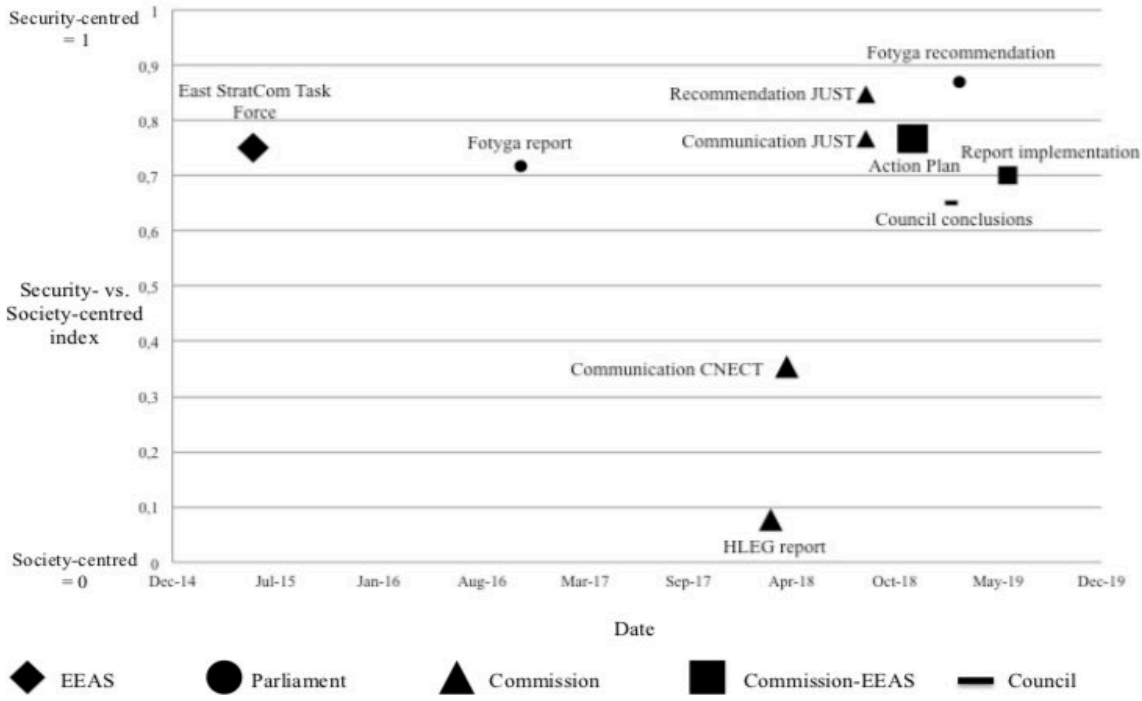
---

[56] European Commission, Communication "Securing free and fair elections" (COM/2018/637), 12 September 2018.
[57] European Commission, Recommendation on election cooperation networks (C/2018/5949), 12 September 2018.
[58] Action Plan against Disinformation, *op. cit.*
[59] Interview ComSG.
[60] European Council, Conclusions (EUCO 9/18), 28 June 2018, p. 6.
[61] *Ibid*.
[62] Council of the European Union, Conclusions on securing free and fair European elections (6573/1/19), 19 February 2019.

first is the abovementioned October 2016 Fotyga report; the second directly derives from it and concerns "follow-up taken by the EEAS two years after the EP report on EU strategic communication".[63] The AFET committee and Ms Fotyga were still in charge, and the Parliament's security-centred perspective remained substantially unchanged. Finally, a report on the implementation report of the Action Plan against Disinformation was issued in June 2019.[64] Like the original Action Plan, it is closer from the security-centred ideal type.

Overall, **the results of our quali-quantitative textual analysis of these ten official documents[65] translate into Graph 1, which evidences the security-centred nature of the EU's response to disinformation.**

Graph 1 : The security-centred nature of the EU's response to disinformation (2015 - Spring 2019)



[63] European Parliament, Recommendation on the Follow up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties ((2018/2115(INI)), Committee on Foreign Affairs, 13 March 2019.
[64] European Commission and High Representative, Report on the implementation of the Action Plan against Disinformation (JOIN/2019/12), 14 June 2018.
[65] As per the method exposed in section 4.

5.2 Analysis H1

Our first hypothesis relates to the concept of 'ideas'. It seeks to examine the extent to which, in the long-term, the cognitive frames attached to disinformation through the process of its construction as a "public problem"[66] have generated a security-centred EU response to disinformation. The phenomenon of disinformation has become a "public problem" by being framed as a war-like external threat arising mostly from Russia. It has indeed arrived on the EU's agenda through the European Council's denunciation of "Russia's ongoing disinformation campaigns" in the context of the 2015 Russia/Ukraine conflict.[67] Here, the concept of construction of public problems is particularly useful in that it allows to think that the 'solutions' that have been preferred by decision-makers are closely related to the way in which the 'problem' was framed.[68] Hence, in order to explore the long-term influence of these ideational dynamics over the formulation of the EU's disinformation policy, we put forward the following hypothesis :

H1: The EU has formulated a security-centred response to disinformation as a result of the initial framing of the problem, namely, as a foreign threat from Russia.

The conscious and unconscious representations bared by the EU policy-makers we interview are of particular interest. We indeed observe a great persistence of this initial framing, despite radical changes of context between 2015 and 2019.

5.2.1 Permeation of the security-centred frame in all EU institutions

The EU's action was preceded by the construction of disinformation as a 'problem' calling for public action. The European Council, in its March 2015 conclusions, imposed the initial security-centred frame in which the phenomenon of disinformation would be perceived by EU policy-makers. According to a participant in the preparation of these conclusions, the

[66] Lascoumes and Le Galès, *op. cit.*, pp. 63-65.
[67] European Council, Conclusions (EUCO 11/15), 20 March 2015, p. 5.
[68] Dubois, *op. cit.*, p. 15.

initial focus on external aspects was "absolutely logic and normal" given the international context; "it was natural".[69] We may come back to this last term.

Our interlocutor in the EEAS points out to the existence of "different perspectives" between the EEAS and the Commission on the definition of disinformation.:

> Sometimes we don't even agree with our own colleagues in the Commission, and the open question is of course between the external and internal kind of issues. (…) How do you define the problem ? (…) We [the EEAS] are looking specifically at coordinated disinformation activities, and they come to a large degree from external actors.[70]

Answering to our '*relance'*, he acknowledges that the Commission service in question is DG CNECT. The security-centred and external framing of disinformation hence does not actually appear as a "natural" one – contrary to what our European Council interlocutor asserts –, given the frictions it has generated. It has nonetheless persisted from 2015 to 2019 and permeated all EU institutions.

Our interviews reveal a **formidable persistence of this frame in the arguably very different context of the run-up to the 2019 European elections**. Even when addressing disinformation as part the 2019 European elections, EU policy-makers seem to have kept considering disinformation as a foreign security issue. The senior Council General Secretariat official we interviewed says disinformation is "mostly dangerous when used by countries: Russia first, but also the United States and China".[71] Our interlocutor in DG JUST describes disinformation as intrinsically external: "If internal, it is not really disinformation. Internal actors use the same techniques, such as divisive narratives, but it can be part of the legitimate democratic process".[72] Unconsciously, most of the EU officials we interviewed associate disinformation with external actors and identify them as the main root cause of disinformation.

---

[69] Interview with a Council of the EU director general from the General Secretariat (General and Institutional policy), Brussels, 12 March 2020. (Hereinafter: EucoAD)
[70] *Ibid*.
[71] Interview EucoAD.
[72] Interview with a European Commission administrator from DG JUST (Equality and Union Citizenship), Brussels, 12 March 2020. (Hereinafter: ComJU).

We observed few mentions of the internal or society-centred aspects of disinformation, and always in relation to the external ones. For example, our interlocutor in the Commission SecGen was the only to mention "trust in the institutions", which he described as "another root cause".[73]

5.2.2. Explaining this persistence despite a change of context: 'cognitive transfer'

How to explain the permeation of the initial framing of disinformation despite the significant change of context in which disinformation has been addressed from 2015 to May 2019?

We acknowledge that an analysis in mere terms of frame might be limited, since it does not allow to **account for the *persistence* of the frame**. As recommended by explaining-outcome process tracing, we introduce a case-specific causal mechanism, which we term as **'cognitive transfer'**. Here, the notion of 'cognitive transfer' serves to explain the implementation, across time and distinct contexts, of a set of knowledge to which are attached certain sets of practices. We derive this causal mechanism from the words of our interlocutor in the Commission's SecGen, who has been a central player in the drafting process of the Action Plan against Disinformation:

> We started from the request of the European Council, which wanted to reinforce this [the EU's response to disinformation] at the periphery [of the EU], but then also wanted to see how this kind of threat could turn into threats inside the EU. There has been a kind of *transfer*. The idea was that if there are common points, then we use the best practices.[74]

[73] Interview ComSG.
[74] *Ibid*.

Our assumption thus goes as in Table 7:

Table 7 : Explanation for H1

Variable	**Causal Variable** →	**Causal Mechanism** →	**Outcome Variable**
Synonym	Independent Variable	Intervening Variable	Dependent Variable
Description	Initial framing of the problem, namely, as a foreign threat from Russia	***Cognitive transfer***	Security-centred EU response to disinformation in the run-up to the 2019 European elections

Structure derived from Kay and Baker, 2015.[75]

When applied to the content of our interviews, this causal mechanism has a strong explanatory capacity. We observe very frequent use of terms belonging to the semantic field of war, in line with the idea of a 'cognitive transfer' of the initial framing of disinformation. For instance, our European Parliament interlocutor highlights that "the idea is to counter" and "ensure preparedness in case of attack".[76] While our Commission SecGen interviewee talks about "handling the threat",[77] our Council senior interlocutor describes disinformation as a "danger for EU institutions".[78]

We moreover notice an enduring emphasis on Russia; despite the fact that the EEAS has developed "a much bigger perspective" of disinformation compared to 2015[79]. This strong focus on Russia and unconscious use of war-related terminology across EU institutions clearly shows a form of cognitive persistence and permeation of the security-centred frame.

One of the most striking illustrations of this mechanism is the designation of the Secretariat of the Task Force on Security Union, pertaining to DG HOME, as the lead coordinator for the implementation of the Action Plan against Disinformation.[80] This structure,

[75] Kay and Baker, *op. cit*., p. 8.
[76] Interview ParlAD.
[77] Interview ComSG.
[78] Interview EucoAD.
[79] Interview EeasAD.
[80] Interview ComHO.

created in 2016, had been leading the Commission's action on topics like counter-terrorism, organised crime or cybersecurity. However, when the Action Plan was adopted in December 2018, the Task Force on Security Union became involved in "disinformation pure" [81] – a major drift. The cabinets of the Commissioners dealing with the Action Plan – President Juncker, High Representative Mogherini, Gabriel for DG CNECT, Jourová for DG JUST – decided to entrust the Task Force on Security Union Secretariat with the coordination of its implementation.[82] Hence, from December 2018 up to May 2019, this structure chaired and set the agenda of the coordination meetings between the relevant services of the Commission. Unsurprisingly, our interlocutor described a "very active" cooperation with the EEAS. Conversely, when asked about the 'awareness raising' and 'media literacy' work stream, he confessed: "it was always on the agenda, but it was more about making sure that it is not forgotten".[83]

A key explanation for this decision, taken at the highest hierarchical level of the Commission, appears to be this cognitive transfer dynamic. Because disinformation had almost always been perceived through the prism of Russia's external threat, the Secretariat of the Task Force on Security Union appeared to decision-makers as the most relevant structure within the Commission to coordinate the implementation of the Action Plan against Disinformation.

Overall, the hypothesis that the EU has formulated a security-centred response to disinformation because of the initial framing of the problem, namely, as a foreign threat from Russia, seems largely confirmed. **The security-centred framing of disinformation, initially constructed by the European Council and the EEAS in the context of the Russia/Ukraine conflict in 2015, subsequently spread to all EU institutions, with a systematic association of the concept of disinformation with external actors**. Due a 'cognitive transfer', this frame

[81] *Ibid.*
[82] *Ibid.*
[83] *Ibid.*

permeated EU institutions including in the very distinct context of the 2019 European elections.

5.3 Analysis H2

The two next hypotheses we formulate are linked to the concept of 'interests'. They aim to explore how, in the short-term horizon of the May 2019 European elections, the EU's perceived need of input and output legitimacy may have pushed it to formulate a security-centred response to disinformation.

The EU's disinformation policy indeed implies significant legitimation stakes. It officially aims at ensuring the integrity of European elections, which constitute the EU's main source of input legitimacy. Also, dealing with the quality of journalistic work, public debate or elections, it entails considerable impact in terms of output legitimacy and policy feedbacks. Hence, to examine the influence of the EU's search for legitimacy over the formulation of the EU's disinformation policy, we put forward the two following hypotheses:

H2a: The EU has formulated a security-centred response to disinformation because it would be the most protective of the European elections integrity in the short-term, and therefore preserve its immediate input legitimacy.

H2b The EU has formulated a security-centred response to disinformation because it would be the most visible in the short-term, and therefore maximize its immediate output legitimacy gains.

Our analysis is mostly interested in exposing the explicit but also implicit intentions of EU policy-makers in designing and implementing the EU's response to disinformation. Interests for enhancing the EU's legitimacy, both input and output, indeed seems to have fostered a security-centred response; still, other political mechanisms need to be taken into account.

5.3.1. H2a: a security-centred response to preserve the EU's input legitimacy ?

The EU's response to disinformation reached its climax as of Autumn 2018. In this perspective, and consistent with the observation that public action is always attached to an interest,[84] **the EU's security-centred response to disinformation can rightly be considered as an attempt to protect the integrity of the only direct electoral process in the EU, hence the primary source of its input legitimacy.**

This assumption is confirmed in our interviews.[85] All our interlocutors highlight that the EU has primarily directed its action at the integrity of the May 2019 European elections. The disinformation 'file' is described as a special one, treated with "a sense of urgency"[86] that seems clearly linked to what they perceived as an unprecedented threat to the European electoral system's integrity: "For the first time, we had the impression that there was a proper targeting of elections".[87] This vision also appears in the Commission, according to our interlocutors in DG JUST and SecGen.[88]

It is confirmed that the EU's response to disinformation has been particularly aimed at securing the May 2019 electoral process: "The main goal was to protect the elections, the defence of national and European elections. There was the need to secure each and every country because if only one has problems, all EU elections fall".[89] Across all EU institutions, the EU's main goal seems to have been the top-down securitisation of the electoral system, so as to ensure a new five-year 'injection' of input legitimacy. By contrast, only our SecGen and DG JUST interlocutors mentioned, in a more bottom-up perspective, the preservation of citizens' trust in the electoral process as a complementary objective.

[84] Lascoumes and Le Galès, *op. cit*., p. 64.
[85] Questionnaire Part II.
[86] Interview CounAD.and EucoAD
[87] *Ibid*.
[88] Interview ComSG.
[89] Interview CounAD.

However, an explanation only in terms of securitization of the 2019 electoral system appears insufficient in the light of our interviews. Three of our interlocutors indeed implicitly point out to another EU intention, somehow linked to the first one but less technical and much more political:

> The main goal was to protect the integrity of the system and citizens' faith in it. But there is a difference between disaffected citizens not willing to vote, and disaffected citizens being manipulated into voting for things seemingly in the interest of someone outside the EU.[90]

It therefore seems that not only the integrity of the electoral process was perceived as facing an unprecedented threat, but also the actual voting results. In even more explicit terms, the EU's goal was to address "also the rise of populist parties", for the reason that "everything anti-European is a danger in itself for the EU institutions".[91] We can draw from these declarations that some EU policy-makers saw the EU as having an interest in halting so-called "populist" votes, which were perceived as directly linked with the interests of external actors, and as actually undermining the EU's input legitimacy. In this perspective, because a security-centred response to disinformation would put a strong emphasis on countering external actors' interferences, it was seen as an opportunity to stem what was perceived as 'anti-European' votes. Our final explanation goes as in Table 8. In other words, **the security-centred approach to disinformation was perceived as the most protective of the EU's input legitimacy not only in terms of electoral system, but also in terms of voting results.**

[90] Interview ComJU.
[91] Interview CounAD.

Table 8 : Explanation for H2a

Variable	Causal Variable →	Causal Mechanism →	Outcome Variable
Synonym	Independent Variable	Intervening Variable	Dependent Variable
Description	Interest to preserve the EU's input legitimacy	***Need to securitize the integrity of the electoral process*** + ***Perceived opportunity to contain 'populist' votes***	Security-centred EU response to disinformation in the run-up to the 2019 European elections

Structure derived from Kay and Baker, 2015.[92]

5.3.2 H2b: a security-centred response to maximize the EU's output legitimacy?

Public policy contributes to determine citizens' attitudes vis-à-vis public institutions, as part of a "policy feedback" process.[93] Its visibility is critical for citizens to link policy outcomes with the action of public authorities and hence grant the latter legitimacy.[94]

Our interviews show that EU institutions have really strived for the visibility of their disinformation policy.[95] An important component of this exceptional communication effort was the setup of a "tripartite forum"[96] between the Commission's DG COMM, DG CNECT and DG JUST, the Parliament's DG COMM, and the EEAS' Strategic Communications division.[97] The more security-centred EU actions were strongly emphasized, as were communications:

> You want people to know that you're doing things. It was very clear that EU institutions are really caring about the forthcoming elections. That was really the driving force at the time, and that's also what gave us the *visibility*, support and interest in this issue. People should know what's going on. The intention was clearly that.[98]

[92] Kay and Baker, *op. cit*., p. 8.
[93] Dupuy and Van Ingelgom, *op. cit.*
[94] *Ibid.*
[95] Interview CounAD.
[96] Report on the implementation of the Communication "Tackling online disinformation: a European Approach", *op. cit*., p. 12.
[97] Interview ParlAD.
[98] Interview EeasAD.

As anticipated in our hypothesis, **focusing on the external aspects of disinformation seems to have constituted a strong element in making the EU's disinformation policy visible to EU citizens and maximizing output legitimacy gains.**

However, this explanation appears insufficient. EU institutions seem to have **anticipated potentially very negative policy feedbacks from a more internal, society-oriented response to disinformation**: "the EU's action has been focused on this external side, because it is much easier. The internal aspect is a minefield".[99] These considerations have obviously, in turn, favoured the choice of the EEAS for addressing disinformation – be it after the March 2015 or June 2018 European Council conclusions – but have also affected the EEAS' scope: "we [the EEAS] have a clear political mandate for working on external aspects; internal is already much more shaky".[100]

Dealing with issues such as journalistic work or public debate therefore seems to have been perceived as far too politically sensitive by EU decision-makers: "We wanted to show that we were not creating a 'Ministry of Truth'".[101] This implicitly shows a real caution from EU institutions from raising allegations of censorship, as well as a clear anticipation of the potential feedbacks that could generate the EU's disinformation policy. A security-centred response, focusing on external aspects and pointing at external actors, appeared as much less 'risky' with a view to enhance the EU's output legitimacy. We identify the two causal mechanisms in Table 9.

[99] *Ibid*.
[100] Interview EeasAD.
[101] Interview ComSG.

Table 9 : Explanation for H2b

Variable	Causal Variable →	Causal Mechanism →	Outcome Variable
Synonym	Independent Variable	Intervening Variable	Dependent Variable
Description	Interest to maximize the EU's output legitimacy	***High visibility of a security-centred response*** + ***Anticipation of potential negative policy feedbacks of a society-centred approach***	Security-centred EU response to disinformation in the run-up to the 2019 European elections

Structure derived from Kay and Baker, 2015.[102]

Overall, the two interests-related hypotheses seem largely confirmed and are also complemented by unforeseen mechanisms. On the one hand, the EU has formulated a security-centred response to disinformation in the run-up to the 2019 European elections because it seemed most appropriate to secure the EU's input legitimacy, not only by safeguarding the electoral process but also by contributing to contain so-called "populist" votes. Moreover, the EU's security-centred response was also perceived by policy-makers as guaranteeing higher output legitimacy gains. It would be visible, and a 'society-centred' response would have focused on "shaky" internal aspects with negative policy feedbacks.

5.4 Analysis H3

Attached to the concept of 'institutions', our last hypothesis looks at the extent to which the EU's security-centred response to disinformation has been driven by inter-service and inter-institutional relations. The EU is composed of segmented institutions, themselves composed of segmented services, which may engage in competitive relations. Characterized by distinct sets of resources and embedded in distinct courses of action, the numerous institutions and services involved have carried concurrent – or competing – work streams. *A*

[102] Kay and Baker, *op. cit.*, p. 8.

priori, the European Council and the EEAS seem to have most endorsed a security-centred approach to disinformation.[103] We thus put forward the following hypothesis:

H3: The EU has formulated a security-centred response to disinformation as a result of the influence of the European Council and the EEAS in inter-institutional competition.

The respective weight of institutions/services in inter-service and inter-institutional decision-making and coordination are of particular interest here. We observe a key influence of these two institutional players, although of different nature.

5.4.1. The European Council: key triggering role and path dependency

There has been a significant level of segmentation of the EU's response to disinformation. The European Council has provided the first trigger and approach of the EU's response back in its March 2015 conclusions, leading to the creation of the EEAS East StratCom Task Force. Then in 2018, two new initiatives emerged, with DG CNECT's April 2018 Communication – introducing the Code of Practice on Disinformation – and DG JUST's September 2018 'Elections Package' – focusing on the cyber protection of elections. These have been the three main EU work streams on disinformation. Each of them being led by a different service, these work streams also entail different, if not diverging, views of disinformation, as expressed by our EEAS interlocutor who points out disagreements with his DG CNECT colleagues.[104] This is well summarised by our interlocutor in DG JUST:

> Within the Commission, political leadership was channelled: there were different commissioners responsible for the different parts. (…) Everyone set objectives building on the leadership's input. Then, having started their respective product, everyone wanted to demonstrate how useful was the thing that they had. In the end, there was a creative *competition* between the three main DGs involved.[105]

[103] For the reasons outlined in section 5.1.
[104] Interview EeasSAD. See section 5.2.
[105] Interview ComJU.

The December 2018 Action Plan then marks the "convergence" of these different work streams.[106] Here, **the European Council has played what we term a key 'triggering' role, not only in the formation of the EEAS' security-centred work strand in 2015, but also later in the conception and design of the Action Plan.**[107] This is what happened with the March 2015 conclusions, but also with the June 2018 conclusions, which called for the presentation of the Action Plan. In both cases, a security-centred approach to disinformation was adopted.

The June 2018 conclusions were explicitly intended to be "in line with the March 2015 European Council conclusions" – the ones establishing the EEAS East StratCom team in the context of the Russia/Ukraine conflict.[108] The disinformation paragraph of the June 2018 conclusions was moreover contained under a "Security and Defence" chapter.[109] Finally, the only specific measure mentioned in these conclusions is that the Action Plan should include "appropriate mandates and sufficient resources for the relevant EEAS Strategic Communications teams".[110] Hence, more than three years later and in a very different context, the European Council identified exactly the same institutional actors and measures to be most appropriate for tackling disinformation.

This observation invites us to look at this institutional process in terms of path dependency. The "path dependency" mechanism shows that once a public policy is formulated in one particular way, alternative policy options become more difficult to implement, since altering the established institutional setting entails ever-increasing costs.[111] Our interviews indeed show a **strong inertia of the security-centred approach to disinformation within the European Council**. First, the European Council identified the EEAS as the most relevant

[106] Interview ComHO.
[107] Interview EucoAD.
[108] European Council, Conclusions (EUCO 9/18), 28 June 2018, p. 6.
[109] *Ibid*.
[110] *Ibid*.
[111] Pierson, *op. cit*., cited in Lascoumes and Le Galès, *op. cit*., p. 84.

institutional actor to address disinformation both in 2015 and 2018 due to the latter's very peculiar institutional position. Accordingly, because it is not a fully-fledged institution nor a fully-fledged Commission service, it "sits in between the chairs" of the Commission and the Council, which gives it "a direct link" with Members States.[112] Our interlocutor even refers to Member States as having the "ownership" of the EEAS. The phenomenon of path dependency is clearly described by the Council General Secretariat administrator:

> The EEAS StratCom was a mechanism that already existed. (…) It is difficult for the Secretariat to come up with a new idea of its own: the conclusions have to be agreed upon quickly, it has to be something acceptable, so something existing is easier.[113]

Being subject to a significant institutional inertia, the European Council has thus repeatedly identified the EEAS as the most relevant EU institutional player to formulate the EU's response to disinformation, hence partly explaining the latter's security-centred nature. In the light of the European Council's key triggering role, this has had significant repercussions on all EU institutions.

5.4.2 A subsequent reliance of EU institutions on the EEAS

As a result of this European Council-triggered empowerment and in the continuation of a path dependency mechanism, **the EEAS has played an ubiquitous role in the design and implementation of the Action Plan against Disinformation**. While the Action Plan marks the "convergence" of the three previously described work streams, it seems that the EEAS has been its main designer, all along the drafting process. Officially, as per the June 2018 European Council conclusions, the Action Plan is a joint document presented by the EEAS and the Commission. However, the EEAS reportedly has played the 'penholder' role, providing most of the input.[114] Our interlocutor from the Commission SecGen refused to provide more details on the drafting process.

[112] Interview EeasAD.
[113] Interview CounAD.
[114] Interview EeasAD.

The EEAS' central designing role has had repercussions on the implementation of the Action Plan. Our Parliament interlocutor suggests a 'side-lining' of his institution.[115] Most importantly, we observe a reliance, if not dependency of EU institutions, on the EEAS capabilities and expertise in the run-up to the 2019 European elections. Our interlocutor in the EEAS indeed describes a "substantial growth" of the EEAS' strategic communication teams, with the latters' staff doubling from 2015.[116] This phenomenon is clearly described by our Parliament interlocutor: "StratCom are experts who do only disinformation (…), they are bigger and have existed for a longer time, whereas in the Parliament and in the Commission, colleagues were doing other different things".[117] Acute institutional asymmetry thus appears, and is also confirmed in the case of the Commission:

> The EEAS had a key influence, they brought a good deal of expertise. They were the first EU capability to actually understand what was going on. They had much better developed monitoring and analysis of examples of disinformation. It was very useful, we relied on their data.[118]

We hence observe a significant reliance of EU institutions on the EEAS, which given its 'seniority' and enhanced capabilities has de facto constituted a central player in the formulation of the EU's response to disinformation. As suggested by its key role in the drafting of the Action Plan against Disinformation, the EU's response hence bore a security-centred approach to disinformation.

Overall, our hypothesis seems largely confirmed, but also invites us to look at the key institutional influence of the European Council and then of the EEAS on the formulation of the EU's response to disinformation in terms of path dependency. Our explanation for H3 hence goes as in Table 10.

---

[115] Interview ParlAD.
[116] *Ibid*.
[117] Interview ParlAD.
[118] Interview ComJU.

Table 10 : Explanation for H3

Variable	Causal Variable →	Causal Mechanism →	Outcome Variable
Synonym	Independent Variable	Intervening Variable	Dependent Variable
Description	European Council and EEAS influence in inter-institutional competition	***Path dependency : reliance on the EEAS as a result of EUCO's key triggering role***	Security-centred EU response to disinformation in the run-up to the 2019 European elections

Structure derived from Kay and Baker, 2015.[119]

Overall, we can assert that the European Council, while exercising a key 'triggering' role in the formulation of the EU's response, has itself been subject to path dependency in the identification of the most appropriate measures and actors for addressing disinformation in 2018-2019. We can also conclude that, as a consequence of the above, the 'seniority' and enhanced capabilities of the EEAS generated a form of institutional dependence of other EU institutions, positioning the EEAS in a central role in the design and implementation of the Action Plan against Disinformation.

6. Conclusion

The EU's security-centred response to disinformation in the run-up to the 2019 European elections can be explained by a combination of ideational, political, and institutional factors. Building on a textual analysis of ten key official documents as well as original empirical material comprising interviews with seven EU officials from five different EU institutions, our explaining-outcome process tracing analysis[120] gives a comprehensive account of the security-centred nature of the EU's disinformation policy. This investigation has eventually

[119] Kay and Baker, *op. cit.*, p. 8.
[120] Beach and Pedersen, *op. cit.*, pp. 63-67.

led to the large confirmation of all of our four hypotheses, as well as the identification, in each case, of tailored causal mechanisms best accounting for this policy outcome.

'Ideas' have been found to constitute a major driver of the EU's security-centred response to disinformation. The initial framing of the problem[121] (namely, as an external threat from Russia), which has been constructed by the European Council and the EEAS in the context of the Russia/Ukraine conflict back in 2015, has indeed played a key early role in delineating cognitive understandings of the disinformation phenomenon and, later, policy options. This initial frame has not only permeated all EU institutions (sometimes generating ideational tensions), but has also persisted across time and across a very distinct context which is that of the 2019 European elections, notably leading to the designation of the DG HOME's Task Force on Security Union Secretariat as lead coordinator for the implementation of the Action Plan against Disinformation as of December 2018. This mechanism, which we identified as a 'cognitive transfer', shows a persisting influence of the security-centred framing of disinformation up to the first semester of 2019.

Secondly, 'interests' have also played a significant role in the formulation of an EU security-centred response to disinformation. On the one hand, it appears that such a response has been favoured by EU decision-makers as it would be most efficient in securing the EU's input legitimacy, which they have indeed perceived as an issue of critical importance. Our interviews also reveal that EU policy-makers have quite directly associated this issue with the containment of so-called "populist" votes,[122] which they regarded as linked with the interests of external actors and considered as harmful for the EU's input legitimacy. In this perspective, a security-centred response putting strong emphasis on external actors has appeared most appropriate. In parallel, we have shown that the EU has formulated such a response as part of an effort to enhance its output legitimacy and generate positive policy feedbacks.[123] Beyond

[121] Gusfield, *op.cit.*, cited in Dubois, *op. cit.*, p. 14.
[122] Interview CounAD.
[123] Dupuy and Van Ingelgom, *op. cit.*

the high visibility of a security-centred response, EU institutions have anticipated the very negative policy feedbacks that a society-centred response could have implied, as it would have led them to focus on much more "shaky"[124] internal aspects.

Finally, 'institutions' constitute strong explanation of the security-centred nature of the EU's disinformation policy. The European Council and then the EEAS have indeed exerted a key institutional influence over the EU's response to disinformation, which is best explained in terms of path dependency.[125] First, while having played a key 'triggering' role in the formulation of the EU's response, the European Council has itself been subject to path dependency in June 2018 as a series of institutional factors of inertia led it to identify, just like in March 2015, the EEAS and strategic communication as the most relevant institutional actor and measure with a view to tackle disinformation in the context of the 2019 European elections. As a continuation of this path dependency mechanism, EU institutions have then appeared to heavily rely on the EEAS, given its 'seniority' and enhanced capabilities. The European Council / EEAS 'path', positioning the latter institution as a central player in the design and implementation of the Action Plan against Disinformation, has thus largely led the EU to formulate a security-centred response to disinformation in the run-up to the 2019 European elections.

The upcoming developments of this policy will be of great interest and call for further research. One possible avenue could be to explore the extent to which the dynamics we have exposed actually sediment or vanish as the EU's disinformation policy stabilizes, in the light of the European Democracy Action Plan that was released in December 2020. In particular, the disappearance of the pre-electoral sense of urgency, which we identified as a significant driver of the security-centred nature of the EU's response, may lead to policy shifts and more emphasis on society-centred aspects. Conversely, the climax reached in the implementation of

[124] Interview EeasAD.
[125] Pierson, *op. cit.*, cited in Lascoumes and Le Galès, *op. cit.*, p. 84.

the EU's disinformation policy in early 2019 may engender path dependencies, resulting in a further enshrinement of its pre-elections security-centred design. Research could finally be motivated by the issue of Covid-19, which has brought disinformation back to centre stage. Interestingly, the most security-centred aspects of the EU's response have resumed to the forefront in this context, with EU reports mostly pointing to coronavirus-related disinformation campaigns originating from Russia and China.[126]

Disinformation has now become an established central issue, which EU institutions will keep a close and persistent eye on. Nonetheless, should the underlying issue of citizens' considerable distrust in public institutions and mainstream media remain overlooked, the demand for alternative narratives shall prevail, and, with it, the pervasive challenge of disinformation over democratic societies.

[126] EU vs. Disinfo, "EEAS special report update: assessment of narratives and disinformation around the Covid-19 pandemic", 24 April 2020. Retrieved 25 April 2020. URL: https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/

Bibliography

Beach, Derek, and Rasmus Brun Pedersen, *Process-tracing Methods: Foundations and Guidelines*, Ann Arbor, University of Michigan Press, 2013.

Belot, Céline, Laurie Boussaguet, and Charlotte Halpern. "Gouverner (avec) l'opinion au niveau européen", *Politique européenne*, vol. 54, no. 4, 2016, pp. 8-23.

Bennett, Lance and Steven Livingston, "The disinformation order: Disruptive communication and the decline of democratic institutions", *European Journal of Communication*, vol. 33, no. 2, 2018, pp. 122-139.

Butcher, Paul, *Disinformation and democracy: The home front in the information war*, European Policy Centre, European Politics and Institutions Programme, 2019.

Council of the European Union, Conclusions on securing free and fair European elections (6573/1/19), 19 February 2019.

Déloye, Yves, and Olivier Ihl, *L'acte de* vote, Paris, Presses de Sciences Po, 2008.

Dubois, Vincent, "L'action publique", in Antonin Cohen, Bernard Lacroix and Philippe Riutort (eds.), *Nouveau Manuel de Science Politique*, Paris, La Découverte, 2009, pp. 311-325.

Online, pp. 1-25, HAL archives ouvertes. URL: https://halshs.archives-ouvertes.fr/halshs-00498038/document

Dupuy, Claire, and Virginie Van Ingelgom. "Comment l'Union européenne fabrique (ou pas) sa propre légitimité. Les politiques européennes et leurs effets-retours sur les citoyens", *Politique européenne*, vol. 54, no. 4, 2016, pp. 152-187.

European Commission, Communication "Tackling online disinformation: a European Approach" (COM/2018/236), 26 April 2018.

European Commission, Communication "Securing free and fair elections" (COM/2018/637), 12 September 2018.

European Commission, Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament (C/2018/5949), 12 September 2018.

European Commission, EU Code of Practice on Disinformation, 26 September 2018.

URL: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission, Report on the implementation of the Communication "Tackling online disinformation: a European Approach" (COM/2018/794), 5 December 2018.

European Commission and High Representative, Action Plan against Disinformation (JOIN/2018/36), 5 December 2018.

European Commission and High Representative, Report on the implementation of the Action Plan against Disinformation (JOIN/2019/12), 14 June 2018.

European Council, Conclusions (EUCO 11/15), 20 March 2015.

European Council, Conclusions (EUCO 9/18), 28 June 2018.

European External Action Service, Action Plan on Strategic Communication (Ares/2015/2608242), 22 June 2015.

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

European Parliament, Recommendation on the Follow up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties (2018/2115(INI)), Committee on Foreign Affairs, 13 March 2019.

EU vs. Disinfo, "EEAS special report update: short assessment of narratives and disinformation around the Covid-19 pandemic", 24 April 2020. Retrieved 25 April 2020. URL: https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/

Fallis, Don, *A Conceptual Analysis of Disinformation*, iConference Paper, 2009.
Foret, François. *Légitimer l'Europe. Pouvoir et symbolique à l'ère de la gouvernance*, Paris, Presses de Sciences Po, 2008.
High level Group on fake news and online disinformation, *A multi-dimensional approach to disinformation*, Luxemburg, Publications Office of the European Union, March 2018.
Hooghe, Liesbet, and Gary Marks, "A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus", *British Journal of Political Science*, vol. 39, no. 1, 2009, pp. 1-23.
Interview with a European Parliament press officer from the Secretariat (Spokesperson's Service), Brussels, 9 March 2020.
Interview with a Council of the EU administrator from the General Secretariat (General and Institutional policy), Brussels, 10 March 2020.
Interview with a European Commission administrator from the Secretariat General (Policy Coordination), Brussels, 10 March 2020.
Interview with a Council of the EU senior administrator from the General Secretariat (General and Institutional policy), Brussels, 12 March 2020.
Interview with a European Commission administrator from DG JUST (Equality and Union Citizenship), Brussels, 12 March 2020.
Interview with a European Commission administrator from DG HOME (Task Force on Security Union Secretariat), video call, 3 April 2020.
Interview with a European External Action Service senior administrator (Strategic Communications), video call, 20 April 2020.
Ireton, Cherilyn, and Julie Posetti (eds.), *Journalism, Fake News & Disinformation*, UNESCO, Paris, 2018.
Kay, Adrian, and Phillip Baker, "What can causal process tracing offer to policy studies? A review of the literature", *Policy Studies Journa*l, vol. 43, no. 1, 2015, pp. 1-21.
Lascoumes, Pierre, and Patrick Le Galès, *Sociologie de l'action publique*, Paris, Armand Colin, 2nd edn, 2012.
E-book, pp. 1-123. URL: https://www.academia.edu/38065238/Lascoumes_-_La_sociologie_de_l_action_publique_0_Armand_Collin_
Palier, Bruno, and Yves Surel, "Les 'trois I' et l'analyse de l'État en action", *Revue française de science politique*, vol. 55, no. 1, 2005, pp. 7-32.
Scharpf, Fritz, *Governing in Europe: Effective and Democratic?,* Oxford, Oxford UP, 1999.
Schmidt, Vivien, "Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput'", *Political Studies*, vol. 61, no. 1, 2012, pp. 2-22.
Surel, Yves, "La mécanique de l'action publique. Le *process tracing* dans l'analyse des politiques publiques", *Revue française de science politique*, vol. 68, no. 6, 2018, pp. 991-1014.

Bruges Political Research Papers / Cahiers de recherche politique de Bruges

No 84/2021

Loïc Carcy, The new EU screening mechanism for foreign direct investments: When the EU takes back control

No 83/2021

Clarisse Corruble, Overtourism and the policy agenda: Balancing growth and sustainability

No 82/2020

Judith Nayberg, Opening the window for merger policy: What drives a reform?

No 81/2020

Anastasia Mgaloblishvili, The overlooked actors in the EU studies: Examining the strategies and objectives of religious actors in the European Union

No 80/2020

Antonio Missiroli and Luigi Lonardo, The evolution of enhanced cooperation in the EU: from EnCo to PeSCo (2009-2019)

No 79/2020

Eva Ambrus, Pattern Recognition: Industry seeking regulation – the case of crowdfunding

No 78/2019

Laura Pierret, The political use of the term "moral hazard": evidence from policymakers of the Eurozone

No 77/2019

Gauthier Schefer, Post-Cotonou and the EU-African relationship: A green light for a renewed cooperation**?**

No 76/2019

Inga Chelyadina, Harmonization of Corporate Tax Base in the EU: An Idea Whose Time Has Come?

See the complete archive at https://www.coleurope.eu/study/european-political-and-administrative-studies/research-publications/bruges-political-research