FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

DECEMBER 2025

Information Manipulation and Interference Countermeasures in the EU: Enhancing Resilience through a Whole-of-Society Approach

Sofia Linna
Defence & Security Research Department

RESEARCH REPORT

FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

Defence & Security Research Department

Written by: **Sofia Linna**
Supervised by: **Elise Alsteens and Jennifer Kalushi**
Edited by: **Theodora Posta**

FINABEL's Research Reports are concise, research-driven publications designed to keep Europe's defence community informed about the latest strategic, military, and geopolitical developments. Released three times per week, these short-form papers offer timely analysis on emerging trends affecting European land forces. Each Research Report is produced by the researchers of FINABEL's Permanent Secretariat, in the goal of supporting decision-making across the European defence landscape.

RESEARCH REPORT

Introduction

In the current media landscape, false and misleading information circulate on a regular basis with the intention to harm individuals, governments, and organisations. Since 2015, the European External Action Service (EEAS) has taken a leading role in identifying, analysing, and responding to foreign disinformation as a result of increased pro-Kremlin propaganda (European Union External Action, 2025). However, other actors also take part in countermeasures aimed at countering disinformation and similar activities. Such actors belong to various policy fields, such as the media and education sectors (García & Oleart, 2024). Additionally, the increased use of artificial intelligence (AI) in information influence activities makes it increasingly difficult to discern false information from truth. This development complicates the EU's responses to not only foreign disinformation, but also to the spread of inaccurate information by EU citizens.

As a result, this paper argues that the EU faces the complex task of developing efficient responses to foreign disinformation while ensuring that information control measures, such as censorship, do not create spill-over effects that risk undermining fundamental rights, free media, and impartial education. Some disinformation cases involve both external and internal actors and thus, the EU must consider specific rights outlined in the Charter of Fundamental Rights before addressing them. A central part to freedom of expression is the 'right to be wrong': if citizens spread false information without malign intentions, it is a democratic right (Chandler Institute of Governance, 2024). The EU must therefore enhance its ability to both counter disinformation campaigns and enhance EU citizens' resilience to such campaigns through for example media literacy activities, without infringing upon citizens' fundamental rights.

Since the Cold War period, Sweden has worked on countering Foreign Information Manipulation and Interference (FIMI) activities through its psychological defence strategy. Psychological defence broadly refers to "the resilience of a country to foreign propaganda" (Pamment & Isaksson, 2024, p.7). This paper argues that certain elements of Sweden's psychological defence structure complement current EU strategies that aim to counter FIMI and boost EU citizens' resilience. More specifically, Sweden has managed to create a system that safeguards against spill-over effects from countermeasures aimed at foreign information manipulation threats to citizens' freedom of expression. The Swedish Psychological Defence Agency's strategy consists of deterrence and resilience, along with strong cooperation structures with other government agencies, civil society, and the media (Pamment & Isaksson, 2024).

1. The Evolution of Information Manipulation and Interference

Today's information threats can be characterised as 'hybrid' and 'complex' in the sense that they involve both external and internal actors. Information and communications technologies are increasingly being used by state and non-state actors that aim to distort truth and divide Member States through harmful activities such as disinformation (Ördén, 2019). Domestic and foreign disinformation differentiate in terms of scale and strategies: domestic disinformation can be created and spread by a heterogenous mix of actors, such as conspiracy theorists, politicians, and lobbyists, while foreign disinformation activities usually consist of state-

backed actors (Wagnsson et al., 2025). These actors often create mirror sites, clones of official news and government websites, to spread false information. This is especially prevalent in Kremlin-led disinformation campaigns against other countries (Pamment & Tsurtsumia, 2025). Disinformation activities by hostile foreign actors are usually subject to larger budgets compared to domestic media outlets, which in turn allows foreign malign information influence actors to take part in hybrid warfare strategies (Wagnsson et al., 2025). While disinformation refers to the deliberate dissemination of false information, misinformation usually refers to misunderstandings. For example, when an individual shares false information that he or she genuinely believe is true, it is considered misinformation (Psychological Defence Agency, 2025).

Russia and China are two major creators and disseminators of FIMI activities. In the latest report of the EEAS from March 2025, 505 disinformation incidents were analysed between November 2023 and November 2024. The report found that both Russian and Chinese FIMI actors targeted 90 countries around the world, with Ukraine, France, and Germany experiencing the largest amount of disinformation operations during the analysed period (European External Action Service, 2025). Although Russia and China are two leading actors in the creation and dissemination of foreign information manipulation activities, the EU is also entrusted with addressing similar activities undertaken by domestic, EU-based actors (Wagnsson et al., 2025). As a result, the EU must develop policies that also address such actors. The following section will therefore present relevant policy developments that aim to counter both foreign and EU-based disinformation threats.

2. Policy Developments

2.1 The Action Plan on Strategic Communication and the East StratCom Task Force

In March 2015, the European Council called upon the EU's Member States to step up their efforts in countering increased Russian propaganda by preparing an Action Plan by June (European Council, 2015). The June 2015 Action Plan on Strategic Communication consisted of three main objectives. First, establishing "effective communication" and promoting "EU policies and values" in Eastern countries bordering the EU. Second, strengthening "the overall media environment" through, for instance, enhanced support for free media. Third, enhancing the public's knowledge of–and resilience to–information influence activities such as disinformation by non-EU actors (European External Action Service, 2015, p.1). During this period, the EU also established the East StratCom Task Force, operating under the Strategic Communications and Information Analysis Division of the EEAS (European External Action Service, 2021).

The Task Force's key mission is to facilitate coordinated efforts in countering disinformation activities by hostile foreign actors such as Russia (European Parliament, 2015). More specifically, the East StratCom Task Force consists of communication experts with Russian language skills that focused on monitoring and analysing Russian media outlets. The Task Force collaborates with a broad range of actors such as experts, non-governmental organisations (NGOs), think tanks, and journalists to expose the creation and dissemination of disinformation (European Parliament, 2015). One key project of the Task Force is EUvsDisinfo, which aims to expose disinformation cases, increase awareness, and enhance citizens' resilience

towards information manipulation activities online. Initially, the project focused on pro-Kremlin disinformation, but it soon expanded its scope of activity to address disinformation in other contexts, such as information influence activities in the Balkans and the Southern neighbourhood of the EU (EUvsDisinfo, n.d).

2.2 The 2018 Action Plan against Disinformation and the Code of Practice

In December 2018, the European Commission (EC) voiced the need to step up efforts for countering hybrid threats in the areas of cybersecurity, communication, and counterintelligence (European Commission, 2018). This led to the development of the 2018 Action Plan against Disinformation, which built on previous initiatives by the EC and activities by the East StratCom Task Force. The Plan emphasised the need to further integrate civil society and the private sector in countering online disinformation (European Commission, 2018). One key policy development during this period was the first ever Code of Practice on Disinformation: leading actors in the advertisement and tech industries agreed on voluntary-imposed standards for fighting disinformation (European Commission, 2022a).

An assessment of the Code was published by the EC in September 2020, within which the report highlighted the need to further improve efforts by developing "transparent key performance indicators" (European Commission, 2020a, para.10). The assessment also voiced the need to obtain more relevant data by signatories to monitor timelines. However, access to such data is dependent on platforms' willingness to share such information with the EC and public authorities (European Commission, 2020a). In addition, the self-reporting of signatories decreased the transparency in progress reports since no neutral third parties could verify the information (Carnegie Endowment for International Peace, 2020).

2.3 The Rapid Alert System, the European Digital Media Observatory, the European Democracy Action Plan, and the Digital Service Act

The EU launched its Rapid Alert System (RAS) in March 2019, which constitutes one of the four pillars of the 2018 Action Plan in countering malign information influence. One key feature of RAS is the possibility for EU institutions and Member States to share disinformation insights on a digital platform (European External Action Service, 2019). Initially, RAS only had a modest impact based on a lack of trust and differences between Member States' perceptions of the "threat of disinformation". On the other hand, smaller cooperation coalitions have emerged between actors with similar opinions and strategies in disinformation countermeasures (Carnegie Endowment for International Peace, 2020). The need for a better integrated, interdisciplinary cross-border network led to the creation of the European Digital Media Observatory (EDMO) project, which was officially launched in June 2020, with the aim to provide fact-checking services through independent experts and coordinate disinformation countermeasures with other actors such as media houses and literacy experts, with the goal of producing recommendations for policy makers (European Commission, 2025a). In terms of media literacy activities, the project has held 1.181 training sessions, hosted 134 public campaigns, and developed 477 educational tools and materials in this area (EDMO, 2025).

On 3 December 2020, the EC emphasised the need to strengthen the EU's resilience in the context of accelerated threats against democratic principles in its presentation on a new plan under the name of the European Democracy Action Plan. The Plan emphasises measures in three main areas: (a) free and fair elections, (b) media freedom and pluralism, and (c) disinformation countermeasures (European Commission, 2020b). Among other things, the Commission presented its vision to restructure the previous Code of Practice and create a "co-regulatory framework" of specific accountability measures and obligations for actors that shape the environments on digital platforms. The reason for this overhaul has its background in the Commission's latter proposal for a Digital Services Act (DSA), which was presented on 15 December 2020. The DSA was viewed as the answer to the growing need for "more fairness, transparency and accountability for digital services' content moderation processes, ensuring that fundamental rights are respected ... [and] comprehensive rules about online advertising, including targeted advertising" (European Commission, 2020c, p.2).

2.4 A Strengthened Code of Practice and the Enforcement of the Digital Services Act

The 2018 Code of Practice was strengthened in June 2022 after another assessment by the EC. In its assessment, the EC highlighted horizontal issues, such as the scope of action and participation. While the focus was on disinformation in information influence activities, the EC voiced the need to also pay attention to the growing risks of misinformation. In addition, the EU could benefit from a broadened participation by new signatories such as providers of private messaging services and more actors from the advertisement sector (European Commission, 2021). As a result of the assessment, the 2022 Code of Practice was strengthened through the involvement of new actors such as advertisers, tech companies, and auditing bodies. In addition, 43 commitments were established and the actions taken under the Code were to complement the DSA (European Commission, 2022b).

The DSA was formally adopted by the Council on 4 October 2022 and entered into force a few weeks later, on 16 November. The development of the DSA was an important milestone for the EU in terms of safeguarding fundamental rights online, countering illegal content online, and providing online transparency measures for users. The Act is, therefore, an updated version of the previous e-Commerce Directive by allowing for up-to-date regulations (European Commission, 2024).

3. Discussion: Balancing Between Coherent and Efficient Disinformation Countermeasures through Engaging Multiple Fields of Practices and Enhancing EU Citizens' Resilience

This paper seeks to prove that the EU has developed and refined multiple institutional mechanisms with the aim to counter disinformation, raise awareness about misinformation, and enhance EU citizens' resilience to information manipulation and influence activities. The DSA and the Code of Conduct on Disinformation reflects the willingness to move away from voluntary-based standards and instead introduce binding commitments that target key stakeholders in industries where disinformation and similar harmful activities take place. In addition, the EU has shown its support for fundamental rights through the DSA and activities within EDMO. Albeit these accomplishments seem solid, it is important to problematise how the very

notion of 'security' is constructed within the EU. It is also necessary to discuss the differences in interests and policy preferences amongst fields of practices as well as safeguards against spill-over effects from FIMI countermeasures to the democratic communication activities of EU citizens.

Policymakers operating in the security and defence–as well as internet communities–tend to define security in "abstract procedural terms". The two key dimensions in this perspective are, therefore, coherence and efficiency. On the other end of the spectrum are the media and education sectors, where security-related values are related to "perspectivism". In broad terms, this means that security-related values are constructed by citizens and their perspectives (Ördén, 2019, p.422). Since 2015, the EU has launched multiple activities where external actors, such as communication and language experts, are tasked with identifying and countering foreign information manipulation. This is particularly evident in the East StratCom Task Force, which focuses on "promoting EU policies towards the Eastern Neighbourhood", through the EEAS. However, this approach has been criticised for prioritising efficiency over supporting a variety of different perspectives (Ördén, 2019, p.431). At the same time, the definition of disinformation is ought to be somewhat polarised depending on the actors involved in various fields of practices on the EU level which, in turn, leads to a competition between policy preferences (see Table 1).

Table 1. EU Preferences in Countering Disinformation Based on Fields of Practices, Interests, and Actors

Field of Practice	EU Public Policy Preferences	Interests	Actors
Security and Defence	Disinformation is broadly defined and is part of hybrid warfare strategies. Focus is on coordinating actors and policies to control the information environment.	• Raise awareness of hybrid threats amongst policy makers (including the national level); • Ensure resources for monitoring activities and the ability to steer EU strategic communication.	Institutional: e.g. EEAS (East StratCom)
Media and Communication	EU law is used to establish new journalistic regulations at EU or national level.	• Protect the media business model from social media; • Attempt to gain EU support for new business models.	Federations of journalists, public broadcasters, federations of media companies
Education	Limited: lack of competence on the EU-level.	• Recognise the importance of education; • Demand new EU action in citizen education.	Teachers trade unions, life-long education
Citizens' Rights	Disinformation's effect on political participation and regulatory consequences.	• Limit internet companies' market power; • Promote new forms of de-centralised communication; • Enshrine new rights.	Access Now, European Consumer Organisation (BEUC)

Source: García & Oleart (2024, p.1403).

The EU faces the challenge of creating efficient defence and security mechanisms for identifying, analysing, and countering disinformation and other information manipulation activities without undermining free media and impartial education systems. More specifically, the EU needs to ensure that the effects of measures aimed at combating state-sponsored FIMI do not spill over into the regulation of democratic speech by "ordinary citizens". Controlling the information environment temporarily. through for example censorship, or steering strategic communication, may be favourable only under certain conditions, such as large-scale *foreign* disinformation campaigns conducted by Russia and China. Such measures are mainly linked to the security and defence sector and its way of defining security in "abstract procedural terms" (Ördén, 2019, p.422).

On the other hand, the EU has been criticised for its lack of attention to strategies that aim to enhance EU citizens' understanding of what disinformation is, and how they best protect themselves from it (García & Oleart 2024; European Court of Auditors, 2021). The lack of attention to other fields of practices affects the way we perceive 'security' in the context of disinformation. More specifically, the education and media communities offer content pluralism and a heterogenous mix of perspectives, which should not be overlooked at the expense of controlling the information environment.

The 2021 assessment of the Code of Practice on Disinformation highlighted the growing risks of misinformation (European Commission, 2021). Based on Sweden's psychological defence strategy's logic, misinformation is best countered through strategies that strengthen public resilience, such as fact-checking and media literacy. These strategies are also the most efficient for targeting disinformation cases that are not considered foreign interference. Based on the Swedish model, disinformation created by a hostile *foreign* actor could, however, be subject to intelligence activities (Pamment & Isaksson, 2024). The Psychological Defence Agency does not have the mandate to target internal actors that create and spread disinformation. In case of disinformation dissemination by a domestic actor, the main strategy is to treat them as a "vulnerability". The Agency's Deputy Head, Mikael Tofvesson, explains the strategy as following: "We keep regular track of harmful narratives, misunderstandings, and potential areas of social tensions, without focusing on who originated this information [...] when we find reason to believe that there is an organised threat to exploit them, we develop a plan to counter the threat" (Chandler Institute of Governance, 2024, para.19). In other words, the Swedish approach has managed to safeguard against spill-over effects from countermeasures against FIMI to domestic disinformation or misinformation cases.

The discussion above highlights the lack of attention to long-term resilience building and inclusion of various policy fields in current EU strategies. However, recent developments show that the EU has acknowledged these shortcomings. The first development was the formation of a special committee on the European Democracy Shield by Members of the European Parliament (MEPs) during the early stages of the current parliamentary term (European Parliament, 2024). he Democracy Shield is a non-legislative initiative that aims to counter FIMI and enhance the support, protection, and empowerment of civil society (European Parliament, 2025, pp.1–2). On November 12, 2025, the EC presented concrete measures within the

Democracy Shield along with a new strategy under the Shield: the EU Strategy for Civil Society (see Tables 2 and 3). These developments reflect the EU's willingness to further address and counter harmful information influence activities through a 'whole-of-society approach' (European Commission, 2025b).

Table 2. Summary of Main Pillars and Key Objectives in the European Democracy Shield and EU Strategy for Civil Society

Measure	Main Pillars / Key Objectives
European Democracy Shield	• Safeguarding the integrity of the information space; • Strengthen EU institutions, free and fair elections, and independent media; • Enhance society's resilience and citizens' engagement.
EU Strategy for Civil Society	• Foster engagement: the establishment of a new Civil Society Platform; • Support and protection: the establishment of a Knowledge Hub on Civic Space to enhance protection measures directed towards organisations under threat; • Sustainable and transparent funding: increased financial support to civil society organisations and the establishment of stronger links with private donors and pro bono legal communities.

Source: European Commission (2025b).

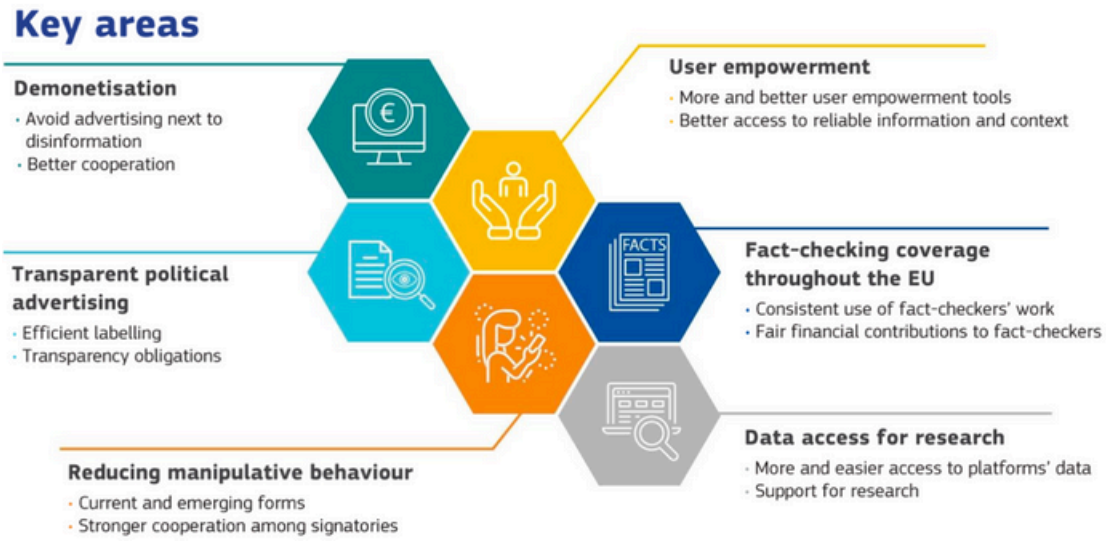
Table 3. Examples of Relevant Measures in the European Democracy Shield

Initiatives
• European Centre for Democratic Resilience working in coordination with the EEAS through RAS. Goal: enhance the resilience to FIMI and disinformation through increased information exchange between Member States; • Stakeholder Platform within the Centre, consisting of civil society organisations, academia, fact-checkers, and media professionals.
• Digital Services Act incidents and Crisis Protocol for relevant authorities.
• European Network of Fact-Checkers, for enhancing fact-checking capacity.
• EU citizenship competence framework that boosts EU resilience and citizens' engagement.
• Recommendation on supporting scientific evidence in policymaking to promote evidence-based EU decision-making.

Source: European Commission (2025b).

Lastly, on 13 February 2025, the EC and the European Board for Digital Services approved the integration of the Code of Practice on Disinformation into the DSA. This led to a conversion of the Code of Practice into the Code of Conduct on Disinformation, which reflects the commitment to depart from a voluntary-based framework and integrate disinformation risks into the DSA framework. In addition, the Code of Conduct now has 42 signatories, such as large online platforms and search engines, fact-checkers, civil society and research organisations, and advertisement stakeholders (European Commission, 2025c). Figure 1 provides further information about the Code of Conduct.

Figure 1. Code of Conduct on Disinformation



Source: European Commission (2025c, p.3).

The above developments reflect the EU's dedication to promoting a whole-of-society approach to disinformation countermeasures, which should not go unnoticed. However, for these measures to have a long-lasting impact, there is a need to: (a) ensure robust accountability mechanisms for the signatories of the Code of Conduct on Disinformation, (b) acknowledge capacity differences in Member States with regard to the implementation of cross-sector cooperation programmes, (c) recognise the differences in EU public policy preferences across various fields of practice, and (d) advance hybrid threat countermeasures in ways that do not negatively affect content pluralism or freedom of speech.

4. Conclusion

The EU faces the complex challenge of countering FIMI by hostile foreign actors such as Russia and China, while ensuring that such countermeasures do not undermine democratic communication within the media and education policy areas. The emergence of more sophisticated hybrid threats could also lead to serious consequences, including spill-over effects from defence and security strategies to the public debate environment. Since 2015, the EEAS has taken a leading role in countering disinformation, and policies have been refined after assessments provided by actors such as the EC. Sweden's psychological defence strategy illustrates that it is possible to counter FIMI on the one hand, while strengthening citizens' resilience through educational measures such as media literacy training, on the other. The Swedish model offers relevant insights for EU policies through the Psychological Defence Agency's cooperation with other government agencies, civil society, and the media.

Recent initiatives such as the European Democracy Shield and the Code of Conduct on Disinformation reflect the EU's willingness to develop a comprehensive system built on two main dimensions: (a) efficient defence and security efforts in the context of FIMI, and (b) a whole-of-society approach that strengthens cross-sector cooperation, enhances media literacy, and protects citizens' fundamental rights, such as their

freedom of expression. The ultimate success of the EU's anti-disinformation strategies also depends on holding signatories of the Code of Conduct on Disinformation accountable, supporting Member States with limited capacities, advancing hybrid threat countermeasures in ways that do not negatively affect content pluralism or freedom of speech within media and education policy fields, and recognising differences in both the definition of 'disinformation' and in policy interests across the security and defence, media and communication, education, and civil society fields.

Bibliography

Carnegie Endowment for International Peace (2020, July 15). The EU's Role in Fighting Disinformation: Taking Back the Initiative. https://carnegieendowment.org/research/2020/07/the-eus-role-in-fighting-disinformation-taking-back-the-initiative?lang=en

Chandler Institute of Governance. (2024). Defence Against the Dark Arts: Sweden's Psychological Defence Agency. https://www.chandlerinstitute.org/governancematters/defence-against-the-dark-arts-swedens-psychological-defence-agency

EDMO. (2025, 27 August). United against disinformation: our work in numbers. https://edmo.eu/edmo-news/united-against-disinformation-our-work-in-numbers/

European Commission. (2025a, November 11). European Digital Media Observatory – EDMO. https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

European Commission. (2025b, November 12). European Democracy Shield and EU Strategy for Civil Society pace the way for stronger and more resilient democracies. *https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660*

European Commission. (2025c). Code of Conduct on Disinformation - With Overview. https://ec.europa.eu/newsroom/dae/redirection/document/112680

European Commission. (2024, February 23). Questions and answers on the Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348

European Commission. (2022a). *A strengthened EU Code of Practice on Disinformation.* https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en

European Commission. (2022b). *2022 Strengthened Code of Practice Disinformation.* https://ec.europa.eu/newsroom/dae/redirection/document/87585

European Commission. (2021, May 26). *European Commission Guidance on Strenhgtening the Code of Practice on Disinformation.* https://ec.europa.eu/newsroom/dae/redirection/document/76495

European Commission. (2020a, September 10). *Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement*. https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

European Commission. (2020b, December 3). European Democracy Action Plan: making EU democracies stronger. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

European Commission. (2020c, December 15). Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. (2020/0361). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825

European Commission. (2018, 12 December). Action Plan against Disinformation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018

European Council. (2015, 20 March). European Council meeting (19 and 20 March 2015) – Conclusions. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Court of Auditors. (2021). Disinformation affecting the EU: tackled but not tamed. (Report No. 09/2021). https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf

European External Action Service. (2025, March). 3rd EEAS Report on Foreign Information Manipulation and Interference Threats – Exposing the architecture of FIMI operations. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

European External Action Service. (2021, 27 October). Questions and Answers about the East StratCom Task Force. https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

European External Action Service. (2019, March). RAPID ALERT SYSTEM – Strenghtening coordinated and joint responses to disinformation. https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf

European External Action Service. (2015). *Action plan on strategic communication.* https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf

European Parliament. (2025). *European Democracy Shield – Q3 2025*. European Parliament. https://www.europarl.europa.eu/legislative-train/carriage/european-democracy-shield/report?sid=9501

European Parliament. (2024). *Foreign interference: how Parliament is fighting the threat to EU democracy.* https://www.europarl.europa.eu/topics/en/article/20240404STO20215/foreign-interference-how-parliament-is-fighting-the-threat-to-eu-democracy

European Parliament. (2015, November). Russia's disinformation on Ukriane and the EU's response. https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571339/EPRS_BRI(2015)571339_EN.pdf

European Union External Action. (2025, March 14). Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

EUvsDisinfo (n.d). About. https://euvsdisinfo.eu/about/

García, L. B., & Oleart, A. (2024). Regulating Disinformation and Big Tech in the EU: A Research Agenda on the Institutional Strategies, Public Spheres and Analytical Challenges. Journal of Common Market Studies, 62(5), 1395-1407. https://doi.org/10.1111/jcms.13548

Pamment, J., & Isaksson, E. (2024). Psychological Defence: Concepts and principles for the 2020s. (Report Series 6/2024). Psychological Defence Agency. https://www.psychologicaldefence.lu.se/article/new-report-concepts-and-principles-psychological-defence

Pamment, J., & Tsurtsumia, D. (2025). Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency. (Report Series 8/2025). Psychological Defence Agency. https://www.psychologicaldefence.lu.se/article/beyond-operation-doppelganger-capability-assessment-social-design-agency

Psychological Defence Agency. (2025, October 28). Glossary. https://mpf.se/psychological-defence-agency/aids/glossary

Wagnsson, C., Östervall, A., & Angwald, A. (2025). Naming the enemy: how to fortify society against foreign disinformation while avoiding excessive vigilance to reliable media. Humanities & Social Sciences Communication, 12(803), 1-12. https://doi.org/10.1057/s41599-025-04844-6

Ördén, H. (2019). Deferring substance: EU policy and the information threat. Intelligence and National Security, 34(3), 421-437. https://doi.org/10.1080/02684527.2019.1553706

F I N A B E L

THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION