upgrade
democracy

STRENGTHEN DEMOCRACY! | BertelsmannStiftung

Up to the challenge?

Strategies to counter disinformation in the EU, UK and US

Charlotte Freihse, Florian Bochert

| BertelsmannStiftung

Up to the challenge?

Strategies to counter disinformation in the EU, UK and US

Charlotte Freihse, Florian Bochert

Content

Introduction 4

1. Zooming in: National strategies countering disinformation 5
   - Action Plan Deepfake (Austria) 8
   - National Strategy for Countering Hybrid Threats (Czech Republic) 9
   - Government-wide Strategy for Effectively Tackling Disinformation (Netherlands) 10
   - The National Concept on Strategic Communication and Security of the Information Space (Latvia) 11
   - Concept of Strategic Communication of the Slovak Republic (Slovakia) 12
   - Online Media Literacy Strategy (UK) 13

   1.1 Zooming out: Differences and similarities between the strategies 14

2. Rethinking strategy: The case of the US 15

3. Beyond strategies: Public institutions to counter disinformation 17

   3.1 VIGINUM (France) 17
   3.2 Psychological Defence Agency (Sweden) 18
   3.3 From strategy to agency: How to go from here 19

4. Next steps: Recommendations for action 21

Publishing credits & legal notice 22

Introduction

In recent years, the threat of disinformation has become increasingly prominent, impacting political stability, public health and social cohesion across the globe. From manipulated social media posts during elections to false information about the COVID-19 pandemic, the challenges posed by disinformation are multifaceted and complex. At the beginning of 2024, the German Federal Foreign Office identified a disinformation campaign, involving approximately 50,000 bot accounts that generated around 2 million fake posts targeting the current government. Last autumn, a bedbug scare in Paris that grabbed headlines worldwide was artificially amplified by social media accounts linked to Russian disinformation activities, a French minister reported. While these events have certainly increased efforts in the respective countries, there is ongoing discourse and discussion about the role of states in countering disinformation and which activities are most effective.[1] In practice, some countries have taken significant steps to combat disinformation, while others have yet to fully recognise or address the issue. To understand the landscape of counter-disinformation efforts in Europe, we looked at all 27 EU member states, the United Kingdom (UK) and the United States (US). Our aim was to assess if and how countries are tackling the disinformation threat, with a specific focus on national strategies that may or may not accompany other measures like legislation or task forces. By focusing mostly on national strategies, we aim to identify pathways for state responses that could be shared and adopted more widely. We also specifically looked at two counter-disinformation agencies in France and Sweden to explore how countries could proceed after having created a national anti-disinformation strategy.

1 Keller, C. I., Freihse, C., & Berger, C. (2024). *State actions against disinformation: Towards a healthy public sphere*. Bertelsmann Stiftung, Gütersloh.

1 Zooming in: National strategies countering disinformation

Looking at all 27 EU member states, the UK and the US, every single one of these countries has a national cyber security strategy and most of these countries have a national AI strategy.[2] Yet, none of these strategies properly considers disinformation. The term disinformation may be mentioned a few times as a buzzword but proper substantive engagement with the topic is lacking. Sometimes, a country's national security strategy mentions the threat of disinformation, but even in those instances, engagement with the topic remains limited. Therefore, this report focuses specifically on national strategies countering disinformation and classifies countries into three groups. **Group A** includes countries that have not yet devised a proper, publicly accessible disinformation strategy countering disinformation. This could indicate either that no finalised strategy exists or that the government has chosen not to openly communicate its strategy. Most EU member states fall into this category. **Group B** consists of six countries where the government has adopted a strategy that specifically focuses on the issue of disinformation. Sometimes, this strategy focuses on one specific aspect of disinformation, such as deepfakes, or on one solution to disinformation, such as media literacy. But disinformation remains the core topic of the strategic document. Another two countries have not created a strategy countering disinformation but have already gone a step further by establishing a governmental agency that is solely and specifically designed to fight disinformation. Such a counter-disinformation agency, like *VIGINUM* in France and the *Psychological Defense Agency* in Sweden, demonstrates a level of government engagement with the issue that goes beyond just an anti-disinformation strategy. Therefore, we have classified France and Sweden as being in **Group C**. An overview of all countries can be found in the table below.

Group A	Belgium, Bulgaria, Croatia, Republic of Cyprus, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Slovenia, Spain, USA
Group B	Austria, Czech Republic, Latvia, Netherlands, Slovakia, United Kingdom
Group C	France, Sweden

Figure 1: Overview status of strategic approach to disinformation in EU member states, UK and US

2 Van Roy, V., Rossetti, F., Perset, K. & Galindo-Romero, L. (2021). *AI Watch – National strategies on Artificial Intelligence: A European perspective.* Publications Office of the European Union, Luxembourg.

This classification is not meant to imply that countries in Group A are inactive in the face of disinformation or that there exists no strategic thinking about how to counter disinformation at the state level. Some countries like Ireland or Germany are currently in the process of creating a national strategy countering disinformation. In some cases, parts of such a strategy can also fall under the responsibility of intelligence agencies and thus remain classified information that is not publicly accessible. For instance, one of several US institutions that is partially responsible for dealing with information manipulation, the Foreign Malign Influence Center (FMIC), was established under the Office of the Director of National Intelligence (ODNI). In addition to that, some countries may have particularly strong legislation in place or may have a ministerial task force concerned with the threat of disinformation, neither of which is considered in our classification. Yet, while governmental responses to disinformation are just as diverse as disinformation is itself, it is difficult to compare legislation, task forces and national strategies all in one brief publication. Therefore, we are limiting our analysis to currently existing and publicly accessible national strategies countering disinformation as a common denominator for comparison.

How to read the structured overview of the strategies:

Before zooming in on the national strategies countering disinformation, it may be useful to explain how we analysed them and what we focused on.[3] Apart from generic information like the title, year and procedural state of the strategy, we first categorised each strategy based on what responsibilities it assigns to the state. Each strategy could fall into one or more out of a total of five categories, which were based on the report *State actions against disinformation: Towards a healthy public sphere* (2024). The five categories are as follows:

- **Mitigating false information:** The state is responsible for governing the content-related dimension of disinformation. It is supposed to dispute false information in the public debate and mitigate, contain or punish its possible effects.
- **Governing digital intermediaries:** The state is responsible for having digital intermediates, like social media and messaging apps, target digital disinformation. For instance, a strategy could propose regulatory frameworks or soft law instruments, such as co-regulation or cooperation agreements.[4]
- **Promoting transparency and quality in government communications:** The state is responsible for communicating effectively and transparently so that citizens trust the information they receive from their government.
- **Strengthening media pluralism and professional journalism:** The state is responsible for facilitating a strong, pluralistic and professional media landscape. It can fulfil this responsibility for instance by improving or updating media and journalism practices and regulations.
- **Building up public institutions:** The state is responsible for creating new administrative bodies or institutions tasked with various aspects of countering disinformation.

3 The Czech and Slovak anti-disinformation strategies are not available in English or German so that our analysis had to rely on an automatic translation of these two strategies.

4 This category is not part of any strategy that we found. However, it is to state that this objective or measures under this category are often achieved through legislation rather than national strategies.

After this categorisation, we consider what specific problem each strategy addresses, for instance whether the strategy focuses on disinformation in general or a specific type of disinformation. We also assess how each strategy frames this problem. Based on Wagnsson (2020),[5] we classify whether a strategy frames the problem as concerning national security, democracy or social cohesion. Next, we summarise if a strategy names the perpetrators spreading disinformation and the topics or actors that are targeted by disinformation. From an organisational perspective, we explain what state institution would be responsible for implementing the strategy and what role non-state actors are supposed to play in this implementation. Lastly, we examine the kind of actions each strategy proposes should be taken to implement the strategy.

In the following part, you will find a detailed overview of the **six national strategies countering disinformation** that we found, including for Austria, Czech Republic, Netherlands, Latvia, Slovakia and the UK.

5 Wagnsson, C. (2020). *What is at stake in the information sphere? Anxieties about malign information influence among ordinary Swedes.* European Security, 29(4), 397 – 415. https://doi.org/10.1080/09662839.2020.1771695

Action Plan Deepfake (Austria)

Date	**2022**
Author	Interministerial working group
Responsibility of the state	Building up public institutions
What problem does the strategy address?	Deepfakes (defined as: *"perfectly manipulated videos, images, or audios in which people are saying or doing things that never actually happened in reality")*
How is the problem framed?	**National Security:** The strategy very much focuses on deepfakes as a threat to public security. It considers that deepfakes could lead to mass demonstrations, election interference, a stock market crash, a government crisis and the erosion of trust in government more generally.
Who are the perpetrators spreading disinformation?	There are no perpetrators named specifically. The strategy only vaguely refers to foreign actors and terrorist organisations as well as to criminals, who could try to create a false alibi through deepfakes.
What are the topics or actors being targeted?	While the strategy does not consider specific topics, it focuses on potential victims, such as public officials and institutions (including democratic elections), businesses and individuals (especially referring to women who could be targeted via pornographic videos).
What agency is responsible?	The strategy prefers building up institutions through an internationally coordinated approach, preferably on the EU level, rather than seeing any national agency as responsible for the fight against deepfakes.
What role do non-state actors have?	The strategy does not actually consider non-state actors much. It does talk a little bit about cooperating with non-state actors and increasing media literacy as measures against deepfakes, but these points are not very prominent.
Action Items	Creation of a working group, more inter-agency cooperation, more public awareness, more research, more international cooperatio

→ full document

National Strategy for Countering Hybrid Threats (Czech Republic)

Date	**2021**
Author	Ministry of Defense
Responsibility of the state	Mitigating false information, Building up public institutions
What problem does the strategy address?	Hybrid threats (defined as: *"hidden and overt activity of state or non-state actors directed against vulnerable elements of the democratic state and society"*)
How is the problem framed?	**National Security:** Just as the concept of hybrid threats is closely tied to the topic of national security, the strategy focuses on disinformation from a security lens. For instance, the second paragraph of the strategy immediately emphasises the role of NATO.
Who are the perpetrators spreading disinformation?	The strategy sees state and non-state actors, particularly *"authoritarian and revisionist powers with regional and even global power aspirations"*, as potential perpetrators.
What are the topics or actors being targeted?	The strategy considers democratic institutions and values like rule of law processes, the national economy, security and defence as the primary targets of hybrid threats.
What agency is responsible?	The strategy makes the State Security Council responsible for the response to hybrid threats.
What role do non-state actors have?	The strategy advocates for a *"whole of society approach"* that fosters government cooperation with the private sector, media outlets, the education sector and non-profits.
Action Items	Raising public awareness of hybrid threats, reducing strategic dependence on countries with different value orientations, conducting stress tests simulating hybrid attacks, improving ministerial cooperation and coordination, further supporting NATO and the EU

⟶ full document

Government-wide Strategy for Effectively Tackling Disinformation (Netherlands)

Date	**Dec 2022**
Author	Ministry of the Interior and Kingdom Relations
Responsibility of the state	Strengthening media pluralism and professional journalism
What problem does the strategy address?	Disinformation (defined as the *"deliberate, mostly covert, dissemination of misleading information with the aim of harming the public debate, democratic processes, the open and knowledge economy or public health")*
How is the problem framed?	**Democracy:** Disinformation is predominantly framed as a threat to free, open public debates and to citizens making informed decisions. While the issue of national security is mentioned, the framing surrounding public debates is much more prominent.
Who are the perpetrators spreading disinformation?	The strategy does consider state actors, specifically Russia, as perpetrators but also focuses on disinformation spread by COVID sceptics and anti-institutional extremists.
What are the topics or actors being targeted?	The strategy addresses disinformation concerning elections and diseases as well as disinformation shown as clickbait to make money through advertisements.
What agency is responsible?	The Dutch Ministry of the Interior and Kingdom Relations is primarily responsible for implementing the strategy.
What role do non-state actors have?	The strategy specifically states that *"the government does not determine what is reliable and what is unreliable information"* and that *"citizens themselves bear primary responsibility in this regard."* Thus, non-state actors are the ones responsible for qualifying and fighting disinformation.
Action Items (selection)	Creation of website with tips and tricks for disinformation, awareness campaigns, use of public alternatives to online platforms, simulation of how government would respond to disinformation campaign, quality assurance in journalism

⟶ full document

The National Concept on Strategic Communication and Security of the Information Space (Latvia)

Date	**Jan 2023**
Author	Government
Responsibility of the state	Mitigating false information, building up public institutions, strengthening media pluralism and professional journalism, promoting transparency and quality in government communications
What problem does the strategy address?	The strategy finds the security of information space to be endangered. By a secure information space, it means *"strategic communication, resilience to internal and external risks of interference in democratic processes, the information space and participation in a coordinated manner to crisis and threat situations".*
How is the problem framed?	**National security:** The greatest danger to the information space is posed by Russia. The strategy thus frames the problem as a danger to Latvia's national security.
Who are the perpetrators spreading disinformation?	Whereas the strategy sees Russia as the main perpetrator and biggest security threat, it also specifically mentions China and Belarus as other potential perpetrators.
What are the topics or actors being targeted?	Disinformation would mainly concern the pandemic, the war in Ukraine, and the topic of migration.
What agency is responsible?	The State Chancellery is supposed to ensure that ministries and local governments cooperate and coordinate the Latvian response to disinformation.
What role do non-state actors have?	The strategy adopts a *"whole-of-government and whole-of-society approach".* It envisions the security of the information space to be strengthened by state institutions, local governments, civil society, the private sector, academia and the general public.
Action Items (selection)	Implementation of national strategic communication, improving resilience against security threats, improving the media environment, creation of partnerships with civil society, more international cooperation

→ full document

Concept of Strategic Communication of the Slovak Republic (Slovakia)[6]

Date	**2023**
Author	Government
Responsibility of the state	Promoting transparency and quality in government communications, building up public institutions
What problem does the strategy address?	The strategy stipulates that inadequate and unsystematic state communication allows actors to systematically spread harmful content. Thus, the main problem is the state's unpreparedness for a rapidly changing information environment and contradictory statements of state agencies.
How is the problem framed?	**Social Cohesion:** It acknowledges the threat of disinformation campaigns coming from foreign countries but mainly has an internal focus on state institutions and their inadequate response to the spread of disinformation.
Who are the perpetrators spreading disinformation?	As perpetrators, the strategy specifically names Russia and right-wing extremists.
What are the topics or actors being targeted?	The strategy mostly focuses on state communication regarding the war in Ukraine and the pandemic.
What agency is responsible?	The Slovak Department for Strategic Communication, which was established within the office of the security council, is responsible for implementing the strategy.
What role do non-state actors have?	The strategy specifically states that *"building resilience requires the commitment and participation of all sectors of society."* It therefore recommends cooperation of the state with civil society, academia and the private sector.
Action Items	Creation of a body that coordinates strategic communication at a national level, raising awareness for the importance of strategic communication, improving communication and cooperation between ministries

6 Since the writing of this report, the government has updated its strategy countering disinformation. You can find the updated version here. The previous version is not online anymore.

Online Media Literacy Strategy (UK)

Date	**July 2021**
Author	Department for Digital, Culture, Media & Sport
Responsibility of the state	Mitigating false information
What problem does the strategy address?	Lack of media literacy (defined as an awareness of online materials and their potential impact together with an awareness of ways to understand the reliability and accuracy of online materials)
How is the problem framed?	**Social Cohesion:** The strategy describes how a lack of media literacy, combined with conspiracy theories and disinformation more generally, can undermine trust in the government, incite violence and even divide society.
Who are the perpetrators spreading disinformation?	This strategy does not focus on potential perpetrators but instead focuses on the potential consumers of disinformation and their media literacy.
What are the topics or actors being targeted?	The strategy mainly concerns itself with the pandemic but also briefly considers the topics of antisemitism and election interference.
What agency is responsible?	As the department that drafted the strategy, the Department for Digital, Culture, Media & Sport is also responsible for its implementation.
What role do non-state actors have?	The strategy is *"focused on supporting organisations to undertake media literacy activity in a more coordinated, wide-reaching, and high-quality way"*. With the government primarily wanting to support non-state actors, the role of non-state actors is large.
Action Items	Creation of a taskforce, creation of an online portal for media literacy resources, more coordination among agencies, public awareness campaign, training programmes for teachers, librarians and youth workers

→ full document

1.1 Zooming out: Differences and similarities between the strategies

The six national strategies countering disinformation are quite different from each other. One only has to look at the question *"What problem does the strategy address?"*: some strategies focus on specific types of disinformation like deep fakes or hybrid attacks, others on causes of disinformation like government communication, again others on solutions to disinformation like media literacy. These differing definitions of the problem take the strategies in completely different directions. As can be seen through the categorisation of *"How is the problem framed?"*, the strategies look at the problem of disinformation in varying ways. Several of them frame the problem as a threat to their national security (AT, CZ, LV), some as a threat to social cohesion (SK, UK), and one as a threat to democracy (NL). At the same time, the *"Responsibility of the state"* also differs markedly. While most of the six strategies hold the state responsible for building up public institutions that counter disinformation, only half of them also make the state responsible for mitigating false information (CZ, LV, UK). The other categories appear even less often, if at all. Concerning the question *"What role do non-state actors have?"*, most strategies actually seem to agree that a *"whole-of-society"* approach is most desirable, and that civil society is crucial for countering disinformation. However, there is much less consensus on whether the government should take a more active role, for instance in terms of countering disinformation from abroad, or remain more passive and focus on supporting civil society efforts.

At this point, a different question naturally arises: What can explain this variety? While any answer must be preliminary due to the small number of cases and due to the limited scope of this report, the timing of each national strategy countering disinformation seems to play a significant role. Some strategies were developed during the COVID-19 pandemic when conspiracy ideologies surrounding masks, vaccines or other topics seemed to threaten societal cohesion and democracy (CZ, UK). Other strategies were developed after Russia had started its war of aggression against Ukraine, which highlighted how disinformation could be a threat to national security (AT, LV, NL, SK). In addition, the geographic location of an EU member state can also help to explain the variety of strategies. Countries in closer proximity to Russia frame the problem of disinformation in terms of national security more often than countries further away: the national strategies of Austria, the Czech Republic and Latvia have a national security framing, while those of the Netherlands, the UK and Slovakia (somewhat of an exception) do not. Other factors like the political orientation of a particular government that developed the strategy certainly had an impact on the diversity of strategies as well.

Since the COVID-19 pandemic has mostly passed while the Russian war of aggression is still ongoing, those national strategies that will be published in the near future are also likely to frame the issue of disinformation in terms of national security, particularly among Eastern EU members.

2 Rethinking strategy: The case of the US[7]

Although this report predominantly focuses on the EU, a look across the Atlantic can serve as a cautionary tale. While several countries have a national strategy countering disinformation and some even have their own agency tackling disinformation, other countries have neither a strategy nor an agency. The United States illustrates this case well. It shows how the politicisation of disinformation can make the development of a national strategy or agency virtually impossible.

The United States has no unified strategy countering disinformation. There are several government agencies in charge of tackling disinformation – each agency with a slightly different focus.[8] The Foreign Malign Influence Center (FMIC) is in charge of assessing if foreign powers like Russia or China are trying to influence US politics, for instance via disinformation. If potential foreign malign influence is found, it is the FBI's Foreign Influence Task Force that conducts further investigations. At the same time, the Cybersecurity and Infrastructure Security Agency (CISA) is supposed to defend US election infrastructure from foreign malign influence while the Global Engagement Center is supposed to direct, synchronise and coordinate the counter-disinformation actions of different agencies. In theory, this division of labour has several advantages, for instance that each agency can focus on the area it has the most expertise in. In practice, however, these different mandates significantly overlap with each other so that the agencies often fight over whose approaches to follow and whose perspectives to adopt. Some agencies, such as the Department of Homeland Security, which CISA is part of, even struggled to harmonise its own intra-agency approach to disinformation.

While some may see a national strategy countering disinformation as a way of simplifying and harmonising the overlapping mandates of the varying agencies, the US is unlikely to develop any such strategy in the near future. At the most basic level, it is unclear what agency would have the final say over the structure and content of the strategy. Beyond that, the whole issue of disinformation has become so controversial that no one seems willing to even suggest the creation of such a strategy. Conservative forces fear that governmental counter-disinformation policies may be used as a cover to censor their voices. Many conservative forces therefore oppose anything having to do with disinformation. The politicisation of this issue has gone so far that it has even become controversial to use the term "disinformation", with many organisations instead using terms like "information manipulation" and "information integrity". But even so, a strategy countering information manipulation is unlikely to emerge anytime soon.

7 We would like to thank Bret Schafer, head of the information manipulation team of the Alliance for Security Democracy, whose insights informed this section.

8 DeVine, M.E. (2023). *The Intelligence Community's Foreign Malign Influence Center (FMIC).* Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF12470/2

Does that limit the ability of the US to respond to disinformation effectively? On the one hand, one may argue that such a strategy is not necessary as long as the different agencies coordinate well enough to mitigate the negative consequences of disinformation. If one has the right people in the right places, a strategy or one specific counter-disinformation agency may not be needed. Local initiatives against disinformation could also step up if the national approach ends up not being effective enough. On the other hand, many of the agencies named above face an uncertain future. Due to the politicisation of the issue, these agencies may no longer receive funding and may eventually be closed down – similarly to how civil society organisations like the Stanford Internet Observatory are already troubled. It remains uncertain how effectively the US was prepared to counter potential disinformation campaigns during the presidential election in November 2024. The extensive use of disinformation by Russia to influence elections in various parts of the world in 2024 underscores the magnitude of the challenge. Nevertheless, the case of the US does illustrate well that the political climate in some countries may simply not be conducive for drafting a national strategy countering disinformation or creating an own anti-disinformation agency. This insight underscores that it is not always policymakers who are to blame for a country not having passed an anti-disinformation strategy yet.

3 Beyond strategies: Public institutions to counter disinformation

3.1. Viginum (France)[9]

Initiative: VIGINUM
Country: France
Director / Head of Service: Marc-Antoine Brillant
Founded: 2021

VIGINUM (Service de vigilance et protection contre les ingérences numériques étrangères) is a key initiative within France's General Secretariat for Defence and National Security (SGDSN), which operates under the Prime Minister of France. Established on 13 July 2021, in response to the Macron Leaks – attempts by Russia to interfere in the 2017 French presidential election – the initiative has grown to include approximately 50 employees. They come from diverse fields such as Open-Source Intelligence (OSINT), Data Science, Political Science/Geopolitics and Digital Marketing. VIGINUM is supported by a scientific and ethical committee that publishes an annual report evaluating its activities.

VIGINUM's mission centres on recognising foreign digital interference. For VIGINUM to act, four different criteria must be fulfilled: (1) a foreign actor has to (2) use inauthentic means to spread (3) false or misleading content that (4) threatens French fundamental interests. These criteria are purposely restrictive because the agency does not want to be perceived as anything like a ministry of truth that dictates what can or cannot be said. If the last three criteria are fulfilled but the disinformation does not originate from a foreign actor, VIGINUM refers the matter to the French Ministry of the Interior. The differentiation between foreign and domestic actors is not always simple because foreign actors often operate via national proxies, requiring VIGINUM to engage in extensive analyses. So far, VIGINUM has identified and exposed networks such as the Russian "Portal Kombat" and RNN,[10] which tried to undermine Western support for Ukraine through imitation of European news and state portals, creation of pro-Russian news portals and dissemination on social media.

In addition, VIGINUM has several related tasks. It provides briefings for social media platforms, academic institutions and political parties before presidential elections.[11] It also monitors and

9 We would like to sincerely thank Laura Brincourt and Yanis Naceur from VIGINUM for having a very insightful conversation with us that helped to inform this section of the report.

10 VIGINUM. (2024). *Portal Kombat: A structured and coordinated pro-Russian propaganda network.* Secrétariat général de la Défense et de la Sécurité nationale, https://www.sgdsn.gouv.fr/files/files/Publications/20240214_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_PART2_ENG_VF.pdf

11 VIGINUM. (2022). *VIGINUM YEAR #1.* VIGINUM, www.sgdsn.gouv.fr/files/files/Publications/RA-Viginum-Annee1-32p-V20_EN_LQP-1.pdf

advises media and election oversight bodies during significant political events, such as the 2022 presidential elections, the Bataclan trials, discussions on French presence in the Sahel region, and the Russian invasion of Ukraine. In doing so, VIGINUM tries to act with a maximum amount of transparency. It employs automated data collection on platforms with over 5 million individual visitors per month in France and non-automated collection from services like VK, Telegram and Gettr. Data is stored for up to six months in two cloud centres in France and is deleted after use.[12] The scientific and ethical committee is informed about the start and extension of data collection and receives an annual data protection report. Between January and September 2022, the majority of collected data came from Twitter (32 %) and Facebook (20 %), with significant amounts also from Telegram, YouTube, Instagram and TikTok.

On the international front, VIGINUM has collaborated with the European External Action Service and German authorities, for instance when it came to the protection of the 2021 Bundestag elections. It also tries to collaborate with the OSINT community, since much of VIGINUM's work only uses open-source intelligence to increase the transparency of its work.

3.2 Psychological Defence Agency (Sweden)

Initiative: Swedish Psychological Defence Agency
Country: Sweden
Director / Head of Service: Magnus Hjort
Founded: 2022

Established in 2022 and operating under the Ministry of Defence, this initiative was founded in response to the anticipated increase in Russian disinformation during parliamentary elections. Organised into three departments – Capability Development, Operations and Administration – it aims to strengthen Sweden's defence against foreign disinformation campaigns.[13] The Capability Development department enhances psychological resilience, networks and advises both public and private institutions in Sweden. The Operations department identifies, analyses and counters disinformation from abroad, producing public reports and developing countermeasures, while the Administration department handles security, budget and other support functions. As of 2024, the organisation employs approximately 60 people.[14]

The primary mission is to identify, analyse and prevent foreign disinformation targeting Sweden or Swedish interests, such as manipulation attempts or efforts to weaken defence capabilities. Serving as the coordination centre for the anti-disinformation system, it ensures effective communication and response. Additionally, it aims to enhance the psychological resilience of the Swedish population against disinformation. During wartime, it is authorised to conduct offensive

12 Prime Minister of France. (2021). *Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères*, www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454057

13 Psychological Defense Agency. (2024). *Organisation*. Psychological Defense Agency, https://mpf.se/psychological-defence-agency/about-us/our-mission/organisation

14 Government Offices of Sweden. (2024). *Swedish Psychological Defence Agency*. Government Offices of Sweden, www.government.se/government-agencies/swedish-psychological-defence-agency

operations in hostile territories, including strategic communication and psychological operations. The focus is mainly on state-sponsored disinformation from Russia, Iran and China, with the current threat level from China considered low. However, the chief of staff has identified Islamist disinformation as an increasing threat.[15]

In 2023, the initiative's expenses amounted to approximately €12 million. The "Don't Be Fooled" campaign was launched to provide the general population with guidance on identifying and countering disinformation. In the same year, the initiative funded eight research projects and investigated the extent of Chinese disinformation targeting Swedish municipalities.[16]

The initiative places a strong emphasis on internal Swedish resilience rather than focusing solely on the perpetrators of disinformation. Psychological defence is a core strategy, continuing a tradition from World War II and the Cold War. This includes counteracting disinformation, maintaining state communication during crises and strengthening the population's defensive capabilities. Unique in its strong research orientation, the initiative is advised by the Swedish Defence Research Agency on impact and legal matters and supports the Psychological Defence Research Institute at Lund University.

To counter potential mistrust labelled as a "ministry of truth", the chief of staff recommends implementing similar institutions only in countries with high public trust and taking a differentiated approach to domestic and foreign disinformation.[17] Domestic disinformation activities might be tolerated while focusing on their impact, whereas foreign disinformation activities are not tolerated and are deterred based on military logic. The initiative is integrated into the Swedish state's defence strategy and engages in dialogue with social media platforms, though it is not tasked with enforcing measures against disinformation. International cooperation extends to the UK, US, EU Eastern StratCom, Finland and Estonia. It also provides handbooks on dealing with disinformation for journalists and communicators, adopting a security policy approach with a focus on internal resilience.

3.3 From strategy to agency: How to go from here

In the following, we aim to offer learnings and insights on our analysis of VIGINUM and the Swedish Psychological Defence Agency. The feasibility of building such organisations to counter disinformation largely depends on the specific context in which they operate. While these organisations are pioneers in establishing public institutions to combat disinformation and may provide valuable methodologies, organisational structures, and approaches, the suitability of these models for other governments is highly dependent on local conditions. This chapter high-

15 Kozłowski, A. (2024). *Combatting disinformation by state agencies: the case of the Swedish Psychological Defence Agency.* New Eastern Europe, https://neweasterneurope.eu/2024/05/07/combatting-disinformation-by-state-agencies-the-case-of-the-swedish-psychological-defence-agency

16 The Swedish Psychological Defence Agency. (2023). *Don't be fooled – Handbook*. Psychological Defense Agency, https://mpf.se/psychological-defence-agency/publications/archive/2023-12-04-don´t-be-fooled---handbook

17 Kozłowski, A. (2024). *Combatting disinformation by state agencies: the case of the Swedish Psychological Defence Agency.* New Eastern Europe, https://neweasterneurope.eu/2024/05/07/combatting-disinformation-by-state-agencies-the-case-of-the-swedish-psychological-defence-agency

lights the potential insights these organisations offer but acknowledges that adopting similar strategies requires careful evaluation, as what works in one context may not be appropriate or effective in another. We limit ourselves to a few points.

- **Transparency and Accountability:** To avoid being seen as a ministry of truth, counter-disinformation agencies ideally operate with as much transparency and accountability as possible. This could be achieved by clearly stating the circumstances under which an agency becomes involved, such as the four criteria under which VIGINUM operates. It could also be achieved by subjecting the agency to the evaluation of an independent committee. The more transparency there is, the better its work can be understood and trusted. The more accountability there is, the more the agency will be seen as a democratically legitimate institution. Both are crucial for avoiding a politicisation of the counter-disinformation agency.
- **Limited Scope:** Counter-intuitively, a more limited scope may allow a counter-disinformation agency to operate much more effectively. VIGINUM and the Swedish Psychological Defence Agency are only considering disinformation spread by foreign actors, at least partially to avoid limiting the freedom of speech of its own citizens. Countering disinformation spread by domestic actors can easily be seen as an attempt to censor the political opposition or other unwanted voices, regardless of whether that is actually the case. Only the prospect of such censorship can politicise a counter-misinformation agency and cause its demise. When devising such an agency, policymakers therefore need to strike a delicate balance between limiting its scope enough to avoid politicisation but not too much to make it become a paper tiger. Nevertheless, even a limited scope still requires transparency and accountability to ensure the agency is fulfilling its mandate properly.
- **Authority:** When it comes to establishing a counter-disinformation agency or division, one administrative question necessarily arises: what office or ministry should the agency be part of? It could be the foreign ministry, interior ministry, office of the president or prime minister, and potentially even several others. Based on our research, we advise a counter-disinformation agency to be placed under the office of the president or prime minister. Disinformation is a topic that concerns many different political areas and ministries, which can easily lead to ministerial infighting over who is responsible. Some of the experts we talked to called inter-ministerial cooperation a “daily struggle”. As part of the office of the president or prime minister, a counter-disinformation agency has enough authority to endure such struggles and to be respected as the main player in a government’s response to disinformation campaigns.

What is most important, however, is that the establishment of such an agency should only be considered if transparency, accountability, and independent oversight are fully guaranteed. Without these safeguards, even an agency with the best intentions could pose significant risks, as demonstrated by past examples in Hungary and Russia (prior to 2022). It is crucial to address these concerns to prevent potential misuse or overreach.

4 Next steps: Recommendations for action

This report's purpose has been to assess if and how countries are tackling the disinformation threat, with a focus on national strategies countering disinformation. By analysing and comparing the few publicly accessible strategies that currently exist in the EU, we hope to have given policymakers some insight into how they could design their own strategy countering disinformation. From our perspective, several key lessons emerged:

- **Comprehensive approach:** A comprehensive approach to defining disinformation is a crucial part of any strategy countering disinformation. In recent years, disinformation has increasingly taken the form of deep fakes or has been part of hybrid warfare. Any strategy trying to successfully counter disinformation needs to acknowledge this inherent complexity of the issue and needs to develop solutions accordingly.
- **Government responsibility:** Considering this complexity, the support of civil society efforts to counter disinformation is unlikely to be sufficient. The state needs to take an active role, whether that be by improving state communication (as seen in Slovakia), by fostering media literacy (as seen in the UK), or by creating a counter-disinformation agency (as seen in France and Sweden). The state has a particularly large responsibility when it comes to countering disinformation from foreign actors. As mentioned previously, however, governmental actions countering disinformation must not come at the detriment of transparency, accountability and independent oversight.
- **Citizen participation:** While efforts to devise a national strategy countering disinformation in Ireland and Germany have not concluded at the time of writing, they illustrate the importance of citizen participation. The development of the Irish national strategy has included an extensive citizen consultation period as one of its key pillars. The German efforts even involved the so-called *Forum Against Fakes*, a combination of citizen council and online participation that allowed citizens multiple ways of voicing their opinion on potential government measures countering disinformation. These examples show how citizen participation may increase the legitimacy and effectiveness of a national anti-disinformation strategy.

Each of these three lessons will hopefully help policymakers when they think about creating or updating their country's national strategy countering disinformation. Yet, the most important lesson is probably the following: awareness of the issue of disinformation is crucial. Whether it comes to national security, social cohesion or democracy, disinformation has the potential to severely harm societies. A national strategy and a government agency countering disinformation are important steps countries can take to prevent these harms and to protect their citizens.

Publishing credits & legal notice

© Bertelsmann Stiftung, November 2024

Bertelsmann Stiftung
Carl-Bertelsmann Straße 256
33311 Gütersloh
www.bertelsmann-stiftung.de

Upgrade Democracy
www.upgradedemocracy.de

Authors
Charlotte Freihse, Florian Bochert

Responsible for content
Charlotte Freihse, Florian Bochert

DOI number
DOI 10.11586/2024161

Citation:
Freihse, Charlotte and Florian Bochert. 2024. *Up to the challenge? Strategies to counter disinformation in the EU, UK and US.* Bertelsmann Stiftung, Gütersloh.

Design
nach morgen

Picture credits
© Freedomz – stock.adobe.com