SPOT ON

Stormy-Annika Mildner, Elisabeth Nöfer, Margaryta Letiago

The Truth and Nothing but the Truth: EU and German Responses to Disinformation in Times of Crisis and War

May 2023

Disinformation is increasingly a threat to democratic decision-making worldwide. In a changing geopolitical environment, which is more and more marked by instability, conflict, and war, disinformation campaigns are used by foreign adversaries to destabilize societies by manipulating citizens and creating distrust in democratic institutions. However, the threat to democracies does not only come from outside but also from within societies, many of which are struggling with polarization and illiberal tendencies. New technological developments such as natural language processing tools driven by Artificial Intelligence (AI) (e.g., ChatGPT) and AI-powered image generators (such as Midjourney) have the potential to both further accelerate and fight the spread of disinformation. While Germany and the European Union (EU) have intensified their efforts to counteract the disinformation environment, more needs to be done – particularly in light of upcoming elections such as the vote for the European Parliament in 2025.

A well-informed and educated electorate is a prerequisite to a flourishing and functioning democracy. In view of current technological advancements and manifold challenges, ranging from a deepening climate crisis, economic recessions, pandemics, and migration to tectonic shifts in the geopolitical order, disinformation has become a cause for serious concern. Disinformation has the potential to destabilize societies and democratic decision-making. It can polarize public opinion, foment anger, exacerbate existing social conflicts, weaken social cohesion, and undermine trust in democratic institutions and processes.

According to a 2022 survey of the Pew Research Institute across 19 countries in North America, Europe, and the Asia-Pacific, the spread of false information online is the third greatest concern overall among the issues tested: A median of 70 percent view the spread of false information as a top threat. The Deloitte Cyber Security Report 2021 found that 75 percent of the surveyed decision-makers from business and politics consider fake news a high risk for the German population (third in the ranking of cyber risks).

Stakeholders across different levels are intensifying their efforts to address the challenge of disinformation, from the EU institutions and the German Federal Government to civil society organizations, research initiatives, and social media platforms. While this policy brief focuses primarily on government initiatives, it is worth noting that technology companies have also stepped up their efforts by monitoring elections, improving content moderation in some countries, removing fake accounts, and implementing features such as providing information about the publisher below videos with news content from government-funded or publicly funded publishers.

What is Disinformation?

Disinformation is commonly understood as a form of false information. According to First Draft News, a leading non-profit organization, the disinformation environment can be categorized into different types of information based on three elements, namely: 1. the different types of content that are created and shared, 2. the motivations of those who create the content, and 3. the way the content is disseminated. Based on these elements, content can be labeled as disinformation, misinformation, or malinformation: Disinformation is false or misleading information that is intentionally disseminated with the intent to cause harm. Misinformation is false or misleading information that is spread by a person or institution unaware of their error and, therefore, not disseminated with the intent of causing harm. Malinformation describes genuine information that is shared or disseminated for

Aspen Institute Germany

personal or corporate interests to intentionally cause harm.

A disinformation campaign is a targeted, organized information attack on a government, institution, company, or individual in which disinformation is used on a large scale with the purpose of deliberately deceiving or misleading individuals. The attack can originate from a host of actors, including governments, state-backed entities, extremist groups, and individuals. Tactics include utilizing selective information, creating false connections between facts, and distorting coherent explanations to falsely attribute blame to adversaries.

Disinformation has become a cause for serious concern

Other terminology, which is sometimes used interchangeably – albeit with shifting and overlapping definitions – are "fake news" and "propaganda." The term "fake news" is often used to refer to false and misleading news articles. At the same time, it has been captured by anti-democratic populists against independent media. Therefore, it is less precise and often politically highly charged. Propaganda can be defined as information, ideas, and/or images which are spread with the intention of influencing people's opinions. Disinformation can be part of this.

The Increasing Risk of Disinformation

Disinformation is not a new phenomenon but has gained prominence over the last years, especially after Russia tried to alter the outcome of the presidential elections in the United States in 2016 through social media disinformation campaigns. Disinformation also played a role in both Germany and the EU in the run-up to the 2017 Bundestag and the 2019 European elections. The full extent and the direct impact of disinformation cannot be accurately determined due to many gray zones, hidden channels, lack of access for researchers to social media platforms, and challenges in user research. This, however, does not make it less of a threat.

The dramatic consequences of disinformation could be witnessed during and after the 2020 presidential elections in the United States. Among them were false claims that the "elections were stolen" from the incumbent Donald Trump by the Democratic candidate Joe Biden, assertations that the election process was rigged and voting machines did not work properly, as well as false claims alleging election fraud. Disinformation, conspiracy theories, and false narratives were important factors in the lead-up to the attack on the U.S. Capitol on January 6, 2021.

The disinformation environment also gained significant momentum during the COVID-19 pandemic, when much of the world moved online and uncertainty about the pandemic, treatment, and vaccinations were high. Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization (WHO), warned in February 2020: "Fake news spreads faster and more easily than this virus and is just as dangerous." He continued: "[W]e're not just fighting an epidemic; we're fighting an infodemic," referring to an information ecosystem that, due to an overwhelming amount of disinformation, could no longer function as a trustworthy source of information.

Since then, the awareness of disinformation and its dangers has risen considerably. However, while many governments, including Germany and the EU, have set up counter strategies, the phenomenon is nowhere near under control. On the contrary, the changing geopolitical environment is expediting the threat of disinformation campaigns. Russia's war against Ukraine not only ended a period of peace, stability, and prosperity in Europe, but it also fuels the systemic rivalry between democracies and autocratic regimes. Democracy and freedom worldwide are in a historically weak moment, according to Freedom House's annual report. Antidemocratic alliances are gaining ground.

Attempts to influence public opinion in Germany, Europe's largest economy, which has long been a target for Russian disinformation, has reached unprecedented heights since Russia's invasion of Ukraine. Using a mix of internet resources, social media, satellite television, and traditional radio and television broadcasting, Russian actors distribute and amplify large amounts of disinformation narratives via text, video, audio, and images to advance their interests. The strategy has been described as a "firehose of falsehood" propaganda model, relying on mass, speed, repetition, and pushing the same message from multiple sources. This pattern is not exclusive to Russian disinformation campaigns and can be observed in disinformation efforts by other actors as well.

Chinese disinformation campaigns have also gained momentum, showing a significant investment by the Chinese government, for example, politicizing the COVID-19 pandemic. China often acts in unison with Russia on disinformation, as a recent study by the German Marshall Fund's Alliance for Securing Democracy shows. For instance, the Chinese Ministry of Foreign Affairs as well as Chinese state media amplified the unsubstantiated claim made by Russia that Ukraine was involved in the development of biological weapons in a network of laboratories connected to the United States. As China and Russia have deepened their relationship, they are aligned in spreading anti-American and anti-NATO narratives. A commentator noted that this "should be seen as part of a broader project to reshape the global information landscape to favor the Kremlin and Beijing's authoritarian political projects."

Disinformation campaigns have become a popular instrument in the domestic and foreign policy toolbox of many authoritarian regimes, such as Russia and China, as well as countries with authoritarian tendencies – also in the EU. The Heinrich Böll Stiftung, for example, found in an analysis of Hungary that home-grown disinformation builds on local media empires with tactics that look remarkably similar to foreign disinformation. Romania faces similar challenges, as well as Bulgaria, where pro-Russian Bulgarian propaganda "is related to Russia's broader disinformation efforts across Europe, but ultimately serves local interests by targeting political or business rivals or the work of civil-society non-profits," as the non-profit news portal Coda Media reported. Disinformation is also rampant in many EU candidacy countries, such as those in the Western Balkans. While Russia's (and in part China's and Turkey's) influence is particularly strong in several Western Balkan countries, disinformation is by no means an exclusively externally driven phenomenon, as several studies point out. Rather, the majority of disinformation is produced and disseminated by domestic actors for domestic purposes, as a study commissioned by the European Parliament found in 2021.

Technology and Disinformation

The plummeting cost of producing and disseminating information, along with the proliferation of online media channels, are significant drivers of disinformation. Social media platforms such as Facebook, Twitter, YouTube, and TikTok, as well as gaming apps like Discord or messenger services like Telegram, are not the cause of the disinformation environment but provide fertile ground for the creation and dissemination of disinformation. A meta-study from 2021 reviewing empirical evidence found that "(a)lthough social media is unlikely to be the main driver of polarization, we posit that it is often a key facilitator." The algorithmic logic and connectedness of social media and the cataclysm of the professional media business model have facilitated the rapid and enduring spread of disinformation.

This is particularly problematic as social media platforms increasingly serve as a source of information for news. According to the Reuters Institute Digital News Report 2022, 32 percent of German internet users in the age of 18 to 24 obtain news via social media, and for 11 percent of adult internet users, social media is the most important news source. Especially younger generations tend to use the Internet – and social media in particular – as their main source of news. The Internet was the most important news source for about 80 percent of the 18- to 24-year-olds surveyed in Germany. Of all information sources, social media served as the main news source for 39 percent of this age group (2019: 22%). In comparison, this share amounted to only eleven percent of all online consumers surveyed (2019: 10%). Eighteen percent of the 18- to 24-year-olds surveyed in Germany attained news exclusively via social media (all adults: 5%). According to the Digital 2022 Global Overview Report by the social media tool Hootsuite and the agency We Are Social, internet users aged 16 to 64 worldwide spent an average of 2.28 hours per day on social media platforms in 2021. In the age group 16 to 24 it is even 3.13 hours for female users and 2.43 for male users.

The changing geopolitical environment is expediting the threat of disinformation campaigns

Advances in generative AI, such as large language models (LLMs) like ChatGPT, have the potential to further exacerbate the problem as the production of disinformation becomes faster, cheaper, and more nuanced in its messages. AI-based multimodal models can automate the production of text, images, videos, voices, and music, making disinformation faster, cheaper, and more adaptable to different languages and contexts.

Disinformation can often be detected by native speakers due to spelling mistakes, poor syntax, or inconsistently applied dialects. The advent of AI has the potential to substantially enhance the persuasiveness of disinformation messages because content can be more easily adapted to different languages or contexts with the help of AI. Although measures have been implemented within ChatGPT to counter the production of disinformation, these safeguards have been found to be susceptible to circumvention. Concerns have also emerged regarding the production of convincing imagery, as images have a powerful emotional

impact. Photorealistic, synthetic imagery can stage an incident with high plausibility. Such AI-generated images cannot be traced back to their original source, although a fact-check through a reverse image search helps to trace their original appearance.

On the other hand, AI can also contribute to increasing resilience against disinformation. Platforms already work with automated detection and takedown of unwanted content, which helps to cope with the amount of content and remove the psychological strain on human content moderators (conversely, data sets and algorithms, especially for AI with ethical safeguards, still have to be annotated and checked by human workers). AI-based tools and LLMs can be utilized by fact-checkers to identify and detect instances of disinformation.

Challenges in the Fight against Disinformation

Countering disinformation faces several challenges.

1. Legal Context and Freedom of Speech: First, liberal democracies, which usually enshrine freedom of expression and information in their basic law/constitution, are vulnerable to disinformation "by design" as the rule of law rightly grants individuals, the media, and foreign actors considerable freedoms in the production and dissemination of expression. This also includes nonsense, deception, and, to a certain extent, even lies if they turn out later to be false. In Germany, for example, there is no specific law prohibiting the dissemination of disinformation. Offline and online offenses that are illegal according to the German Criminal Code (StGB) are prohibited, such as sexual harassment and hate speech in the form of defamation or incitement to hatred (Volksverhetzung). Accordingly, anti-semitic conspiracies are categorized as illegal incitement to hatred. However, identifying illegal content is not always easy. "Dog whistling" illustrates – a kind of coded language that only the "insider" understands – provides a good example of why it can be difficult to identify. It is a gray area, as topics are alluded to without explicitly naming them. A "humorous" meme culture has developed in the far-right around such illegal statements.

Therefore, the public largely relies on private social media platforms and the enforcement of their community rules. As such, the German Network Enforcement Act (NetzDG) obliges social media platforms to "notice and takedown" illegal content while maintaining the principle of exemption from liability. The Digital Services Act (DSA) will replace the NetzDG and will require platforms to act against "illegal content" in a self-regulatory approach. What constitutes illegal content is determined by the individual Member States.

With generative AI, the production of disinformation becomes faster, cheaper, and more nuanced in its messages

The German state media authorities also play an important role in countering disinformation. However, they can only regulate telemedia with journalistic editorial contents disseminating news and political information. The nationwide ban on Russian state media RT in Germany, for example, was first imposed by the media authority Berlin-Brandenburg because it had not obtained a broadcast license. Media authorities cannot regulate social media platforms *(media intermediaries)* because they are exempt from liability for user content.

2. Cognitive Drivers: It is important to understand the cognitive drivers that make disinformation persuasive. People are prone to believe falsehoods when it confirms their preexisting beliefs. Believing conspiracy theories can be a strong driver in the expression of identity and in-group formation. This has been shown to occur even in people with high levels of education. Humans are also, on average, more likely to spread false news than truths. According to a study by researchers from the Massachusetts Institute of Technology (MIT) published in Science in 2018, truth took up to six times as long as falsehoods to reach an audience on Twitter, and false information reached more people. At the same time, some cognitive drivers also have a positive impact on the fight against disinformation. For example, most recipients in Germany have been found to be skeptical of news content on social media, which also applies to intentionally misleading stories.

3. Societal and Political Environment: Even though a causal relationship between the consumption of disinformation and changes in behavior and attitudes is hard to establish, disinformation has an impact above all where there is a fertile breeding ground, such as in highly polarized societies and countries with ethnic tensions. A partisan media landscape that propagates home-grown disinformation, as well as low levels of trust, further increases vulnerability to disinformation. A diverse, high-quality, independent, and trusted media system acts as a shield against disinformation. It contributes to ensuring that citizens have access to a broad range of viewpoints and reduces the influence of specific interest groups. Especially public service media have been found to do a good job of increasing democratic resilience.

Regulatory Approaches in the EU

The first policy actions by the EU were launched in the course of Russia's invasion of Crimea in February 2014. At an EU summit in March 2015, EU state leaders assessed the annexation of Crimea as illegal and stressed "the need to challenge Russia's ongoing disinformation campaigns." In the same year, the East StratCom Task Force was founded as a part of the Strategic Communications and Information Analysis Division of the External Action Service (EEAS) with the objective of countering Russia's ongoing disinformation campaigns. It hosts the website "EU vs. Disinfo," where it publishes trends and narratives based on Russian media monitoring, promotes EU policies in the Eastern Neighborhood countries, and aims to strengthen pro-European media outlets in the region. The "Action Plan on Strategic Communication," which was prepared by the European External Action Service (EEAS) and published on June 22, 2015, proposed three objectives: First, "effective communication and promotion of EU policies and values towards the Eastern neighbourhood," second, the support of "independent media" within Member States and in the Eastern neighborhood and third, "increased public awareness of disinformation activities by external actors, and improved EU capacity to anticipate and respond to such activities." In April 2016, the adoption of a "Joint Framework on Countering Hybrid Threats" marks a more consolidated European agenda towards foreign actors and security. The "Action Plan against Disinformation" of December 5, 2018 stresses the need to intensify strategic communication campaigns, strengthen the East StratCom's data analysis skills, and create a "Rapid Alert System" on disinformation that facilitates the communication between Member States and EU institutions in this matter. The latter was established in March 2019.

AI can also contribute to increasing resilience against disinformation

As the governance of private platform companies significantly determines how successfully disinformation content spreads, the EU has also intensified its regulatory efforts in this regard. Platform providers have, so far, largely not been held responsible under the liability exemption. This means that under current legislation in the EU, all "providers of information society services," including social media platforms, are freed from responsibility for third-party content if they are not aware of illegal activity or content. The liability exemption goes so far that in accordance with the e-Commerce Directive, Member States are prohibited from imposing a general obligation on platform providers to monitor content for illegal activities actively. While this safeguard enhances freedom of expression and independence from state intervention, it also places constraints on combating illegal activities.

In 2018, the EU established a voluntary Code of Conduct on Disinformation, which was strengthened in 2022. The Code, which to date has 34 signatories, obliges platforms to de-monetize advertising that includes disinformation, label political ads, grant independent researchers more access to platforms' data, and cooperate with fact-checking institutions, among other obligations (i.e., reviewing measures to reduce fake accounts, bot-driven amplification, and deep fakes). The signatories also commit to publish reports on how they are tackling online disinformation. The first, which was due in February 2023, was, however, met with considerable criticism by civil society organizations. For example, the European Fact-Checking Standards Network (EFCSN) found that "the platforms have fallen short of their commitments."

In addition, the DSA, implemented in 2022 with effect as of February 2024, requires large platforms to implement clear terms of service and transparent content moderation policies. They also have to establish efficient complaint-handling mechanisms, empowering users to report problematic content. Independent authorities will monitor platforms' compliance with the new rules. However, the DSA maintains the liability exemption, i.e., the general principle that platform providers are not responsible for, and therefore not obliged to act on, hosted content that is illegal or may cause harm.

The EU is also working on the "Proposal for a Regulation on the Transparency and Targeting of Political Advertising" (published in 2021, it is currently in the trilogue phase between the Commission and Council). The legislation is motivated by the exploitation of targeted and covertly financed advertising to social media users and aims at mitigating risks of electoral interference. As such, it intends to limit the use of personal data for political advertisements, prohibits certain forms of targeting, and aims to impose transparency obligations on providers of political advertising services. The proposal strikes a sensitive balance between freedom of expression and

countering disinformation. It is planned to be implemented before the elections to the European Parliament in 2024.

The proposed EU Artificial Intelligence (AI) Act is intended to decrease harm from AI-based systems, including language models and generative AI like ChatGPT. It introduces a governance structure to hold risky AI-based systems deployed in the EU accountable to protect fundamental rights, democracy, the rule of law, and safety. However, it is important to note that topics with societal ramifications and the potential to undermine democracy are not explicitly included within these provisions. Therefore, the AI Act has been criticized for falling short in countering information manipulation.

A more effective and coordinated response is needed to safeguard the foundations of liberal societies

Last but not least, the proposed European Media Freedom Act (EMFA) touches upon the issue of disinformation as it aims to increase users' access to quality content on social media. It aims to ensure media pluralism and editorial independence, including stable funding of public service media and the transparency of media ownership. It also targets very large online platforms' (VLOPs) gatekeeping power over access to the content of traditional media. Once implemented, the act will also increase the leverage of national media authorities, who will form an oversight board at the EU level.

The Way Forward

Although awareness of the dangers of disinformation is growing rapidly, the preceding overview shows that a more effective and coordinated response is needed to safeguard the foundations of liberal societies. As such, concrete measures against disinformation must always be viewed as part of a broader societal, economic, and political framework.

Beyond Fact-Checking: Initiatives to fact-check and debunk false news must not only continue but be strengthened. At the same time, it is important to keep in mind that these efforts are not effective in every case due to cognitive drivers. Thus, measures need to account for the motivations of individual media user groups. An interesting approach is the project "Der Fabulant" from the news portal Hessenschau, which belongs to the German television and radio broadcasting company Hessischer Rundfunk. The state-funded project provides humorous contributions to conspiracy narratives with the aim of debunking them. However, such initiatives need to be better tested in terms of impact.

Beyond Debunking: Debunking and prebunking are two valuable approaches in combating disinformation. Debunking involves the systematic identification and exposure of false or misleading information, providing evidence-based corrections to falsehoods that have already been disseminated. This approach helps to restore accuracy and mitigate the spread of disinformation. Pre-bunking focuses on proactively inoculating individuals against disinformation by providing them with the necessary tools to recognize and resist false narratives before they encounter them. By preemptively exposing people to the techniques and strategies employed in disinformation campaigns, pre-bunking empowers individuals to critically evaluate information, fostering resilience against manipulation. By combining debunking and prebunking strategies, government institutions that engage in public communication can effectively counter disinformation and minimize its harmful effects on individuals and democratic processes.

Media Literacy and Education: Complex digital information environments require special skills to navigate them. Media and Information Literacy (MIL) has been found to be one of the main solutions against the threat of disinformation in democracies, as these skills encompass the ability to access, analyze, evaluate, and create media. MIL should be integrated into school curricula, extended to higher education and formal training, and draw inspiration from successful initiatives in countries like Finland, the Baltic states, and Estonia. Innovative approaches need to be developed that cater to diverse societal groups, including marginalized populations, and address private media consumption and the needs of out-of-school adults. Periodic *#EUvsDisinfo Hackathons* could be a format to develop creative and competitive MIL ideas.

AI Literacy: MIL must keep pace with technological developments. As such, they should educate users about the functioning, strengths, limitations, and capabilities of generative AI. Critical thinking skills enable citizens to discern and evaluate chatbot-generated responses or photorealistic imagery better.

Research: Society needs to invest in research and data collection to improve understanding of the structure, scope, spread, and impact of disinformation. This requires access for researchers while respecting users' privacy rights. Their knowledge should inform and shape targeted strategies against disinformation. Collaboration between academic institutions, research organizations, and policy-makers, are more promising than siloed approaches.

Platform Responsibility: Platform companies must take on greater responsibility for content moderation. While they should take a more assertive approach in fighting disinformation, they also must avoid over-blocking. For example, Ukrainian journalists' fact-checking was falsely considered as hate speech by some social media platforms, which undermines constructive efforts. Precise and transparent guidelines, as well as complaint processes, must be established to ensure consistent and impartial decision-making regarding content removal. In addition, abilities in non-anglophone languages and understanding of cultural contexts need to be significantly improved.

Governance: Measures against disinformation must be integrated into the institutional fabric of governance at all levels. This ensures continuous adaptation and evolution of strategies to counter disinformation in a rapidly changing landscape.

Civil Initiatives: Civil initiatives have made notable progress by developing innovative and effective approaches. However, they frequently encounter difficulties due to limited and short-term funding. It is essential to evaluate these initiatives and provide continuous funding to institutionalize successful projects while ensuring their independence from state influence.

Collaboration and International Cooperation: Strengthening transnational collaboration with EU partners and other countries is vital for a unified and effective response to disinformation, as disinformation often spreads across borders. It is crucial to exchange best practices and lessons learned and coordinate efforts to counter cross-border disinformation campaigns.

Elisabeth Nöfer
Program Officer in the Digital Program, Aspen Germany

Dr. Stormy-Annika Mildner
Executive Director, Aspen Germany

Margaryta Letiago
Program Assistant in the Digital Program, Aspen Germany

This text represents the personal views of the authors. The authors do not speak on behalf of the institution which they are associated with.

About this series

This publication is part of the event series Democracy 2.0, hosted by the Aspen Institute Germany in partnership with Microsoft Berlin. The two-part workshop series brings together international experts on wartime digital operations from politics, business, academia and civil society. More information can be found here.

The Aspen Institute Germany would like to thank intern Frances Eden for her valuable contribution to the fact-checking process.

Publisher: Aspen Institute Germany e.V.
Editor: Dr. Stormy-Annika Mildner
Design & Layout: Jahongir Zaynobiddinov