

AN INTERNATIONAL STRATEGY VS. DISINFORMATION AS WARFARE

by Angelos T. Kolokouris

**Copyright: @ 2026 Research Institute for European and American Studies
(www.rieas.gr) Publication date: 28 October 2026**

Note: The article reflects the opinion of the author and not necessarily the views of the Research Institute for European and American Studies

PREAMBLE

In early October 2026, DISINFO 2026, the annual conference convened in Vilnius by the Brussels-based EU DisinfoLab, became an unexpected flashpoint. A plenary session framing the United States itself as a source of foreign information manipulation and interference, prompted Washington, according to Reuters, to lobby allied governments to distance themselves. To be specific, the clearest immediate trigger was the plenary session “USA as a FIMI threat: acknowledge, adapt, push back.” A bewildering theme, when most allied governments, for a number of years, face considerably damaging attacks from well-known enemies. As a result, Lithuania, the host country, cancelled its participation; Canada revised its role in several sessions; and the European External Action Service removed its branding. France alone remained a visible government supporter. That controversy served as the impetus for the present article. Whatever one makes of the panel's framing, the episode exposed a fissure among the very democracies that face the same adversaries. The article treats disinformation not as a nuisance of the digital age but as a form of warfare, and it seeks to draw attention to the imperative of cooperation among allies; without such an international cooperation, no national strategy can succeed.

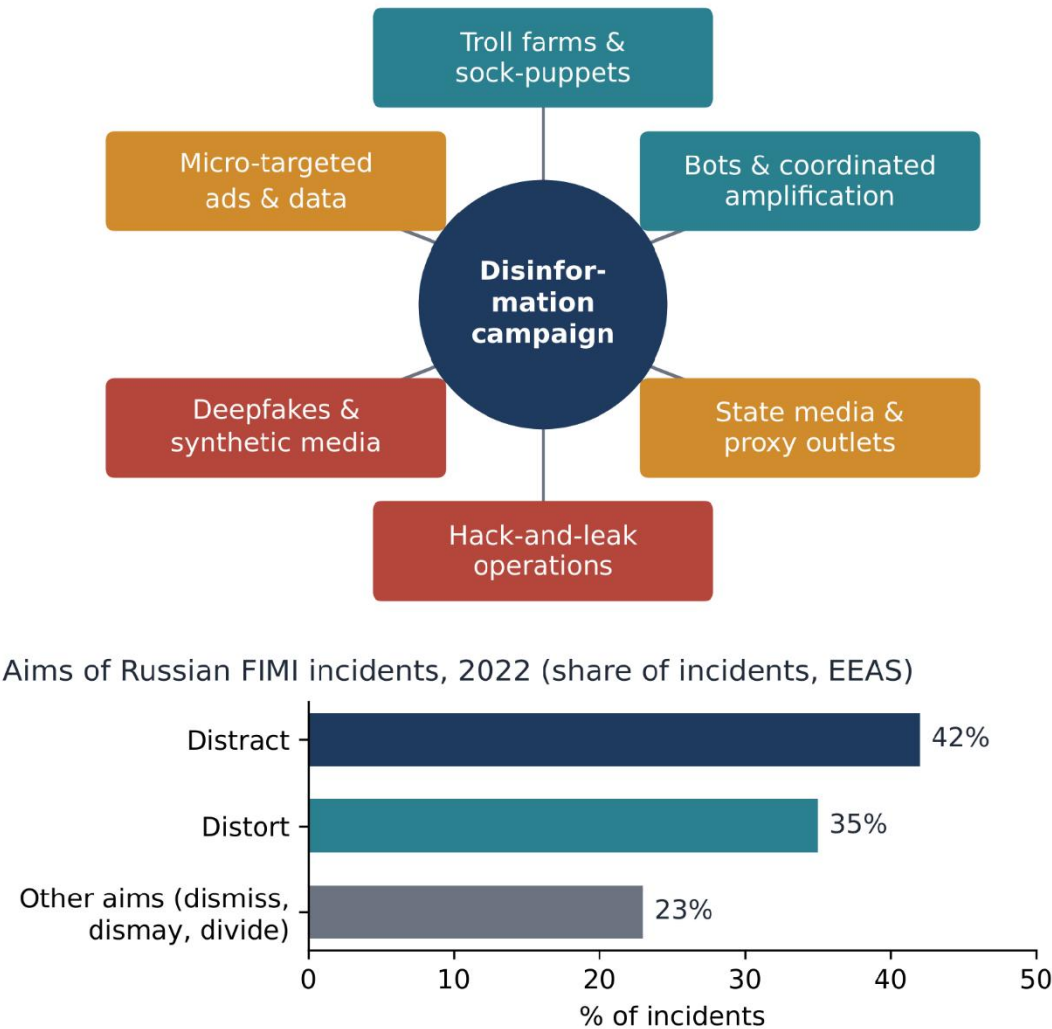
1. WHAT DISINFORMATION IS

Disinformation is false, manipulated or misleadingly framed information that is created and spread deliberately in order to deceive and to cause harm (Wardle & Davakhana, 2017). Intent separates it from misinformation, which is false but shared in good faith: once an unwitting user passes a fabricated story on, disinformation becomes misinformation (Slidable Hansen, 2017). In its strategic form, disinformation is not an isolated lie but an organized, often state-directed effort. In that sense, it is the heir of Soviet “active measures”, that exploits existing grievances to shape a target society’s perceptions and decisions (Olejnik, 2024; Rid, 2020).

2. THE MOST EFFECTIVE TOOLS OF DISINFORMATION-AS-WARFARE CAMPAIGNS

Contemporary campaigns combine six instruments (Figure 1). Troll farms such as St Petersburg’s Internet Research Agency run sock-puppet accounts that pose as ordinary citizens and harass critics (Aru, 2016). Bots and coordinated networks amplify narratives, while state outlets such as RT supply “source” content that trolls push across platforms (Zanetti et al., 2019). Hack-and-leak operations weaponize authentic stolen material; micro-targeted advertising exploits harvested personal data (Tuttle, 2019); and deepfakes promise cheap, convincing audiovisual fabrication (Chesney & Citron, 2019). Their aims follow the logic of dismiss, distort, distract, dismay and divide: in 2022, 42% of Russian incidents recorded by the EU sought to distract and 35% to distort (Olejnik, 2024).

Figure 1. Core tools and documented aims of disinformation campaigns



Sources: Olejnik (2024), citing EEAS (2023); Aro (2016); Chesney & Citron (2019); Tuttle (2019). 'Other' is the residual share.

3. DISINFORMATION AS WARFARE

3.1. *DIFFERENT FORMS OF DISINFORMATION*

Disinformation as warfare takes several forms. *Strategic influence operations* in peacetime slowly erode trust in institutions and alliances. *Hybrid-warfare disinformation* accompanies military action, as in Russia's "non-linear" campaigns in Ukraine, where information shapes the battlespace alongside proxies, cyberattacks and economic pressure (Araźna, 2015; Splidsboel Hansen, 2017). *Electoral interference* targets democratic votes (Tuttle, 2019). *Psychological operations* aim at enemy troops and civilians in wartime. *Laundered disinformation* passes through proxies, sympathizers and seemingly independent outlets to hide its origin, while *computational propaganda* automates the whole cycle with bots and algorithms (Bradshaw & Howard, 2019; Horowitz, 2019).

3.2. *A SAMPLE OF DISINFORMATION-AS-WARFARE CASES*

Operation INFEKTION (1983–1987). The KGB planted, in a pro-Soviet Indian newspaper, the claim that the Pentagon engineered HIV/AIDS, then amplified it worldwide; the myth still circulates (Rid, 2020).

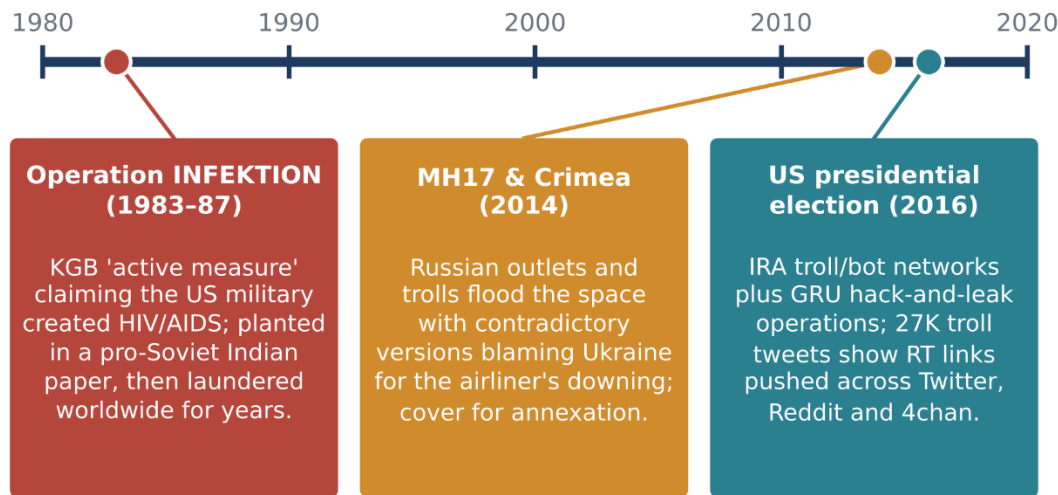
MH17 and Crimea (2014). After a Russian-supplied Buk missile downed Malaysia Airlines Flight 17 over eastern Ukraine, Russian media and trolls flooded audiences with contradictory theories blaming Ukraine, aiming to confuse rather than convince (Olejnik, 2024; Paul & Matthews, 2016).

U.S. presidential election (2016). Internet Research Agency troll and bot networks and GRU hack-and-leak operations sought to polarize American voters (Mueller, 2019; Zannettou et al., 2019).

3.3. *POSSIBLE EFFECTS*

Effects range from confusion and polarisation to declining trust in media, science and elections, harassment of journalists, and behavioural harm such as vaccine hesitancy. Yet RAND finds limited evidence that campaigns change strongly held beliefs; their power lies in intimidating, dividing and discrediting (Cohen et al., 2021).

Figure 2. Three emblematic cases of disinformation as warfare



Sources: Rid (2020); Olejnik (2024); Splidsboel Hansen (2017); Mueller (2019); Zannettou et al. (2019).

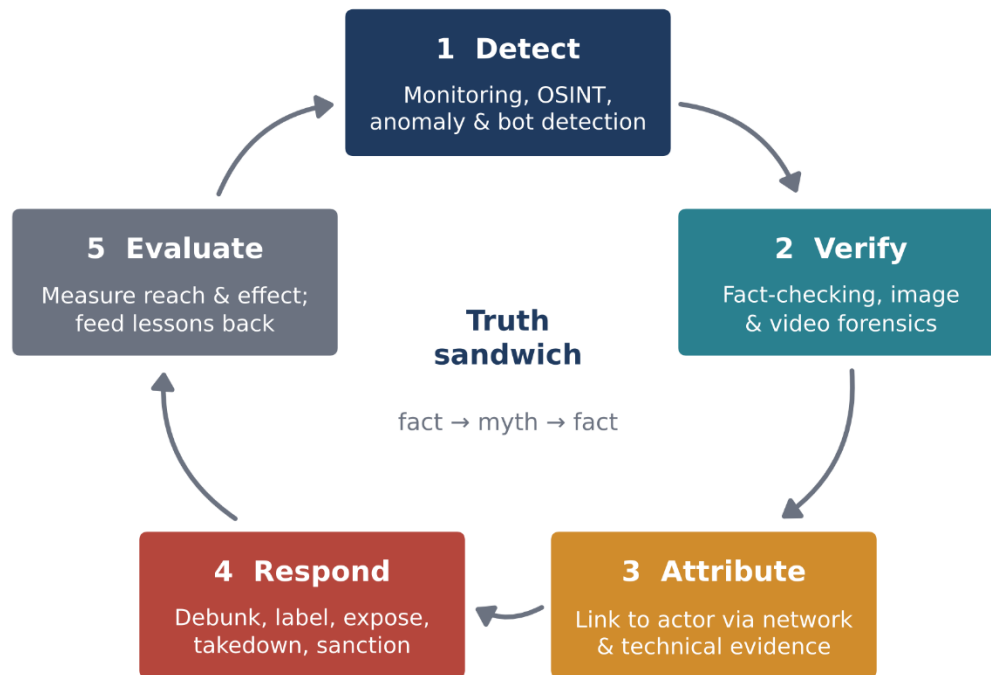
3.4. **DANGERS TO NATIONAL SECURITY**

For national security, disinformation is a cheap, deniable force multiplier. It can weaken social cohesion and the legitimacy of government, the “horizontal” and “vertical” legitimacy that hybrid strategies target, and thereby a nation’s will to resist (Splidsboel Hansen, 2017). It can distort leaders’ situational awareness during crises, provoke panic or violence, strain alliances such as NATO and the EU, and erode civil–military trust and troop morale. It can also prepare the ground for kinetic action, as in Crimea in 2014. Deepfakes add the risk that fabricated orders or incidents trigger escalation (Chesney & Citron, 2019; Cohen et al., 2021).

4. **POSSIBLE MECHANISMS FOR DEBUNKING DISINFORMATION CAMPAIGNS**

Effective debunking is a cycle rather than a single correction (Figure 3). Monitoring and open-source intelligence detect suspicious narratives and coordinated accounts; fact-checkers and forensic analysts verify claims and media; analysts attribute campaigns using network and technical evidence; and governments, platforms and media respond through corrections, labelling, account takedowns and public exposure. Corrections work best when quick, delivered by trusted messengers and structured as a “truth sandwich”: lead with the fact, flag the myth once, restate the fact (Lewandowsky & van der Linden, 2021). Because falsehood spreads faster than truth (Vosoughi et al., 2018), speed and measured impact matter.

Figure 3. The debunking cycle

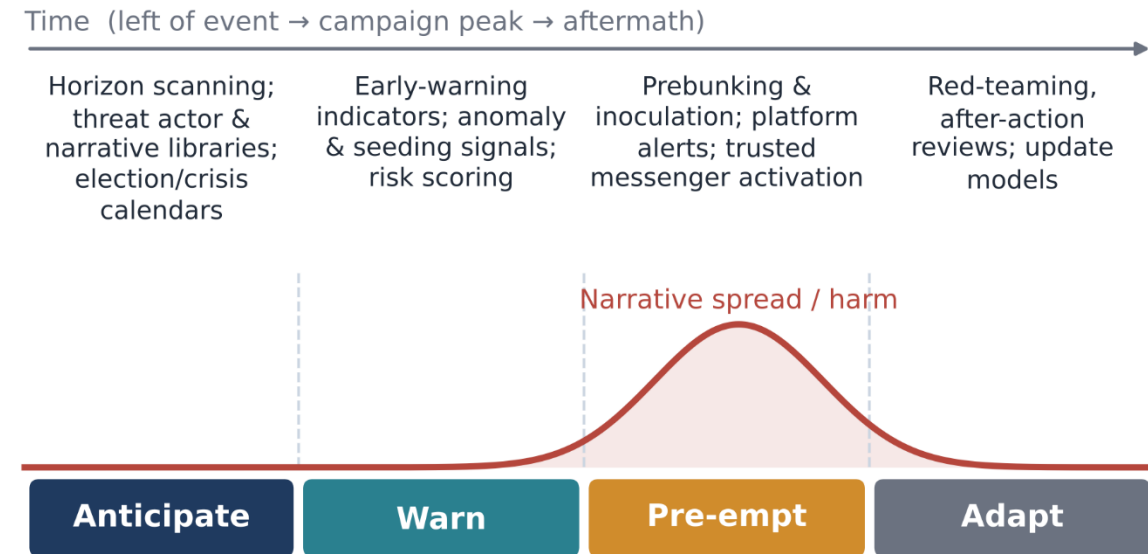


Based on Cohen et al. (2021), Lewandowsky & van der Linden (2021) and Olejnik (2024).

5. APPROACHES TO ORGANIZING PREDICTIVE COUNTER-DISINFORMATION SECURITY

Predictive security moves effort “left of launch” (Figure 4). First, *anticipation*: horizon scanning of adversary doctrine, recurring narratives and high-risk moments such as elections, summits or military exercises. Second, *early warning*: indicators such as bursts of new accounts, synchronized posting, or seeding on fringe platforms like 4chan before mainstream amplification (Zanetti et al., 2019), combined into risk scores. Third, *pre-emption*: preventive measures and psychological awareness, which measurably improve people’s ability to spot manipulation techniques (Rozenbaum et al., 2022), plus pre-agreed protocols with platforms. Finally, *adaptation* through red-teaming and after-action reviews. Prioritization matters, since not every incident deserves a response that may amplify it (Olejnik, 2024).

Figure 4. Organising predictive counter-disinformation security



Illustrative curve, based on Roozenbeek et al. (2022), Cohen et al. (2021) and EEAS (2023).

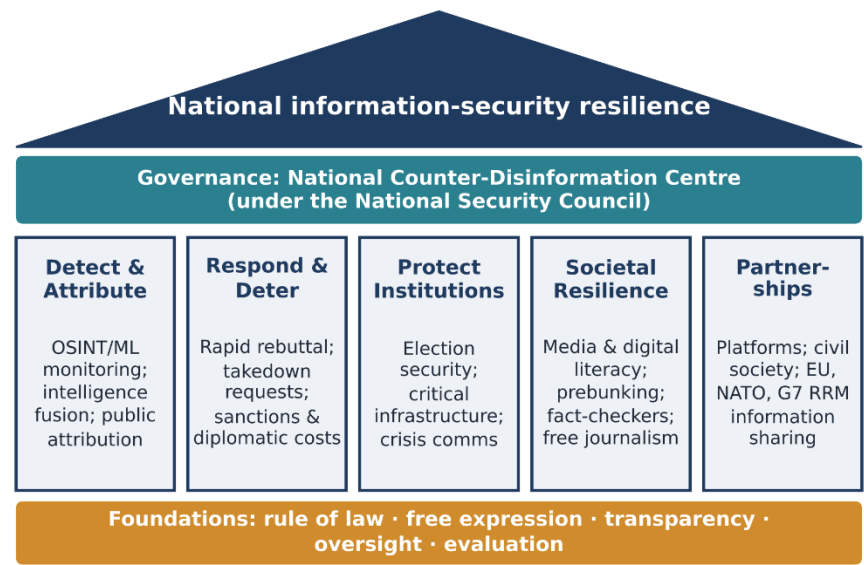
6. THE POSSIBLE ROLE OF MACHINE LEARNING IN DEBUNKING EFFORTS

Machine learning makes detection possible at scale. Supervised classifiers flag likely false content from linguistic, source and propagation features (Shu et al., 2017); graph analytics and anomaly detection expose bot networks and coordinated inauthentic behavior; computer-vision models detect manipulated images and deepfakes; and statistical models such as Hawkes processes estimate how narratives travel between platforms (Zanetti et al., 2019). Reinforcement learning, in which an agent learns by trial and reward (Harmon & Harmon, 1996), could help optimize when and how to respond. Yet adversaries use the same AI to generate content, and models produce false positives. Machine learning should therefore support, not replace, human analysts, under transparent and accountable governance.

7. A NATIONAL STRATEGY AGAINST WARFARE-DISINFORMATION

A national strategy should be whole-of-society and anchored in democratic values (Figure 5). A National Counter-Disinformation Centre under the National Security Council would coordinate ministries, intelligence services and the armed forces, overcoming the fragmentation RAND observed in the United States (Cohen et al., 2021). Five pillars follow: detection and attribution; rapid response and deterrence, including sanctions; protection of elections and critical institutions, drawing on models such as Canada's election-security arrangements (Tuttle, 2019); societal resilience through media literacy and independent journalism, as in Finland (Aro, 2016; Horowitz, 2019); and partnerships with platforms, civil society, the EU and NATO. Every measure must respect freedom of expression.

Figure 5. Architecture of a national strategy against warfare-disinformation



Based on Cohen et al. (2021), Horowitz (2019), Tuttle (2019) and Aro (2016).

8. CONCLUSION: RESTORING THE INTERNATIONAL ALLIED FRONT

The case for allied cooperation is not new; it was made first, and most forcefully, by the United States. Two decades ago, American scholars, think tanks such as RAND and government agencies were already mapping how hostile states weaponise information, building on Cold War experience of exposing Soviet active measures. Washington then worked systematically to inform its European allies of the threat and to motivate them to build comparable capabilities. Through the State Department's Global Engagement Center, established in 2016, the United States funded research, shared analytic tools and supported a joint international initiative of friendly and trustworthy nations, culminating in the 2024 Framework to Counter Foreign State Information Manipulation. Its underlying lesson was plain: disparate national efforts against well-resourced and persistent adversaries such as Russia, China and Iran are doomed to fail, because disinformation crosses borders faster than any single government can respond. Seen in this light, the contributors to the DISINFO 2026 controversy were ill-advised. Losing focus of the forum domain, which is dedicated to countering foreign manipulation, weakens the very coalition that America helped to build, and hands the adversaries an easy propaganda victory. The related causes of the controversy must be reconsidered immediately, and the ensuing damage to allied trust and joint capability urgently repaired. The organization of such strategically important conferences should take into account contributions and reviews by allied institutions, as they do not only facilitate the exchange of ideas and concerns, but they project coherent allied messages and strategic postures.

About the author

Angelos Kolokouris, born in Vlahiotis-Laconia Greece, obtained a BSc in physics from CUNY USA, followed by graduate studies in nuclear engineering and an interdisciplinary Master's in quantum mechanics at Penn State, and doctoral studies in Philosophy (Mathematical Logic) and Computer Science at Temple University, focusing on the Logical Foundations of AI. In the 1980s and thereafter, his companies played a pioneering role in theoretical & applied AI, developing PROLOG interpreters & systems tools and implementing major AI systems in critical civic and defense areas. He works on AI policy and R&D mostly to (a) counter disinformation and (b) implement predictive AI systems.

9. RELEVANT BIBLIOGRAPHY

- Araźna, M. (2015). Conflicts of the 21st century based on multidimensional warfare – “hybrid warfare”, disinformation and manipulation. *Security and Defence Quarterly*, 8(3), 103–129.
- Aro, J. (2016). The cyberspace war: Propaganda and trolling as warfare tools. *European View*, 15(1), 121–132. <https://doi.org/10.1007/s12290-016-0395-5>
- Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. Oxford Internet Institute.
- Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147–155.
- Cohen, R. S., Beauchamp-Mustafaga, N., Cheravitch, J., Demus, A., Harold, S. W., Hornung, J. W., Jun, J., Schwille, M., Treyger, E., & Vest, N. (2021). *Combating foreign disinformation on social media: Study overview and conclusions* (RR-4373/1-AF). RAND Corporation.
- Harmon, M. E., & Harmon, S. S. (1996). *Reinforcement learning: A tutorial*. Wright Laboratory, Wright-Patterson Air Force Base.
- Horowitz, M. A. (2019). Disinformation as warfare in the digital age: Dimensions, dilemmas, and solutions. *Journal of Vincentian Social Action*, 4(2), Article 5.
- Lewandowsky, S., & van der Linden, S. (2021). Countering misinformation and fake news through inoculation and prebunking. *European Review of Social Psychology*, 32(2), 348–384. <https://doi.org/10.1080/10463283.2021.1876983>
- Mueller, R. S., III. (2019). *Report on the investigation into Russian interference in the 2016 presidential election* (Vol. 1). U.S. Department of Justice.
- Olejník, L. (2024). *Propaganda: From disinformation and influence to operations and information warfare*. CRC Press.
- Paul, C., & Matthews, M. (2016). *The Russian “firehose of falsehood” propaganda model: Why it might work and options to counter it* (PE-198-OSD). RAND Corporation. <https://doi.org/10.7249/PE198>
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances*, 8(34), Article eabo6254. <https://doi.org/10.1126/sciadv.abo6254>

- Splidsboel Hansen, F. (2017). *Russian hybrid warfare: A study of disinformation* (DIIS Report 2017:06). Danish Institute for International Studies.
- Tuttle, D. (2019). *Campaigns of disinformation: Modern warfare, electoral interference, and Canada's security environment* [Master's capstone project, University of Calgary]. SSRN. <https://ssrn.com/abstract=3437117>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (DGI(2017)09). Council of Europe.
- Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web. In *Companion Proceedings of the 2019 World Wide Web Conference* (pp. 218–226). ACM. <https://doi.org/10.1145/3308560.3316495>