

National Strategies on Countering Disinformation in Selected EU Countries: Lessons for Poland

Project acronym:	SAUFEX
Due date of deliverable:	Jul 25, 2024
Actual submission date:	Jul 25, 2024
Work Package	
Lead Beneficiary:	
Dissemination level:	PUB
Status:	Draft/ Issued

Research Paper

Ву

Paweł Kasprzyk

WARSAW 2024



National Strategies on Countering Disinformation in Selected EU Countries: Lessons for Poland

Research Paper

Ву

Paweł Kasprzyk

WARSAW 2024

Document history		
Revision	Date	Description
1		First draft
2		

Contributors	Beneficiary Short Name	Details of contribution
pkpawelkasprzyk@gmail.		Structure and outlines. Lead Author
com		
Bram Alkema	DROG	Codependencies in the project
		Layout
All & Person	All	Checks and text

Table of Changes

	Document history		
	Type	Bookmark	Version
1	Add		2

Table of Contents

Summary	1
Introduction	2
Disinformation and Foreign Information Manipulation and Interference as	
Threat to Democratic Societies	
Challenges in Countering Disinformation for Democratic States	
Further Challenges	
Introduction to Foreign Information Manipulation and Interference (FIMI)	11
The Polish Information Landscape and Approaches to Countering Disinfo	
and FIMI	
The Disinformation Threat Landscape in Poland	
The Polish Legal System's Regulations Against Online Harms	
Polish Institutional Approaches to Countering Disinformation	
Cross-Sectoral Cooperation and the Role of Civil Society	
Existing National Strategies for Countering Disinformation in EU Member	
The European Union's Approach to Countering Disinformation	
EU Member States' National Strategies for Countering Disinformation	
The Netherlands	
Latvia	
Ireland	25
Comparative Analysis	
Analysis of the Dutch and Irish National Strategies for Countering Disinfo	rmation
27	
How Do the Selected Strategies Characterise the Threat of Disinformation	?28
What Is the Role of FIMI in the Existing European National Strategies for	71
Countering Disinformation?	
What Approaches to Countering Disinformation and FIMI Do the Strategic Envisage?	
Dutch Strategy Approaches	
Track 1: Strengthening the Free and Open Public Debate	
Track 2: Reducing the Influence of Disinformation	
Irish Strategy Approaches	
Role of Non-State Actors	
International Cooperation	
Legislative Frameworks	
Differences in Approaches	
Funding and Resource Allocation	
Specific Measures Against FIMI Navigating the Democratic Dilemma	
inavidating the Democratic Dilemma	57

Final Remarks	38
Bibliography	41
Analysis Material	48
Annex	
Track I: Strengthening the Public Debate	49
Action: Retaining the Pluralistic Media Landscape	49
Action: Strengthening Citizens' Resilience	49
Action: Stimulating and Using Public Alternatives to Online Platforms	49
Track II: Reducing the Influence of Disinformation	50
Efforts Depending on the Content of Disinformation	50
Increasing Awareness in Governmental Organisations About Disinform 50	ation.
National and International Standards	50
Efforts Depending on the Disseminator or Producer of Disinformation	50
Commitment to the Responsibility of Traditional Media and Online Platfor	ms51
Traditional Media	
Social Media Platforms	51
Knowledge Development	51

Summary

Modern societies produce and consume information at a fundamentally bigger scale and higher speed than before. The driving force behind this change---technological advancement---has also allowed for the proliferation of false or misleading information to 'pollute' the information environment and challenges the fact-based exchange of information underpinning democratic debate. As a consequence, societal trust in democratic institutions, political processes, and values is diminishing. States and international organisations struggle to reform existing architectures to meet the new reality while preserving principal democratic values.

This research paper examines the national strategies for countering disinformation of the Netherlands and Ireland. It explores current EU approaches to countering disinformation with an emphasis on the concept of Foreign Information Manipulation and Interference (FIMI), guided by the following research questions:

- How do the selected strategies characterise the threat of disinformation?
- What is the role of FIMI?
- What approaches to countering disinformation and FIMI do the strategies envisage?

The analysis of the selected strategies revealed that both the Netherlands and Ireland have adopted definitions of disinformation and misinformation as provided by the EU. Ireland and the Netherlands share an understanding that the threat of disinformation lies in the societal harm it carries for democracies. The main difference between the two terms is the presence of malintent in the former and lack thereof in the latter.

Moreover, the strategy planners of both countries identified the European External Action Service's (EEAS) concept of FIMI as a key concern due to an increased use of information operations and disinformation by foreign actors. The Netherlands considers FIMI in the broader context of hybrid threats and the risk it poses to national security and the stability of international organisations. Importantly, the FIMI concept's focus on behaviour and operational methods, as well as a holistic approach mobilising whole-of-society resources, have all been incorporated in the strategies, albeit without the particular focus on the "foreign" element.

Both national strategies underlined that the democratic rule of law, freedom of speech, and media must take centre stage in countering disinformation. Both also emphasised the importance of cross-sectoral cooperation among civil society, the private sector, and transnational partners. Both countries also considered targeted media literacy and educational measures and campaigns. Finally, both countries emphasise the importance of implementing and enforcing a number of legislative frameworks at the EU level, most notably the EU Digital Services Act (DSA). However, as the strategies focus on countering disinformation, only a few action items explicitly targeting FIMI have been identified.

The key findings of the analysis are mirrored against the Polish disinformation threat landscape and approaches to countering disinformation and FIMI. Polish state agencies and civil society organisations have scaled up capabilities and measures to counter disinformation in Poland. However, there are no clear guidelines for public institutions on counteracting disinformation, and a decentralised approach hinders situational awareness and efforts of a coordinated response. While Polish society is increasingly polarised and less than half of Poles trust their government and standard media, the paper concludes that developing a national strategy to counter disinformation would be a good point of departure.

Introduction

Information is part of the human ecosystem, no less essential than water, air and food for it helps determine in a similar way one's survival and quality of life.

--- Robert Kupiecki (2020)¹

The information environment is changing rapidly due to technological advances and the extensive use of information technology in modern societies' daily lives. Technological advances have certainly altered how information is produced, shared, and consumed.² Sociology scholar Manuel Castells (2004) characterised the modern era as 'the Information Age' and the emergence of 'Network Societies', showcasing larger cultural and structural changes from industry-based to modern communication technology-powered societies.³

Media pluralism, freedom of speech, and open public deliberations are key tenets of a democratic society.⁴ Access to a variety of independent news sources and holding free discussions in the public sphere are considered to help people make informed choices and rational decisions. However, the carrying out of these key principles has been altered by the rapid technological development in digital communication tools and new forms of civic engagement.

A March 2024 report from the Organisation for Economic Co-operation and Development (OECD) stated, "mis- and disinformation presents a fundamental risk to

¹R. Kupiecki, *Disinformation and International Relations: Sources, Aims, Actors, Methods* in *Disinformation and the Resilience of Democratic Societies*, R. Kupiecki & A. Legucka (eds.), 15--36. The Polish Institute of Foreign Affairs, Warsaw, 2023. ISBN 978-83-67487-20-7, p. 15. ²J.M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, New York University Law Review, vol. 79(1), 2004 Yale Law School, Public Law Working Paper No. 63, 1--55. DOI: http://dx.doi.org/10.2139/ssrn.470842, [date published 03.12.2003], pp. 1--5.

³M. Castells (ed.), *The Network Society---A Cross-cultural Perspective*, Edward Elgar Publishing, Inc., Cheltenham, United Kingdom, 2004, ISBN: 1-84376-505, pp. 3--9.

⁴European 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) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0790 [date published 03.12.2020].

the free and fact-based exchange of information underpinning democratic debate." The dissemination of false and misleading information is widely understood to deceive and obstruct public debates, polarise societies, and undermine democratic processes. The rapid growth of online platforms has also opened up new vulnerabilities by fundamentally changing the reach and nature of disinformation, as well as the speed with which it spreads. Moreover, digital technologies and their regulations have brought new dimensions to authoritarian regimes, making it easier to manipulate content and monitor dissent and political opponents.

There exist a variety of concepts and definitions to describe risks to the online information environment. In 2020, the Carnegie Endowment for International Peace provided an overview of four categories: misinformation, disinformation, influence operations, and foreign interference. These can be either domestically grown or foreign-inspired campaigns.⁸

The European Union defines misinformation as "false or misleading content shared without harmful intent though the effects can be still harmful." The definition of disinformation includes the sharing of false and misleading content but requires the "intention to deceive or secure economic or political gain, and which may cause public harm." Disinformation may be disseminated in a variety of forms, including satire, misleading content, fabricated, false or fake content, or misattributed and manipulated content. To

Additionally, malinformation refers to situations in which genuine information is spread opportunistically or represented out of context to cause harm. These operations often involve moving private information to the public domain, for instance, through hack and leak operations. These terms need to be separated from terrorist, violent, or illegal content online, which usually have separate measures or

⁵The Organisation for Economic Co-operation and Development (OECD). Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity.

https://www.oecd-ilibrary.org/sites/d909ff7a-en/1/3/1/index.html [date published 04.03.2024].

⁶R. Kupiecki, *Disinformation and International Relations: Sources, Aims, Actors, Methods*, p. 19. ⁷S. Cipers, T. Meyer & J. Lefevere, *Government Responses to Online Disinformation Unpacked*, Internet Policy Review vol. 12(4), 1--19. DOI: https://doi.org/10.14763/2023.4.1736 [date published 11.12.2023], p. 3.

L. Turčilo & M. Obrenović, *Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy.* Heinrich Böll Foundation, 2020, 1--38. https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_ENG.pdf [date published 25.08.2020], p. 4.

⁸J. Pamment, *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework.* Carnegie Endowment for International Peace, Washington DC, United States, 1--18. https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720 [date published 24.09.2020].

⁹European Commission. *Tackling Online Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation [date published 08.05.2024].

¹⁰R. Kupiecki, *Disinformation and International Relations: Sources, Aims, Actors, Methods*, pp. 26--27.

¹¹L. Turčilo & M. Obrenović, *Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy*, p. 8.

legal frameworks to deal with.

On the other hand, the main difference between information influence and disinformation is in the operational components. Accordingly, disinformation highlights the intent in the message content, while information influence focuses on the communication techniques establishing a coordinated effort to influence a society. Influence operations may be defined as coordinated and persistent adversarial efforts by malign individuals or groups to influence society through hybrid means. In

In a December 2023 Eurobarometer, the most frequently listed threat to democracy was "false and/or misleading information in general circulating online and offline" (38 percent), followed by "growing distrust and scepticism towards democratic institutions" (32 percent of respondents). The spread of false or manipulated information is also increasingly permeating Polish society---according to the 2024 report *Disinformation through the Eyes of Poles* by the Digital Poland Foundation, as many as 84 percent of Poles have encountered fake news. Despite the growing awareness of the phenomenon of disinformation, only half of Poles feel safe on the internet. The spread of the phenomenon of disinformation, only half of Poles feel safe on the internet.

Disinformation diminishes societal trust in institutions, political processes, and values in democratic states. It weakens the foundations of good governance and restricts people's rationality in deciding on issues as important and requiring true and verified information as, for example, their health or security.¹⁶

These threats have forced democratic governments to reassess their responsibilities regarding the safety of the online space. European states and international organisations have taken a variety of measures tailored to guard three key normative

_

¹²J. Pamment, *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework*. ¹³The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) characterises hybrid threats as "coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means." Such means include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force aiming to influence different forms of decision-making at the local, state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). *Hybrid Threats as a Concept*. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ [date published 01.01.2024].

H. Smith & G. Giannopoulos, *The Landscape of Hybrid Threats: A Conceptual Model*, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)/Joint Research Centre, 1--54. ISBN 978-92-76-29819-9 [date published 01.02.2021], pp. 32--33.

14 European Union. *Eurobarometer Key Findings*.

https://europa.eu/eurobarometer/surveys/detail/2966 [date published 12.12.2023].

¹⁵P. Mieczkowski & M. Kilian-Grzegorczyk (eds.), *Dezinformacja Oczami Polaków*. Fundacja DigitalPoland, 1--133. ISBN 978-83-971647-0-3.

https://digitalpoland.org/en/publications/download?id=34ce5eac-1789-426c-af9b-cc091f5c23a8 [date published 01.04.2024], pp. 11, 15.

¹⁶R. Kupiecki, F. Bryjka & T. Chłoń, *Dezinformacja Międzynarodowa. Pojęcie, Rozpoznanie, Przeciwdziałanie.* Wydawnictwo Naukowe Scholar, Warsaw, 2022, p. 98.

goods: self-determination or national security, accountable representation of democratic governance (election regulation), and open public deliberation.¹⁷ Specific choices of actions and their scale vary between different countries.

Ultimately, there is no one-size-fits-all solution to this problem. Several states have focused on investing in media literacy and education programs to strengthen their civil society's resilience. Some have established new institutional structures for enhanced content monitoring capabilities, such as the French VIGINUM (Vigilance and Protection Service against Foreign Digital Interference)¹⁸ or the Swedish Psychological Defence Agency.¹⁹ The diverse set of policy interventions also includes imposing foreign sanctions, disruption, supporting local journalism, and counter-messaging campaigns. Only a few have developed dedicated strategies, policies, or laws targeting disinformation or influence operations.²⁰

As the digital realm and information flow without country borders, national governments cannot solve the issue alone. Additionally, in response to increased scrutiny from states and civil society, online platforms have established content moderation initiatives and partnerships with fact-checking organisations to respond to these threats.

This research paper examines the national strategies for countering disinformation in selected EU countries. At the time of writing, three countries have a strategy while Ireland's strategy is being finalised. These countries are the Netherlands, Latvia, and Romania. This thesis will focus on the Dutch and Irish strategies.

In addition to the characterizations described above, the EU's European External Action Service (EEAS) has developed another concept to counter the disinformation

¹⁷The latter refers to threats to the quality of public debate and deliberation.

D.M. West, How to Combat Fake News and Disinformation.

https://www.brookings.edu/articles/how-to-combat-fake-news-and-disinformation/ [date published 18.12.2017].

C. Tenove, Protecting Democracy from Disinformation: Normative Threats and Policy Responses, The International Journal of Press/Politics, 25(3), 2020, 517--537. DOI: 10.1177/1940161220918740 [date published 25.05.2020], pp. 517, 520--521.

¹⁸General Secretariat for Defence and National Security of France (SGDSN). *Vigilance Service and Protection Against Foreign Digital Interference*.

https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques [date published 17.11.2022].

¹⁹Swedish Psychological Defence Agency.

https://www.mpf.se/psychological-defence-agency/about-us/our-mission [date published 15.03.2024].

²⁰J. Bateman & D. Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace, Washington DC, USA, 1--119. https://carnegieendowment.org/2024/01/31/countering-disinformation-effectively-evidence-based-policy-guide-pub-86272 [date published 31.01.2024], pp. 1--8.

M.G. Sessa, Connecting the Disinformation Dots---Insights, Lessons, and Guidance from 20 EU Member States, EU DisinfoLab and Friedrich Naumann Foundation for Freedom, December 2023, 1--12.

https://www.disinfo.eu/wp-content/uploads/2023/12/20231204_Connecting-disformation-dots_comparative-study-1.pdf [date published 05.12.2023], p. 9.

phenomena, the Foreign Information Manipulation and Interference (FIMI) concept. Foreign information manipulation and interference has increasingly been recognized as a political and security threat for the EU. Since 2015, the EEAS has taken the leading role in the EU in addressing FIMI. The EEAS defines FIMI as "a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character,"²¹

By examining the Dutch and Irish national strategies, the research paper aims to scope and understand the current approaches to countering disinformation in the EU and explore the emphasis on foreign information manipulation and interference in the existing national strategies.

These research objectives will be explored through the following research questions:

- How do the selected strategies characterise the threat of disinformation?
- What is the role of FIMI in the existing European national strategies for countering disinformation?
- What approaches to countering disinformation and FIMI do the strategies envisage?

The analysis will be conducted through a comparative analysis of the Dutch and Irish strategies. Comparative analysis is to identify, describe, and explain similarities and differences between both quantitative and qualitative comparisons of units of analysis.²² The objective is not only to find variance, but the findings provide context and allow for a deeper understanding of the specificity between the study objects and reveal unique aspects of a particular entity that would be hard to detect otherwise.²³ As literature for the analysis, the thesis will use the 2022 Dutch strategy to counter disinformation. While the Irish strategy is not finalised, publicly available information on working group meetings and scoping papers will be analysed instead.

The thesis will begin with an extensive review of existing literature on disinformation and FIMI, emphasising their threats to democratic societies to set up the research problem. The review will also examine the tactics and consequences of disinformation and FIMI on democratic societies. Before introducing and analysing the disinformation strategies of the Netherlands and Ireland, the thesis will introduce the Polish information landscape and explain the current Polish system of countering disinformation and FIMI.

At the moment, Poland does not have a dedicated strategy for countering

²¹European Union External Action Service (EEAS). *Tackling Disinformation, Foreign Information Manipulation & Interference*.

https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en [date published 27.05.2024].

²²S. Drobnič, *Comparative Analysis* in *Encyclopedia of Quality of Life and Well-Being Research*, A.C. Michalos (ed.), Springer, Dordrecht, 2014. ISBN: 978-94-007-0753-5, pp. 1125--1127.

²³M.C. Mills, G.G. van de Bunt, J.G.M. de Bruijn, *Comparative Research: Persistent Problems and Promising Solutions, International Sociology*, 2006, vol. 21(5): 619--631. DOI: 10.1177/0268580906067833, pp. 621--622.

disinformation. By exploring the three research questions, the study aims to provide practitioners in Poland and other countries with a deeper understanding of the current trends in Europe concerning the countering of disinformation and offer insights to the problem by largely following the EEAS concept of Foreign Information Manipulation and Interference (FIMI). The key findings of the analysis will then be mirrored against the Polish case to seek answers to the possible applicability of a national strategy for Poland in countering disinformation.

Disinformation and Foreign Information Manipulation and Interference as a Threat to Democratic Societies

Mis- and disinformation or information manipulation are not new phenomena; information distortions and propaganda have existed for centuries. For example, disinformation as a political tool of influencing others in interstate relations has been used in times of war and peace from the earliest times. "The goal has always been to gain an advantage over the opponent, to disrupt their situational awareness, and thus to make it difficult to overcome the decision fog---the inherent uncertainty of a decision concerning a more or less distant future."²⁴

However, digitalisation has fundamentally changed its reach and impact. In a fast-paced information environment, individual users continue to interpret and search for information that suits their own views and attitudes, possibly helping to spread false content and providing the opportunity for foreign actors to interfere.²⁵ It is an issue eroding the democratic systems across Europe.

Since the mid-2010s, disinformation has become a central topic for the EU due to Russian information manipulation and interference accompanying its war against Ukraine in 2014, the 2016 Brexit referendum, the 2017 French presidential election, and the 2019 European Parliament election. The 2020 COVID-19 pandemic witnessed an unprecedented surge of global misinformation and disinformation narratives, conspiracies, and questioning of health and science authorities amplified by the increased use of information technologies, such as social media. The false information on the virus, vaccines, and cures was spread online by private individuals, groups, foreign states and often amplified by news outlets and politicians. This caused an unprecedented questioning and mistrust of state authorities and verified science in democratic societies and alienated societies and even families.

²⁴R. Kupiecki, *Disinformation and International Relations: Sources, Aims, Actors, Methods*, pp. 17--18.

²⁵A. Westerwick, B. Johnson & S. Westerwick, "Confirmation Biases in Selective Exposure to Political Online Information: Source Bias vs. Content Bias," *Communication Monographs*, 84(3), 2017: 343--364. DOI: 10.1080/03637751.2016.1272761 [date published 08.05.2017], pp. 5--9. ²⁶K. Juhász, "European Union Defensive Democracy's Responses to Disinformation," *Journal of*

²⁶K. Juhász, "European Union Defensive Democracy's Responses to Disinformation," *Journal of Contemporary European Studies*, 1--20. DOI: <u>10.1080/14782804.2024.2317275</u> [date published 15.02.2024], pp. 1, 16.

E. Ferrara, S. Cresci & L. Luceri, "Misinformation, Manipulation, and Abuse on Social Media in the Era of COVID-19," *Journal of Computational Social Science*, 3, 271--277. DOI: 10.1007/s42001-020-00094-5 [date published 22.11.2020], pp. 272--273.

²⁷S.L. Vériter, C. Bjola & J.A. Koops, "Tackling COVID-19 Disinformation: Internal and External Challenges for the European Union," *The Hague Journal of Diplomacy*, 15(4), 569--582. DOI: 10.1163/1871191X-BJA10046 [date published 21.10.2020], pp. 570--573.

Challenges in Countering Disinformation for Democratic States

Democratic societies are founded on the principle that free, equal, and engaged citizens deliberate on common affairs with the aim to reach a consensus and make decisions on public matters, such as in elections. Ideally, their decisions should be rational and based on the best available information. Decision-making grounded in facts and truth allows individuals to debate and make informed decisions based on rationality.²⁸

Securing access to accurate information is essential for making rational decisions. Properly processed data enables individuals or groups to choose actions that optimally achieve their goals without harming others.²⁹ Lack of access and a common baseline of truth may lead to ideological or virtual reality bubbles with fractured beliefs and truths, altering democratic politics from mutual persuasion and tolerance, and descending into a process of endless partisan manipulation and polarisation.³⁰ This then increases negative sentiment and mistrust towards state institutions and official messaging, which opens society to vulnerability from foreign interference and more disinformation.

An example of a baseline of truth is social confidence in election results. Yet according to the U.S. National Intelligence Council report on Foreign Threats to the 2020 U.S. Federal Elections, by denigrating mail-in voting, highlighting alleged irregularities, and accusing the Democratic Party of engaging in voter fraud, "throughout the election cycle, Russia's online influence actors sought to affect U.S. public perceptions of the candidates, as well as advance Moscow's long standing goals of undermining confidence in U.S. election processes and increasing socio-political divisions among the American people." As observed by the non-profit Brookings Institution, "The 'big lie' reinforced by President Trump about the 2020 election results amplified the Russian efforts and has lasting implications on voters' trust in election outcomes." ³²

In many democracies, the spread of disinformation can be traced to growing legitimacy problems. The UN Special Rapporteur on Freedom of Opinion and Expression, Irene Khan, stated that "disinformation is not the cause but the consequence of societal crises and the breakdown of public trust in institutions. Strategies to address disinformation are unlikely to succeed without more attention being paid to these underlying factors." Although for any democracy the need to

²⁸G. Terzis, D. Kloza, E. Kużelewska & D. Trottier (eds.), *Disinformation and Digital Media as a Challenge for Democracy*, Intersentia, 2020, ISBN: 9781839700422, p. xix.

²⁹R. Kupiecki, *Disinformation and International Relations: Sources, Aims, Actors, Methods*, pp. 16--17.

³⁰G. Terzis et al., *Disinformation and Digital Media as a Challenge for Democracy*, p. vi. ³¹U.S. National Intelligence Council, *Foreign Threats to the 2020 U.S. Federal Elections* (ICA 2020-00078D), 1--10.

https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf [date published 10.03.2021], p. 3.

³²G.R. Sanchez & K. Middlemass, "Misinformation Is Eroding the Public's Confidence in Democracy," <u>Brookings Institution</u> [date published 27.07.2022].

³³United Nations General Assembly, *Disinformation and Freedom of Opinion and Expression*:

address these underlying factors would be undeniable, an information environment dense with disinformation can lead to a vicious circle of cause and consequence, effectively destabilising a democratic country. Moreover, "declining citizen confidence in institutions undermines the credibility of official information in the news and opens publics to alternative information sources. Those sources are often associated with both nationalist (primarily radical right) and foreign (commonly Russian) strategies to undermine institutional legitimacy and destabilise centre parties, governments and elections."³⁴

Therefore, it would seem that an erosion of trust in public institutions, processes, and authorities leads people to all sorts of charlatans who then further diminish that trust by means of disinformation.

In the modern digital world, the role of information gatekeepers performed by traditional media has largely been broken, and information is now produced, shared, and consumed by individuals on a mass scale with little, if any, quality control. This change has allowed malign actors to directly target and permanently influence the behaviour of large groups of people (including in other countries) more freely than ever. By intentionally 'weaponizing' disinformation in a coordinated manner, malign foreign actors aim to destroy cultural or common-sense foundations of societies as a whole.

The omnipresent disinformation in the modern information space ceases to be an anomaly and becomes a common phenomenon which coexists with reliable knowledge.³⁵ The prevalence of disinformation coupled with advanced digital capabilities of fabricating data makes it increasingly difficult to distinguish between true and false content. This may lead to a disruption of the ability to identify trusted and authentic content, as well as to undermining citizens' trust in the media and official information messages. As a consequence, this may constitute the basis for a dissolution of societies and threatens democratic processes.

Further Challenges

The primary issues in countering disinformation by democratic states are related to classifying and defining relevant concepts for regulatory purposes and policy-making, and balancing democratic norms with content moderation, online platform control with economic incentives, and innovation.

While establishing a basic understanding of truth and accurate information is

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Irene Khan (A/HRC/47/25).

https://www.eods.eu/template/default/compendium/Part%204/009_Disinformation_and_freedom_of_opinion_and_expression.pdf [date published 13.04.2021], p. 5.

³⁴W.L. Bennett & S. Livingston, "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions," *European Journal of Communication*, 33(2), 2018, 122--139. DOI: 10.1177/0267323118760317 [date published 02.04.2018], p. 122.

³⁵R. Kupiecki, *Disinformation and International Relations: Sources, Aims, Actors, Methods*, p. 35.

important, countering disinformation is also challenging due to the inherent nature of the political and legal systems of democracies, specifically in relation to upholding the principle of media pluralism and the dissemination of information.³⁶ Democratic states also struggle to balance freedom of expression and free speech with harmful content, hate speech, and disinformation, protecting user privacy, and rewarding economic innovation in Big Tech. Democracies rely on broad social consent, a culture of freedom of choice, and tolerance.³⁷ Disinformation actors can exploit this culture of freedoms and inconsistency of behaviour to influence the functioning of democratic societies.

Critics of countermeasures often invoke threats to freedom of expression or assert the risks of so-called 'truth ministries.' For instance, Karppinen (2019) noted that narratives on regulations that undermine freedom of expression are "often mobilised by those in power to block reforms and close down debate" while underestimating other obstructions to public discourse such as algorithm distortion or large platform dominance.³⁹

The starting point of many national and international efforts in countering disinformation often falls under pre-bunking or de-bunking activities. Pre-bunking refers to pre-emptive strategies and actions to halt disinformation before it occurs. Examples of these strategies are increasing citizens' resilience through media literacy programmes or active official communication of the potential threats ahead of large events, such as elections. De-bunking includes counter-messaging to expose false narratives that are already circulating in the information domain. A prominent example of de-bunking is fact-checking.

However, a lack of conceptual clarity also affects the acceptance of counter-disinformation policies.⁴² Despite increasing efforts in mitigating and countering disinformation, information influence, and foreign interference, there is no agreed terminology or common consensus for categorising capabilities for countering

Responses," *The International Journal of Press/Politics*, 25(3), 2020, 517--537. DOI: 10.1177/1940161220918740 [date published 25.05.2020], p. 531.

³⁶Ibid., p. 31.

³⁷S. Feldstein, "Introduction" in *Issues on the Frontlines of Technology and Politics*, S. Feldstein (ed.), Carnegie Endowment for International Peace, Washington DC, USA, 2021, 1--6. https://carnegieendowment.org/2021/10/19/issues-on-frontlines-of-technology-and-politics-pub-28555 [date published 19.10.2021], p. 1.

³⁸K. Karppinen, "Freedom without Idealization: Non-ideal Approaches to Freedom of Communication," *Communication Theory*, 29(1), 66--85. DOI: <u>10.1093/ct/qty013</u> [date published February 2019], p. 72.

³⁹Ibid., p. 68.

disinformation or influence operations.⁴³ The differences of terminology, organisational structures, and policies may partly be explained by differences in geography, history, and political systems. The lack of systematic and explicit understanding of the threat or its consequences challenges the formation of clear policy regulations, laws, and educational programmes aimed to increase civil resilience against disinformation.⁴⁴

Moreover, state and international responses tend to be constricted and focus on a certain emergent technology (such as artificial intelligence) instead of considering a more comprehensive approach to the complex problem in different sectors of society, such as education, journalism, and political institutions, and ignore the underlying problems behind disinformation and foreign information manipulation.⁴⁵

Introduction to Foreign Information Manipulation and Interference (FIMI)

The EU's External Action Service (EEAS) has introduced a comprehensive concept to counter threats in the information space.

The EEAS defines FIMI (Foreign Information Manipulation and Interference) as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner."

Accordingly, FIMI is set apart from misinformation and disinformation. Unlike in the case of misinformation, it is spread intentionally to deceive the public, and FIMI does not refer solely to false or misleading information, unlike disinformation. This latter aspect of the concept is a welcome evolution as malicious actors have long understood that the best influence operations are not simply limited to false information. As pointed out by the EU DisinfoLab: "not all disinformation is FIMI, and FIMI is not only disinformation."

⁴³J. Pamment, *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference*, NATO Strategic Communications Centre of Excellence, Riga, Latvia, 1--33. ISBN: 978-9934-619-13-7. https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255 [date published 05.12.2022], pp. 8--9, 33.

⁴⁴C. Tenove, "Protecting Democracy from Disinformation," p. 531.

⁴⁵J. Bateman & D. Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide*, Carnegie Endowment for International Peace, Washington DC, USA, 1--119. https://carnegieendowment.org/2024/01/31/countering-disinformation-effectively-evidence-based-policy-guide-pub-86272 [date published 31.01.2024], pp. 14, 44.

T. Hale, D. Held & K. Young, *Gridlock: Why Global Cooperation Is Failing When We Need It Most*, Polity Press, Cambridge, United Kingdom, 2013, pp. 1--4.

⁴⁶European Union External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats---Towards a Framework for Networked Defence*, 1--36. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf [date published 07.02.2023], p. 4.

⁴⁷N. Hénin, "FIMI: Towards a European Redefinition of Foreign Interference," EU DisinfoLab, 1--11.

The main nuances between the concepts of FIMI and disinformation are:

- A refocusing of interest on behaviour and operating methods (while counter-disinformation activities often look at the content and tackling of narratives).
- Increased use of terms and processes from cyber-threat intelligence (enabling us to expand the toolbox of countermeasures beyond the current focus on strategic communication and debunking of misleading or false narratives).⁴⁸
- A holistic approach mobilising whole-of-society's resources, favouring the adoption of common terminology.

Thus, on the one hand, FIMI can be perceived as a narrower concept than disinformation because it refers to foreign activity alone, leaving out domestically grown activities. On the other hand, it should also be perceived as wider as it does not limit itself to false or misleading information. Instead, the focus is on the manipulative behaviour exhibited in the process of delivering the information, such as an artificial amplification of a narrative through fake social media accounts thereby influencing a public debate.⁴⁹

The concept of FIMI is increasingly used across the EU and its Member States. The origins of the concept may be traced to 2019,⁵⁰ when the issue of foreign digital interference and the potential benefits of standardising the description of observed incidents and the terminology came to the attention of the EEAS. The concept was further developed in two other EU official documents key to the evolution of the concept: the December 2020 European Democracy Action Plan⁵¹ and the 2022 Strategic Compass,⁵² which called for the development of an EU FIMI-dedicated toolbox. The doctrinal evolution concludes with the first EEAS report on Foreign

https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [date published 07.04.2023], p. 4.

⁴⁸The EEAS FIMI framework builds on experience in cybersecurity, where the forensic analysis focuses on threat actor behaviour throughout the entire timeline of their attempted attack (the so-called "Kill Chain" model), which has helped to better understand systemic vulnerabilities and how to spot and close their exploitation. At the heart of the Kill Chain perspective on FIMI is the systematic and granular data collection on "Tactics, Techniques, and Procedures" (TTPs), which are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. This method allows us to ask what a threat actor was doing before they were able to deploy a message; where in the attack chain they are currently and what their next step(s) may be.

European Union External Action Service (EEAS), 1st EEAS Report on Foreign Information Manipulation and Interference Threats, p. 4.
⁴⁹Ibid., p. 25.

⁵⁰N. Hénin, "FIMI: Towards a European Redefinition of Foreign Interference," p. 4.

⁵¹European 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.

⁵²European Union External Action Service (EEAS), *A Strategic Compass for Security and Defence*, 1--64.

https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [date published 24.03.2022], pp. 12, 40.

Information Manipulation and Interference Threats from February 2023.53

According to the EEAS definition, FIMI operators "can be state or non-state actors, including their proxies inside and outside of their own territory." Therefore, the analytical framework is applicable to all regions and actors as well as foreign and domestic analyses for its actor-agnostic design. Hence, it may be used by all stakeholders regardless of their respective focus. Member States can adapt the framework according to their own analytical limitations and institutional division of competences concerning either domestic or foreign disinformation actors.

The approach offered by the EEAS focuses on behaviour rather than content (narrative) or the actor involved. Importantly, the focus on behaviour enables expanding the toolbox of countermeasures beyond strategic communication and debunking of misleading or false narratives. It helps to alleviate some of the institutional difficulties in engaging with content, which is highly political by nature, such as allowing the EEAS to avoid accusations of censorship or authoritative decision-making on what is true or false.

FIMI is a growing political and security challenge highlighting the need for a common defence framework. The FIMI concept permits the EEAS to maintain situational awareness of developments in the information space without limiting its monitoring and analysis function to specific actors. Instead, it sets out best practices for fighting disinformation through sharing data and analysis, and can inform effective action.

Adopting a whole-of-society approach will be needed to enhance resilience and leverage the broadest capacities and competencies. However, this can be realistically achieved only if the large variety of actors engaged in countering FIMI speak a common language.⁵⁶

⁵³European Union External Action Service (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats.*

⁵⁴Ibid., p. 4.

⁵⁵States remain central FIMI threat actors. Moreover, the EEAS admits that its mandate and strategic priorities have limited the focus on influence operations conducted by two state actors, namely Russia and China. Ibid., p. 8.

⁵⁶To help operationalise the concept, the EEAS recommends following a Kill Chain taxonomy of FIMI TTPs developed by the Disinformation Analysis and Risk Management (DISARM). It sets out best practices for fighting disinformation through sharing data and analysis, and can inform effective action.

European Union External Action Service (EEAS), 1st EEAS Report on Foreign Information Manipulation and Interference Threats, pp. 29--30.

The Polish Information Landscape and Approaches to Countering Disinformation and FIMI

Poland has not developed a national information strategy, let alone one dedicated specifically to countering FIMI or disinformation. However, these threats are acknowledged in other Polish national strategies.

On 12 May 2020, the President of the Republic of Poland approved a National Security Strategy of the Republic of Poland, the basic state document regarding security and defence. The strategy recognises the Russian Federation as a threat actor that undertakes "multi-faceted and comprehensive actions using non-military means (including: cyber-attacks, disinformation) to destabilise the structures of Western states and societies and to create divisions among Allies." It makes clear that the digital revolution "also creates room for disinformation and manipulation of information, which requires effective strategic communication activities." Specific provisions of the strategy call for the building of capabilities to protect the information space, counteract disinformation, and increase public awareness of threats related to the manipulation of information through education.

However, possible threats in the information space were presented superficially, and no concrete solutions in the fight against disinformation are indicated.⁵⁹ The threats, as well as risks associated with technological developments and new global challenges, were described in more detail in two other documents: a draft *Information Security Doctrine of the Republic of Poland*⁶⁰ and the *Cybersecurity Strategy of the Republic of Poland for 2019--2024*.⁶¹ Some systemic recommendations have also been offered by representatives of civil society, which also highlighted a need to devise a national information security strategy.⁶²

This chapter will describe the Polish disinformation threat landscape and introduce

⁵⁷Biura Bezpieczeństwa Narodowego, *The National Security Strategy of the Republic of Poland*, 1--38.

https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_ _2020.pdf [date published 12.05.2020], p. 6.

⁵⁸Ibid., p. 8.

⁵⁹P. Berlińska-Wojtas, "Bezpieczeństwo informacyjne RP w dobie COVID-19," *Zeszyty Naukowe Zbliżenia Cywilizacyjne* XVII(1)/2021, 33--50. DOI: <u>10.21784/ZC.2021.003</u> [date published 28.03.2021], p. 42.

⁶⁰Biura Bezpieczeństwa Narodowego, *Doktryna Bezpieczeństwa Informacyjnego RP* (projekt), 1--15.

⁶¹Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata* 2019-2024, 1--25.

https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [date published 30.12.2019].

⁶²Forum Przeciwdziałania Dezinformacji, *Przeciwdziałanie Dezinformacji w Polsce: Rekomendacje Systemowe*, 1--20.

https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacji.pdf [date published 08.12.2022].

Polish approaches to countering disinformation and FIMI. The objective of this chapter is to provide insights into the current Polish responses and to set up the discussion on whether Poland would benefit from a national strategy on countering disinformation.

The Disinformation Threat Landscape in Poland

Addressing the Sejm on 25 April 2024, the Minister of Foreign Affairs Radosław Sikorski presented information on Polish foreign policy priorities in 2024. Countering disinformation featured prominently among them. The Minister highlighted the importance of international coordination and reaching audiences worldwide with reliable information: "We must fight it in word and deed. In word, countering different propaganda outlets, both in traditional media and on social networks," the Minister said.⁶³

As anywhere, Poland faces disinformation from both internal and external sources. The 2023 EU DisinfoLab report titled *Disinformation Landscape in Poland* identified anti-vaccine, anti-EU, and anti-refugee false narratives to be commonly circulating in Poland along with disinformation about COVID-19, women's reproductive rights, sexual education, and the LGBT+ community.⁶⁴

However, as this thesis focuses on foreign information manipulations and interference, this chapter will elaborate on external threats and influence campaigns targeting Poland. Polish intelligence agencies systematically report about Russia's and Belarus's continued operations against the Republic of Poland.⁶⁵ Russia's propaganda and disinformation against Poland have main objectives of:⁶⁶

- Targeting the citizens' belief in the future

- Including narratives questioning state capacity to function to undermine

⁶³Ministry of Foreign Affairs Republic of Poland, *Information of Minister of Foreign Affairs on Polish Foreign Policy Tasks in 2024.*

https://www.gov.pl/web/diplomacy/information-of-minister-of-foreign-affairs-on-polish-foreign-policy-tasks-in-2024 [date published 25.04.2024], p. 18.

⁶⁴M. Zadroga, *Disinformation Landscape in Poland*. EU DisinfoLab, 1--10.

https://www.disinfo.eu/wp-content/uploads/2023/12/20231203_PL_DisinfoFS.pdf [date published 03.12.2023], pp. 6--8.

⁶⁵Służby Specjalne, "Dezinformacja przeciwko Polsce."

https://www.gov.pl/web/sluzby-specjalne/dezinformacja-przeciwko-polsce2 [date published 03.12.2023].

⁶⁶M. Tyburski, "Russian Disinformation War Against Poland After the Invasion of Ukraine," Warsaw Institute.

https://warsawinstitute.org/russian-disinformation-war-against-poland-after-the-invasion-of-uk raine/ [date published 27.10.2023].

Kosciuszko Institute, Civic Resilience Initiative, Detector Media & Open Information Partnership, *Resilience to Disinformation*, 1--56.

https://www.gov.pl/web/diplomacy/lublin-triangle-presents-joint-report-on-russian-disinformat ion-and-propaganda [date published 08.12.2022], pp. 4--5.

T. Chłoń & K. Kozłowski, "Selected Case Studies of Systemic Disinformation: Russia and China" in *Disinformation and the Resilience of Democratic Societies*, R. Kupiecki & A. Legucka (eds.), 37--68. The Polish Institute of Foreign Affairs, Warsaw, 2023. ISBN 978-83-67487-20-7, p. 43.

- the trust of the democratically elected government⁶⁷
- By ridiculing the security structures (such as the army) of the Republic of Poland⁶⁸
- By inducing fear and confusion in society

- Undermining trust between and within societal groups

- By building distrust between and polarising communities based on language, sexuality, or religion or by using historical controversies⁶⁹ (such as the Volyn massacre, or a socioeconomic crisis caused by Ukrainian refugees)
- By inoculating false narratives of Poland's 'imperialist' goals in Ukraine and Belarus⁷⁰

- Discrediting international cooperation

- By targeting NATO and the EU (how their membership is not beneficial for the target country/the risk of war on Polish territory)
- By discrediting and isolating Poland within the Transatlantic community and on the international arena⁷¹

- Creating and promoting pro-Kremlin circles⁷²

- By discrediting individuals and groups critical of Russia
- By influencing the state's sovereign decisions to suit the best possible interests of Russia

The Russian disinformation toolbox pursues these objectives through saturating the information space with repeated narratives which present alternative versions of reality through deflection and denial of responsibility for its own malign actions, belittling other actors' activities, and distracting and confusing the public with emotional stories. These narratives are then amplified and repeated endlessly because pounding audiences with disinformation has proven to be effective.⁷³

⁶⁷T. Chłoń & K. Kozłowski, "Selected Case Studies of Systemic Disinformation: Russia and China," p. 43.

⁶⁸Ibid., p. 50.

⁶⁹G. Gigitashvili, "Russia-aligned Hacktivists Stir Up Anti-Ukrainian Sentiments in Poland," The Digital Forensic Research Lab (DFRLab)/The Atlantic Council.

https://dfrlab.org/2022/09/09/russia-aligned-hacktivists-stir-up-anti-ukrainian-sentiments-in-poland/ [date published 09.09.2022].

M. Tyburski, "Russian Disinformation War Against Poland After the Invasion of Ukraine."

⁷⁰Digital Forensic Research Lab/Atlantic Council, "Russian War Report: Kremlin-Controlled Outlet Rehashes Narrative that Poland Plans to Annex Western Ukraine." https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-kremlin-controlled-ou

https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-kremlin-controlled-outlet-rehashes-narrative-that-poland-plans-to-annex-western-ukraine/ [date published 04.11.2022].

T. Chłoń & K. Kozłowski, "Selected Case Studies of Systemic Disinformation: Russia and China," p. 47.

⁷¹A. Legucka, "Targeting Poland: History as a Tool of Russian Disinformation" in *Disinformation and the Resilience of Democratic Societies*, R. Kupiecki & A. Legucka (eds.), 69--89. The Polish Institute of Foreign Affairs, Warsaw, 2023. ISBN 978-83-67487-20-7, p. 87.

⁷²T. Chłoń & K. Kozłowski, "Selected Case Studies of Systemic Disinformation: Russia and China," p. 43.

⁷³EUvsDisinfo, "Deny, Deflect, Distract, Confuse. Repeat." https://euvsdisinfo.eu/deny-deflect-distract-confuse-repeat/ [date published 10.08.2023].

These false or misleading narratives are orchestrated overtly through public diplomacy channels and covertly through a multitude of deceptive techniques such as creating websites impersonating well-established media (e.g., the Doppelganger campaign),⁷⁴ creating forged documents (sometimes in combination with conducting cyber-attacks, e.g., the posting of an inauthentic document on the Polish War Studies University website⁷⁵ or distributing messages about alleged recruitment to the Lithuanian--Polish--Ukrainian Brigade⁷⁶), posting across online platforms to obfuscate origins of a (dis)information, or the use of automated bots or the hiring of people to proliferate comments on the internet that would seem genuine.

After Russia launched its full-scale invasion of Ukraine in February 2022, thousands of social media accounts have shifted overnight from anti-vaccine narratives to anti-Ukrainian content.⁷⁷ By portraying Ukrainians as ungrateful for the help provided by Poles, threatening negative consequences of Ukrainian refugees for the Polish job market, access to medical and educational services, and an increase in crime rates in the country, these campaigns attempt to plant fear and doubt in the Polish public and divide Poland and Ukraine.⁷⁸ One of Ukraine's most prominent supporters, Poland is constantly a target of Russian information manipulation and interference by the Kremlin.

Of course, Russian disinformation targeting Poland is not new.⁷⁹ While the Polish people have remained resilient against Russian disinformation narratives, political and societal polarisation stands out as a vulnerability that can be exploited in foreign interference and influence campaigns.

Polish society has become more and more polarised since 2015 due to divided and increasingly hostile party politics and its diffusion into society and local communities. The divisions are witnessed both through zero-sum 'us versus them' thinking, normative and ideological discord, or by 'affective polarisation', in other words, voters expressing more negative sentiment about opposing parties than positive emotions

[date published 19.04.2023].

77#FakeHunter/Polish Press Agency, "Anti-Ukrainian Propaganda Has Replaced Much Anti-Vaccine Propaganda, Although the Sources Are Often the Same and Tend to Work in the

⁷⁴A. Alaphilippe, G. Machado, R. Miguel & F. Poldi, *Doppelganger -- Media Clones Serving Russian Propaganda*. EU DisinfoLab & Qurium, 1--26. https://www.disinfo.eu/doppelganger [date published 27.09.2022].

⁷⁵Służby Specjalne, "Atak dezinformacyjny na Polskę [PL/EN]." https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske [date published 23.04.2020].

⁷⁶CSIRT Ministerstwa Obrony Narodowej, "Trwa operacja dezinformacyjna przeciwko RP---UNC1151 dezinformuje o rekrutacji do LITPOLUKRBRIG." https://csirt-mon.wp.mil.pl/pl/articles/6-aktualnosci/dezinformacja-o-rekrutacji-do-litpolukrbrig/

Interests of the Kremlin---According to Analysis by Fakehunter." https://fake-hunter.pap.pl/en/node/21 [last accessed 01.06.2024].

⁷⁸A. Legucka, "Russia Ramps Up Disinfo Campaigns Ahead of European Parliament Elections," The Polish Institute of International Affairs.

https://www.pism.pl/publications/russias-ramps-up-disinfo-campaigns-ahead-of-european-par liament-elections [date published 05.06.2024].

 $^{^{79}}$ A. Legucka, "Targeting Poland: History as a Tool of Russian Disinformation," p. 71.

about their preferred political party.80

Another main vulnerability of Polish society concerns the low level of trust in state and media institutions. Trust in the news media is closely linked to trust in political institutions, sometimes referred to as the 'trust nexus'. Accordingly, the connection between trust in the media and trust in politics is particularly strong in politically polarised societies. According to the 2024 Globsec Trends report, merely 47 percent trust their standard media in spring of 2024, and 44 percent of Poles expressed trust in their government. Between trust in the connection of the standard media in spring of 2024, and 44 percent of Poles expressed trust in their government.

The Polish Legal System's Regulations Against Online Harms

Until recently, Poland did not have a specific act that would provide legal solutions regarding disinformation. On 30 August 2023, the Polish president Andrzej Duda signed an amendment to the Penal Code which introduces penalties for spreading disinformation when conducted in collaboration with foreign intelligence services.⁸³

According to the new article 130(9) of the Penal Code:

"Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, conducts disinformation, consisting in disseminating false or misleading information, with the aim of causing serious disruptions in the system or economy of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member or persuading a public authority of the Republic of Poland, an allied state or an international organisation of which the Republic of Poland is a member to take or refrain from taking specific actions shall be punishable by imprisonment for a period of not less than eight years."

This legal amendment has received criticism that the notion of disinformation is too vast in terms of content and that this provision could open the door to investigations against journalists or NGOs on having a relationship with a foreign intelligence service.⁸⁵

⁸⁰H. Tworzecki, "Poland: A Case of Top-Down Polarization," *The ANNALS of the American Academy of Political and Social Science*, 681(1), 2019, 97--119. DOI: 10.1177/0002716218809322 [date published 20.12.2018], pp. 97--101, 106--112.

⁸¹E. Humprecht, "The Role of Trust and Attitudes toward Democracy in the Dissemination of Disinformation---A Comparative Analysis of Six Democracies," *Digital Journalism*, 2023, 1--18. DOI: 10.1080/21670811.2023.2200196 [date published 10.05.2023], p. 3.

⁸²Globsec, GLOBSEC Trends 2024 CEE: A Brave New Region?, 1--99.

https://www.globsec.org/sites/default/files/2024-05/GLOBSEC%20TRENDS%202024.pdf [date published 01.05.2024], pp. 70, 81.

⁸³Polish Press Agency, "President Signs Bill on Tougher Penalties for Espionage." https://www.pap.pl/en/news/president-signs-bill-tougher-penalties-espionage [date published 30.08.2023].

⁸⁴Kancelaria Sejmu, *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 grudnia 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy -- Kodeks karny* (Dz. U. 2024 poz. 17). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240000017/T/D20240017L.pdf, p. 37 (author's translation from Polish).

⁸⁵T. Wahl, "Rule of Law Developments in Poland: May--October 2023," *Eucrim*. https://eucrim.eu/news/rule-of-law-developments-in-poland-may-october-2023/ [date

In light of Russia's war of aggression against Ukraine, Poland swiftly implemented sanctions on Russia's propaganda outlets. As early as 24 February 2022, the National Broadcasting Council removed from the distributed programs register Russian channels: RT (Russia Today), RT Documentary, RTR Planeta, Sojuz TV, and Rossiya 24.⁸⁶ The list of sanctioned channels has since been expanded, including through the implementation of sanctions imposed at EU level.⁸⁷

Moreover, the Polish Penal Code includes provisions for protection against hatred of ethnic, religious, or racial groups, including a special provision on Holocaust denial. Specific clauses also prohibit the promotion of totalitarian regimes, such as fascist or communist.⁸⁸ Prosecution of false information may be based on personal injury grounds, such as defamation.

Polish Institutional Approaches to Countering Disinformation

Polish governmental institutions have in recent years become more aware of the risks posed by disinformation and foreign information manipulation. Nationally, disinformation and FIMI are dealt with by units within the Chancellery of the Prime Minister, National Security Bureau, Ministry of Defence, Cyberspace Defence Forces, Government Security Centre, Ministry of Digital Affairs, and intelligence agencies. In addition, the Ministry of Foreign Affairs engages in international cooperation on countering disinformation including through policy making at EU level, involving for instance the FIMI toolbox, sanctions, proactive media campaigns, and by funding of small-scale projects countering FIMI.

Poland has also put forward new initiatives and established new administrative structures to address the growing threats in the information domain. For example, in 2022 a separate Department for the Protection of Information in Cyberspace was established at the Polish Research and Academic Computer Network (NASK).⁸⁹ However, currently no consolidated documenting methodology exists that would provide a single data access point.

This decentralised approach may hinder the situational awareness and efforts of a

published 14.11.2023].

⁸⁶Krajowa Rada Radiofonii i Telewizji/Serwis Rzeczypospolitej Polskiej, "Rosyjskie programy wykreślone z rejestru programów rozprowadzanych."

https://www.gov.pl/web/krrit/rosyjskie-programy-wykreslone-z-rejestru-programow-rozprowad zanych [date published 24.02.2022].

⁸⁷E. Kaca, "Znaczenie sankcji UE w przeciwdziałaniu rosyjskiej dezinformacji." https://www.pism.pl/publikacje/znaczenie-sankcji-ue-w-przeciwdzialaniu-rosyjskiej-dezinformacii [date published 28.05.2024].

⁸⁸See articles 133, 212, 216, 256, 257 of the Penal Code.

Kancelaria Sejmu, Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej w sprawie ogłoszenia jednolitego tekstu ustawy -- Kodeks karny.

M. Zadroga, Disinformation Landscape in Poland, p. 10.

Demagog, "Kursy online." https://platforma.demagog.org.pl/kursy/ [last accessed 01.06.2024].

⁸⁹Naukowa i Akademicka Sieć Komputerowa (NASK), "Kim jesteśmy."

https://www.nask.pl/pl/o-nas/kim-jestesmy/3261,O-NASK.html [last accessed 01.06.2024].

coordinated approach of Polish state institutions and units to counter disinformation and FIMI campaigns. For instance, the EU DisinfoLab report on the *Disinformation Landscape in Poland* pointed out: "Polish intelligence services do not have a clear policy for reporting disinformation threats. There are also no clear guidelines for public institutions on counteracting disinformation, and no permanent structures in the government are dedicated to this issue."

Nevertheless, Polish authorities have attempted to fuse existing knowledge on the domestic information environment and foreign activity by setting cross-ministerial and cross-institutional working-level contacts across the government administration. An example of such an initiative is the establishment in 2018 of a cross-governmental advisory body to the Government Crisis Management Team (RZZK) on hybrid threats focused on early identification of hybrid threats and support for coordination in this area.⁹¹

Cross-Sectoral Cooperation and the Role of Civil Society

Cross-sectoral cooperation is pursued with the aim to strengthen the role and responsibility of the state in the field of media education. In November 2021, the National Broadcasting Council and representatives of state authorities and public institutions signed a declaration on the coordination of activities in the field of media education in Poland. The declaration recognizes that basic tasks in the field of media education are the responsibility of the education system, as well as those state authorities, institutions, and organisations that have organisational and financial resources to carry out practical activities to develop media, information, and digital competences.⁹²

Media education is currently part of the curriculum at primary and secondary school levels in Poland. Moreover, a number of media literacy, cybersecurity, and FIMI awareness-raising campaigns have been issued through the collaboration of government institutions, the private sector, and civil society. Prominent examples include the #FakeHunter website⁹³---a joint project by the Polish Press Agency (PAP) and the government agency GovTech Polska launched in April 2020, *Disinfo Radar* online reports⁹⁴ published by the Government Centre for Security (RCB), and the 'Fejkoodporni' (Fake-resistant)---a social campaign launched in January 2022 by the Ministry of National Defense consisting of research, conferences, and debates

⁹⁰M. Zadroga, Disinformation Landscape in Poland, p. 10.

⁹¹Departament Porządku i Bezpieczeństwa Wewnętrznego, *Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi* (Nr ewid. 16/2023/P/22/029/KPB). https://www.nik.gov.pl/kontrole/P/22/029/ [date published 28.11.2023], p. 91.

⁹²Ministerstwo Edukacji Narodowej, "Ministerstwo Edukacji i Nauki podpisało deklarację o współpracy w sprawie edukacji medialnej."

https://www.gov.pl/web/edukacja/ministerstwo-edukacji-i-nauki-podpisalo-deklaracje-o-wspol pracy-w-sprawie-edukacji-medialnej [date published 17.11.2021].

⁹³#FakeHunter/Polish Press Agency, "Join the Fight Against Disinformation." https://fake-hunter.pap.pl/en/o-projekcie [last accessed 01.06.2023].

⁹⁴Rządowe Centrum Bezpieczeństwa, "Disinfo Radar." <u>https://www.gov.pl/web/rcb/disinfo-radar</u> [date published 05.01.2023].

engaging the public and private sector entities.95

Civil society organisations also play a significant role in the field of media education and the countering of FIMI and disinformation. A number of NGOs, think tanks, and academia monitor, analyse, and report on disinformation and work towards resilience building. These initiatives include the Media Education project run by the Modern Poland Foundation the independent fact-checking organisation Demagog 7, and the INFO OPS Poland Foundation on operations. 98

⁹⁵Krajowa Rada Radiofonii i Telewizji, "Fejkoodporni -- Kampania Ministerstwa Obrony Narodowei."

https://www.gov.pl/web/krrit/fejkoodporni--kampania-ministerstwa-obrony-narodowej [date published 22.02.2022].

⁹⁶Edukacja Medialna, "Serwis Edukacja Medialna zawiera scenariusze, ćwiczenia i materiały do prowadzenia zajęć w szkołach, domach kultury i bibliotekach." https://edukacjamedialna.edu.pl/info/o-nas/ [last accessed 01.06.2024].

⁹⁷Demagog, "Odporni na dezinformację. Warsztaty z fact-checkingu dla mediów." https://demagog.org.pl/analizy_i_raporty/odporni-na-dezinformacje-warsztaty-z-fact-checkingu -dla-mediow-lokalnych/ [date published 12.07.2023].

⁹⁸INFO OPS Polska, "Przeciwdziałanie dezinformacji i zwiększanie świadomości istniejących zagrożeń w tym obszarze." https://infoops.pl/dyplomacja-publiczna/ [last accessed 01.06.2024].

Existing National Strategies for Countering Disinformation in EU Member States

In order to better assess the approach of the EU Member States towards countering disinformation, research of existing strategies at national level was conducted for this study. The research revealed that the majority of EU countries do not have a dedicated strategy for countering disinformation, let alone a strategy for countering FIMI. Instead, instances of addressing disinformation are found within broader legal frameworks and policies.⁹⁹

In many cases, the problem of disinformation is recognised in other strategic documents, most notably in national security strategies (e.g., Germany, Lithuania, Poland, Spain), and/or cybersecurity strategies (e.g., Belgium, France, Italy, Poland), and/or countering hybrid threats strategies (e.g., France, Austria, Slovenia, Czechia). Occasionally, disinformation and FIMI are mentioned in other documents of strategic nature, for example, Slovakian action plan for coordination of countering hybrid threats efforts (2022--2024), a concept for strategic communication of the Slovak Republic, Danish 2023 foreign and security policy strategy, German strategy on China, or French military doctrine.¹⁰⁰

The European Union's Approach to Countering Disinformation

To provide a wider perspective to national strategies, the thesis will briefly introduce the EU's approaches to counter FIMI and disinformation, beyond the earlier introduced dedicated FIMI concept.

The EU's landmark regulation, the Digital Services Act (DSA), which entered into full effect in February 2024, created binding obligations for very large online platforms and search engines to counter illegal online content. It also established transparency and oversight measures and rules for content moderation. These rules aim to safeguard fundamental rights of online users and establish accountability to mitigate systemic risks such as disinformation or election manipulation. For the first time, the DSA provides a uniform legal framework across the EU to counter risks related to disinformation and foreign interference.¹⁰¹

At the core of the EU's efforts to counter disinformation is also the 2022 Code of

⁹⁹M.G. Sessa, *Connecting the Disinformation Dots---Insights, Lessons, and Guidance from 20 EU Member States*, EU DisinfoLab and Friedrich Naumann Foundation for Freedom, December 2023, pp. 9--10.

¹⁰⁰The scoping of national strategies was done through diplomatic channels, including direct contacts with embassies personnel.

¹⁰¹European Commission, *Questions and Answers on the Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 [date published: 23.02.2024].

European Commission, *The Digital Services Act Package*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [date published: 16.02.2024].

Practice on Disinformation. The code sets broad commitments and measures to counter online disinformation for its voluntary signatories, from fact-checking and advertising industries, to researchers and civil society representatives. These measures include demonetising the dissemination of disinformation, securing the transparency of political advertising, and providing researchers better access to data. Disinformation and foreign interference are also dealt with within the hybrid threats framework.¹⁰²

The EU's Strategic Compass introduced the EU Hybrid Toolbox and the Foreign Information Manipulation and Interference Toolbox. The latter aims to strengthen the EU's ability to "detect, analyse and respond" to threats. In 2015, the EEAS' East StratCom Task Force established the flagship project EUvsDisinfo to counter pro-Kremlin disinformation. The service produces reports, studies, and interviews to raise awareness on disinformation, and a database which according to the website has over 15,000 examples of Russian disinformation in over ten languages.

The EU has also established measures to protect the freedom of media and ensure the independent functioning of public service media. In March 2024, the EU introduced its new Media Freedom Act that obliges Member States to protect journalists and media independence against political or economic interference.¹⁰⁵ The Act also establishes responsibilities on the media on transparency of ownership and state advertising funds.

Other EU policies and action plans to respond to and build resilience against foreign information manipulation include the 2024 Artificial Intelligence Act¹⁰⁶ for regulating the risks of AI and the Defence of Democracy package, adopted ahead of the European Parliament election in June 2024 to enhance transparency and accountability through legislative and non-legislative measures to tackle the threat of covert foreign influence in democratic processes. It also encourages citizens and civil society organisations to participate in building civil resilience.¹⁰⁷

_

¹⁰²European Commission, *The 2022 Code of Practice on Disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation [date published: 24.04.2024].

¹⁰³European Union External Action Service (EEAS), *A Strategic Compass for Security and Defence*, pp. 12, 40.

¹⁰⁴J. Pamment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework.

EUvsDisinfo, "'To Challenge Russia's Ongoing Disinformation Campaigns': Eight Years of EUvsDisinfo."

https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/ [date published: 05.07.2023].

¹⁰⁵European Commission, *European Media Freedom Act*.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en [date published: 15.03.2024]. ¹⁰⁶European Parliament, *Artificial Intelligence Act* (P9_TA(2024)0138).

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf [date published: 13.03.2024].

¹⁰⁷European Commission, *Defence of Democracy -- Commission Proposes to Shed Light on Covert Foreign Influence*. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453 [date published: 12.12.2023].

EU Member States' National Strategies for Countering

Disinformation

Only three EU countries currently have a strategy dedicated to countering disinformation: Latvia¹⁰⁸, Romania, and the Netherlands.¹⁰⁹ In Ireland,¹¹⁰ work on a similar strategy is well underway and is therefore also discussed herein. The Romanian strategy is not publicly available and will therefore be excluded from further examination.

Below is a brief summary of the existing or planned strategies dedicated to countering disinformation.

The Netherlands

The first Government Strategy against disinformation of the Netherlands was announced by the Minister of the Interior and Kingdom Relations in October 2019. The strategy was constructed around three lines of action: prevention, strengthened messaging, and, if necessary, response. However, the policy focus was on prevention of disinformation.

In December 2022, a new All-Government Strategy for Effectively Combating Disinformation was published. The new Dutch strategy highlighted the importance of establishing a set of actions for countering disinformation. According to the new strategy, in case of a threat to national security, public health, or social and/or economic stability, the government may take certain actions. In addition to the three lines of action listed in the previous strategy, two more have been added in the new document: strengthening free and open public debate (including by means of maintaining a pluralistic media landscape and the importance of investigative journalism), and reducing the impact of disinformation (including by raising awareness of disinformation among state institutions).¹¹²

¹⁰⁸Cabinet of Ministers of the Republic of Latvia, *The National Concept on Strategic Communication and Security of the Information Space 2023--2027*, 1--23. https://www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija [date published: 20.03.2023].

¹⁰⁹Ministry of the Interior and Kingdom Relations (of the Netherlands), *Government-wide* Strategy for Effectively Tackling Disinformation, 1--18.

https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-e-strategy-for-effectively-tackling-disinformation [date published: 23.12.2022].

¹¹⁰Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland), *National Counter Disinformation Strategy Working Group*.

https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group/ [date published: 30.03.2023].

¹¹¹House of Representatives of the Netherlands, *Policy Efforts to Protect Democracy Against Disinformation*.

https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019D41916&did=2019D41916&did=2019D41916 [date published: 18.10.2019].

¹¹²Ministry of the Interior and Kingdom Relations (of the Netherlands), *Government-wide* Strategy for Effectively Tackling Disinformation, pp. 5--7.

Latvia

In January 2023, the Latvian Council of Ministers approved a concept report on security of the national strategic communication and information space for 2023--2027. The aim of the new concept is to contribute to the security of the information space, including through enhanced strategic communication capabilities, strengthening the media environment, and improving the Latvian society's media and information literacy. According to the concept report, it is expected that the implementation of solutions provided in the concept report will strengthen society's sense of belonging to Latvia, Europe, and its values, and citizens' support and trust in government policies and communication will gradually increase.

The concept introduced six basic directions for action. These consist of:

- Employment of national strategic communication and capacity development
- Measures of resilience of the information space
- Strengthening the media environment and a resilient society
- International cooperation and partnerships with the national civil society, the private sector, and academia¹¹³

The national strategy is complemented with an action plan, which is not publicly available.

Ireland

In 2020, the Irish Government established the Future of the Media Commission and tasked it with developing recommendations for sustainable public funding and other support to ensure the viability, independence, and ability of the media in Ireland to meet public service objectives. The Commission's report, released on July 12, 2022, contains a total of 50 recommendations that, in effect, constitute a strategic agenda for the transformation of the Irish media sector. One of them is the development of a national strategy to counter disinformation.¹¹⁴

The working group began its work in February 2023. It operates in three subgroups whose purpose is to inform the development of the Irish strategy:

- 1. Existing countermeasures
- 2. The emerging regulatory environment
- 3. Supporting journalism and providing public interest information

According to the government's plan, the strategy was to be ready by the end of 2023.¹¹⁵

¹¹³Cabinet of Ministers Republic of Latvia, *The National Concept on Strategic Communication and Security of the Information Space 2023--2027*, pp. 2--4.

¹¹⁴The Future of Media Commission (of Ireland), *Report of the Future of Media Commission*, 1--274. https://www.gov.ie/en/publication/ccae8-report-of-the-future-of-media-commission/ [date published: 12.07.2022], pp. 257--258.

¹¹⁵Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland), Multi-stakeholder Working Group Established to Develop a National Counter Disinformation Strategy.

https://www.gov.ie/en/press-release/6ece9-unpublished-multi-stakeholder-working-group-established-to-develop-a-national-counter-disinformation-strategy/ [date published: 21.02.2023].

The Irish national strategy for countering disinformation objectives are focused to enact coordinated efforts with relevant government ministries and agencies to counter coordinated campaigns targeting Ireland, developing effective monitoring and building relationships between different national actors, including researchers and media platforms. The latter would also require supporting fact-checking and disinformation research and independent journalism in countering disinformation and viewing for new initiatives in media literacy. While the Irish strategy builds a more comprehensive approach, it is yet to be finalised.

Following a brief introduction to comparative analysis as a research methodology, this research paper will compare the Dutch and Irish national strategies within the framework of the research questions established in the introduction. As literature for the analysis, the thesis will use the 2022 Dutch All-Government Strategy for Effectively Combating Disinformation. While the Irish strategy is not finalised, information will be drawn from publicly available strategy working group reports, citizen scoping paper, and terms of reference.

Comparative Analysis

Comparative analysis is a research methodology used to identify, describe, and explain similarities and variance between two or more comparison units of analysis. It is an old and widely used mode of inquiry in a variety of research fields. In social sciences, these units of study may include political, sociological, or geographical ones in either cross-national or regional comparisons.¹¹⁶ This research paper's comparative units are the Dutch and Irish approaches to countering disinformation.

The objective of comparative analysis is not merely to compare social units. Instead, the findings provide deeper understanding of the specificities of and between the units of comparison to better comprehend the wider context of the research topic 117---here countering disinformation and FIMI in EU countries.

This research paper will utilise comparative analysis because it allows an adequate framework to analyse the key aspects, similarities, and differences between the national strategies against disinformation. The analysis will be guided by the following research questions:

- How do the selected strategies characterise the threat of disinformation?
- What is the role of FIMI in the existing European national strategies for countering disinformation?
- What approaches to countering disinformation and FIMI do the strategies envisage?

¹¹⁶R. Azarian, "Potentials and Limitations of Comparative Method in Social Science," *International Journal of Humanities and Social Science* vol. 1 No. 4, 2021, 113--125. URN: <u>urn:nbn:se:uu:diva-429014</u> [date published: 18.12.2020], pp. 115--116.

¹¹⁷D. Collier, "The Comparative Method" in *Political Science: The State of the Discipline*, Ada W. Finifter (ed.), 105--119, American Political Science Association, 1983, ISBN-10: 091565458X, p. 105.

As with any research method, the comparative analysis also has its limitations. These are related to the scale of analysis and underlying presumptions in case or unit selection and issues of causality. For example, the research results may depend on the choices of selected comparison units and the assumptions affecting these choices in the first place. Another challenge involves the conducted generalised deductions from a narrow choice of compared units. For example, in the thesis, geographical differences, history, and experiences with disinformation may affect the state's understanding of the problem of FIMI and the selected countermeasures. These limitations should be regarded when applying the findings to the Polish case, although wider generalisations are not within the scope of the thesis.

A comparative analysis may broaden the perspective beyond a national focus and bring different contexts to the discussion to reveal our national practice's overlooked basis and assumptions.¹²⁰ Therefore, this analysis may reveal some particularities of the Polish case, feeding into the discussion of whether Poland would benefit from a national strategy to counter disinformation.

¹¹⁸M.C. Mills, G.G. van de Bunt, J.G.M. de Bruijn, "Comparative Research: Persistent Problems and Promising Solutions," p. 621.

R. Azarian, "Potentials and Limitations of Comparative Method in Social Science," pp. 115--116.

119 R. Azarian, "Potentials and Limitations of Comparative Method in Social Science," pp. 116--118,
121

M.C. Mills, G.G. van de Bunt, J.G.M. de Bruijn, "Comparative Research: Persistent Problems and Promising Solutions," *International Sociology*, 2006, vol. 21(5): 619--631. DOI: 10.1177/0268580906067833, pp. 620--621.

¹²⁰R. Azarian, "Potentials and Limitations of Comparative Method in Social Science," pp. 117--118.

Analysis of the Dutch and Irish National Strategies for Countering Disinformation

For the purposes of this research, the thesis will compare the Dutch and Irish national strategies. This is due to practical considerations---the Romanian strategy is not publicly available, and neither is the action plan complementing the Latvian strategy. The Netherlands was chosen because it provides a longer tradition of strategies to counter disinformation dating back to 2019. It also includes concrete actions to counter disinformation, highlighting the need for additional countermeasures in the quickly changing information environment. While the Irish strategy is not finished, its wide consultation process across society and comprehensive approach to disinformation are expected to provide additional information on the problem and the process of forming a national strategy. These aspects provide both analytical value and insights into mirroring the process of establishing a national disinformation strategy with the Polish case.

How Do the Selected Strategies Characterise the Threat of Disinformation?

The Dutch government's decision to review its 2019 strategy for tackling disinformation stems from the observation that the dissemination of both disinformation and misinformation has developed since then.¹²¹ Moreover, concerns about disinformation have increased among the Dutch population, with a 2022 Dutch Media Authority report showing that 35 percent of respondents are concerned about what is real and what is fake on the internet. A public survey on disinformation also revealed that four in ten respondents feel that the government is not taking adequate action to counteract disinformation. Therefore, a renewed analysis of the problem was deemed necessary.¹²²

Although mainly focused on disinformation---which is characterised by the intention to cause societal harm (e.g., to public debate, democratic processes, the open and knowledge economy, public health)---the 2022 Dutch strategy acknowledges the need to also address misinformation as it too can cause similar societal harm.¹²³¹²⁴ According to the strategy:

"The dissemination of disinformation, both domestic and foreign, may disturb the public debate, cause unrest and uncertainty and may even have a disruptive effect on our society as a whole and on the lives of individual people in this society." ¹²⁵

¹²¹Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 5.

¹²²Ibid., p. 5.

¹²³The Dutch national strategy on countering disinformation provides the following definition:

¹²⁴Ibid., p. 1.

¹²⁵Ibid., p. 1.

Furthermore:

"The dissemination of disinformation may be ideologically/politically and/or economically motivated, which means that disinformation may pose a problem in various ways." ¹²⁶

An example of how the dissemination of false information may pose a threat to the democratic rule of law, even if done without the intention to cause harm, are conspiracy theories, some of which may even prompt extremist actions in the physical space.¹²⁷

Similarly, the Irish strategy planners acknowledge the potential harm of disinformation to democratic society. In Ireland, the need for more coordinated and strategic action to combat the damaging impact of disinformation on Irish society and democracy was recognised by the Future of Media Commission in its July 2022 final report. Among a total of 50 recommendations, which in effect constitute a strategic agenda for transforming Ireland's media sector, the Commission recommended the development of a National Counter-Disinformation Strategy.¹²⁸

According to the scoping document, which formed the basis of a written public consultation process, disinformation is a problem:

"Because it is designed to create doubt and disruption. It distorts the nature of public discourse, undermining trust in sources of reliable information and negatively impacting people's ability to make informed decisions based on accurate information." 129

The scoping document further discussed societal vulnerabilities that could be potentially targeted by disinformation actors:

"Disinformation campaigns may also exploit economic or social inequalities, creating further division in society, and so countering disinformation can be looked at in the broader context of addressing inequalities in general." ¹³⁰

The Working Group of the Irish national strategy has found disinformation to be an evolving phenomenon, a global challenge that is difficult to define and that threatens human rights and democratic values. The Irish strategy planners propose to think about disinformation by focusing on overall harms and its role in wider trends such as polarisation or inequality instead of individual pieces of content (and whether they are true or false). Disinformation can be considered harmful when it undermines people's ability to make informed decisions or leads to adverse outcomes such as damaging public health, causing the integrity of democratic elections to suffer, or scapegoating

¹²⁶Ibid., p. 2.

¹²⁷Ibid., p. 3.

¹²⁸The Future of Media Commission (Ireland), *Report of the Future of Media Commission*, pp. 257--258.

¹²⁹Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland), *National Counter Disinformation Strategy Scoping Paper*, p. 6.

¹³⁰Ibid., p. 6.

social groups. In other words, willingness to endorse or promote disinformation may be recognised as a symptom of deeper societal issues that need to be addressed.¹³¹

The scoping document has adopted definitions of disinformation and misinformation provided in the European Democracy Action Plan and, as in the Dutch case, the Irish strategy will mainly focus on disinformation but expects that measures to "counter disinformation will, to a large degree, also help counter misinformation." ¹³²

The Irish Working Group defined disinformation as:

"False information that is created or distributed with the intent to deceive." 133

Moreover, it characterised the nature of harmful disinformation campaigns as varying considerably in terms of who is responsible (states, foreign actors, ideological groups, or individuals), their motivations, the channels they use, the time frame of their campaigns, and the audiences they target.

Accordingly, both strategies note the variety of actors who spread disinformation. The Dutch strategy considers how disinformation is disseminated. The rapid and targeted dissemination of disinformation via large and internationally operating platforms has been made possible through the use of, for example, coordinated networks, bot accounts, and fake accounts. It also becomes increasingly complicated to recognise disinformation. While the platforms' underlying recommendation systems sometimes promote disinformation at the expense of reliable information, the gatekeeper role in the information landscape that the traditional media fulfilled has come under pressure with the arrival of new revenue models.¹³⁴

Thus, the scoping activities conducted by the Irish Working Group have led to observations that in many instances resemble the approach put forward in the Dutch strategy. Both the Dutch and the Irish strategy planners underline that the democratic rule of law, freedom of speech, and freedom of the press must take centre stage and that qualifying disinformation as such and fact-checking are not primary government duties. However, both also view the problem of technological developments having contributed to the rapid dissemination of disinformation with a vast reach and therefore a need for freedom of speech but curtailing freedom of reach. Finally, both also recognise that the public debate is increasingly conducted on large and internationally operating platforms and that it becomes increasingly complicated to recognise disinformation, and therefore, place strong emphasis on stimulating and using public alternatives to online platforms.

While both the Netherlands and Ireland have embarked on crafting a

¹³¹Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland), *National Counter Disinformation Strategy Subgroup 1 Report: Countermeasures*, pp. 3--4.

¹³²National Counter Disinformation Strategy Scoping Paper, p. 3.

¹³³National Counter Disinformation Strategy Subgroup 1 Report: Countermeasures, p. 12.

¹³⁴Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, pp. 4--5.

government-wide strategy for countering disinformation, Ireland has put more emphasis on conducting wide public consultations as part of the process. The multi-stakeholder working group (the Working Group) tasked with developing the strategy agreed on their terms of reference in March 2023 and aimed to complete its work by the end of that year. At the outset, a commitment was given to consultation with the public. The Dutch strategy itself, however, does foresee the starting of discussions with various groups of citizens about disinformation, and the role for independent media, academia, and civil society in addressing disinformation is noted.

What Is the Role of FIMI in the Existing European National Strategies for Countering Disinformation?

According to the Dutch Government-wide Strategy for Effectively Tackling Disinformation, the approach to addressing FIMI fits within the broader approach to address hybrid threats. It is also said to fit within the EU's Common Security and Defence Policy (CSDP), of which, at least according to the strategy, counteracting hybrid threats is a key component.¹³⁶

Fully acknowledging that disinformation is not disseminated by state actors alone, the strategy nevertheless points to an increasingly assertive attitude and an increased use of information operations and disinformation to serve political interests by foreign state actors. The Dutch strategy notes that "state actors have a wide range of resources at their disposal, with disinformation and influencing being commonly used tools that are often applied as part of hybrid campaigns." Russian narratives that had spread on Dutch-language social media groups in relation to the COVID-19 pandemic are given as an example, and the Russian invasion of Ukraine is provided as a reference point to how disinformation may be an instrument of state actors and actors affiliated with them.

The Irish strategy also acknowledges the escalation in the European security environment and increased foreign interference in democracies. The National Counter Disinformation Strategy Working Group acknowledges that:

"Due to ongoing conflict in Ukraine and other countries, increasing tensions between world powers, and the desire of certain nations and very large trade and commercial organisations to influence European democratic processes, the European Union and many of its individual nations have become increasingly concerned with disinformation and other hybrid threats." ¹³⁸

Despite the documents not mentioning specific threat actors or foreign information

¹³⁵Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland), *National Counter Disinformation Strategy Working Group*.

¹³⁶Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 10.

¹³⁷Ibid., pp. 3--4.

¹³⁸Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland), *National Counter Disinformation Strategy Subgroup 2 Report: Regulatory and Research Mechanisms*, p. 10.

campaigns targeting Ireland, based on online reporting by the Group it can be observed that FIMI has been identified as a key area of concern.

For example, FIMI is specifically mentioned in the Irish sub-working group focused on identifying mechanisms and research measures that support innovation in areas critical to compliance in the emerging regulatory environment. Initial scoping activities carried out by the Group revealed that FIMI campaigns are often designed to exert influence on a country or region, disrupt society, and reduce trust in democratic institutions and the rule of law. Common tactics include targeting groups in society to increase division, targeting marginalised groups, or promoting disinformation campaigns and conspiracies that make effective government and the delivery of services more difficult.¹³⁹

Likewise, the Dutch strategy makes several references to FIMI as a specific point of concern that poses a risk to national security, but also for the stability and security of international organisations that the Netherlands is part of, such as the EU and NATO.¹⁴⁰ However, as the strategy focuses on countering disinformation, only a few action items directly and explicitly targeting FIMI have been identified in terms of concrete results expected from ministries up to and including 2025.¹⁴¹ Nevertheless, multiple of the introduced countermeasures would likely also serve the purpose of countering FIMI since disinformation is often a key component of FIMI.

As both the Dutch and the Irish strategies focus on the wider phenomenon of disinformation, their inclusion of the EEAS concept of FIMI is notable. Both strategies place FIMI as part of hybrid threats but also belonging to the concept of disinformation. Key elements of the EEAS' concept of FIMI---which refocuses interest on behaviour and operating methods and suggests an increased use of terms and processes from cyber-threat intelligence as well as a holistic approach mobilising whole-of-society's resources---have all been incorporated in the strategies, albeit without the particular focus on the 'foreign' element. Thus, for the lack of a foreign actor focus in the two strategies, the basic guidelines of the FIMI concept appear to be adopted in the domestic context (what one could arguably refer to as domestic information manipulation and interference---DIMI). Therefore, the FIMI concept has proved useful for the national policymakers in the making of their counter-disinformation strategies.

What Approaches to Countering Disinformation and FIMI Do the Strategies Envisage?

The Dutch and the Irish strategies share a common concern over the effect of disinformation and foreign interference on the functioning of the democratic processes of the state. They highlight, for instance, the role of the government and the

¹³⁹Ibid., p. 10.

¹⁴⁰Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 3.

¹⁴¹Ibid., p. 17.

coordinated approach of state institutions and agencies to counter the threat but also place some emphasis on civil society, namely through approaches to media literacy and cooperation between state agencies, research, and media institutes in the country.

While the Dutch Government-wide Strategy for Effectively Tackling Disinformation clearly states what countermeasures to disinformation and FIMI are foreseen (see annex), the Irish strategy is not finalised. Therefore, for the purpose of this analysis, the drafted countermeasures are deduced from publicly available information on working group meeting notes and the scoping paper. Moreover, as specific countermeasures are planned and adopted according to the national legal, political, and institutional contexts, the analysis will instead focus on the approaches to countermeasures envisaged in the strategies.

Dutch Strategy Approaches

The basic principle guiding the Dutch strategy is that qualifying disinformation as such and fact-checking are not primary duties for the government, with the exception:

"Where national security, public health or social and/or economic stability are at stake the government can act and debunk disinformation." 143

The Dutch strategy has been structured around two tracks showcasing different approaches to countermeasures:

Track 1: Strengthening the Free and Open Public Debate

The emphasis is on "retaining the pluralistic media landscape, strengthening citizens' resilience, and encouraging and using public alternatives to online platforms." The aim of the objectives is to assist in reducing "the influence that harmful misinformation and conspiracy theories have on the open public debate and ensure that citizens are able to actively participate in the public debate."

Track 2: Reducing the Influence of Disinformation

This track covers measures addressing the content of disinformation, the producer or disseminator, the responsibilities of the traditional and social media, and the development of knowledge in general.¹⁴⁶

Irish Strategy Approaches

The Working Group tasked with drafting the Irish National Counter Disinformation Strategy shared five guiding principles around which the strategy could be developed

¹⁴²Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland), *National Counter Disinformation Strategy Working Group*.

¹⁴³Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 1.

¹⁴⁴Ibid., p. 6.

¹⁴⁵Ibid., p. 6.

¹⁴⁶Ibid., p. 6.

and which, in the process of public consultation, it sought opinion on:147

- 1. Counter disinformation and protect freedom of speech using a rights-based approach
- 2. Counter disinformation by building resilience and trust---at individual and societal levels
- 3. Counter disinformation through increased cooperation, collaboration, and coordination
- 4. Counter disinformation through corporate accountability and regulatory enforcement
- 5. Counter disinformation through evidence-based countermeasures and interventions

The key aspects of the terms of reference agreed on by the Group were centred around exploring existing countermeasures, the current and emerging regulatory environment, and the support of free, independent, high-quality journalism and the protection of public interest information.¹⁴⁸

Role of Non-State Actors

Both the Dutch and the Irish strategy planners clearly envisage a role for non-state actors in awareness-raising efforts and other aspects of the strategies' implementation, including civil society organisations, researchers, academia, journalists, independent media, and online platforms stakeholders. The role of libraries, museums, and other civil society organisations is also considered in the context of encouraging media literacy, which is believed to make citizens more resilient to disinformation. Both countries also consider the use of targeted media literacy and educational measures and campaigns, such as the Dutch awareness programme to increase knowledge and skills regarding the value of journalism in society.

International Cooperation

There is strong recognition in both the Dutch and the Irish cases that, as a global phenomenon, disinformation requires cooperation from a broad and diverse range of stakeholders, and transnational networks play an important role in countering efforts. An example given by both of such an internationally facilitated network is the European Digital Media Observatory (EDMO), a partly EU-funded hub for fact-checkers, academics, and other relevant stakeholders to collaborate with each other.¹⁵¹

_

¹⁴⁷National Counter Disinformation Strategy Scoping Paper, pp. 10--12.

¹⁴⁸Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland), *National Counter Disinformation Strategy Revised Terms of Reference*.

¹⁴⁹Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 7; *National Counter Disinformation Strategy Subgroup 1 Report: Countermeasures*, p. 10.

¹⁵⁰Ibid., pp. 7, 10--11.

¹⁵¹Ibid., p. 12.

Several other networks are identified by the Irish Working Group: European Platform of Regulatory Authorities (EPRA), European Regulators Group for Audio-Visual Media Services (ERGA), Global Online Safety Network (GOSRN), European Advertising Standards Alliance (EASA), and the International Fact-Checking Network (IFCN). Both countries are committed to developing an effective response, where possible in collaboration with national and international partners (primarily within the EU context, albeit both also mention the OECD, and the Dutch strategy also makes an explicit mention of NATO and the G7). 153

Legislative Frameworks

Both countries emphasise the importance of implementing and enforcing a number of legislative frameworks at the EU level, most notably the EU Digital Services Act (DSA), the European Media Freedom Act, and the (voluntary) EU Code of Practice on Disinformation. The Irish Working Group also recalls the EU Artificial Intelligence Act, the Digital Markets Act, and the EU Audiovisual Media Services Directive in this regard.

Differences in Approaches

The approaches in the two strategies differ most in the setup of the overall coordination function and individual organisations' responsibilities. The Dutch strategy clearly states that:

"The Minister of the Interior and Kingdom Relations has a coordinating responsibility for the policy against disinformation." 154

Besides this, every governmental organisation also has its own responsibility for drafting an effective and appropriate response to disinformation, as each ministry must be able to respond effectively and appropriately when it faces disinformation affecting its own policy area. Moreover, an indication is made for each of the specific countermeasures provided in the strategy as to which state body is the lead for its execution (see annex).

The available scoping material for the Irish strategy did not suggest the Working Group gave consideration to aspects of the strategy's implementation coordination. However, neither the Dutch nor the Irish strategists call for the creation of a dedicated counter-FIMI agency (such as France's VIGINUM and Sweden's Psychological Defence Agency).

Differences of approach also seem to occur regarding the possible introduction of new legislation. While proposing new legislation is not part of the Irish National

Saufex - GA 101132494

¹⁵²National Counter Disinformation Strategy Subgroup 1 Report: Countermeasures, pp. 5--6, 8; National Counter Disinformation Strategy Subgroup 2 Report: Regulatory and Research Mechanisms, p. 21.

¹⁵³Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 7.

¹⁵⁴Ibid., p. 13.

¹⁵⁵Ibid., p. 2.

Counter Disinformation Strategy Terms of Reference, the Dutch strategy states that: "The Ministry of Justice and Security takes the lead in the development of an integrated assessment framework for the government's role in illegal and harmful material to create clarity for both the government (at the national and regional levels) and citizens and the IT industry." ¹⁵⁶

Furthermore, the Dutch strategy notes that:

"A lack of clarity existed both in the national government and among municipal authorities about the GDPR and data processing frameworks." 157

It also mentions that work is ongoing to clarify the legal framework for online monitoring by municipal authorities as part of public security and law and order.

Noteworthy, the General Data Protection Regulation (GDPR) has also caught the attention of the Irish strategy planners, albeit in the context of enforcing the GDPR's security principle to protect people from dangerous profiling such as micro-targeted digital advertising and 'Real-Time Bidding' systems.¹⁵⁸

Funding and Resource Allocation

The Irish Working Group has dedicated much consideration to the issue of funding measures in support of countering disinformation. In the context of the global digital transformation, it has found that:

"The key challenge facing the Irish market is one of sufficient revenue to allow media players to invest in and produce Irish content." 159

It notes that the government accepted, in principle, to transform the existing statutory Broadcasting Fund into a Media Fund. Accordingly, the wider scope and a platform-neutral approach could include schemes to support the exploration of new business models working towards sustainability.¹⁶⁰

Furthermore, the Department of Foreign Affairs has been operating a pilot Global Ireland Media Challenge Fund to enable media to engage the Irish public on the global geopolitical landscape and Ireland's place in it. It also found that the level of resources made available to fact-checkers does not correspond to the depth of their contribution to countering disinformation. It suggests that consideration should be given to the establishment of a pilot training programme on fact-checking in conjunction with industry stakeholders and Ireland's commission for regulating broadcasters and online media, and supporting media development.¹⁶¹

¹⁵⁶Ibid., p. 10.

¹⁵⁷Ibid., pp. 8--9.

¹⁵⁸National Counter Disinformation Strategy Subgroup 2 Report: Regulatory and Research Mechanisms, p. 5.

¹⁵⁹National Counter Disinformation Strategy Subgroup 3 Report: Independent Journalism and Protecting Public Interest Information, p. 15.

¹⁶⁰Ibid., pp. 14, 19--20.

¹⁶¹Ibid., pp. 14, 19--20.

The Netherlands, on the other hand, dedicated considerable attention to the promotion of their norms and values to internationally shared standards for tackling disinformation. Especially the EU is viewed as a norm-setter in guiding towards the Dutch objective:

"European instruments such as the DSA and the EU's Code of Practice help the Netherlands to do this by indicating that platform regulation protecting fundamental rights is a feasible option for addressing disinformation... The Netherlands advocates an alternative to content control that safeguards human rights and effectively counteracts disinformation campaigns." ¹⁶²

Specific Measures Against FIMI

Few measures designed specifically to counter FIMI are provided in the Dutch strategy and the Irish mapping activities. As noted earlier, both countries' strategy planners focus on the wider phenomenon of disinformation, and FIMI is accounted for mostly insofar as the concept has shifted attention from narratives to behaviour (information manipulation). Nevertheless, FIMI is incorporated in the Dutch strategy under "Efforts depending on the disseminator or producer of disinformation" (Track II), which points to the EU FIMI toolbox and EU Rapid Alert System (platform for exchange of information and best practices) as well as the development of a Government-Wide Response Framework against state threats as countermeasures.¹⁶³

The Irish Working Group, on the other hand, suggests three potential solutions:

- Multidisciplinary research and the creation and funding of multidisciplinary teams to provide accurate and up-to-date tracking data on the key issues.
- Collaborative fora between the key actors, including state bodies and agencies.
- Targeted media literacy and educational measures and campaigns to grow understanding of civic rights and democratic values.¹⁶⁴

The strategy also suggests an increase in:

"Long-term funding for media literacy and other social and educational programmes and funding for research into methods to detect, analyse and disrupt disinformation campaigns would help mitigate this issue." 165

Navigating the Democratic Dilemma

Both strategies showcase the problems of the democratic dilemma: navigating the complex interplay between protecting civil freedoms (such as freedom of expression and free speech) and combating harmful content, hate speech, and disinformation,

¹⁶²Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, p. 9.

¹⁶³Ibid., p. 17.

¹⁶⁴National Counter Disinformation Strategy Subgroup 2 Report: Regulatory and Research Mechanisms, p. 11.

¹⁶⁵Ibid., p. 11.

while simultaneously safeguarding user privacy and promoting economic innovation in Big Tech. The two states slightly differ in their approaches to finding the right balance. The Irish strategy planner's bottom-up approach involving public consultations from the onset contrasts with the Dutch strategy, which has taken a top-down, government-led approach with specific action points to be executed by assigned ministries. The Dutch strategy also seems more threat-oriented than the Irish approach, which places the protection of a pluralistic, independent, and functional media environment at its core.

The two countries share a similar interest in effectively enforcing measures provided within EU frameworks, especially the Digital Services Act. Moreover, both strategy planners highlighted the importance of the whole-of-government approach, freedom of media, and partnerships both domestically and internationally as appropriate measures to counter disinformation.

"Regardless of the content, the producer/spreader or the dissemination method, disinformation is the deliberate, mostly covert, dissemination of misleading information with the aim of harming the public debate, democratic processes, the open and knowledge economy or public health. This means that it may affect national security. It is a form of harmful, but often legal, behaviour. Disinformation does not necessarily contain incorrect information. It may be a combination of factual, incorrect or partially incorrect information, but it is always intended to mislead people and to do harm."

Final Remarks

Over the past decade, only a few EU countries have developed a national strategy for countering disinformation. However, it is plausible that this trend will continue, and Poland should not be left behind. The structural changes in modern society caused by technological advancements, coupled with increasing threats from foreign actors exploiting these changes to the detriment of the Polish state and society, make it imperative for Poland to devise a strategy that ensures its ability to prevent and protect against threats occurring in the information space.

While Foreign Information Manipulation and Interference (FIMI) has been instrumental in pushing states to increase their understanding of and attention to the problem of disinformation, the qualitative and quantitative changes in how information is consumed in modern society require states to reevaluate their role as framework providers and actors within the information domain. So, what can Poland learn from the Dutch and Irish strategy planners?

Although the harm of disinformation has become clear, the phenomenon cannot simply be addressed through national security lenses alone; it needs a whole-of-government approach and a whole-of-society agreement. Developing a national strategy to counter disinformation would be a good starting point. By crafting the strategy through a whole-of-government approach, the process itself

could help build bridges between existing ministerial silos and foster a sense of community. Moreover, it would incentivise different ministries to prioritise the problem and seek solutions within their purview. Inviting representatives of local governments at the regional level should also be considered.

Issues that particularly antagonise political divides should be left out of the initial discussion---for example, possible social campaigns concerning the EU. An actor-agnostic approach focusing on behaviour (instead of a strict focus on content), as offered by the FIMI concept, could help mitigate some of the most contentious issues, such as suspicions of impeding freedom of speech. This approach would highlight the risk of foreign interference to national security, a top value to any society. While a whole-of-society approach should be previewed in the strategy, public consultations should not be part of the strategy-making process itself to avoid politicisation and derailing of the process. However, the strategy should be systematically revised, building on increased public mandate and factoring in new developments.

A clear indication of the democratic values that the strategy aims to protect---such as freedom of speech, rule of law in interventions, and corporate accountability---should be explicitly stated. The importance of the EU legislative and policy framework, including the implementation and compliance with the EU Code of Practice on Disinformation and the Digital Services Act, should also be underscored.

The nature of harmful disinformation campaigns varies considerably in terms of who is responsible (individuals or foreign states and/or their proxies), their tactics, and their motivations, such as financial or political gains. Therefore, it is necessary to develop multiple countermeasures simultaneously. These will typically range from activities to increase situational awareness, resilience building, regulation, and diplomatic responses. The EU's toolbox for countering FIMI provides useful guidance in this respect. However, when crafting a national strategy for countering disinformation, Poland should also draw inspiration from existing national strategies such as those of Ireland and the Netherlands. For example, Poland would be wise to follow the approach of the Irish strategy planners, who have identified the need for strengthening an independent media environment and financial sustainability of entities creating national content. The Dutch strategy, on the other hand, could provide useful guidance on an overall coordination approach and assigning tasks to specific ministries.

The strategy should also look into possible improvements to the current institutional framework. The lack of a consolidated documenting methodology that would provide a single data access point, as well as the lack of clear guidelines for public institutions on counteracting disinformation, hinder the situational awareness and efforts of a coordinated approach by Polish state institutions to counter disinformation and FIMI campaigns. Consideration should also be given to the feasibility and potential added value of creating governmental agencies dedicated to monitoring and analysing FIMI, as done by France and Sweden.

The harm to Polish state institutions and to the quality of public debate caused by acts of foreign information manipulation and interference has been well acknowledged by both the government and civil society. Hence, there is no lack of expertise, but rather insufficient capacities and coordination, including through common action.

While the focus could be on foreign campaigns, a potential Polish strategy for countering disinformation should address the underlying causes of social polarisation. A divided society is not only a vulnerability exploited by disinformation and FIMI actors but also a factor that could slow down the devising and implementing of necessary countermeasures. Neither the EU nor the Dutch or Irish national strategies have provided much guidance on addressing this problem beyond advising media literacy measures. Resilience-building needs anchoring in public trust in state institutions, and Poland will need to find ways to strengthen government legitimacy.

Bibliography

- Alaphilippe, A., Machado, G., Miguel, R., & Poldi, F. (2022, September 27). *Doppelganger Media Clones Serving Russian Propaganda*. EU DisinfoLab & Qurium. Retrieved from https://www.disinfo.eu/doppelganger
- Azarian, R. (2020). Potentials and limitations of comparative method in social science. International Journal of Humanities and Social Science, 1(4), 113–125. URN: urn:nbn:se:uu:diva-429014
- Balkin, J. M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review*, 79(1), 1–55.
- Bateman, J., & Jackson, D. (2024, January 31). Countering Disinformation Effectively: An Evidence-Based Policy Guide. Carnegie Endowment for International Peace.

 Retrieved from
 - https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide
- Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, 33(2), 122–139. https://doi.org/10.1177/0267323118760317
- Berlińska-Wojtas, P. (2021). Bezpieczeństwo informacyjne RP w dobie COVID-19 [Information security of the Republic of Poland in the era of COVID-19]. Zeszyty Naukowe Zbliżenia Cywilizacyjne, 17(1), 33–50. https://doi.org/10.21784/ZC.2021.003
- Biura Bezpieczeństwa Narodowego. (2020, May 12). *The National Security Strategy of the Republic of Poland*. Retrieved from https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf
- Biura Bezpieczeństwa Narodowego. (2015, July 24). *Doktryna Bezpieczeństwa Informacyjnego RP (projekt)* [Information Security Doctrine of the Republic of Poland (draft)]. Retrieved from https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf
- Butcher, P., & Neidhardt, A.-H. (2021, November 29). From Debunking to Prebunking: How to Get Ahead of Disinformation on Migration in the EU. European Policy Centre. Retrieved from https://feps-europe.eu/wp-content/uploads/2021/11/From-debunking-to-prebunking-How-to-get-ahead-of-disinformation-on-migration-in-the-EU.pdf
- Cabinet of Ministers of the Republic of Latvia. (2023, March 20). The National Concept on Strategic Communication and Security of the Information Space 2023–2027. Retrieved from https://www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija
- Castells, M. (Ed.). (2004). *The Network Society: A Cross-cultural Perspective*. Edward Elgar Publishing.
- Chan, M. S., Jones, C. R., Hall Jamieson, K., & Albarracín, D. (2017). Debunking: A meta-analysis of the psychological efficacy of messages countering misinformation. *Psychological Science*, 28(11), 1531–1546. https://doi.org/10.1177/0956797617714579
- Chłoń, T., & Kozłowski, K. (2023). Selected case studies of systemic disinformation: Russia and China. In R. Kupiecki & A. Legucka (Eds.), *Disinformation and the Resilience of Democratic Societies* (pp. 37–68). The Polish Institute of Foreign Affairs.
- Cipers, S., Meyer, T., & Lefevere, J. (2023). Government responses to online disinformation unpacked. *Internet Policy Review*, 12(4), 1–19. https://doi.org/10.14763/2023.4.1736

- Collier, D. (1983). The comparative method. In A. W. Finifter (Ed.), *Political Science: The State of the Discipline* (pp. 105–119). American Political Science Association.
- CSIRT Ministerstwa Obrony Narodowej. (2023, April 19). *Trwa operacja dezinformacyjna przeciwko RP—UNC1151 dezinformuje o rekrutacji do LITPOLUKRBRIG* [A disinformation operation against the Republic of Poland is underway—UNC1151 disinforms about recruitment to LITPOLUKRBRIG]. Retrieved from
 - https://csirt-mon.wp.mil.pl/pl/articles/6-aktualnosci/dezinformacja-o-rekrutacji-do-litpolukrbrig/
- Demagog. (2023, July 12). *Odporni na dezinformację. Warsztaty z fact-checkingu dla mediów* [Resistant to disinformation. Fact-checking workshops for the media]. Retrieved from
 - https://demagog.org.pl/analizy_i_raporty/odporni-na-dezinformacje-warsztaty-z-fact-checkingu-dla-mediow-lokalnych/
- Demagog. (n.d.). *Kursy online* [Online courses]. Retrieved June 1, 2024, from https://platforma.demagog.org.pl/kursy/
- Departament Porządku i Bezpieczeństwa Wewnętrznego. (2023, November 28). Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi [Preparing the state for threats related to hybrid activities] (Nr ewid. 16/2023/P/22/029/KPB). Retrieved from https://www.nik.gov.pl/kontrole/P/22/029/
- Digital Forensic Research Lab/Atlantic Council. (2022, November 4). Russian War Report: Kremlin-Controlled Outlet Rehashes Narrative That Poland Plans to Annex Western Ukraine. Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-kremlin-controlled-outlet-rehashes-narrative-that-poland-plans-to-annex-western-ukraine/
- Drobnič, S. (2014). Comparative analysis. In A. C. Michalos (Ed.), *Encyclopedia of Quality of Life and Well-Being Research*. Springer. https://doi.org/10.1007/978-94-007-0753-5
- Edukacja Medialna. (n.d.). *Serwis Edukacja Medialna* [Media Education Service]. Retrieved June 1, 2024, from https://edukacjamedialna.edu.pl/info/o-nas/
- European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). (2024, January 1). *Hybrid Threats as a Concept*. Retrieved from https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
- European Commission. (2020, December 3). European Democracy Action Plan (COM(2020) 790 final). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC079
- European Commission. (2024, May 8). *Tackling Online Disinformation*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/online-disinformation
- European Commission. (2024, February 23). Questions and Answers on the Digital Services Act. Retrieved from
 - https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348
- European Commission. (2024, February 16). *The Digital Services Act Package*. Retrieved from
 - https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
- European Commission. (2024, April 24). *The 2022 Code of Practice on Disinformation*. Retrieved from
 - https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
- European Commission. (2024, March 15). European Media Freedom Act. Retrieved from
 - https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en

- European Commission. (2023, December 12). Defence of Democracy Commission Proposes to Shed Light on Covert Foreign Influence. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453
- European Parliament. (2024, March 13). *Artificial Intelligence Act* (P9_TA(2024)0138). Retrieved from
 - https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf
- European Union. (2023, December 12). *Eurobarometer Key Findings*. Retrieved from https://europa.eu/eurobarometer/surveys/detail/2966
- European Union External Action Service (EEAS). (2024, May 27). *Tackling Disinformation, Foreign Information Manipulation & Interference*. Retrieved from https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-ma nipulation-interference_en
- European Union External Action Service (EEAS). (2023, February 7). *1st EEAS Report on Foreign Information Manipulation and Interference Threats—Towards a Framework for Networked Defence* (EEAS Data & Reporting Unit). Retrieved from https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf
- European Union External Action Service (EEAS). (2022, March 24). A Strategic Compass for Security and Defence. Retrieved from https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
- EUvsDisinfo. (2023, August 10). *Deny, Deflect, Distract, Confuse. Repeat.* Retrieved from https://euvsdisinfo.eu/denv-deflect-distract-confuse-repeat/
- EUvsDisinfo. (2023, July 5). 'To Challenge Russia's Ongoing Disinformation Campaigns': Eight Years of EUvsDisinfo. Retrieved from https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/
- #FakeHunter/Polish Press Agency. (n.d.). Anti-Ukrainian Propaganda Has Replaced Much Anti-Vaccine Propaganda, Although the Sources Are Often the Same and Tend to Work in the Interests of the Kremlin—According to Analysis by FakeHunter. Retrieved June 1, 2024, from https://fake-hunter.pap.pl/en/node/21
- #FakeHunter/Polish Press Agency. (n.d.). Join the Fight Against Disinformation.
 Retrieved June 1, 2023, from https://fake-hunter.pap.pl/en/o-projekcie
- Feldstein, S. (2021, October 19). Introduction. In S. Feldstein (Ed.), *Issues on the Frontlines of Technology and Politics* (pp. 1–6). Carnegie Endowment for International Peace. Retrieved from
 - https://carnegieendowment.org/files/202110-Feldstein_Frontlines_final3.pdf
- Forum Przeciwdziałania Dezinformacji. (2022, December 8). *Przeciwdziałanie Dezinformacji w Polsce: Rekomendacje Systemowe* [Countering Disinformation in Poland: Systemic Recommendations]. Retrieved from https://ffb.org.pl/wp-content/uploads/2023/02/Raport_Przeciwdzialanie_dezinformacii.pdf
- Ferrara, E., Cresci, S., & Luceri, L. (2020). Misinformation, manipulation, and abuse on social media in the era of COVID-19. *Journal of Computational Social Science*, 3, 271–277. https://doi.org/10.1007/s42001-020-00094-5
- General Secretariat for Defence and National Security of France (SGDSN). (2022, November 17). Vigilance Service and Protection Against Foreign Digital Interference. Retrieved from https://www.sqdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-e

t-protection-contre-les-ingerences-numeriques

Gigitashvili, G. (2022, September 9). *Russia-Aligned Hacktivists Stir Up Anti-Ukrainian Sentiments in Poland*. The Atlantic Council. Retrieved from <a href="https://dfrlab.org/2022/09/09/russia-aligned-hacktivists-stir-up-anti-ukrainian-senti-ukrainian-

- ments-in-poland/
- Globsec. (2024, May 1). GLOBSEC Trends 2024 CEE: A Brave New Region? Retrieved from
 - https://www.globsec.org/sites/default/files/2024-05/GLOBSEC%20TRENDS%20202 4.pdf
- Hale, T., Held, D., & Young, K. (2013). *Gridlock: Why Global Cooperation Is Failing When We Need It Most*. Polity Press.
- Hénin, N. (2023, April 7). FIMI: Towards a European Redefinition of Foreign Interference. EU DisinfoLab. Retrieved from
 - https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf
- House of Representatives of the Netherlands. (2019, October 18). *Policy Efforts to Protect Democracy Against Disinformation*. Retrieved from https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019D41916
- Humprecht, E. (2023). The role of trust and attitudes toward democracy in the dissemination of disinformation—A comparative analysis of six democracies. *Digital Journalism*, 1–18. https://doi.org/10.1080/21670811.2023.2200196
- INFO OPS Polska. (n.d.). Przeciwdziałanie dezinformacji i zwiększanie świadomości istniejących zagrożeń w tym obszarze [Countering disinformation and increasing awareness of existing threats in this area]. Retrieved June 1, 2024, from https://infoops.pl/dyplomacja-publiczna/
- Juhász, K. (2024). European Union defensive democracy's responses to disinformation. Journal of Contemporary European Studies, 1–20. https://doi.org/10.1080/14782804.2024.2317275
- Kaca, E. (2024, May 28). Znaczenie sankcji UE w przeciwdziałaniu rosyjskiej dezinformacji [The importance of EU sanctions in countering Russian disinformation]. Retrieved from https://www.pism.pl/publikacje/znaczenie-sankcji-ue-w-przeciwdzialaniu-rosyjskiej-dezinformacji
- Kancelaria Sejmu. (2024). Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 grudnia 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy Kodeks karny [Announcement of the Marshal of the Sejm of the Republic of Poland of December 7, 2023, on the publication of the uniform text of the Penal Code] (Dz. U. 2024 poz. 17). Retrieved from https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240000017/T/D20240017L.p df
- Karppinen, K. (2019). Freedom without idealization: Non-ideal approaches to freedom of communication. *Communication Theory*, 29(1), 66–85. https://doi.org/10.1093/ct/qty013
- Kosciuszko Institute, Civic Resilience Initiative, Detector Media, & Open Information Partnership. (2022, December 8). Resilience to Disinformation. Retrieved from https://www.gov.pl/web/diplomacy/lublin-triangle-presents-joint-report-on-russia n-disinformation-and-propaganda
- Krajowa Rada Radiofonii i Telewizji. (2022, February 24). *Rosyjskie programy wykreślone z rejestru programów rozprowadzanych* [Russian programs removed from the list of distributed programs]. Retrieved from https://www.gov.pl/web/krrit/rosyjskie-programy-wykreslone-z-rejestru-programow-rozprowadzanych
- Krajowa Rada Radiofonii i Telewizji. (2022, February 22). Fejkoodporni Kampania Ministerstwa Obrony Narodowej [Fake-proof Ministry of National Defence campaign]. Retrieved from https://www.gov.pl/web/krrit/fejkoodporni--kampania-ministerstwa-obrony-narodowej

- Kupiecki, R. (2023). Disinformation and international relations: Sources, aims, actors, methods. In R. Kupiecki & A. Legucka (Eds.), *Disinformation and the Resilience of Democratic Societies* (pp. 15–36). The Polish Institute of Foreign Affairs.
- Kupiecki, R., Bryjka, F., & Chłoń, T. (2022). *Dezinformacja Międzynarodowa. Pojęcie, Rozpoznanie, Przeciwdziałanie* [International Disinformation. Concept, Recognition, Counteraction]. Wydawnictwo Naukowe Scholar.
- Legucka, A. (2023). Targeting Poland: History as a tool of Russian disinformation. In R. Kupiecki & A. Legucka (Eds.), *Disinformation and the Resilience of Democratic Societies* (pp. 69–89). The Polish Institute of Foreign Affairs.
- Legucka, A. (2024, June 5). Russia Ramps Up Disinfo Campaigns Ahead of European Parliament Elections. The Polish Institute of International Affairs. Retrieved from https://www.pism.pl/publications/russias-ramps-up-disinfo-campaigns-ahead-of-european-parliament-elections
- Mieczkowski, P., & Kilian-Grzegorczyk, M. (Eds.). (2024, April 1). *Dezinformacja oczami Polaków* [Disinformation through the eyes of Poles] (pp. 1–133). Fundacja DigitalPoland. Retrieved from https://digitalpoland.org/en/publications/download?id=34ce5eac-1789-426c-af9b-cc091f5c23a8
- Mills, M. C., van de Bunt, G. G., & de Bruijn, J. G. M. (2006). Comparative research: Persistent problems and promising solutions. *International Sociology*, 21(5), 619–631. https://doi.org/10.1177/0268580906067833
- Ministerstwo Cyfryzacji. (2019, December 30). Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 [Cybersecurity Strategy of the Republic of Poland for 2019–2024]. Retrieved from https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024
- Ministerstwo Edukacji Narodowej. (2021, November 17). Ministerstwo Edukacji i Nauki podpisało deklarację o współpracy w sprawie edukacji medialnej [The Ministry of Education and Science signed a declaration of cooperation on media education]. Retrieved from
 - https://www.gov.pl/web/edukacja/ministerstwo-edukacji-i-nauki-podpisalo-deklaracje-o-wspolpracy-w-sprawie-edukacji-medialnej
- Ministry of Foreign Affairs Republic of Poland. (2024, April 25). *Information of Minister of Foreign Affairs on Polish Foreign Policy Tasks in 2024*. Retrieved from https://www.gov.pl/web/diplomacy/information-of-minister-of-foreign-affairs-on-polish-foreign-policy-tasks-in-2024
- Naukowa i Akademicka Sieć Komputerowa (NASK). (n.d.). *Kim jesteśmy* [Who we are]. Retrieved June 1, 2024, from https://www.nask.pl/pl/o-nas/kim-iestesmy/3261,O-NASK.html
- Organisation for Economic Co-operation and Development (OECD). (2024, March 4). Facts Not Fakes: Tackling Disinformation, Strengthening Information Integrity. Retrieved from
 - $\frac{\text{https://www.oecd-ilibrary.org/sites/d909ff7a-en/1/3/1/index.html?itemId=/content/publication/d909ff7a-en\&csp=037651e38039b75bbb486a006bf55a63&itemIGO=oecd&itemContentType=book}$
- Pamment, J. (2020, September 24). The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework. Carnegie Endowment for International Peace.

 Retrieved from
 - https://carnegieendowment.org/research/2020/09/the-eus-role-in-fighting-disinformation-crafting-a-disinformation-framework
- Pamment, J. (2022, December 5). A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference.

 NATO Strategic Communications Centre of Excellence. Retrieved from

- https://stratcomcoe.org/publications/a-capability-definition-and-assessment-fram ework-for-countering-disinformation-information-influence-and-foreign-interfere nce/255
- Polish Press Agency. (2023, August 30). President Signs Bill on Tougher Penalties for Espionage. Retrieved from
 - https://www.pap.pl/en/news/president-signs-bill-tougher-penalties-espionage
- Rządowe Centrum Bezpieczeństwa. (2023, January 5). Disinfo Radar. Retrieved from https://www.gov.pl/web/rcb/disinfo-radar
- Sanchez, G. R., & Middlemass, K. (2022, July 27). Misinformation Is Eroding the Public's Confidence in Democracy. Brookings Institution. Retrieved from https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confide nce-in-democracy/
- Sessa, M. G. (2023, December 5). Connecting the Disinformation Dots—Insights, Lessons, and Guidance from 20 EU Member States. EU DisinfoLab and Friedrich Naumann Foundation for Freedom. Retrieved from https://www.disinfo.eu/wp-content/uploads/2023/12/20231204_Connecting-disform ation-dots_comparative-study-1.pdf
- Służby Specjalne. (2023, December 3). Dezinformacja przeciwko Polsce [Disinformation against Poland]. Retrieved from https://www.gov.pl/web/sluzby-specialne/dezinformacja-przeciwko-polsce2
- Służby Specjalne. (2020, April 23). Atak dezinformacyjny na Polskę [PL/EN] [Disinformation attack on Poland]. Retrieved from
 - https://www.gov.pl/web/sluzby-specialne/atak-dezinformacviny-na-polske
- Smith, H., & Giannopoulos, G. (2021, February 1). The Landscape of Hybrid Threats: A Conceptual Model. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) & Joint Research Centre. https://doi.org/10.2826/004146
- Swedish Psychological Defence Agency. (2024, March 15). About Us: Our Mission. Retrieved from
 - https://www.mpf.se/psychological-defence-agency/about-us/our-mission/
- Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. The International Journal of Press/Politics, 25(3), 517-537. https://doi.org/10.1177/1940161220918740
- Terzis, G., Kloza, D., Kużelewska, E., & Trottier, D. (Eds.). (2020). Disinformation and Digital Media as a Challenge for Democracy. Intersentia.
- Turčilo, L., & Obrenovic, M. (2020, August 25). Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy. Heinrich Böll Foundation. Retrieved from https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_ENG.pdf
- Tworzecki, H. (2018). Poland: A case of top-down polarization. The ANNALS of the American Academy of Political and Social Science, 681(1), 97–119.
 - https://doi.org/10.1177/0002716218809322
- Tyburski, M. (2023, October 27). Russian Disinformation War Against Poland After the Invasion of Ukraine. Warsaw Institute. Retrieved from https://warsawinstitute.org/russian-disinformation-war-against-poland-after-the-i nvasion-of-ukraine/
- U.S. National Intelligence Council. (2021, March 10). Foreign Threats to the 2020 US Federal Elections (ICA 2020-00078D). Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf
- United Nations General Assembly. (2021, April 13). Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Irene Khan (A/HRC/47/25). Retrieved from
 - https://www.eods.eu/template/default/compendium/Part%204/009_Disinformatio

- n and freedom of opinion and expression.pdf
- Vériter, S. L., Bjola, C., & Koops, J. A. (2020). Tackling COVID-19 disinformation: Internal and external challenges for the European Union. The Hague Journal of Diplomacy, 15(4), 569-582. https://doi.org/10.1163/1871191X-BJA10046
- Wahl, T. (2023, November 14). Rule of Law Developments in Poland: May-October 2023. Eucrim. Retrieved from
 - https://eucrim.eu/news/rule-of-law-developments-in-poland-may-october-2023/
- West, D. M. (2017, December 18). How to Combat Fake News and Disinformation. Brookings Institution. Retrieved from
 - https://www.brookings.edu/articles/how-to-combat-fake-news-and-disinformatio n/
- Westerwick, A., Johnson, B., & Westerwick, S. (2017). Confirmation biases in selective exposure to political online information: Source bias vs. content bias. Communication Monographs, 84(3), 343–364. https://doi.org/10.1080/03637751.2016.1272761
- Zadroga, M. (2023, December 3). Disinformation Landscape in Poland. EU DisinfoLab. Retrieved from
 - https://www.disinfo.eu/wp-content/uploads/2023/12/20231203_PL_DisinfoFS.pdf

Analysis Material

- 1. Ministry of the Interior and Kingdom Relations of the Netherlands. (2022, December 23). Government-wide Strategy for Effectively Tackling Disinformation (pp. 1--18). Retrieved from https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation
- 2. The Future of Media Commission (Ireland). (2022, July 12). Report of the Future of Media Commission (pp. 1--274). Retrieved from https://www.gov.ie/en/publication/ccae8-report-of-the-future-of-media-commission/
- 3. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland). (2024, March 30). National Counter Disinformation Strategy Revised Terms of Reference. Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/251678/24b088ef-662c-445e-ade4-f2deeeec8ceb.pdf#page=null
- 4. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland). (2023, September). National Counter Disinformation Strategy Subgroup 1 Report: Countermeasures (pp. 1--12). Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/271393/aac95e8b-b668-49e3-9198-bdd88dfalc4f.pdf#page=null
- 5. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland). (2023, September). National Counter Disinformation Strategy Subgroup 2 Report: Regulatory and Research Mechanisms (pp. 1--28). Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/271394/d3b4bf05-09c5-4668-8 d7a-17b74bclecdf.pdf#page=null
- 6. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland). (2023, September). National Counter Disinformation Strategy Subgroup 3 Report: Independent Journalism and Protecting Public Interest Information (pp. 1--24). Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/271395/b78d4935-108a-489f-8a-08-ecf2d16ad37d.pdf#page=null
- 7. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (Ireland). (2023, September). National Counter Disinformation Strategy Scoping Paper (pp. 1--15). Retrieved from https://www.gov.ie/pdf/?file=https://assets.gov.ie/286028/37ceb147-b155-4655-af17-df6189be7928.pdf#page=null

Annex

Concrete Actions and Results to Be Achieved as Provided in the Dutch Government-wide Strategy for Effectively Tackling Disinformation¹⁶⁶:

Track I: Strengthening the Public Debate

Action: Retaining the Pluralistic Media Landscape

Results up to and including 2025:

- Investments in increasing the professionalism of local broadcasters.
- Exploration of ways to expand support for investigative journalism.
- Harmonised regulations on media freedom in EU Member States within the Ministry of Foreign Affairs (MFA), making the media more resilient against hybrid conflicts and the dissemination of disinformation.

Action: Strengthening Citizens' Resilience

Results up to and including 2025:

- An increase in citizens visiting <u>isdatechtzo.nl</u> for tips and tricks on how to recognise disinformation.
- Completion of an awareness programme to enhance knowledge and skills regarding the value of journalism in society.
- Regular use of national government communication channels to share tips on recognising disinformation or to warn citizens about potential disinformation surrounding important events.
- Greater awareness and resilience among internet users regarding posting and consulting online material.
- Efforts to strengthen and protect the democratic rule of law include attention to the relationship between disinformation and social unrest.

Action: Stimulating and Using Public Alternatives to Online Platforms

Results up to and including 2025:

- In collaboration with PublicSpaces, the first PubHubs have been established, providing support to public organisations in developing alternatives.
- Application of Pol.is network democracy to three cases for the national government and for new developments covered by the Value-Driven Digitalisation Work Agenda.

¹⁶⁶Formatted and summarised by the author in accordance with the 2022 Dutch national strategy on countering disinformation. Source: Ministry of the Interior and Kingdom Relations (Netherlands), *Government-wide Strategy for Effectively Tackling Disinformation*, pp. 14--18.

Track II: Reducing the Influence of Disinformation

Efforts Depending on the Content of Disinformation

Increasing Awareness in Governmental Organisations About Disinformation

Results up to and including 2025:

- Consistent inclusion of misinformation and disinformation topics in study programmes and training courses for communication professionals within the national government.
- Local and regional governments are equipped to respond to disinformation during election periods.
- Expanded expertise in communication related to crises and national security.
- Drafting of guidelines for municipal authorities on using online monitoring tools to guarantee public order and safety.
- Simulation exercises conducted and evaluated before the 2023 Provincial Council and Water Board elections to practise rapid and proportionate responses to disinformation by government organisations.
- Development of an integrated assessment framework for the government's role concerning illegal and harmful material.

National and International Standards

Results up to and including 2025:

- Attention to promoters and spreaders of extremist messages, including extremist conspiracy theories, in a forthcoming extremism strategy.
- Increased awareness and resilience among internet users regarding posting and consulting online material.
- Conducting initial debates on alternative platforms that endorse public values.

Efforts Depending on the Disseminator or Producer of Disinformation

Results up to and including 2025:

- Completion and implementation of negotiations for an effective Foreign Information Manipulation and Interference (FIMI) toolbox, safeguarding fundamental rights.
- Development of a Government-Wide Response Framework against state threats.
- Establishment of an EU Rapid Alert System as a component of the FIMI toolbox.

Commitment to the Responsibility of Traditional Media and Online

Platforms

Traditional Media

Results up to and including 2025:

- Enhancement of quality assurance in journalism through self-regulation and adherence to the Media Act.

Social Media Platforms

Results up to and including 2025:

- Promotion of initiatives to make reliable content more visible and to guarantee authenticity.
- Holding online platforms accountable for compliance with the Digital Services Act (DSA) and the Code of Practice on Disinformation.
- Efforts to reduce the impact of negative deepfakes, collaboration with fact-checkers, ensuring transparency in political advertisements, and tracing botnets through the EU Code of Practice on Disinformation.
- Government contribution to the effective supervision of the DSA.
- Establishment of a central reporting or knowledge centre accessible to citizens for reporting unlawful online material and having it assessed.
- Securing permanent funding for DSA supervision and enforcement.
- Implementation of necessary legislation required for DSA supervision and enforcement.

Knowledge Development

Results up to and including 2025:

- Identification of the local impact and nature of disinformation and conspiracy theories.
- Completion of a pilot project for responsible data sharing with researchers to understand the dissemination and extent of disinformation.
- Provision of access for researchers to online platform data.
- Establishment of permanent information exchange on disinformation with European and international partners.
- Active roles taken by independent media, academia, and civil society in addressing disinformation.
- Formation of a network of independent experts and knowledge exchange through roundtable meetings organised by the Netherlands Institute for Sound and Vision.