CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

JUNE 2020

Future Threats, Future Solutions | #1

The EU's Role in Fighting Disinformation: Taking Back the Initiative

James Pamment

The EU's Role in Fighting Disinformation: Taking Back the Initiative

James Pamment

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

+
CONTENTS

About the Project

This paper is the first of a three-part series called Future Threats, Future Solutions that looks into the future of the European Union's (EU) disinformation policy.

This series was commissioned by the European External Action Service's (EEAS) Strategic Communications Division and prepared independently by James Pamment of the Partnership for Countering Influence Operations (PCIO) at the Carnegie Endowment for International Peace. Over one hundred experts, practitioners, and scholars participated in five days of workshops, made written submissions, and/or completed surveys that fed into these papers. The resulting publications are the sole responsibility of the author and do not reflect the position of the EEAS or any individual workshop participant.

The first paper, "Taking Back the Initiative," focuses on future threats and the extent to which current EU disinformation policy instruments can meet the challenge. With the coronavirus pandemic erupting during the drafting of these papers, the overview of current instruments has been supplemented with discussion of lessons learned from the ongoing experience of this crisis. This first paper also outlines the overall policy recommendations detailed in the three papers.

The second paper, "An EU Disinformation Framework," establishes a terminology and framework around which EU institutions can organize their disinformation policy. The paper begins with a discussion of terminology and then outlines the ABCDE (actors, behavior, content, degree, effect) framework for analyzing influence operations. This supports further analysis of areas of institutional responsibility, including ownership of different aspects of the disinformation policy area.

The third paper, "Policy Interventions for the 2020s," outlines three areas of intervention necessary for developing an EU disinformation policy capable of meeting future threats. The first is work that deters actors from producing and distributing disinformation. The second consists of nonregulatory interventions, which focus primarily on policies that can be enacted informally with stakeholders. The third covers regulatory interventions, including legislative responses based upon an auditing regime.

Foreword

Lutz Güllner

Understanding the challenge that disinformation constitutes for our societies is a prerequisite for the development of proper policies and strategies to effectively address it. This has become particularly clear during the COVID-19 crisis: we have seen that disinformation can do real damage; in some cases, it can even kill. Disinformation knows no digital or physical borders, and this has proven to be true time and again: disinformation poses a global threat to open and democratic societies.
The COVID-19 infodemic has highlighted the complex environment in which false information spreads: one of the lessons learned from this crisis is the need to clearly differentiate between the various forms of false or misleading content and to calibrate appropriate responses. To this end, it is important to distinguish between illegal and legal content, as well as whether there is a clear intention to mislead. Especially the latter is a key element in the distinction between misinformation, that is, the organic and unintentional spread of falsehoods, and disinformation—intentional and coordinated manipulations designed to exploit tensions in our societies, harm us, and interfere in our public debates.

Another category includes influence operations by third countries. Disinformation is often part of such influence operations, in combination with other tactics of manipulative interference. For example, pro-Kremlin disinformation actors have spread conspiracy theories and orchestrated disinformation campaigns, sowing confusion and targeting the EU, its member states, and its neighbours by alleging a lack of solidarity and an internal crisis within the EU. China has used the crisis to promote its image, present its state system as better equipped to tackle the pandemic than democracies, and deflect blame over the handling of the virus.

Everyone has a role to play in tackling disinformation. Governments cannot and should not be the only ones to tackle disinformation and influence operations. Especially researchers, independent journalists, and fact-checkers have been at the forefront of monitoring, analyzing, and reporting about disinformation, and they have provided valuable insights into the spread of disinformation. A calibrated response is needed from all parts of society, depending on the degree of harm, the intent, the form of dissemination, the actors involved, and their origins.

This series of papers addresses these issues. It helps us to better understand the nature of the threat and the scope of the challenge at hand. The insights of these publications will feed into the EU's ongoing work on disinformation.

Lutz Güllner is the head of strategic communications at the European External Action Service.

Introduction

Amid the coronavirus pandemic, Europe and the West are grappling with a host of thorny dilemmas posed by disinformation and foreign influence operations. While these problems predate the viral outbreak, the public health crisis has certainly exacerbated them. Brussels has taken some steps to meet this set of challenges, some of which are already paying dividends.

But there is more that Europe can do to make its response more effective. Specifically, the EU should formulate shared terminology for combating disinformation, assertively deter adversaries who are spreading disinformation and conducting influence operations, craft sensible nonregulatory interventions to protect online users, and establish an independent, transparent auditing regimen for certain online platform functions.

The Future Disinformation Threat Landscape

Europe and the West are targets of disinformation, influence operations, and foreign interference. And the responses of most Western countries have been piecemeal and slow, hampered by legal restraints and bureaucracy and lacking in real political understanding of the problem and evidence of its impact.

Adversaries include states, organizations, and individuals. They have developed well-established techniques and have laid the groundwork in terms of building networks, disseminating narratives, and tapping into local issues to gain unwitting grassroots supporters for current and future campaigns. This puts the EU and its member states at a disadvantage when it comes to countering these malicious activities.

The following factors give adversary actors a significant advantage. Some of them pertain to the nature of the disinformation activities they pursue. These adversary actors often employ low-cost, low-risk, and high-reward tactics. They are first movers and use marginal technological advantages, meaning that their activities can be fully under way before they are noticed. Moreover, they are less restricted by legal, ethical, and bureaucratic constraints, and the broad range of illegitimate influence tools and techniques available to them make it difficult to identify and counteract the full extent of their campaigns.

Adversaries also benefit from the limitations and drawbacks of the EU's approach to date. Targeted countries can often muster only limited political will to acknowledge disinformation and particularly to attribute, punish, and deter adversary actors. In addition, it is easier to craft mitigation plans that focus on a single event, like an election campaign, rather than ones that focus on ongoing public discourse.

Moreover, relevant government actors often have limited technical capabilities to monitor, identify, analyze, attribute, and share information about disinformation. Even digital platforms themselves are limited in their capabilities to identify problematic cross-platform behavior. To make matters worse, traditional media often leverage aspects of these influence campaigns in their coverage, unwittingly amplifying central disinformation narratives. Finally, the evidence of harm caused by disinformation and influence operations is patchy, and sufficient evidence for the effectiveness of countermeasures is lacking.

In Europe, experts view Russia as the dominant hostile actor currently spreading disinformation. However, the political consensus to attribute these activities to Russia, which was strong in the aftermath of the annexation of Crimea and the 2016 U.S. presidential election, has waned.[1] Experts regard Russia as having achieved widespread penetration of its narratives in multiple countries across Europe and elsewhere in the world.

There is a sense that its deployment of a wide range of narratives implies that it is not sure what will or will not work, and the low cost of such operations affords it a strategy of trial and error. Russia's scattershot approach to disinformation entails running multiple campaigns simultaneously, with some achieving notoriety while the vast majority of them fail to attract attention from the target audiences or gain traction. Experts express concerns about the extent to which learning from previous successes and failures can increase the efficacy, and therefore the impact, of future Russian disinformation activities.

Experts also raise concerns about influence operations run by China. Many view China as Russia's superior in terms of its potential capabilities and intent to spread disinformation and develop influence campaigns, as well as to coordinate them with broader forms of soft power. Not all its disinformation activities appear particularly sophisticated at present, but experts express much interest in how it might develop and test techniques at home before expanding their reach abroad. However, Western countries have, to date, attributed few influence operations to China. This is due to political concerns rather than a lack of attributable activities.

Traditionally known for its cyber capabilities, Iran also poses an increasing disinformation challenge. Smaller authoritarian and semi-authoritarian states like it may increasingly see disinformation and interference, in conjunction with other hybrid activities, as low-cost, high-reward opportunities to achieve limited political goals in EU member states.[2] They will likely predominantly aim such activities at their own populations, including through mainstream political parties and their supporters. Disinformation seeded domestically can then be drawn upon as a source for foreign interference. Experts also express increasing concerns that EU member states themselves are becoming a source of misinformation and disinformation.

The three papers in this series establish a five-part framework for analyzing influence operations known as the ABCDE framework (actors, behavior, content, degree, effect):

- **Actors**: Experts are concerned about Russia and China spreading disinformation, as well as emboldened smaller countries with authoritarian or semi-authoritarian governments. In addition, they are concerned about political parties and governments within the EU becoming sources of disinformation.

- **Behavior**: Experts are concerned about increasingly sophisticated efforts to evade automated detection—for example, by mobilizing authentic digital-platform accounts to engage in inauthentic behavior. Adversary actors will likely boost a greater number of accounts with fewer followers to avoid detection, thereby blurring the lines between authentic and inauthentic and between coordinated and uncoordinated behavior. Experts also anticipate a broader integration of hybrid influence techniques and disinformation.

- **Content**: Experts expect grand narratives, conspiracy theories, and rumors (like those currently deployed in disinformation activities) to persist. These will be opportunistic and continue to blur the lines between reasonable expression and harmful content. Use of synthetic content such as deep-text and deepfakes will likely become more common, although technological solutions for identifying synthetic content will likely develop in tandem.

- **Degree**: Adversary actors have an increased tendency to produce content on self-hosted websites (including state media–affiliated web platforms) that are then used to spread disinformation on multiple digital platforms. Removal of this content by individual platforms does not affect the source. Adversary actors may use inorganic and semi-organic networks to flood hashtags and search terms to make it harder to access trustworthy information. Paid services for boosting digital platform profiles, in conjunction with existing tools allowed by the platforms, will continue to enable platform distortion. Experts also expect continued microtargeting of content, in conjunction with wider manipulation of public discourse.

- **Effect**: Adversary actors will likely continue their efforts to polarize and discredit institutions and prominent individuals, including, in particular, efforts to tarnish trust in nonpartisan actors. Existing societal divisions and current affairs provide a sufficient basis for polarization campaigns. By integrating disinformation with broader hybrid influence campaigns, adversary actors will be able to threaten public health or safety with greater frequency.

The second paper in this series discusses the utility and application of the ABCDE framework in greater depth. The framework is useful because it provides a standardized means of collecting, analyzing, and presenting information about disinformation.

Current EU Policy on Disinformation

The EU has taken some actions to counter disinformation and is grappling with how to counter its adversaries in the information space. But its current policy on disinformation is characterized by a lack of terminological clarity, unclear and untested legal foundations, a weak evidence base, an unreliable political mandate, and a variety of instruments that have developed in an organic rather than a systematic manner. The limited successes the EU has achieved so far—in terms of the creation of instruments such as the Code of Practice on Disinformation, the Action Plan Against Disinformation, the East StratCom Task Force, and the Rapid Alert System—have been hard earned.

One should not underestimate the challenges posed by the different approaches of member states and EU institutions to the disinformation problem; for example, many member states do not recognize the problem, do not publicly attribute particular malign activities to the offending adversaries, or are under political pressure to limit support to EU-level activities to counter disinformation. Within EU institutions, significant ownership and coordination challenges abound. In this context, the creation of these instruments should be considered a bureaucratic success. However, adversary states can turn this inconsistent approach to their advantage, potentially weakening the processes that are in place and undermining the EU's countervailing system as a whole.

Fundamental Rights

Disinformation is a term that defines a policy area but lacks a firm legal basis, though some principles enshrined in human rights–related legislation are relevant. The Charter of Fundamental Rights of the European Union (ECHR) and the International Covenant on Civil and Political Rights (ICCPR) enshrine the rights to freedom of expression, to privacy, and to political participation.[3] The

EU and its member states have the positive obligation to enable an environment where freedom of expression can be enjoyed. Many argue that disinformation and public debate driven by artificial intelligence undermine this fundamental right.

Article 10 of the ECHR and Article 19 of the ICCPR make provisions for freedom of expression that protect the right to think and express oneself without interference as well as offer a degree of protection to those who spread disinformation on the same grounds.[4] Article 8 of the ECHR and Article 17 of the ICCPR protect the right to privacy, which may be relevant in areas such as the use of personal data to target groups and individuals with disinformation.[5] Finally, Article 25 of the ICCPR and Article 21 of the Universal Declaration of Human Rights codify the right to participate in public affairs and elections, which aspects of disinformation may diminish.[6] In all these cases, these fundamental rights are relatively unexplored in relation to disinformation.

Some scholarly work has explored whether state-backed information operations may breach international law related to the principle of nonintervention. Others have noted that influence operations that threaten the use of force likely breach Article 2(4) of the United Nations Charter, which explicitly prohibits the threat or use of force.[7] The more general principle of nonintervention, which "provides a state with the right to be sovereign within its own territory, free from external interference," requires that states do not coerce one another in their relations.[8] This principle applies most obviously to political expression, particularly in the context of elections. The targeting of critical infrastructure by influence operations, including election systems if they are protected as such by individual member states, should be considered intervention.[9] However, political campaigns—and public debate—are unlikely to be covered.

Some have argued that the principle of nonintervention also protects the right to self-determination and freedom of thought and, therefore, the right to "the conditions that enable the people to form authority and will and to make free choices."[10] An influence operation can thus be coercive if it "substitutes the authentic process of self-determination with an artificially constructed process in order to generate particular attitudes and results aligned to the intervenor's will."[11] The right to freedom of thought offers a potential human rights focus on influence operations that could be grounded in a better understanding of manipulation techniques rather than content alone.

Additional applications of fundamental freedoms among EU member states specifically include content-related restrictions on expression under private and criminal law, such as defamation, insult, and incitement to hatred or violence. Member states also regulate their respective election frameworks, including rules on political campaigning, campaign finance, political parties, and political advertising. Their relevant bodies of national security legislation are also of relevance in relation to foreign interference.

The EEAS Strategic Communications Division

There are two specific divisions within the European External Action Service (EEAS) tasked with assuming various strategic communications responsibilities relevant to disinformation.[12] The Communications Policy and Public Diplomacy side leads outreach to EU and external audiences on EU foreign affairs, security and defense, and external action, developing political communications on behalf of the high representative for foreign affairs and security policy. It provides guidance, training, and strategic support to EU delegations and missions/operations. The division also manages communications campaigns, internal communication, social media accounts, and digital platforms as well as public and cultural diplomacy. It does not have a formal role related to disinformation but rather fulfills advocacy and engagement functions for political and cultural EU objectives, including support to all digital media campaigns.

The Task Forces and Information Analysis side focuses on the Western Balkans and Europe's eastern and southern neighborhoods. Its main role is to develop and implement proactive communications activities and campaigns, including political advocacy and initiatives in public and cultural diplomacy for these regions. It provides analytical support for evidence-based communications and policies and has a specific mandate to address disinformation and foreign manipulative interference in the information space through the task forces (see below).[13] It is responsible for implementation of the EU's Action Plan Against Disinformation and the Rapid Alert System (see below) and for the development of future policy in this field. It also has the mandate to support independent media and civil society in the two neighborhoods and the Western Balkans.

The East StratCom Task Force

The EU first addressed disinformation as a matter of priority for security reasons. Following its annexation of Crimea in February 2014, Russia demonstrated disinformation to be a key method of hybrid warfare. In response to representations from a small group of concerned member states, the European Council "stressed the need to challenge Russia's ongoing disinformation campaigns" in March 2015.[14]

This push resulted in the creation of the East StratCom Task Force within the EEAS's Strategic Communications Division. The task force was established to effectively communicate and promote EU policies toward the eastern neighborhood; strengthen the overall media environment in the eastern neighborhood and in member states, including by supporting media freedom and strengthening independent media; and improve the EU's capacity to forecast, address, and respond to disinformation activities by Russia.[15]

Many observers hoped that the East StratCom Task Force would find evidence of how Russian state-sponsored disinformation infiltrated Western media debates and support civil society to push back against it.[16] The task force produces a weekly review of pro-Kremlin disinformation targeting the West as a flagship product on the EUvsDisinfo web platform, and its database features over 8,000 examples of disinformation.[17] Its team has now grown to sixteen staff members with extensive (but presently outsourced) capabilities in the areas of media monitoring and strategic communications, following three years of funding from the European Parliament. This funding source expires at the end of 2020 and is not renewable.

The EU Code of Practice on Disinformation

The EU has also sought to collaborate with private companies to help stem the tide of hostile disinformation. In September and October 2018, it launched a Code of Practice on Disinformation together with roadmaps for implementation from partners in the private sector. Running for a twelve-month trial period (which covered the European Parliament elections in May 2019), the code was an experiment in voluntary self-regulation by the tech industry.

Signatories made commitments in five areas: online advertisements, political advertising, integrity of services, transparency for consumers, and transparency for researchers.[18] Private sector partners published reports detailing their actions to mitigate disinformation. However, the signatories self-reported their progress, and the information was not verified by an external body. The lessons from this process will feed into further EU policy developments in this area. A recent Carnegie paper details some of the most important lessons from the code process.[19]

The Action Plan Against Disinformation

In December 2018, the European Commission launched its Action Plan Against Disinformation, which remains a key pillar of EU policy, granting mandates to several operational instruments. This measure placed disinformation within the context of hybrid threats and highlighted the role of strategic communications by the EEAS “as a priority field for further work.”[20] The action plan emphasized four areas of work: improving the capabilities of EU institutions to detect, analyze, and expose disinformation; strengthening coordinated and joint responses to disinformation; mobilizing the private sector to tackle disinformation; and raising awareness and improving societal resilience.[21] It proposed maintaining the mandate of the East StratCom Task Force and reviewing the mandates of the Western Balkans and South Task Forces.[22] The action plan recommended an expansion of their resources and capabilities, as well as the creation of a Rapid Alert System to strengthen coordination among EU institutions, member states, and other relevant international networks. It also proposed initiatives in the areas of strategic communications, media literacy, and high-quality journalism.

The Rapid Alert System

The EEAS launched the Rapid Alert System in March 2019 to enable common situational awareness related to disinformation spread across EU member states, as well as the development of common responses.[23] The system consists of a rudimentary platform for information sharing, as well as a network of points of contact in the various EU member states. The Rapid Alert System is intended to connect to existing real-time monitoring capabilities inside and outside of the EU, such as the Emergency Response Coordination Centre and the EEAS Situation Room, as well as the G7 Rapid Response Mechanism and the North Atlantic Treaty Organization (NATO), though this goal has been only partially realized. The system is therefore, in theory at least, an important platform for information sharing from an international perspective.

So far, relatively few highly engaged EU member states share information through the Rapid Alert System. Major differences in how member states view the threat of disinformation are reflected in the use of the platform. In particular, a lack of trust between member states has led to low levels of information sharing and engagement. A successful aspect appears to be the networks and relationships formed among small coalitions of like-minded actors. Regular meetings have been held since early 2019, but the system's alert function had not yet been triggered as of June 2020.

Election Observation Missions

EU-affiliated election observation missions also have a role to play. In October 2019, the European Council issued a document titled "Council Conclusions on Democracy," which observed new challenges to democracy emerging around the world.[24] These include the undermining of democratic processes and institutions, low levels of trust, shrinking democratic space for civil society, increased violations of human rights and fundamental freedoms, and manipulation using online technologies. This last point includes issues of disinformation, hate speech, privacy, and campaign funding. The European Council made commitments to strengthening the EU's democracy-building capabilities around the world, including promoting instruments created to mitigate the effects of online interference during elections.

As a first step, election observation missions of the EU and its member states have been developing a methodology to monitor online political campaigns. In the case of EU missions, this methodology has been road tested in elections in Peru, Sri Lanka, and Tunisia, and it will become a standard part of all future missions. It will, in addition, create a basis for EU support to strengthen research, monitoring, and oversight capacities in third-country academic circles and civil society.

The European Democracy Action Plan and Digital Services Act

In addition to the aforementioned measures, the European Commission is also developing two major new policies. First, it is preparing the 2020–2024 European Democracy Action Plan,[25] which includes specific commitments to project EU values worldwide.[26] This will likely include significant policy commitments at the intersection of disinformation, electoral protection, digital technologies, and public-private partnerships. In this regard, it will set out next steps for building on the Code of Practice and the Action Plan Against Disinformation. Second, building on existing e-commerce rules, the EU is preparing a Digital Services Act.[27] Among other things, this measure will set out regulatory powers for the EU over digital platforms, which are likely to include powers of regulation and auditing relating to online disinformation.

Lessons From the Coronavirus

Disinformation has been an ongoing threat to the EU during the coronavirus pandemic. The ability of EU institutions to handle this challenge provides a valuable snapshot of the strengths and weaknesses of their current policy instruments. This paper does not analyze the overall EU response to the pandemic but instead concentrates on the lessons relevant to the future of EU disinformation policy. It assumes that the EU continues to grapple with disinformation threats with some distinctive characteristics, as highlighted by multiple sources.[28]

- **Actors:** Russia and China are running public-image campaigns in the West linked to their overall handling of the crisis, campaigns that have disinformation components. There also have been some limited activities attributed to other state actors such as Iran. Meanwhile, many active criminal groups—some of whom may be state-backed—are taking advantage of the coronavirus pandemic to spread clickbait, phishing scams, and blackmail. Amid the confusion, a wide range of politicians, influencers, and individuals are distributing misinformation and/or disinformation.

- **Behavior:** Russia's and China's messaging campaigns seek to improve the reputations of their governments by comparing their handling of the pandemic to how Western governments have been handling it, in some cases by falsely representing the actions of the EU and its member states. These campaigns involve coordinated efforts, parts of which are transparently led by official sources such as state media and parts of which are covert. They target multiple pressure points and use tactics beyond disinformation, such as sowing multiple narratives, making payments to online influencers, trolling dissenters, and making diplomatic representations to EU institutions to repress attribution of malign activities. Legitimate public relations activities related to the provision of aid have been accompanied by disinformation campaigns about the actions of the EU and its member states. Furthermore, state and nonstate actors alike are employing hybrid and cyber techniques, in many cases exploiting the public's coronavirus-related health concerns.

- **Content:** There is a broad range of health-related coronavirus disinformation, some of which can be linked to existing long-term, pro-Kremlin disinformation narratives. A great deal of this content is harmful and involves, for example, spreading false health information, attacking the reputations of critical public health institutions, or serving as a pretext for cyber intrusions designed to compromise computer networks. There also have been many conspiracy theories seemingly created to detract attention from the origins of the pandemic and China's initial handling of it.

- **Degree:** There is insufficient evidence to accurately assess the size and scope of the campaigns, but it is clear that at least two major state-backed campaigns are ongoing. They are conducted across platforms and in multiple languages, aimed at a wide variety of domestic and international audiences. Some content is being seeded on state media and other controlled websites prior to distribution on digital platforms in order to facilitate cross-platform distribution and mitigate the effects of removal from platforms. Aspects of these campaigns could be considered within the remit of traditional public diplomacy and soft power, while at times they draw upon communications techniques associated with influence operations.

- **Effects:** There are profound health and public safety risks associated with the disinformation connected to these campaigns, as well as to the activities of criminal and hacker groups. These campaigns aim to undermine trust in institutions and to poison the climate of debate. Some aspects of these campaigns demonstrate efforts to erode freedom of thought and expression. Some of these activities also pose emerging short-term and long-term risks to personal, organizational, and national security.

The EU institutions were committed to exposing the threat of disinformation during the early phases of the pandemic. However, a lack of coherent policy—for example, in terms of supporting member states such as Italy that were exposed to the virus early on—contributed to an environment in which disinformation could spread more readily. Lacking in clear strategic communications of their own policies at that point, the EU institutions focused on exposing disinformation spread from Russia and misinformation spread by individuals. The focus allowed the disinformation policy area to achieve perhaps its highest-ever profile within the EU institutions, but at the same time this outcome risked politicizing and placing undue pressure on the instruments for countering disinformation.

As of early June 2020, the EUvsDisinfo web platform had identified around 570 cases of coronavirus-related disinformation emanating from pro-Kremlin media.[29] Simultaneously, in light of the increased political and public interest in disinformation, the EEAS Strategic Communications and Information Analysis Division produced special reports on coronavirus disinformation, which were published on the EUvsDisinfo platform as EEAS special reports. These summarize the research available from multiple international sources and serve as snapshots of findings from the expert community rather than independent research conducted by the EEAS.[30]

Subsequent leaks of these reports, and the decision to produce separate public and internal versions, demonstrate the ad hoc nature of the processes by which these documents were created. The details of the most serious leaks, which relate to alleged Chinese pressure on the EU to change the third report, are not discussed here.[31]

Some immediate recommendations tailored to various relevant actors for the future of EU disinformation policy are outlined below.

Recommendations for the European Commission

- **Formulate tailored responses to state-sponsored disinformation**: Disinformation touches on many different policy areas. When dealing with adversarial state actors, disinformation policy responses should be tailored specifically to deter the particular country or actor in question by altering their strategic calculus in a coherent, coordinated fashion. (For more information, see the third paper in the series, "Policy Interventions for the 2020s.")

- **Troubleshoot issues that arose in the recent response to Chinese disinformation**: China is not a new disinformation actor, and the StratCom task forces had already recruited a China specialist prior to the outbreak of the pandemic. Furthermore, use of diplomatic representations to assert pressure is a standard means of pushback used by actors accused of disinformation by the EU and its member states, including Russia, and this tactic is sometimes part of broader hybrid influence campaigns. Commissioners should review the information-sharing structures that exist between them and the EEAS to better understand why their stance toward Chinese disinformation lacked preparedness in this instance. Commissioners should review which other state-based disinformation actors could provoke similar challenges in the future by, for example, including their staffers on joint training, red-team drills, and risk-assessment exercises.

- **Take a long-term view and anticipate the future trajectory of disinformation campaigns**: The coronavirus pandemic is likely to continue in some form or another for several months and possibly years. Risk assessments for the next stages of the crisis should focus on proactive intervention to address the vulnerabilities in current societal debates. For example, the development and global rollout of a vaccine is likely to be exploited by disinformation actors, including state-backed actors.

- **Offer appropriate backing to bodies tasked with responding to disinformation**: Attribution to state actors always requires a clear political mandate—institutions such as the EEAS need political protection if they are to attribute publicly, so as not to be vulnerable to pushback from actors who are publicly shamed. However, research and monitoring teams need to be able to report on what they are seeing, accurately depict the views of the broader scientific and intelligence communities, and speak truth to power. Commissioners and the EEAS should agree on language around attribution in EEAS special reports and on the EUvsDisinfo web platform. (A suggestion on how to do this is outlined in the second paper in this series, "An EU Disinformation Framework.")

- **Develop new, more nuanced terminology for disinformation**: Part of the controversy surrounding attribution is a product of current EU disinformation policy not being fit for purpose, not least because the term "disinformation" is used as a catchall to cover a range of influence activities. New terminology is required to add nuance and precision to EU policy. (A suggestion to that end is outlined in the second paper in this series, "An EU Disinformation Framework.")

- **Be transparent and supportive of actions taken to combat disinformation**: Public statements by the spokesperson for European Commission Vice President for Values and Transparency Věra Jourová, High Representative Josep Borrell, and European Commission President Ursula von der Leyen have not served the staff or journalists working on these reports well.[32] Given the personal risks associated with analyzing the disinformation of hostile foreign actors, commissioners should demonstrate to staff that personal safety is highest on their list of priorities.

Recommendations for the EEAS Strategic Communications Division

- **Clearly demarcate the origins of EEAS-linked analytical reports**: There should be a clear distinction between work produced by the EEAS's task forces according to their monitoring and analysis methodologies and its special reports that summarize and assess the findings of the international research community and governments. Special reports should be framed as all-source research and open-source intelligence analysis. They should follow a common and systematic framework, and each statement should be linked to the source and, where possible, to a degree of confidence in those findings. The overall assessment of the EEAS should be clearly demarcated from the all-source summaries. (A proposal framework is outlined in the second paper in the series, "An EU Disinformation Framework.")

- **Create a secure way for reports to be revised**: The issuance of internal and public reports has created confusion, not least because both are unclassified. The EEAS needs a secure process by which to gain political approval from the European Commission for its assessments in the special reports when such a step is appropriate. This process needs to ensure revisions can be made without the risk of leaks, so that a single report can be amended without the need to create separate versions. However, this political process should only impact the EEAS's overall assessment of all available evidence, not the all-source research and open-source intelligence summaries.

- **Fully utilize the Rapid Alert System**: While the Rapid Alert System was used to share reporting among EU member states, an alert related to the pandemic has not yet been triggered.[33] Given the threat to public health that coronavirus disinformation represents, this seems like a missed opportunity. The system remains an underused resource that solves coordination and information-sharing problems between the EU institutions and member states in theory, but it has not performed a significant role in practice. The EU should further analyze why the Rapid Alert System has not fulfilled its potential during this crisis.

- **Adopt a more strategic role**: The Strategic Communications Division has been proactive in becoming a hub for reporting on coronavirus disinformation among the EU institutions. This role also needs a strategic angle; for example, this could entail conducting risk assessments for short- and medium-term disinformation threats and sharing these with the institutions and member states.

Recommendations for the East StratCom Task Force

- **Insulate EUvsDisinfo analysis from day-to-day politics**: The EUvsDisinfo platform should be kept separate from other forms of EEAS analysis. It currently has a disclaimer stating that it does not represent official EU policy, and it should retain this arm's length distance to protect its work from day-to-day political pressures.

- **Double down on EUvsDisinfo's mission and methods**: The identity of the EUvsDisinfo platform should be strengthened with a clearer statement of its goals, research methodologies, and political mandate. It should be strengthened so it can represent its results as products of rigorous monitoring and analysis methodologies, rather than judgment calls that can be swayed by political considerations. A clear statement of purpose and methodologies should also help the platform avoid accusations of mission creep and bias, and such a statement would allow the wider research community to better engage with its methods and results.

An EU Disinformation Policy for the 2020s

An approach for the next stage of EU policy on disinformation—particularly with respect to the European Democracy Action Plan— is outlined below. It defines a way ahead and lays out the main options that should be considered to meet future threats. It rests on four pillars, which build on the principles described above and create a coherent stance fit for the current and near-future threat landscape.

The four pillars are:

- **A new approach to terminology**: developing EU-specific terminology and a disinformation framework and delegating responsibility for different terms and areas of work to specific EU institutions;
- **A new assertiveness**: formulating proactive methods for deterring adversaries from spreading disinformation and conducting influence operations and manipulative interference;
- **A new consultative process**: crafting nonregulatory interventions that enhance the ability of digital platforms to protect users from disinformation; and
- **A new regulatory regime**: establishing independent auditing of key elements of platform functions with a differentiated approach to data transparency.

The EU should first revise the terminology used to support disinformation policy and analysis to make it easier to distinguish between different aspects of the problem. Disinformation is currently used as a catchall term that does not help the EU institutions define different areas of problematic behavior. It muddles the actions of individuals inadvertently sharing incorrect information with the hybrid influence campaigns of hostile states.

A first step is therefore to create a rigorous framework designed to define the scope of the challenge and assign responsibilities. The second paper in this series proposes terminology and a framework capable of systematizing the EU institutions' disinformation work, which is briefly outlined below.

Terminology and Framework

Four terms should become authoritative definitions preferred by all EU institutions in their engagements with stakeholders: misinformation, disinformation, influence operations, and foreign interference. The benefit of differentiating terms is to align democratic concerns—such as freedom of expression, data transparency, and privacy—with the concerns of national and European security, including around elections. To resolve these tensions, the paper recommends using terminology that reflects institutional ownership of various policy areas.

Misinformation should be defined as the distribution of verifiably false content without an intent to mislead or cause harm. Countermeasures should be developed from the perspective of home affairs and the health of public debate, and they should fall under the responsibility of the European Commission's Directorate-General for Justice and Consumers (DG JUST); the Directorate-General for Communications Networks, Content, and Technology (DG CNECT); the Directorate-General for Education and Culture (DG EAC); the Directorate-General for Communication (DG COMM); and the Joint Research Centre (JRC).

By contrast, disinformation should be defined as the creation, presentation, and dissemination of verifiably false content for economic gain or to intentionally deceive the public, which may cause public harm. Countermeasures should cover security considerations, strategic communications for countering disinformation, oversight of digital platforms, and research collaboration, and they should fall under the responsibility of the above institutions as well as the Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR) and the EEAS.

Meanwhile, influence operations should be defined as coordinated efforts to influence a target audience using a range of illegitimate and deceptive means, in support of the objectives of an adversary. The development of countermeasures should be the responsibility of the EEAS, in conjunction with other institutions listed above, in line with its responsibilities for external relations, foreign interference, threat monitoring and analysis, resilience building in the EU's neighborhoods, and third-country election monitoring.

Finally, foreign interference should be defined as coercive, deceptive, and/or nontransparent efforts by a foreign state actor or its agents to disrupt the free formation and expression of political will, during elections, for example. The development of countermeasures should be the responsibility of the EEAS, in conjunction with the other institutions listed above, and these countermeasures should emphasize the distinct nature of responses targeting foreign state actors. Integrating such responses with intelligence, hybrid, and cyber capabilities would also be required for countering influence operations and foreign interference.

This terminology is escalatory. Foreign interference can involve several influence operations. Influence operations can include many examples of disinformation. Disinformation can cause or be derived from misinformation. Institutional ownership should be developed on this understanding; for example, the EEAS would be responsible for countering disinformation spread by pro-Kremlin sources on the grounds that such disinformation is part of influence operations and a tool of foreign interference.

Actor-Specific Approaches

The benefit of this approach is that misinformation and disinformation are treated primarily as problems of democracy to be dealt with by improving the health of public debate, while influence operations and foreign interference are treated as security concerns in the context of attempting to influence the calculus of adversary actors. This approach also acknowledges that actor-specific knowledge is a necessary foundation of the disinformation debate. The third paper in the series, "Policy Interventions for the 2020s," outlines the main options for action, which are summarized below.

- **Reshape adversaries' strategic calculus**: The EU should consider its interventions from the perspective of denying adversary actors the benefits of their actions in addition to domestic concerns such as data transparency. Interventions should be designed to influence adversaries' calculus so that they no longer perceive disinformation, influence operations, and manipulative interference as beneficial courses of action.

- **Leverage strategic communications and public diplomacy to dissuade adversaries from using disinformation and influence operations**: Some current EU instruments, such as the EEAS's Strategic Communications Division and the East StratCom Task Force, make strong contributions to developing societal and institutional resilience. Modern, data-driven strategic communications and public diplomacy are central to maintaining and projecting these capabilities. To further develop their potential, EU policymakers should reconsider how these elements contribute to a cumulative posture aimed at dissuading adversary actors from spreading disinformation and conducting influence operations and manipulative interference.

- **Situate disinformation responses in broader geopolitical strategies**: EU policy toward Russia, China, and other identified adversary actors should be assertive in integrating disinformation-related concerns into its broader engagement posture. Policymakers should consider regulatory and nonregulatory interventions related to disinformation not merely from a data-transparency perspective but also from a geopolitical perspective. Raising costs, denying benefits, and denying capabilities should be core motivations driving policy interventions. Actor-specific capabilities should be augmented where appropriate by integration with intelligence, hybrid, and cyber resources.

Regulatory and Nonregulatory Interventions

The third paper in the series, "Policy Interventions for the 2020s," outlines a range of regulatory and nonregulatory measures that should be developed into a coherent, comprehensive EU disinformation policy. Nonregulatory measures are particularly important, as digital platforms have multiple tools at their disposal for modifying user behavior. Building on the results of the Code of Practice on Disinformation, the EU should work with and better support platforms in establishing guidelines on best practices that set clear standards of responsible platform behavior aligned with fundamental freedoms.

The paper details several examples where EU guidance on areas such as terms of service, terminology, promoting/demoting content, political parties, and research collaboration could be beneficial to current and emerging digital platforms, member states, and the international community. The paper suggests the following:

- **Design nonregulatory measures through stakeholder dialogue**: A range of nonregulatory interventions should be developed on the basis of a collaborative, iterative, and recurring format for policy and operational dialogue among different parts of the stakeholder community.

- **Craft guidelines relevant to the full range of policy actors**: Guidelines should be developed in multiple areas to provide support and direction to stakeholders seeking to mitigate the impact of disinformation, including digital platforms, member states, civil society, and researchers. These would represent best practices and would set expectations for the broader stakeholder community.

The European Commission will likely favor regulatory interventions, particularly in areas where the voluntary code of practice fell short of delivering the desired results. The paper on policy interventions outlines an overall approach to regulation that places the onus on digital platforms to fulfill a duty of care, while enabling independent verification of their results. It suggests a differentiated approach to data access, on the grounds that data transparency should be viewed as a means of improving policymaking, not as an end in itself.[34]

This approach includes the following tasks.

- **Establish a regulatory environment involving reporting by and auditing of digital platforms**: The EU should establish a regulatory process based around three steps: a statement of expected outcomes, a reporting mechanism for digital platforms, and an auditing mechanism for independent verification of results.

- **Encourage collaborative, cross-sector research**: The EU should support collaborative models of cross-sector research and information sharing to enable analysis of data made available by digital platforms, in support of the public interest and sound policymaking.

- **Consider regulations for addressing social media manipulation**: The EU should explore regulatory interventions into the market for social media manipulation, including demonetization of disinformation.

- **Delineate duties and consequences clearly**: Definitions of digital platform responsibilities and the consequences of breaches should be clearly defined. Such definitions should maintain a focus on improvement, learning, and iterative development of evidence-based policymaking.

The overall package of policy recommendations presented here is designed with a view not just to solving European problems but rather to creating a default global disinformation policy for democracies to adapt to local conditions. The recommendations promote evidence-based policymaking based on a logical alignment between terminology, interventions, and empirical data. They balance concerns about fundamental freedoms with security and distinguish between the types of problems that disinformation entails and the types of actors that it involves. Interventions are designed to reframe the issue in terms of influencing the calculus of adversary actors so that they no longer perceive disinformation and interference as a beneficial course of action.

About the Author

James Pamment is co-director of the Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace. He is also an associate professor in strategic communication at Lund University and a special adviser to the European Centre of Excellence for Countering Hybrid Threats. His academic research is about how states influence one another through strategic communication, diplomacy, intelligence, aid, and propaganda. He holds a PhD from Stockholm University.

Pamment is the lead author of "Counter Influence Strategies for Communicators" (Swedish Civil Contingencies Agency or MSB, 2018), the "RESIST Counter-Disinformation Toolkit" (UK Government Communication Service, 2019), and "The 4S Model" for hybrid deterrence (European Centre of Excellence for Countering Hybrid Threats, 2020), among others. His Lund University team has provided training to thousands of civil servants in dozens of countries on countering disinformation and hybrid threats.

Notes

[1] In a speech in January 2020, Vice President of the European Commission for Values and Transparency Věra Jourová named Russia and China as "specific external actors . . . that are actively using disinformation and related interference tactics to undermine European democracy." See Věra Jourová, "Opening Speech of Vice-President Věra Jourová at the Conference 'Disinfo Horizon: Responding to Future Threats,'" European Commission, January 30, 2020, https://ec.europa.eu/commission/presscorner/detail/en/speech_20_160.

[2] See the annotated list of foreign influence efforts in Diego A. Martin and Jacob N. Shapiro, "Trends in Online Foreign Influence Efforts," Empirical Studies of Conflict Project, July 8, 2019, https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_foreign_influence_efforts_2019jul08_0.pdf.

[3] Judit Bayer, Natalija Bitiukova, Petra Bárd, Judit Szakács, Alberto Alemmano, and Erik Uszkiewicz, *Disinformation and Propaganda: Impact on the Functioning of the Rule of Law in the EU and Its Member States* (Brussels: European Union, 2019), 70, 74, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf; and Michael Meyer Resende, Marek Mracka, and Rafael Goldzweig, "EU EOMS Core Team Guidelines for Observing Online Campaign (2.0)," European Union Election Observation, June 3, 2019, 4–7.

[4] Bayer et al., *Disinformation and Propaganda*, 74; and Resende, Mracka, and Goldzweig, "EU EOMS Core Team Guidelines for Observing Online Campaign (2.0)," 5–6.

[5] Bayer et al., *Disinformation and Propaganda*, 74; and Resende, Mracka, and Goldzweig, "EU EOMS Core Team Guidelines for Observing Online Campaign (2.0)," 7.

[6] Bayer et al., *Disinformation and Propaganda*, 74; and Resende, Mracka, and Goldzweig, "EU EOMS Core Team Guidelines for Observing Online Campaign (2.0)," 6–7.

[7] Duncan Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (Spring 2018): 39.

[8] Duncan Hollis, "Why States Need an International Law for Information Operations," *Lewis and Clark Law Review* 11, no. 4 (2007): 1050; Hollis, "The Influence of War; The War for Influence," 40; and Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," European Journal of International Law *EJIL: Talk!* (blog), August 26, 2019, https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace.

[9] Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace."

[10] Ibid.

[11] Ibid.

[12] "Strategic Communications," European External Action Service, https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en.

[13] The concept of foreign manipulative interference has been used on occasion in official documentation without being defined. The second report in this series offers a detailed terminological discussion.

[14] "European Council Conclusions on External Relations (19 March 2015)," European Council, March 19, 2015, http://www.consilium.europa.eu/en/meetings/european-council/2015/ 03/19-20/.

[15] High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan Against Disinformation," December 5, 2018, 4, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

[16] For a discussion of the East StratCom Task Force's launch period policies, see Corneliu Bjola and James Pamment, "Revisiting Containment Strategy in the Digital Age," *Global Affairs* 2, no. 2 (May 2016): 131–142, https://doi.org/10.1080/23340460.2016.1182244.

[17] "EUvsDisinfo," European Union East StratCom Task Force, https://euvsdisinfo.eu.

[18] "EU Code of Practice on Disinformation," European Commission, September 26, 2018, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454.

[19] James Pamment, "EU Code of Practice on Disinformation: Briefing Note for the New European Commission," Carnegie Endowment for International Peace, March 3, 2020, https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187.

[20] High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan Against Disinformation," 1.

[21] Ibid., 5.

[22] Ibid.

[23] "Factsheet: Rapid Alert System," European External Action Service, March 2019, https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.

[24] "Democracy: EU Adopts Conclusions," European Council, October 14, 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/10/14/democracy-eu-adopts-conclusions.

[25] "Human Rights and Democracy: Striving for Equality Around the World," European Commission, March 25, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_492.

[26] "Legislative Train Schedule: A New Push for European Democracy," European Parliament, https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-european-democracy-action-plan.

[27] "New EU Rules on E-commerce," European Commission, last updated March 8, 2020, https://ec.europa.eu/digital-single-market/en/new-eu-rules-e-commerce.

[28] "EEAS Special Report: Disinformation on the Coronavirus—Short Assessment of the Information Environment," EUvsDisinfo, March 19, 2020, https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment; "EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic," EUvsDisinfo, April 1, 2020, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic; "EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic (Updated 2–22 April)," EUvsDisinfo, April 24, 2020, https://euvsdisinfo.eu/eeas-special-report-update-2-22-april; "Coronavirus Disease (COVID-19) Advice for the Public: Myth Busters," World Health Organization, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters; Jeff Kao and Mia Shuang Li, "How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus," ProPublica, March 26, 2020, https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus; Laurence Dodds, "China Floods Facebook With Undeclared Coronavirus Propaganda Ads Blaming Trump," *Telegraph,* April 5, 2020, https://www.telegraph.co.uk/technology/2020/04/05/china-floods-facebook-instagram-undeclared-coronavirus-propaganda; and Betsy Woodruff Swan, "State Report: Russian, Chinese and Iranian Disinformation Narratives Echo One Another," *Politico*, April 21, 2020, https://www.politico.com/news/2020/04/21/russia-china-iran-disinformation-coronavirus-state-department-193107.

[29] "Coronavirus: Stay Up To Date," EUvsDisinfo, https://euvsdisinfo.eu/disinformation-cases/?disinfo_keywords%5B%5D=106935&date=.

30 “EEAS Special Report: Disinformation on the Coronavirus—Short Assessment of the Information Environment,” EUvsDisinfo; “EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic,” EUvsDisinfo; and “EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic (Updated 2-22 April),” EUvsDisinfo.

31 Alberto Nardellli, “The EU Was Accused of Watering Down a Report About Chinese Coronavirus Disinformation. In Response, It Has Attacked Leaks and Whistleblowers,” *BuzzFeed News*, May 5, 2020, https://www.buzzfeed.com/albertonardelli/eu-china-coronavirus-disinformation-report.

32 Josep Borrell Fontelles, “EEAS Special Report on the Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic: Opening Statement by Josep Borrell Fontelles, High Representative and Vice-President of the EC,” European Parliament, April 30, 2020, https://multimedia.europarl.europa.eu/en/eeas-special-report-on-the-narratives-and-disinformation-around-the-covid-19coronavirus-pandemic_I190055-V_v; and Hannah Ritchie, “EU Chief Denies Disinformation Report Was Watered Down for China, CNN, May 1, 2020, https://edition.cnn.com/2020/05/01/europe/eu-ursula-von-der-leyen-amanpour-china-intl/index.html.

33 Samuel Stolton, “EU Rapid Alert System Used Amid Coronavirus Disinformation Campaign,” Euractiv.com, March 4, 2020, https://www.euractiv.com/section/digital/news/eu-alert-triggered-after-coronavirus-disinformation-campaign.

34 Mark MacCarthy, “Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers and Industry,” Transatlantic Working Group on Content Moderation Online and Freedom of Expression,” February 12, 2020, 1, 10, https://www.ivir.nl/publicaties/download/Transparency_MacCarthy_Feb_2020.pdf.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org