CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

SEPTEMBER 2020

Future Threats, Future Solutions | #2

The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework

James Pamment

The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework

James Pamment

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, "Crafting an EU Disinformation Framework," establishes terminology and a 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, "Developing 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.

Introduction

For the European Union (EU) to mount an effective defense against the various threats it faces in the information space, the various institutions that compose it must work better in concert. To do so, the EU and its many affiliated bodies should adopt commonly held terms for discussing the challenges they face, clearly delineate institutional responsibilities based on each body's comparative strengths, and formulate countermeasures that more fully leverage those advantages.

Shared EU Terminology

The European Union (EU) should first revise the relevant terminology used by its various institutions in order to distinguish between different aspects of the problem of countering disinformation. The term disinformation itself is currently being used as a catchall that does not assist policymakers in defining different areas of activity or potential countermeasures. This conceptual groundwork muddles the distinctions between often unwitting individuals who inadvertently share factually incorrect information with the deliberate tactics of hybrid influence operations organized by hostile states. These problems can be averted by adopting four terms that define specific aspects of the problem: misinformation, disinformation, influence operations, and foreign interference.

Framing the policy area in this way has several benefits. For instance, this approach to the problem:

- allows EU institutions to use shared terminology, thereby strengthening consistency and coordination;
- enables stakeholders, including digital platforms, to use these terms in reports to the EU, rather than using their own preferred terminology (as in the Code of Practice on Disinformation), thereby strengthening coherence of knowledge and oversight;
- encourages member states to build a sense of community standards by adopting these terms;
- defines institutional ownership and responsibilities based on the terminology, facilitating interinstitutional collaboration; and
- helps develop countermeasures based on a clear definitional basis, scope, and institutional ownership, thereby strengthening the EU's policy response.

Misinformation

The term misinformation invites analysis of actors' truthfulness and intent. It refers to untrue information that individuals spread without any intent to mislead, though the effects of such misinformation can still be harmful. It is incorrect to refer to the spread of misinformation as campaigns because the lack of intent indicates that its spread is uncoordinated.

Individuals, states, and other actors have the right to express views that are unverifiable or false. A legislative response would need to weigh this fundamental right against any harm caused to others' ability to form their own ideas as a consequence of such false information. A significant legislative response to misinformation at the EU level is therefore unlikely and undesirable because it might infringe upon protected rights to freedom of expression.

However, digital platforms can and do develop policies for combating the spread of false or misleading content at scale under their terms of service. The EU should engage with these online platforms at the nonregulatory level to discuss, for example, guiding principles for aligning their terms of service with fundamental freedoms. (For more information on this topic, see the third paper in this series: "Developing Policy Interventions for the 2020s.")

With these points in mind, misinformation should be defined as the distribution of verifiably false content without an intent to mislead or cause harm. The portfolio for countering such unreliable information should be developed from the perspectives of home affairs, education, and the health of public debate.

Initiatives to counter misinformation could include various means of supporting societal resilience such as:

- efforts by digital platforms like enhancing their terms of service;
- commitments to fostering a healthier information space like media literacy training and better content labeling;
- and attempts to increase third-party accountability like journalism training, greater media pluralism, and enhanced digital media–monitoring capabilities.

Disinformation

Currently, EU institutions use the term disinformation as a catchall label for a range of activities loosely related to misleading information. The European Commission defines it as "verifiably false content that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm."[1] This definition is fine in and of itself, but it should not be used for everything. Its use should be confined to describing disinformation, not to conflate it with related activities like misinformation, influence operations, and foreign interference. Because disinformation entails malign intent, the argument about freedom of expression is not as compelling with respect to disinformation as it is with misinformation. Still, only limited EU case law suggests that spreading disinformation breaches fundamental rights except in the most harmful of cases.

EU terminology could operationalize disinformation to signify a range of defined deceptive communication techniques that depart from acceptable norms of online public discourse. In that spirit, disinformation should be defined as the creation, presentation, and dissemination of "verifiably false content" for "economic gain or to intentionally deceive the public, and may cause public harm."

Countermeasures to combat disinformation should include:

- efforts to deter actors from spreading disinformation, such as enhanced strategic communication, public diplomacy, and attribution capabilities;
- nonregulatory instruments such as enhanced terms of service employed by digital and media platforms and guidelines for promoting and demoting content on digital platforms; and
- regulatory approaches such as independent auditing of digital platform threat-mitigation activities (see the third paper in this series, "Developing Policy Interventions for the 2020s," for more information on this topic).

Influence Operations

The term influence operations captures the coordinated, adversarial nature of persistent efforts by malign individuals or groups to influence a society. It implies that an adversary actor's influence efforts use hybrid as well as informational means. The EU Action Plan on Disinformation recognizes

that disinformation is often part of a hybrid campaign.[2] Because misinformation and disinformation may be part of an influence operation, many of the same legal considerations and countermeasures apply to the respective parts of the operation.

However, a major difference between misinformation/disinformation and influence operations can be seen by looking at the broader picture of hybrid adversary activities—including coercion, sedition, and election interference—for which such information is being deployed in cases of influence operations. While misinformation and disinformation refer to false information, truthful information can also play a role in influence operations, either when a hack or leak is timed opportunistically or when words or events are taken out of context. The goal behind such operations usually relates to something bigger than the information component itself. Influence operations therefore position the problem in a security-focused context because misinformation and disinformation are framed as tactics employed by adversary actors (state or nonstate, foreign or domestic) engaged in hybrid activities as part of a larger influence operation with broader, often loftier goals.

With all this in mind, 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." Countermeasures should include:

efforts to build societal resilience and change the calculus of actors who conduct influence operations, including by way of strategies to deny capabilities and deny them the benefits they seek;
nonregulatory efforts to create norms for behavior on digital platforms around, for example, the removal of campaign-level activities related to influence operations; and
regulatory approaches such as legislating against the market for social media manipulation. (For more on this topic, see the third paper in this series, "Developing Policy Interventions for the 2020s.")

Foreign Interference

The term foreign interference emphasizes an actor's intent to interfere with others' fundamental human right to political expression and thereby the sovereignty of democratic governments. The UN Human Rights Committee used the term manipulative interference in the 1990s with reference to the right to vote in an environment free from manipulation and coercion.[3] That term reappeared in a 2019 UNHRC paper the committee published called "Freedom of Expression and Elections in the Digital Age,"[4] as well as in a 2019 European Council resolution on supplementary efforts to enhance digital resilience and counter hybrid threats.[5] These uses define interference as attempts to hinder the free expression of political will, particularly in the case of interference in the sovereign political matters of another state.[6]

Foreign interference should be defined as coercive, deceptive, and/or nontransparent efforts—during elections, for example—to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents.

Countermeasures to foreign interference should include:

- actor-specific strategies to counter the capabilities of adversary actors and deny them the benefits they seek, including and supported by a range of punitive options;
- nonregulatory efforts to create norms for behavior on digital platforms around, and including, those pertaining to attribution and the behavior of political actors; and
- regulatory approaches such as a duty of care for digital platforms (see the third paper in the series, "Developing Policy Interventions for the 2020s" for more details).

The ABCDE Framework

In addition to new terminology, the EU institutions would also benefit from a shared framework for conducting analyses and assessments. Several such frameworks already exist, though they have different points of emphasis and purposes. Outlined here is one based upon some of the existing approaches developed by the stakeholder community.[7]

This particular one, known as the ABCDE framework, has several advantages for EU policymakers. For one thing, it rests on approaches that have been developed within governments, industry actors, and the research community, and its components have been tried and tested over a relatively long period. Key elements of this framework have already been recognized and adopted by industry actors, governments, and researchers, meaning that it could potentially facilitate information exchanges and a coherent dialogue. This approach sets a standard that can be tailored to the needs of individual institutions or teams, yet it simultaneously retains its coherence and consistency. It can be used to help diagnose which part of the terminology should be used; to structure analysis, reporting, and information requests to stakeholders; and to design countermeasures. When assessing information from multiple sources, this framework can provide a means of assessing the likelihood of each proposition, supporting more transparent and accurate assessments.

The framework in question breaks down the disinformation problem into smaller operative factors that can be framed as questions. Similar approaches have been used in previous studies to identify the relevance of disinformation terminology to normative, legal, and academic frameworks.[8] Here, it is used to support the efforts of EU institutions, member states, digital platforms, and other stakeholders to speak the same language when thinking about and communicating about the problem.

The Elements of the ABCDE Framework

The key elements of the framework are the five ABCDE components: actor, behavior, content, degree, and effect (see table 1). This rubric should be used whenever the framework is deployed. The questions supporting each component set out below are examples that help explain the purpose and intent of the components—they constitute a tool that can be tailored to a given user's specific needs.

TABLE 1
The ABCDE Framework

Actor	*What kinds of actors are involved?* This question can help establish, for example, whether the case involves a foreign state actor.
Behavior	*What activities are exhibited?* This inquiry can help establish, for instance, evidence of coordination and inauthenticity.
Content	*What kinds of content are being created and distributed?* This line of questioning can help establish, for example, whether the information being deployed is deceptive.
Degree	*What is the overall impact of the case and whom does it affect?* This question can help establish the actual harms and severity of the case.
Effect	*What is the overall impact of the case and whom does it affect?* This question can help establish the actual harms and severity of the case.

Actor: The actor component of the framework enables an assessment of the actor(s) involved in the case. The aim is to discern which kinds of actors produce and engage with the suspected disinformation. This is not always easy to discern. Sometimes actors disguise their origins and purposes. This component offers a means of collecting and analyzing all available information to make an assessment. This can include secondary information, such as an attribution made by a digital platform or in a journalistic investigation.

Relevant questions to ask include:

- Individual(s): Is the person involved acting in his or her private capacity?
- Nonstate actor(s): Is the actor affiliated with a private or nongovernmental organization?
- Media platform(s): To what degree is the platform of distribution independent?
- Political actor(s): Does the individual act on behalf of a recognized political entity?
- Foreign state(s): Is the actor an agent or proxy of a foreign government?

Behavior:
The behavior component assesses to what extent deception or other illegitimate communication techniques are part of the case. In particular, this component can be used to analyze an actor's intent and evidence of coordination—two very strong indicators of problematic behavior that could help shape potential countermeasures.

Important questions to ask include:

- Transparency: Is the actor disguising his or her identity or actions?
- Dependency: Is the individual acting on behalf of another party?
- Authenticity: Is the actor using illegitimate communication techniques?
- Infrastructure: Is there evidence of back-end coordination?
- Intent: Does the behavior suggest a malign intent?

Content: The content component of the framework focuses on the information that is used in the case. Such considerations can help define how serious and problematic the content is. This part of the inquiry includes analyzing narratives and could, for example, support an initial assessment of harm caused by those narratives. This aspect of the framework could also capture examples of synthetic content such as deep text and deepfakes, which would be additional indicators of risk.

Relevant questions to ask include:

- Truthfulness: Is the content verifiably untrue or deceptive?
- Narrative(s): Does the content align with known disinformation narratives?
- Language(s): Which languages are used in the spread of the disinformation or other online content in question?
- Synthetic: Is the content manipulated or artificial?
- Expression: Is the content reasonable self-expression protected by fundamental freedoms?
- Harm: Is the content harmful?

Degree: The degree component unpacks information related to the distribution of the content in question and the audiences it reaches in a particular case. Assessing the scale of the problem can, for example, help decisionmakers gauge whether countermeasures are desirable. This component could capture networks, hashtags, shares, and other relevant signifiers of the degree of distribution and online engagement.

Important questions to ask include:

- Audience(s): Who constitutes the content's main target audience(s)?
- Platform(s): Is it possible to map which channels or platform(s) are used to distribute the content and how they interact?
- Virility: Is the content going viral on social media platforms in a way that would suggest an inauthentic boost to online engagement?
- Targeting: Is the content tailored or microtargeted, and, if so, to which audiences?
- Scale: Does the scale indicate a single operation or an ongoing campaign?

Effect: The effect component of the ABCDE framework uses indicators of impact to understand how much of a threat a given case poses. Indicators can be drawn together on the basis of the first four components to reach an assessment of the overall effects of the case.

Useful questions to ask include:

- Climate of debate: Is the online content issue-based? Does it, for example, involve false information, polarization, or trolling?
- Trust/reputation: Is the content target-based? Does it, for example, involve false rumors, cybersecurity hacks, forgeries and/or media leaks?
- Fundamental freedoms: Is the content denying a fundamental freedom? For example, does it seek to deny freedom of expression or of political deliberation?
- Public health: Does the content threaten individuals' health, physical wellbeing, or medical safety?
- Public safety: Does the content threaten individuals' physical wellbeing or public order?
- Election integrity: Does the content dissuade voters from participating in elections or seek to undermine the results of an election?
- National security: Does the content threaten the territorial integrity or the national security of a sovereign state?

Framework-Based Analysis, Assessment, and Reporting

The ABCDE framework can be used to analyze data from a variety of sources, including governments, one's own monitoring sources, researchers, industry actors, and journalists. On the basis of the components, the framework can support a transparent means of analyzing available evidence to support rigorous assessments and reporting. An example of the shape such analysis could take may include a proposition (or assertion), the source of the information, and an assessment of the likely

veracity of the information (see table 2). Conducting analysis in this format allows for a clear and transparent process that can be complemented by top-line assessments. As explained in the first paper in the series, "Taking Back the Initiative," assessments should be kept separate from analysis, as they reflect political and other contextual considerations. This is particularly important in cases of attribution, where several pieces of evidence can be and often are considered before reaching an assessment.

The ABCDE framework can be used to give structure to reports of any length and outline available data in a clear and coherent manner. The example questions above corresponding to each component suggest ways in which scripts could be used to focus reporting according to mandate and scope, and how the framework could be adapted to the strengths of the data under consideration. The five components could also provide a template for requesting and receiving information and data from various stakeholders. For example, under the actor component, an EU institution may wish to request information from a digital platform about which state actors have been identified and with what degree of confidence.

TABLE 2

A Rubric for Framework-Based Analysis, Assessment, and Reporting

	Proposition	Source	Likelihood
Analysis	State media outlets in Country X are spreading conspiracy theories about the source of the coronavirus.	Broadsheet newspaper	Verified by the East Stratcom Task Force
	Country X is the source of a variety of deceptive messages about the number of coronavirus deaths in several EU member states on alternative media websites and social media channels.	An open-source intelligence unit of an EU member state's Ministry of Foreign Affairs	Not verified but likely
	Country X has employed public relations agencies to run a campaign that includes thousands of fake accounts.	Online news source	Not verified
	Country X is seeding deceptive messaging about the source of the coronavirus on the dark web.	Intelligence source	Judged highly likely by intelligence sources
	Country X's diplomatic representatives are suggesting in private that there will be repercussions if any country disputes their coronavirus figures.	The ministries of foreign affairs of several EU member states	Confirmed
Assessment	Country X is conducting overt and covert influence operations aimed at distracting from its domestic handling of the coronavirus crisis		

The Organization of the EU's Disinformation Policy

This paper has outlined four terms and a framework that EU institutions and other relevant stakeholders should use consistently to synchronize their efforts to combat misinformation, disinformation, influence operations, and foreign interference.

Delineating Institutional Responsibilities

The ABCDE framework can help diagnose which term most appropriately characterizes a given case (see table 3). By using the characteristics of various malign activities to diagnose them, EU actors will be better equipped to assign institutional responsibilities for managing various aspects of the challenge to different EU bodies based on their comparative strengths.

EU policymakers should clearly delineate which institutions have the mandate and resources to best deal with the operational aspects of each term when they determine institutional ownership over policy matters and countermeasures. Those institutions would then be the owners of a particular term for the purpose of coordinating response efforts. The key point here is that the EU should treat misinformation and disinformation primarily as an internal democratic and public discourse problem, whereas interference by adversary actors, including through the dissemination of disinformation, can be approached as an external actor problem.
Relevant institutions within the EU should more clearly signal their respective roles by adopting the corresponding term best tailored to the actors and phenomena they each are contesting.

Different aspects of addressing misinformation could be led by the directorates-general with the corresponding expertise. The Directorate-General for Justice and Consumers (DG JUST) and the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) could take ownership on matters of transparency and media policy. The Directorate-General for Communication (DG COMM) could run point on factual communication and raising awareness within the EU. The Directorate-General for Education, Youth, Sport and Culture (DG EAC) could focus on public education within the EU. Finally, the European Commission's Joint Research Centre (JRC) could be tasked with applied research.

Meanwhile, on media and civil society support in the Eastern Neighborhood, the disinformation portfolio could also involve the Directorate-General for Neighborhood and Enlargement Negotiations (DG NEAR) and the European External Action Service (EEAS), and the EEAS could take ownership on fact-based communication and awareness raising in the neighborhoods. This task would also involve the StratCom task forces, which fall under the EEAS as the primary platform for monitoring, analyzing, and exposing disinformation.

TABLE 3

Framework-Based Diagnoses

Misinformation	
Actor	Any, but less likely to be a large organization or state actor
Behavior	Key indicator: There should be no evidence of an intent to deceive
Content	Often legitimate expression of an opinion or piece of information that is verifiably deceptive or untrue
Degree	There should be limited evidence of coordination, at least from the original source
Effect	Any

Disinformation	
Actor	Any
Behavior	Key indicator: There should be evidence of deliberately deceptive behavior
Content	Key indicator: The content should include verifiably deceptive or untrue elements
Degree	Any
Effect	Any

Influence Operation	
Actor	Any, but likely to be a large organization or state actor
Behavior	Key indicator: There should be evidence of back-end coordination and inauthentic behavior, potentially combining a variety of influence techniques aimed at a common goal
Content	Any, often including multiple types in combination to achieve a goal
Degree	Key indicator: The scale of the operation should indicate coordination
Effect	Any, but should further the objectives of the identified actor(s)

Foreign Interference	
Actor	Key indicator: There should be indications of a state actor and/or its proxies
Behavior	There should be evidence of back-end coordination and inauthentic behavior, potentially combining a variety of influence techniques aimed at a common goal
Content	Any, often including multiple types in combination to achieve a goal
Degree	Any
Effect	Key indicator: Any, but should further the objectives of the identified foreign state actor(s)

Efforts to deal with influence operations and foreign interference should be led by the EEAS, in conjunction with other institutions listed above, based on their respective responsibilities for helping oversee external relations, foreign interference, monitoring and analysis, resilience building in the neighborhoods, and third-country election monitoring. Integration of these institutional apparatuses with European intelligence, hybrid, and cyber capabilities would also be required. In short, the EEAS and the European Commission's various directorates-general each have their own comparative strengths to draw on in combating disinformation and related activities (see table 4).

TABLE 4

Focal Points for EU Institutions in the Information Space

Term	Institutional Responsibility	Focal Points
Misinformation	DG JUST DG CONNECT DG COMM DG EAC JRC	*Behavior:* Strengthen democracy, protect political participation, develop social responsibility in public debate, and conduct research into the psychological dimensions of misinformation
		Content: Spearhead rebuttals and fact checking, foster proactive communication, cultivate media literacy education, and train journalists
		Effect: Engage in limited digital-media monitoring capabilities focused on areas of identified risk (like public health, for example)
Disinformation	DG JUST DG CONNECT DG COMM DG EAC JRC DG NEAR EEAS	*Actor:* Pursue limited public attribution and exposure of actors caught overtly and deliberately spreading disinformation
		Behavior: Engage in the same activities listed for misinformation, plus norms around digital communication and engagement with digital platforms on coordinated inauthentic behavior and product design
		Content: Engage in the same activities listed for misinformation
		Effect: Engage in the same activities listed for misinformation
Influence operations	EEAS and others	*Actor:* Engage in the same activities listed for disinformation, but some sources may be less overt
		Behavior: Engage in the same activities listed for disinformation, plus intensified cooperation with digital platforms
		Content: Engage in the same activities listed for disinformation
		Degree: Monitor and assess an adversary actor's capabilities to track networks and scale
		Effect: Target digital monitoring capabilities on areas of identified risk
Foreign interference	EEAS and others	*Actor:* Wield technical and political attribution capabilities
		Behavior: Engage in the same activities listed for influence operations, plus even more intensified collaboration with digital platforms
		Content: Engage in the same activities listed for influence operations
		Degree: Engage in the same activities listed for influence operations, plus intelligence briefings where appropriate
		Effect: Engage in the same activities listed for influence operations, plus risk-based capabilities connected to security and elections

Institutional coordination can either be centralized or decentralized. Centralized coordination would be conducted through an interinstitutional task force or agency whose role is to ensure that the activities of all institutions are aligned. Such coordination may not be necessary, however. A decentralized approach would rely upon lead organization(s) to manage efforts focused on each term, based on a diagnosis of the case at hand. DGs JUST, CONNECT, and/or COMM would be strong candidates to lead on misinformation and disinformation. The EEAS would have a particularly important role in coordinating countermeasures aimed at disinformation that are part of a wider influence operation or foreign interference campaign, as well as broader efforts to influence the calculus of adversary actors (see the third paper in the series, "Developing Policy Interventions for the 2020s" for more details).

Monitoring and Analysis

The StratCom task forces provide a unique platform for combining monitoring, analysis, and proactive strategic communication. Though unusual within the EU, this function is equivalent to capabilities that have been developed in larger foreign ministries (such as those housed in the Global Engagement Center at the U.S. Department of State, for instance), ita function that provides considerable value for a reasonable price. The additional value of the task forces is in the fact that these three activities are combined with an operational emphasis, which makes them very different from traditional EU structures. In updating their mandate for the 2020s, the task forces should be envisioned as platforms for monitoring disinformation and providing analysis and as strategic communication centers of excellence designed to serve the EU institutions, member states, and neighborhoods. They should retain an operational focus and not develop into think tanks or research institutions.

The monitoring function of the StratCom task forces should be expanded with a political mandate to monitor disinformation beyond pro-Kremlin sources and to cover additional strategically relevant regions such as sub-Saharan Africa. This mandate must be carefully defined to offer the task forces relative autonomy once the overall strategic direction is set. Monitoring is currently outsourced by the task forces; this function should be brought in- house and developed up to the standards of some of the leading international think tanks and companies working in this area, with external contractors complementing internal capabilities where needed.

A central role for the task forces should be sharing information and liaising between the EU and the media; NGOs; research institutes; the tech industry; and the intelligence, hybrid, and cyber communities. Secret intelligence should not be included within this mandate, but the task forces should be hubs for disinformation-related open-source intelligence and other nonsecret information sharing. Monitoring and analysis produced by the task forces should follow a methodology that is stated

transparently and open to scrutiny. Given their arm's length status as semi-independent bodies, the task forces that perform monitoring and analysis need to be protected from day-to-day political considerations.

The funding for the StratCom task forces should be secured for the length of the mandate of the European Commission (five years). The pros and cons of continuing to house them within the EEAS versus establishing them as a separate agency with member-state support should be weighed when the funding levels of the EU's budget, the Multiannual Financial Framework, are next discussed and negotiated.

Other EU institutions require monitoring and analysis capabilities of their own, but these should be consistent in format and more limited in scope than those of the StratCom task forces. The EU delegations, DG COMM, and the European Parliament spokesperson unit should temporarily adopt the RESIST model,[9] until such time as they are able to adopt a standard framework for EU institutions such as ABCDE. Other communications units within EU institutions should have basic capabilities in the areas of digital monitoring and countermeasures in line with those proposed in the RESIST and/or ABCDE models. Information sharing is crucial, and here the task forces have a particular role to play as a source of expertise within EU institutions.

Proactive Communications and Public Diplomacy

The EU's communications approach follows a very traditional structure and process. It is designed around one-way communication and old-school media relations, with press spokespersons playing a central coordinating role. The bureaucracy produces "lines to take" in dealing with the media following extensive consultancy with policy officers, helps organize media events, and facilitates interviews. This information is then pushed out to the delegations. Public diplomacy activities tend to be niche and centered on events such as Europe Days and film festivals. In many cases, communication campaigns are outsourced to contractors, which often provide project management expertise rather than the necessary strategic communication skills. While there are many good examples of innovative and exceptional work scattered across the EU institutions, their overall impact is limited by the lack of wider professional communication planning and practice. Proactive communication around disinformation is hampered by these broader structural, organizational, and competency issues.

Alongside bringing monitoring capabilities in-house, the EU should hire more communications professionals who understand the contemporary practice of strategic communication, as it exists outside of the Brussels bubble. Public diplomacy work would benefit from contractors with local knowledge who understand modern, data-driven communication. As well as formal networks, they should be able to make use of the informal ones that delegations are unlikely to work with.

The EU should more clearly define its audiences for proactive communication aimed at mitigating the impact of disinformation. Its messaging and branding remains fragmented and incoherent. The institutions compete to brand their respective work, yet few outside of Brussels would care about the institutional distinctions. Too much work is conducted for the benefit of audiences in Brussels, much of which ends up being translated by delegations and pumped out to nobody in particular. The EU also communicates largely in technical or bureaucratic language rather than in terms that make the most sense to ordinary audiences. The East StratCom Task Force's forthcoming Anatomy of Disinformation campaign will be an interesting example of work that seeks to reach new and important audiences by simplifying the language and focusing on the target audience.

The EU's current communication processes are not radically different from those of twenty years ago. Its strategic communication is not yet data driven and entails considerable bureaucratic labor with very limited purpose or effect. On the public diplomacy side, institutions and delegations should assess the tools they currently use and their suitability for their intended purposes. A radical process of modernization and professionalization is required, even for the relatively niche activity of supporting efforts to combat disinformation.

The proactive communications function of the StratCom task forces should build on disinformation monitoring and analysis to improve the targeting and impact of agreed-upon EU strategic communication and public diplomacy activities. They should provide expertise at the intersection of monitoring, analysis, and strategic communication. The task forces should offer capacity building, awareness raising, and other forms of support to the EU institutions, delegations, willing member states, and relevant actors outside of the EU, such as election observation bodies. Training for EU staff on communications around disinformation could also fall within the task forces' mandate. The task forces should be developed into the EU's public-facing hub for providing insights and expertise to the initiatives of all other EU institutions working on disinformation, as well as engagement with the broader stakeholder community.

The EUvsDisinfo platform and campaign is an excellent example of public-facing work that can be expanded. There is no need for additional platforms to be created if, for example, the EU decides to expand the task forces' mandate beyond pro-Kremlin sources. The EU will need to develop the EUvsDisinfo database into a more useful resource that goes beyond simply logging individual examples of disinformation. In particular, its content should be available in more languages, integrated better into the Rapid Alert System, and aligned better with proactive communication activities. It should become the key platform for EU engagement on disinformation with the public. For this to be possible, the EU needs to invest in the back end of the database. The data should be more accessible to developers, researchers, other governments, and the private sector, and the methodology should be promoted and debated openly. The studies and reports section of the platform could be developed, for example, into a searchable library.

Countermeasures

The terms and framework outlined here provide a means of thinking about areas of responsibility and countermeasures. For example, if the actor assessment indicates that a given case appears to involve foreign interference, this would help to define a pathway to developing suitable countermeasures. Consequently, the EEAS should own the issue and interventions designed to influence a given adversary's calculus (see the third paper in the series, "Developing Policy Interventions for the 2020s"). Table 5 offers guidelines for how countermeasures may be approached. Specific projects and activities could be commissioned within these guidelines.

Below are some examples of the kinds of projects that could fit under each countermeasure program. Many of these principles are further explored in the third paper in the series: "Developing Policy Interventions for the 2020s." These include various forms of democracy-building initiatives, norm-defining initiatives, resilience-building initiatives, and adversary-influencing efforts.

TABLE 5
Designing Suitable Countermeasures

Term	Countermeasures
Misinformation	Democracy-building initiatives Norm-defining initiatives
Disinformation	Democracy-building initiatives Norm-defining initiatives, including exposure of activities and/or offending actors where appropriate Resilience-building initiatives
Influence operations	Democracy-building initiatives Norm-defining initiatives, including exposure of activities and/or offending actors where appropriate Resilience-building initiatives Efforts to influence an adversary's calculus
Foreign interference	Democracy-building initiatives, especially involving elections Norm-defining initiatives, including attribution Resilience-building initiatives, especially around elections Efforts to influence an adversary's calculus and that particular adversary actor's specific capabilities

Democracy-building initiatives: fact-checking initiatives; media literacy training; journalist training; media pluralism programs; working with schools; enhanced digital media monitoring capabilities; and programs of research into the impact of misinformation and disinformation, digital platforms, and health of public debate.

Norm-defining initiatives: enhanced strategic communication, public diplomacy, and attribution capabilities; nonregulatory instruments such as enhanced terms of service on digital and media platforms and guidelines for promoting and demoting content on digital platforms; regulatory instruments such as independent auditing of digital platform threat mitigation activities; and programs of research into the impact of disinformation and ethics, legitimacy, and law.

Resilience-building initiatives: rethink the Rapid Alert System and other community-building resources; resilience-building programs in the neighborhoods; nonregulatory efforts to create norms for behavior on digital platforms around, for example, the removal of campaign-level activities; and regulatory instruments such as legislating against the social media manipulation market.

Adversary-influencing efforts: enhanced mandate to deny capabilities and deny benefits of spreading disinformation through, for example, attribution; actor-specific strategies to deny capabilities and deny benefits, supported by punitive options; nonregulatory efforts to create norms for behavior on digital platforms around, for example, attribution and the behavior of political actors; and regulatory approaches such as a duty of care for digital platforms.

About the Author

James Pamment is a nonresident scholar in the Technology and International Affairs Program at the Carnegie Endowment for International Peace and co-director of the Partnership for Countering Influence Operations there.

Notes

1 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation," *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions,* December 5, 2018, 1, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf.

2 Ibid., 3.

3 United Nations Human Rights Committee, "Human Rights Committee Discusses Free and Fair Elections," Department of Public Information Press Release HR/CT/433, October 18, 1995, https://www.un.org/press/en/1995/19951018.hrct433.html.

4 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "Freedom of Expression and Elections in the Digital Age," United Nations Human Rights Special Procedures, June 2019, 3, https://www.ohchr.org/Documents/Issues/Opinion/ElectionsReportDigitalAge.pdf.

5 General Secretariat of the Council, "Complementary Efforts to Enhance Resilience and Counter Hybrid Threats," Council of the European Union, December 10, 2019, https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf.

6 Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," EJIL:Talk!, August 26, 2019, https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/.

7 Adapted from Camille François, "Actors, Behaviors, Content: A Disinformation ABC: Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses," Transatlantic Working Group on Content Moderation Online and Freedom of Expression, September 20, 2019, https://science.house.gov/imo/media/doc/Francois%20Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf; Alex Alaphillipe, "Adding a 'D' to the ABC Disinformation Framework," Brookings Institution, April 27, 2020, https://www.brookings.edu/techstream/adding-a-d-to-the-abc-disinformation-framework/; the DIDI diagnosis tool in James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed, *Countering Information Influence Activities: The State of the Art* (Stockholm: Swedish Civil Contingencies Agency, 2018), https://www.msb.se/RibData/Filer/pdf/28697.pdf; and the impact assessment tools in James Pamment, Henrik Twetman, Alicia Fjällhed, Howard Nothhaft, Helena Engelson, and Emma Rönngren, *RESIST Counter-Disinformation Toolkit* (London: UK Government Communication Service, 2019).

8 Duncan Hollis, "Why States Need an International Law for Information Operations," *Lewis & Clark Law Review* 11, no. 4 (2007): 1023–1061; Pamment, Nothhaft, Agardh-Twetman, and Fjällhed, *Countering Information Influence Activities: The State of the Art*; and Kristine Berzina and Etienne Soula, "Conceptualizing Foreign Interference in Europe," Alliance for Securing Democracy, March 19, 2020, https://securingdemocracy.gmfus.org/what-is-foreign-interference-conceptualizing-foreign-interference-in-europe/.

9 See Pamment, et al., *RESIST Counter-Disinformation Toolkit*.

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

CarnegieEndowment.org