

PRE-2022 EU COUNTER-DISINFORMATION POLICY: STRENGTHS, GAPS, AND POST-LLM RELEVANCE

Eryk MARCHLEWSKI

Military University of Technology, Warsaw, Poland (eryk.marchlewski@wat.edu.pl)

DOI: 10.19062/2247-3173.2026.27.11

Abstract: *Disinformation is not new, but social media has made it faster, cheaper, and harder to trace. This paper reviews the EU's main counter-disinformation measures developed before 2022, including strategic communication in the European External Action Service, the East StratCom Task Force and EUvsDisinfo, the Action Plan against Disinformation, the Rapid Alert System, and cooperation with online platforms through the Code of Practice. The analysis links these policy tools to evidence from cognitive psychology on why misinformation spreads. Research shows that people can often distinguish true from false headlines when asked, yet still share false content online. Sharing may reflect inattention, social incentives, and quick, automatic reactions rather than firm belief. Using a qualitative review of psychological literature and official EU documents, the paper assesses how well pre-2022 EU measures target key behavioural drivers and identifies where the fit is strong and where gaps remain - especially around attention at the moment of sharing. Finally, the paper briefly considers how the post-2022 spread of large language models (LLMs) changes the environment by increasing content volume and variation, which can weaken slow, case-by-case responses. The study highlights which pre-2022 lessons remain useful under LLM-driven scale and which measures may require redesign or stronger safeguards to protect trust and open debate.*

Keywords: *disinformation, cognitive warfare, fake news, EU policy, psychological warfare*

1. INTRODUCTION

Democratic societies depend on a shared ability to agree on basic facts. When false or misleading content spreads widely, it can weaken trust in institutions, distort public debate, and reduce the ability to respond to crises. Digital platforms and messaging apps can amplify misleading claims quickly, at low cost, and across borders [1]. This problem matters for the European Union (EU) because open debate, free media, and cross-border information flows are core features of the EU model [2], yet those same features can be exploited by organised influence campaigns. The period after 2022 is especially important because large language models (LLMs) became widely available and rapidly adopted, which made it easier to produce convincing text at scale and to adapt messages to different audiences [3]. For that reason, it is useful to understand what the EU built before this turning point.

Data on daily social media use suggests that the long period of year-by-year growth slowed around 2020 and has since remained stable [4], at roughly the mid-140s minutes per day (Fig.1). This matters for the present study because it indicates that, by the early 2020s, social networking had reached a high and relatively saturated level of daily attention among the average internet user. At the same time, the total number of internet users worldwide has continued to grow [5], which means that even if time-per-user stabilises, the overall reach and potential impact of online information flows can still increase over time.

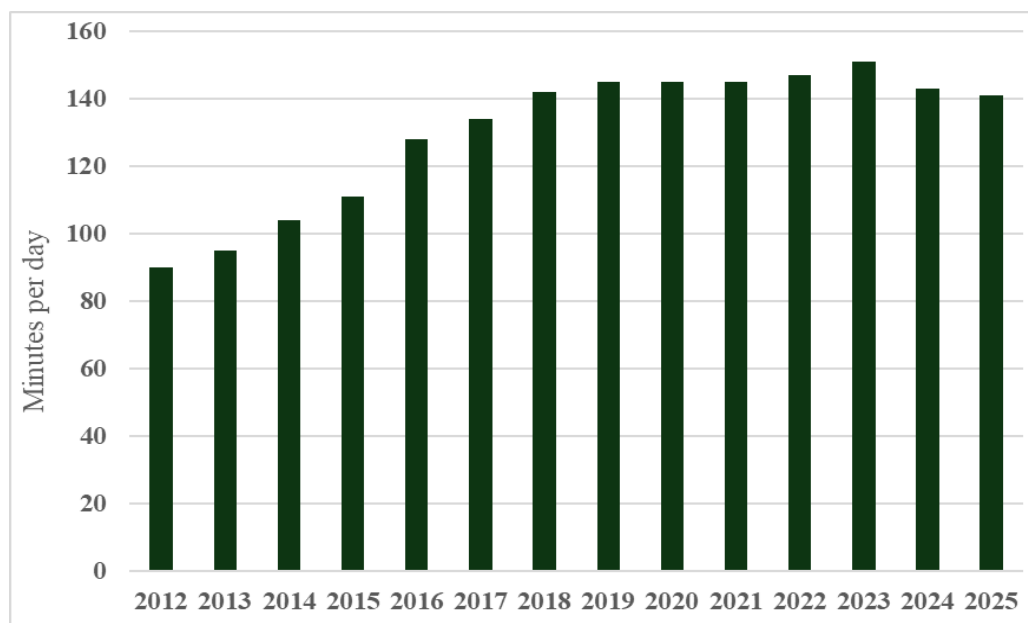


FIG. 1 Daily time spent on social networking by internet users worldwide from 2012 to 2025 [4].

Previous research provides two main lines of insight. First, cognitive psychology and behavioural research show that misinformation belief and sharing are shaped by reasoning, knowledge, attention, emotions, and social incentives [6]. Several studies [7,8,9] report that analytic thinking and knowledge can predict truth discernment more strongly than political alignment alone. A key finding is that sharing online does not always mean belief: many users share false headlines even when they can recognise inaccuracy when asked directly, and simple “accuracy prompts” can reduce sharing of false content in experiments [9]. Second, EU-focused work describes and assesses policy responses such as the European External Action Service (EEAS) [10], the East StratCom Task Force and EUvsDisinfo [11,12], the Action Plan against Disinformation [13], the Code of Practice on Disinformation [13], and the Rapid Alert System (RAS) [14]. Existing policy reviews often focus on institutions, coordination, and platform cooperation, but they do not always connect these tools to evidence about how people actually judge and share information online.

This paper focuses on EU counter-disinformation actions taken before 2022 for two reasons. First, pre-2022 measures form the core “first generation” of EU counter-disinformation policy [11-14], created in response to earlier waves of online manipulation. Second, 2022 is treated as a break point because LLM-based tools changed the environment: content can be generated faster, in larger volumes, and in more varied styles, which can strain detection, fact-checking, and moderation systems [3]. Even though this paper does not aim to analyse the post-2022 period in detail, a brief discussion of LLMs helps explain why the pre-2022 toolkit should be assessed as a baseline, and it supports a practical goal: identifying which earlier countermeasures became less effective under AI-driven scale, and which lessons remain useful.

A gap follows from this. There is limited integrated assessment of the EU’s pre-2022 counter-disinformation toolkit using a clear behavioural lens. Policy discussions often assume that misinformation spreads mainly because people believe it, and that the best fix is correction or removal. If a meaningful share of harmful sharing is driven by inattention, social rewards, and fast “one-click” behaviour [6,7], then some policies may be poorly targeted, while other low-cost interventions may be underused. In addition, measures that reduce the reach of content can create censorship narratives if rules are unclear, which can damage trust and reduce resilience.

Four research questions guide this paper:

1. What were the main EU counter-disinformation instruments and priorities before 2022, and how were they expected to work?
2. What does cognitive psychology suggest about why people believe and share misinformation, especially the difference between belief and sharing?
3. How well did key EU measures before 2022 match these psychological mechanisms?
4. Which lessons from the pre-2022 period remain useful in an LLM-shaped information space, and which tools need redesign or stronger safeguards to remain effective?

2. METHODOLOGY

This paper uses a qualitative approach based on two inputs: (1) research from cognitive psychology on misinformation and online sharing, and (2) official EU documents on counter-disinformation policy published before 2022. The main goal is to describe the EU measures that existed before 2022, assess their strengths and limits, and then relate them to what psychology suggests about how misinformation spreads.

First, a focused review of psychological literature was conducted to identify the main psychological factors that make people vulnerable to misinformation and that encourage sharing of low-quality content. The review looked for findings that are clearly linked to online environments, such as limited attention, fast and automatic thinking, the role of analytic reasoning and knowledge, emotional triggers, and social motivations for sharing. The purpose of this step was to create a short list of psychological factors that could later be compared with policy measures.

Second, the paper reviewed official EU resources issued before 2022. These included public reports, policy documents, action plans, and materials published by EU institutions and relevant EU bodies. The documents were used to describe what the EU was doing to address disinformation before the widespread public use of LLMs. For each EU measure, the analysis focused on its stated goals, the type of action it proposed, and the main problem it aimed to solve.

Third, the paper compared the psychological factors identified in the first step with the EU measures identified in the second step. The aim was to check whether EU actions were aimed at the right parts of the problem. For example, some measures are meant to reduce exposure to false content, while others aim to improve citizens' ability to judge information, or to change how platforms handle misleading content. This comparison was used to discuss the likely relevance and limits of the EU approach before 2022.

Finally, the paper briefly considers what changed after 2022 with the rapid spread of LLMs. This part is not a full analysis of post-2022 policy. Instead, it highlights how easier and faster content generation can affect the usefulness of earlier countermeasures. It points to areas where older approaches may become less effective and areas where lessons from the pre-2022 period may still apply.

3. REVIEW OF PSYCHOLOGICAL LITERATURE

3.1 Why misinformation works in a high-information environment

Psychological research highlights a basic constraint: people face far more information than they can carefully check [15]. In online settings, decisions about what to read, trust, or share are often made quickly and with limited attention [15]. Under these conditions, emotions, habits, and mental shortcuts can shape reactions more than careful reasoning [16]. This is especially important during crises, when fear and uncertainty can increase the spread of rumours and low-quality claims [17].

A common assumption is that misinformation spreads mainly because citizens accept content that matches their political identity. However, evidence suggests that political agreement with a headline is not always the main factor behind the ability to tell true from false claims [7]. Instead, differences in reasoning can explain why some people are better at judging accuracy than others [7]. In survey findings, reasoning is described as more strongly linked to “truth discernment” than political agreement, while political agreement is more strongly linked to what people say they believe in general [7].

This point matters for policy because it shifts attention away from a simple “polarization explanation”. Political views can shape attitudes, but improving people’s ability to judge information may depend more on reasoning skills and knowledge than on trying to “depolarize” society directly [7].

3.2 The role of reasoning

A recurring idea in the psychological literature is that misinformation is more likely to be accepted when people rely on quick, intuitive thinking rather than careful reasoning [16]. This phenomenon is illustrated with the Cognitive Reflection Test example (“bat and ball” problem), where an intuitive but wrong answer comes to mind quickly, and the correct answer tends to appear only after a brief step of reflection. The main point is not the puzzle itself, but the general pattern: people often accept the first plausible response unless they stop and think. In online environments, this tendency is relevant because people often scan headlines rapidly, switch between topics, and react under time pressure [18].

There are two additional factors that interact with reasoning:

a) Knowledge can protect against misinformation, especially when claims can be checked against basic scientific understanding. (Respondents exposed to false COVID-19 claims were better able to judge accuracy when they had stronger background knowledge [19].).

b) Overconfidence can increase vulnerability. The idea is straightforward: if people trust their first impression too much, they are less likely to pause and check whether they might be wrong. Overconfidence can therefore reduce the chance that reflective thinking will be used when evaluating claims [20].

3.3 Sharing vs. belief

Another common assumption is that people share content mainly because they believe it is true. However, previous research provides evidence that challenges this: people can rate true headlines as more accurate than false ones when asked directly about accuracy, yet the truth of a headline has much less influence on whether people say they would share it [9]. In other words, sharing intentions can be much higher than accuracy judgments for false headlines, suggesting that many users may share content they would recognise as inaccurate if they stopped to think.

This is a key point for policy because it implies that misinformation spread is not only a “belief problem.” It is also a “sharing problem,” shaped by platform architecture, fast decisions, and social incentives [21].

Three explanations have been proposed to understand why sharing can happen even when belief is weak:

a) Confusion (accuracy–sharing gap).

One possibility is that people share false content because they genuinely believe it. However, a large share of sharing remains unexplained by confusion alone, because many respondents do not both believe and share when accuracy is measured directly [9].

b) Preference or political motives.

Another possibility is that people knowingly share false content because it supports a political message, creates chaos, or is entertaining/shocking. This can explain some cases, but it does not appear to explain most sharing behaviour in the studies [22].

c) Inattention.

The third explanation is that many people generally prefer to share true content, but the social media setting distracts them from thinking about accuracy at the moment of sharing. Experimental results report that when participants are prompted to think about accuracy, sharing of false headlines drops sharply (a large reduction relative to baseline) [23].

This “inattention” idea fits the everyday experience of social media: rapid scrolling, emotional cues, social rewards, and little cost to sharing. It also leads to a practical insight: some interventions can reduce misinformation spread not by changing ideology, but by changing what users pay attention to when deciding to share.

4. EU COUNTER-DISINFORMATION POLICY BEFORE 2022

EU institutions treated disinformation as a cross-border risk that can affect elections, public trust, and crisis response [24]. The challenge was not limited to falsehoods shared by individual users. Organised influence operations were seen as able to exploit open media environments and online platforms to shape public debate [24]. Because the EU is built on open public discussion and freedom of expression, the response had to balance effectiveness with legitimacy and legal limits. This section provide the reader with insights on evolution and development of EU institutional struggle again disinformation threats (Fig.2).



FIG. 2 Chronology of EU actions against disinformation [25]

4.1 EEAS and the first specialised response capacity

A central role in the EU response was played by EEAS, which supports the EU’s external action and coordinates parts of its crisis and security work. Within the EEAS, the East StratCom Task Force was established in 2015 following concerns about pro-Kremlin disinformation [26]. Its work focused on improving understanding of disinformation techniques, monitoring narratives, and supporting EU strategic communication.

A key public-facing output connected to this work is EUvsDisinfo, which is described as a flagship initiative of the East StratCom Task Force [12]. Its stated aim is to identify and analyse disinformation campaigns (especially those linked to pro-Kremlin sources), raise awareness, and strengthen public resilience. The project relies on media monitoring and data analysis in multiple languages and publishes case-based descriptions of disinformation narratives [12].

4.2 Linking disinformation to “hybrid threats” (2016–2018)

Before 2022, counter-disinformation efforts were increasingly connected to broader EU work on hybrid threats. In 2016 the EU adopted a Joint Framework on countering hybrid threats [27], and in the same year a Hybrid Fusion Cell was created within EEAS structures [28] to support analysis and situational awareness. In 2017 the European Centre of Excellence for Countering Hybrid Threats was established in Helsinki [29], supporting cooperation and knowledge exchange across participating states and institutions. In 2018, a Joint Communication on strengthening resilience and capabilities against hybrid threats was adopted [30], signalling that disinformation was treated as part of a wider security problem, not only a media problem.

This framing matters because it shaped the type of solutions pursued: not only public communication, but also coordination, early warning, and information sharing between EU bodies and Member States (MS).

4.3 The Action Plan against Disinformation (2018)

A major step in the pre-2022 approach was the Action Plan against Disinformation [31]. It presented a four-part approach aiming to strengthen EU capacity and cooperation:

a) Improved detection and analysis

The plan called for reinforcing relevant EEAS capacities and improving access to analytical tools and specialised staff. The main problem addressed here was limited capacity to identify campaigns early and understand patterns across countries.

b) Coordinated response

The Action Plan proposed stronger coordination among EU institutions and MS, including setting up the RAS [14]. The main problem was fragmentation: disinformation campaigns can move quickly across borders, while responses were often national, slow, or uncoordinated.

c) Online platforms and industry

A key element was engagement with platforms through the Code of Practice on Disinformation. The main problem targeted was the role of platform systems in amplifying low-quality or coordinated content.

d) Raising awareness and empowering citizens

The plan emphasised media literacy and awareness activities, including dedicated programmes and awareness-raising campaigns. The main problem was that even good detection and coordination are not sufficient if large parts of the population remain vulnerable to misleading content.

4.4 Flagship instruments before 2022

4.4.1 Code of Practice on Disinformation

The Code of Practice was introduced in 2018 as a self-regulatory framework involving major online platforms and other stakeholders (including the advertising sector, academia, and civil society). It aimed to reduce the impact of disinformation through voluntary commitments. Key areas included: transparency of sponsored content; detection of fake accounts and bots; transparency and the ability to verify algorithms; access to diverse information sources; and monitoring by research institutions and public authorities [30].

4.4.2 RAS

RAS was launched in March 2019, following the Action Plan. It was designed to support information sharing among Points of Contact from EU institutions and MS, including regular exchanges on ongoing campaigns. It was launched before elections to the European Parliament and linked to election-related cooperation structures. The system was used in 2020 to tackle COVID-19-related disinformation campaigns. It also enabled participants to flag high-priority cases for quick attention, with no automatic trigger - cases were assessed individually [14].

4.4.3 EUvsDisinfo

EUvsDisinfo started in 2015 as a flagship project linked to the East StratCom Task Force of the EEAS. Its purpose is to identify, analyse, and document disinformation narratives and raise public awareness of manipulation techniques. It draws on media monitoring and data analysis in multiple languages and publishes descriptions of cases of disinformation and recurring patterns [12].

5. ALIGNMENT BETWEEN PSYCHOLOGICAL MECHANISMS AND EU POLICY TOOLS

This section links the two parts of the review: the psychological drivers of misinformation and the main EU measures introduced before 2022. The goal is to check whether the EU response was aimed at the same points where misinformation spreads in practice. Some measures mainly try to reduce exposure (ex. by limiting amplification on platforms), while others try to improve citizens' ability to judge information (ex. through media literacy) or improve institutional response (ex. by sharing alerts and information across MS).

To keep this comparison clear, the table below (Table 1) lists key EU instruments and shows which psychological mechanisms they most directly address. The aim is to highlight where the fit seems strong, where it is only indirect, and where gaps may exist. This helps identify the strengths and limits of the pre-2022 toolkit, and it also sets up the later discussion on which types of measures remain useful in a faster, higher-volume information environment.

Table 1. Mapping EU measures (pre-2022) to psychological drivers of disinformation spread.

EU Action	Type of action	Psychological mechanisms addressed	Year
East StratCom Task Force	Monitoring/analysis Strategic communication support Identifying and countering false narratives	Confusion Information overload Preference/political motives	2015
EUvsDisinfo	Monitoring/analysis Documentation of disinformation cases/narratives Exposing manipulation techniques	Confusion Overconfidence Inattention	2015
Code of Practice on Disinformation	Platform governance Self-regulatory commitments Political/sponsored content transparency Reduction of fake accounts' volume Supporting access to diverse information sources	Inattention Preference/political motives Information overload Confusion	2018
RAS	Coordination Support quicker, consistent responses Early warning Shared situational awareness	Confusion Information overload	2019

6. THE IMPLICATIONS OF INTRODUCTION OF LLMS FOR THE PRE 2022 COUNTERMEASURES

After 2022, widely available LLMS made it much easier and cheaper to produce persuasive text at scale, translate content across languages, and rapidly rewrite messages for different audiences. This shift increased the volume and speed of low-quality or manipulative content and lowered the skill barrier for creating credible-looking narratives [3].

As a result, several pre-2022 countermeasures that work well in a lower-volume environment can become harder to maintain, not because they are conceptually wrong, but because they are easier to overwhelm.

This section does not assess post-2022 EU policy in detail. Instead, it uses the pre-2022 baseline to highlight two points: (1) which earlier strategies become less effective when content generation and variation become much faster, and (2) which lessons still apply because they target human behaviour and system incentives rather than only individual pieces of content. The focus is on likely relevance and limits rather than definitive impact evaluation.

6.1 Usefulness of EU approaches in post-LLM reality

Several pre-2022 approaches become harder to sustain when content is produced and reshaped at high speed. Reactive, case-by-case corrections can lose impact when the same claim appears in many slightly different versions across platforms and languages. Manual monitoring and narrative tracking can also become more resource-intensive when content volume rises and when bots can produce and spread messages continuously. In addition, public awareness advice that relies on spotting low effort signals (such as poor grammar or obvious mistakes) is less reliable when AI-generated content is fluent and consistent.

On the other hand, many lessons from the pre-LLM period remain relevant because they focus on how people process and share information, and on how platforms amplify content. Measures that reduce impulsive sharing by making accuracy more noticeable can still work, because sharing decisions often depend on attention and social incentives rather than on strong belief. Media literacy can also remain useful when it teaches practical habits (ex. pause before sharing, check sources, compare across outlets) instead of “spot the fake”. Platform-level interventions that reduce amplification incentives - such as limiting fake accounts and bots, improving transparency around ads and sponsorship, and enabling researcher access - remain important because they shape the environment in which misinformation spreads. Finally, coordination and early warning continue to matter under higher volume, and safeguards that protect trust and legitimacy become more important when countermeasures risk are framed as censorship.

6.2 Using LLMs on defence

The post-2022 shift is not only a challenge for defenders. LLM-based tools can help with faster triage, summarising trends, and multilingual monitoring, which can reduce workload and improve response speed. When used carefully, this defensive support can partially mitigate the scale advantage of attackers, while keeping the emphasis on approaches that target behaviour, incentives, coordination, and trust rather than trying to chase every individual false claim.

CONCLUSION

The author of this article assessed the EU’s main counter-disinformation measures before 2022 and compared them with key psychological drivers of misinformation belief and sharing. The review suggests that the pre-2022 toolkit was strongest where it addressed reasoning and knowledge and the structure of the information environment: media literacy efforts aimed to improve judgment skills, while platform-focused measures and coordination tools aimed to reduce amplification and improve institutional response.

At the same time, the behavioural evidence reviewed earlier points to a recurring gap: a large part of harmful spread can be driven by inattention and fast, low-cost sharing, even when users are able to recognise inaccuracy when asked directly. This implies that some pre-2022 tools may be less effective than expected if they focus mainly on correcting content after it spreads, rather than shaping the conditions under which people decide to share.

Finally, the analysis highlights a governance risk: countermeasures that are unclear or perceived as top-down control can damage trust and feed censorship narratives, which can undermine resilience.

The post-2022 spread of LLMs does not make earlier lessons irrelevant, but it shifts priorities. Measures that depend on slow, case-by-case responses face stronger scale pressure when content can be produced and rewritten rapidly. In contrast, approaches that target user behaviour, platform incentives, and coordination remain vital and should be strengthened. LLMs may also support defenders through faster detection and multilingual monitoring, but their use should be paired with clear safeguards and transparency to protect legitimacy. Overall, the pre-2022 EU toolkit provides a useful baseline: it shows which parts of the response architecture are durable under higher-volume conditions and where redesign is needed to keep counter-disinformation policy both effective and consistent with open democratic debate.

REFERENCES

- [1] L. McIntyre, *Post-Truth*, Cambridge, MA, USA: MIT Press, 2018;
- [2] European Parliament, Council of the European Union, and European Commission, *European Declaration on Digital Rights and Principles for the Digital Decade*, Solemn Declaration, Dec. 15, 2022, accessed on 04 Apr. 2026;
- [3] J. A. Goldstein, G. Sastry, M. Musser, R. DiResta, M. Gentzel and K. Sedova, *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*, arXiv preprint arXiv:2301.04246, Jan. 2023, accessed on 06 Apr. 2026;
- [4] Statista, *Daily time spent on social networking by internet users worldwide from 2012 to 2025 (in minutes)*, Statista Statistics Database (Statistic ID: 433871), accessed on 06 Apr. 2026;
- [5] International Telecommunication Union, *Global Connectivity Report 2025*, Geneva, Switzerland: ITU, 2025, accessed on 06 Apr. 2026;
- [6] G. Pennycook and D. G. Rand, *The Psychology of Fake News*, Trends in Cognitive Sciences, vol. 25, no. 5, pp. 388–402, May 2021, doi: 10.1016/j.tics.2021.02.007, accessed on 07 Apr. 2026;
- [7] G. Pennycook and D. G. Rand, *Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning*, Cognition, vol. 188, pp. 39–50, July 2019, doi: 10.1016/j.cognition.2018.06.011, accessed on 07 Apr. 2026;
- [8] M. V. Bronstein, G. Pennycook, A. Bear, D. G. Rand and T. D. Cannon, *Belief in Fake News is Associated with Delusionality, Dogmatism, Religious Fundamentalism, and Reduced Analytic Thinking*, Journal of Applied Research in Memory and Cognition, vol. 8, no. 1, pp. 108–117, Mar. 2019, doi: 10.1016/j.jarmac.2018.09.005, accessed on 07 Apr. 2026;
- [9] G. Pennycook, Z. Epstein, M. Mosleh, A. A. Arechar, D. Eckles and D. G. Rand, *Shifting attention to accuracy can reduce misinformation online*, Nature, vol. 592, pp. 590–595, 2021, doi: 10.1038/s41586-021-03344-2, accessed on 07 Apr. 2026;
- [10] Council of the European Union, *Council Decision 2010/427/EU of 26 July 2010 establishing the organisation and functioning of the European External Action Service*, Official Journal of the European Union, L 201, 3 Aug. 2010, pp. 30–40, accessed on 07 Apr. 2026;
- [11] European External Action Service, *Questions and Answers about the East StratCom Task Force*, 27 Oct. 2021, accessed on 07 Apr. 2026;
- [12] EUvsDisinfo, *About*, EUvsDisinfo (East StratCom Task Force / EEAS), accessed on 07 Apr. 2026;
- [13] European Commission (DG CONNECT), *2022 Strengthened Code of Practice on Disinformation*, 16 Jun. 2022, accessed on 07 Apr. 2026;
- [14] European External Action Service, *Factsheet: Rapid Alert System*, 05 Mar. 2019, accessed on 07 Apr. 2026;
- [15] P. Lorenz-Spreen, B. M. Mønsted, P. Hövel and S. Lehmann, *Accelerating dynamics of collective attention*, Nature Communications, vol. 10, Art. no. 1759, Apr. 2019, doi: 10.1038/s41467-019-09311-w, accessed on 09 Apr. 2026;
- [16] D. Kahneman, *Thinking, Fast and Slow*, New York, NY, USA: Farrar, Straus and Giroux, 2011, accessed on 09 Apr. 2026;
- [17] World Health Organization, *Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation*, WHO News item, Sep. 23, 2020, accessed on 09 Apr. 2026;

- [18] S. Frederick, *Cognitive Reflection and Decision Making*, Journal of Economic Perspectives, vol. 19, no. 4, pp. 25–42, Fall 2005, doi: 10.1257/089533005775196732, accessed on 11 Apr. 2026;
- [19] J. Roozenbeek, C. R. Schneider, S. Dryhurst, J. Kerr, A. L. J. Freeman, G. Recchia, A. M. van der Bles and S. van der Linden, *Susceptibility to misinformation about COVID-19 around the world*, Royal Society Open Science, vol. 7, no. 10, Art. no. 201199, 2020, doi: 10.1098/rsos.201199, accessed on 11 Apr. 2026;
- [20] B. A. Lyons, J. M. Montgomery, A. M. Guess, B. Nyhan and J. Reifler, *Overconfidence in news judgments is associated with false news susceptibility*, Proceedings of the National Academy of Sciences of the United States of America, vol. 118, no. 23, e2019527118, 2021, doi: 10.1073/pnas.2019527118, accessed on 11 Apr. 2026;
- [21] M. Del Vicario, S. Gaito, W. Quattrociocchi, M. Zignani and F. Zollo, *Public discourse and news consumption on online social media: A quantitative, cross-platform analysis of the Italian Referendum*, arXiv preprint arXiv:1702.06016, Feb. 2017 (revised Jun. 2017), doi: 10.48550/arXiv.1702.06016, accessed on 11 Apr. 2026;
- [22] M. B. Petersen, M. Osmundsen and K. Arceneaux, *The Need for Chaos and Motivations to Share Hostile Political Rumors*, American Political Science Review, vol. 117, no. 4, pp. 1486–1505, Nov. 2023, doi: 10.1017/S0003055422001447, accessed on 09 Apr. 2026;
- [23] G. Pennycook and D. G. Rand, *Nudging Social Media toward Accuracy*, The ANNALS of the American Academy of Political and Social Science, vol. 700, no. 1, pp. 152–164, Mar. 2022, doi: 10.1177/00027162221092342, accessed on 10 Apr. 2026;
- [24] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On the European democracy action plan*, COM(2020) 790 final, Brussels, Dec. 3, 2020, accessed on 10 Apr. 2026;
- [25] European Parliamentary Research Service, *Overview of EU joint and coordinated action against disinformation*, EP Think Tank (Ephthinktank), Jul. 19, 2023, accessed on 10 Apr. 2026;
- [26] European Council, *European Council meeting (19 and 20 March 2015) – Conclusions*, EUCO 11/15, Brussels, Mar. 20, 2015, accessed on 10 Apr. 2026;
- [27] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats – a European Union response*, JOIN(2016) 18 final, Brussels, 6 Apr. 2016, accessed on 15 Apr. 2026;
- [28] Publications Office of the European Union, *Intelligence Analysis and Reporting (INTCEN.1) – EU Whoiswho*, EU Whoiswho directory entry, accessed on 15 Apr. 2026;
- [29] The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), *About us*, Hybrid CoE, accessed on 15 Apr. 2026;
- [30] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN(2018) 16 final, Brussels, 13 Jun. 2018, accessed on 15 Apr. 2026;
- [31] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation*, JOIN(2018) 36 final, Brussels, 5 Dec. 2018, accessed on 15 Apr. 2026.