Revista JURÍDICA PORTUCALENSE

www.upt.pt

Nº 39 | Universidade Portucalense | Porto | 2026

https://doi.org/10.34625/issn.2183-2705(39.1)2026

Anatolii Zinenko, Ivo Svoboda, Tetiana Dereshchuk, Nataliia Shevchenko, Maryna Shapovalenko

EU Policy on Countering Disinformation and its Impact on the Information Security of Member States

DOI: https://doi.org/10.34625/issn.2183-2705(39.1)2026.ic-7

Secção

Investigação Científica / Scientific Research*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review* / The articles in this section have undergone a blind peer review process.

EU Policy on Countering Disinformation and its Impact on the Information Security of Member States

Política da UE de Combate à Desinformação e seu Impacto na Segurança da Informação dos Estados-Membros

Anatolii ZINENKO[1]
Ivo SVOBODA[2]
Tetiana DERESHCHUK[3]
Nataliia SHEVCHENKO[4]
Maryna SHAPOVALENKO[5]

ABSTRACT: The purpose of this research is to evaluate the effectiveness of the European Union (EU), through the regulation, institution, and technology framework of the EU, to protect its member states' national information infrastructure from disinformation and to enhance overall information security. In order to assess this, we will examine the effect of the regulatory actions taken by the EU (i.e., the Digital Service Act and the NIS2 Directive) on the national information systems of each of the member states and the confidence of the citizens of those states in those systems. A multidisciplinary methodology will be used to analyze these topics. Specifically, Legal Dogmatics, Comparative Law, Socio-Legal Analysis, and Legal Monitoring will be used together to provide a comprehensive assessment of the data collected for this project from over 280 different sources, between 2015 and 2024. The results of this research show an emerging trend toward legal convergence in approaches to address disinformation and hybrid threats in the EU context among the member states, however, it also shows significant disparities among member states regarding their ability to enforce compliance, govern digital technologies, and withstand hybrid threats. Ultimately, the research indicates there exists a structural conflict between the protection of the free flow of information and the regulation of misinformation and this structural conflict occurs in the context of the broader geopolitics of information confrontation. Overall, the research concludes that for the EU to effectively improve its collective information security, coordination of EU policies, implementation of advanced technologies such as artificial intelligence, and enhanced cooperation among member states will be necessary.
KEYWORDS: disinformation; EU policy; information security; cybersecurity; digital security; media literacy.

RESUMO: O artigo analisa a eficácia da política da UE de combate à desinformação através

[1] Postgraduate Student, Interregional Academy of Personnel Management, Kyiv, Ukraine; ORCID: 0009-0001-8493-5940; email: anatoliizinenko@outlook.com
[2] Associate Professor, Guarantor of Security Management Studies, AMBIS, Praha, Česka Republika; ORCID: 0000-0002-0941-4686; email: ivosvoboda@outlook.com
[3] PhD., Associate Professor of the Department of International Relations, Faculty of History, Politology and International Relations, Vasyl Stefanyk Precarpathian (Carpathian) National University, Ivano-Frankivsk, Ukraine; ORCID: 0000-0002-5348-9394; email: tetianadd@yahoo.com
[4] PhD in History, Associate Professor of the Department of International Relations and Social Sciences, Faculty of Humanities and Pedagogy, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine; ORCID: 0000-0002-6570-4944; email: nataliiashevchenko2025@outlook.com
[5] Doctor of Political Science, Associate Professor, Professor of the Department of Political Science, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine; ORCID: 0000-0002-9128-8008; email: marynashapovalenko@outlook.com

da utilização de mecanismos regulamentares, institucionais e tecnológicos. O objetivo é determinar o impacto dos actos regulamentares da UE (a Lei dos Serviços Digitais e a Diretiva NIS2) na estabilidade das infra-estruturas de informação nacionais e no nível de confiança do público. A metodologia de investigação é interdisciplinar e abrange abordagens dogmáticas, sócio-jurídicas, de direito comparado, bem como de controlo jurídico. A base analítica inclui mais de 280 fontes: Legislação da UE, práticas nacionais, documentos estratégicos e estatísticas para 2015-2024. Os resultados do estudo indicam uma harmonização gradual das respostas jurídicas entre os Estados-Membros, embora ainda existam diferenças significativas em termos de eficácia da aplicação da lei, do nível de governação digital e da capacidade de combater as ameaças híbridas. A análise revela igualmente uma tensão normativa entre a garantia da liberdade de expressão e a necessidade de regular eficazmente a propagação da desinformação - um aspeto ainda pouco estudado na ciência jurídica. As conclusões sublinham a necessidade de políticas coordenadas e adaptativas apoiadas por ferramentas tecnológicas modernas, nomeadamente a inteligência artificial, e de uma cooperação transfronteiriça reforçada. A eficácia da integração de tecnologias de deteção de ameaças em tempo real também requer uma atenção especial.
PALAVRAS-CHAVE: desinformação; política da UE; segurança da informação; cibersegurança; segurança digital; literacia mediática.

1. Introduction

Digital communications platforms enable the dissemination of disinformation across international borders, create regulatory disparities and create vulnerabilities within interdependent Information infrastructures. Thus the diffusion of disinformation is an issue to EU Member States' political stability, democracy, and information security. Disinformation has evolved into a geostrategic tool to destabilize democracies, discredit public institutions and disrupt the European Union's strategic cohesion[6].

Disinformation campaigns are capable of impacting election processes, polarizing society, and increasing hybrid threats (combining cyber attacks with manipulative information strategies)[7]. Because of these capabilities, counter-disinformation is now considered as part of the EU's overall security and governance framework; counter-disinformation must be addressed through a unified approach by the EU to safeguard both the right of free expression, while also developing effective mechanisms to secure information across EU Member States. As such, countering disinformation is now not simply an area of media law but rather a central component

[6] EUROPEAN COMMISSION. Code of practice on disinformation. Digital strategy. 2025. Available from https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

[7] STASIUK, Nadiia. Particular aspects of legal prevention and counteraction to domestic violence in Ukraine. *European Political and Law Discourse*, 2020, vol. 7, no. 4, pp. 185–189. https://doi.org/10.46340/eppd.2020.7.4.28

of EU Security and Governance[8].

Although there is increasing scholarly and policy-based interest in combating disinformation, several fundamental questions continue to be under-researched[9]. Specifically, the practical effectiveness of the European Union's (EU) legal tools and institutional arrangements for combating disinformation have been inadequately researched as well as how they may contribute to strengthening member state national information security systems[10]. An important issue is the challenge of creating legal consistency among the diverse legal traditions, enforcement capabilities, and governance models of EU member states, and how it limits the EU from responding to transnational information threats with unity. A second area of limited development within legal literature is the inter-relationship between anti-disinformation policies and more general democratic governance principles, such as transparency, accountability and citizen engagement[11].

This study hypothesizes that, although EU policy in combatting disinformation has developed a broad regulatory framework that will shape the national responses of EU member states regarding information security, the practical effect of this policy varies greatly among EU member states due to their differing legal traditions, technological capability, institutional resource base and political commitment. The novel contribution of the research in terms of its methodology lies in providing a comprehensive analysis of EU policy regarding combating disinformation as a dynamic variable which impacts both the national information security architecture of each EU member state and the broader strategic posture of the EU in the evolving global geo-political arena.

The purpose of this study is to critically evaluate EU's policy instruments for combating disinformation and to evaluate its capacity to strengthen the Information Security of EU member states. The objective of achieving the purpose of this study are as follows:

[8] BARHOUMI, Ouala. NIS 2: Where are European countries in transposing the directive? *Wavestone*. 2024. Available from https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive/

[9] THE NIS 2 DIRECTIVE. 2025. Available from https://www.nis-2-directive.com

[10] MELNYK, Dmytro S., et al. Practice of the Member States of the European Union in the field of anti-corruption regulation. *Journal of Financial Crime*, 2022, vol. 29, no. 3, pp. 853-863. https://doi.org/10.1108/JFC-03-2021-0050

[11] SEMENETS-ORLOVA, Inna, et al. Human-centered approach in new development tendencies of value-oriented public administration: Potential of education. *Economic Affairs* (New Delhi), 2022, vol. 67, no. 5, pp. 899-906. https://doi.org/10.46852/0424-2513.5.2022.25

(1) To investigate EU legal and institutional instruments intended to counter disinformation and to compare them to principles related to information security;

(2) To analyze how EU policies have influenced national information security strategies and systems; and to identify the variables explaining why there were different results across EU member states;

(3) To identify challenges and opportunities to governance associated with the application of EU's counter-disinformation policy instruments considering democratic values, principles of public governance, and a human-centered approach to security.

Disinformation for the purposes of this research is considered to be intentional misleading or manipulation of information through false information to influence public opinion or disrupt the operation of institutions. Information security, then, encompasses all the measures taken by an organisation to protect their information systems, communication networks and digital infrastructure from either authorized access, unauthorized use, manipulation or destruction in order to maintain confidentiality, integrity and availability. The hybrid threat is therefore defined as a complex and multi-dimensional action that combines cyber operations, disinformation campaigns, and other tools of influence, that are used in conjunction with one another to take advantage of social vulnerabilities, and undermine the political stability and/or sovereignty of states. Therefore, these theoretical concepts will serve as the basis for analysing the impact of EU policy on the information security of member states.

2. Literature Review

EU member states have been affected by growing digital dependence on one another in terms of an emerging systemic threat to both information security and democratic resilience at the level of EU member states. The academic literature is increasingly characterizing disinformation as a multifaceted problem that intersects with information security, constitutional law, media regulation and geopolitical rivalry rather than simply as a form of communication distortion. The purpose of this literature review is to categorize the various ways of thinking about this issue, to identify theoretical (doctrinal) and empirical gaps and to develop a comprehensive analytical model for assessing the effectiveness of EU counter-disinformation policy.

Research has been conducted regarding the normative and constitutional limitations of government regulation against the spread of disinformation. A number of authors have investigated this subject from the legal perspective to analyze the

potential complexities in creating the definition of disinformation as an object of regulation. The relationship between regulation of disinformation and the protection of freedom of expression has been discussed. The authors conclude that if there is to be any type of regulatory action, it should be limited, provide transparency and be supported by democratic legitimacy; a position which is consistent with the constitutional and proportionality-based approaches taken by Hueso (2022)[12]. Additionally, the research of Machowicz (2022)[13] supports the view that the quantity and quality of the information available to citizens is an essential factor in their ability to fully engage in the meaningful exercise of freedom of expression. It was demonstrated that low-quality or manipulative information would negatively affect the substantive aspects of freedom of expression, thus providing justification for proportionate regulatory measures to protect citizens from such types of information. Therefore, based upon the research of Hueso (2022)[14] and Machowicz (2022)[15], it can be concluded that the regulation of disinformation does not necessarily conflict with basic civil liberties, as long as the regulations remain certain and proportional.

Security-based perspectives have often viewed disinformation as part of hybrid threats. Sheremet et al. (2021)[16] view disinformation as a key component of information warfare; specifically they focus on the post-Soviet and Eastern European context where institutional fragility and low media literacy make the populace vulnerable to disinformation campaigns. Zvozdetska (2021)[17] has defined disinformation as a threat to both national security and EU cohesion and also that the erosion of trust with the public is a major risk factor for this type of threat. The studies by Sheremet et al.

[12] HUESO, Lorenzo C. Who, how and what to regulate (or not regulate) in the face of disinformation. *Teoría Y Realidad Constitucional*, 2022, vol. 49, pp. 199–238. https://doi.org/10.5944/trc.49.2022.33849
[13] Machowicz, K. (2022). The impact of the quality of information on the use of freedom of expression. *Studia Iuridica Lublinensia*, *31*(3), 189–201. https://doi.org/10.17951/sil.2022.31.3.189-201
[14] HUESO, Lorenzo C. Who, how and what to regulate (or not regulate) in the face of disinformation. *Teoría Y Realidad Constitucional*, 2022, vol. 49, pp. 199–238. https://doi.org/10.5944/trc.49.2022.33849
[15] Machowicz, K. (2022). The impact of the quality of information on the use of freedom of expression. *Studia Iuridica Lublinensia*, *31*(3), 189–201. https://doi.org/10.17951/sil.2022.31.3.189-201
[16] SHEREMET, Oleg S., et al. Political and legal aspects of the information warfare. *Revista Amazonia Investiga*, 2021, vol. 10, no. 45, pp. 31–41. https://doi.org/10.34069/ai/2021.45.09.3
[17] ZVOZDETSKA, Oksana. Disinformation as a threat to the EU National security: Issues and approaches. *Modern Historical and Political Issues*, 2021, vol. 43, pp. 30–39. https://doi.org/10.31861/mhpi2021.43.30-39

(2021)[18] and Zvozdetska (2021)[19] were conducted before the Digital Services Act was implemented and the NIS2 Directive came into effect, thus the two studies do not evaluate how the EU's updated regulatory environment will affect national information security systems.

A research that also studies the connection of disinformation to cybersecurity is another example of how uncoordinated are the current ways to address this issue. Leroy & Zolotaryova (2023)[20] study the vulnerabilities of the critical infrastructure due to cyber attacks combined with disinformation campaigns, but mainly from a technical point of view, they did not analyze the coordination mechanisms for legal harmonization at national level. Antipova (2023)[21] focuses on strategic communication as an element of the State information security, she highlights the role of public authorities in developing resilient narratives; however she does not study the coordination among national bodies and EU regulatory tools.

Vandezande (2023)[22], provides an exhaustive doctrinal overview of the NIS2 Directive at the EU regulatory level, to identify a strong enhancement of the supervision, and reporting obligation, with a broadening of the sectors included within the NIS2. Although this research allows for a clarification of the responsibility of institutions, it does not analyze how the cyber security regulations interact with specific instruments against disinformation as is the case with the Code of Practice on Disinformation or the European Democracy Action Plan. In addition, Çağlayan (2022)[23] identifies the innovations that are being developed by the EU with regard to cybersecurity; however, he did not address the problem of legal enforcement in the area of counter-disinformation policy, thus continuing the identification of the gap

[18] SHEREMET, Oleg S., et al. Political and legal aspects of the information warfare. *Revista Amazonia Investiga*, 2021, vol. 10, no. 45, pp. 31–41. https://doi.org/10.34069/ai/2021.45.09.3

[19] ZVOZDETSKA, Oksana. Disinformation as a threat to the EU National security: Issues and approaches. *Modern Historical and Political Issues*, 2021, vol. 43, pp. 30–39. https://doi.org/10.31861/mhpi2021.43.30-39

[20] LEROY, Iryna and ZOLOTARYOVA, Iryna. Critical infrastructure defense: Perspectives from the EU and USA cyber experts. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 2023, vol. 5, pp. 165–170. https://doi.org/10.33271/nvngu/2023-5/165

[21] ANTIPOVA, Olha. Strategic communications as a component of state information security. Law *Journal of the National Academy of Internal Affairs*, 2023, vol. 13, no. 1, pp. 44-52. https://doi.org/10.56215/naia-chasopis/1.2023.44

[22] VANDEZANDE, Niels. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 2023, vol. 52, 105890. https://doi.org/10.1016/j.clsr.2023.105890

[23] ÇAĞLAYAN, Mehmet U. Review of some recent European cybersecurity research and innovation projects. *Infocommunications Journal*, 2022, vol. 14, no. 4, pp. 70–78. https://doi.org/10.36244/icj.2022.4.10

identified between technical innovation and normative implementation.

Munkøe & Mölder (2022)[24] provide a broader perspective of the geopolitical and strategic aspects of the EU's cybersecurity governance, where they place the EU's cybersecurity governance in the context of global digital competition and describe the structural difficulties that the EU faces in addressing future threats generated by new technology such as AI-generated disinformation. While Munkøe & Mölder (2022)[25] assess the EU's current cybersecurity governance, their analysis is based primarily on the EU's current regulatory framework which existed prior to DSA (Digital Services Act). Therefore, their analysis does not include any changes made to the EU's regulatory framework after the DSA was implemented in 2022. Martins & Jumbert (2020)[26] examine how security narratives are constructed in the co-production of border technologies, and specifically demonstrate how the EU uses digital tools to construct those security narratives; however, because their examination focuses on border technologies, it is limited in its applicability to broader information security governance. Négyesi (2024)[27] provides an additional layer to this discussion of the EU's cybersecurity governance by demonstrating the potential benefits of using AI to identify information security threats, while at the same time noting the ethical and legal concerns regarding the use of algorithms to govern cybersecurity.

The research has shown that there are many ongoing research gaps within the field of study of EU regulation. The first gap is related to the lack of an integrative framework of EU regulations (in particular how they interact with each other) including the DSA; the Code of Practice on Disinformation; and Cybersecurity Directives such as NIS2. Secondly, the literature lacks sufficient examination of horizontal coordination across the Member States of the European Union (i.e., the differences in the ability of states to enforce policies and the differing levels of institutional resource). Thirdly, there is limited empirical legal analysis of the use of AI based tools for legitimate counter-

[24] MUNKØE, Malthe and MÖLDER, Holger. Cybersecurity in the era of hypercompetitiveness: Can the EU meet the new challenges? *Revista CIDOB D Afers Internacionals*, 2022, vol. 131, pp. 69–94. https://doi.org/10.24241/rcai.2022.131.2.69

[25] MUNKØE, Malthe and MÖLDER, Holger. Cybersecurity in the era of hypercompetitiveness: Can the EU meet the new challenges? *Revista CIDOB D Afers Internacionals*, 2022, vol. 131, pp. 69–94. https://doi.org/10.24241/rcai.2022.131.2.69

[26] MARTINS, Bruno. O. and JUMBERT, Maria G. EU Border technologies and the co-production of security 'problems' and 'solutions.' *Journal of Ethnic and Migration Studies*, 2020, vol. 48, no. 6, pp. 1430–1447. https://doi.org/10.1080/1369183x.2020.1851470

[27] NÉGYESI, Imre. Possibilities of using artificial intelligence in EU and UN peacekeeping activities. *Revista Academiei Forţelor Terestre*, 2024, vol. 29, no. 1, pp. 11–19. https://doi.org/10.2478/raft-2024-0002

disinformation purposes. Fourthly, there is still considerable conceptual ambiguity in the literature. For example, disinformation can be viewed as a cybersecurity risk, a democratic governance risk, or a free speech risk and therefore it is difficult to develop legal policy responses that are consistent. Fifthly, many of the studies contained within the existing literature were completed prior to 2022 and therefore do not provide sufficient insight into the practical effects of the new EU regulatory frameworks enacted since then.

3. Methods

3.1. Research design

The empirical stage of the study lasted from January to November 2024 and is presented in the form of a diagram (Figure 1). The analysis was carried out by an interdisciplinary research team, which included legal scholars and cybersecurity experts. The main objective of the study was to assess the relationship between the EU regulatory policy in the field of countering disinformation and its impact on the information security systems of the Member States.

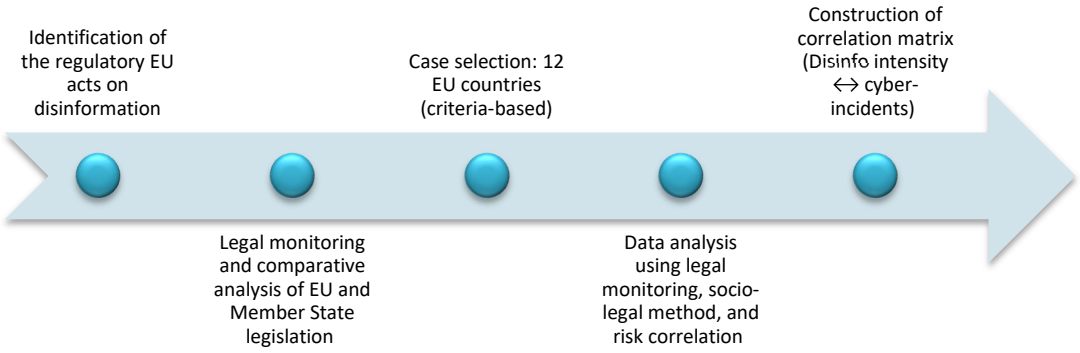

Figure 1. Research stages

Source: developed by the author based on MiniTAB data[28]

3.2. Sampling

A multi-level sampling strategy was implemented to ensure a representative analysis of the impact of EU policy on countering disinformation on the information security of Member States. The sample covered four groups of sources selected in accordance with research legal methods:

[28] MINITAB. Data analysis, statistical & process improvement tools. 2025. Available from https://www.minitab.com/en-us/

1. Regulatory legal acts of the EU and Member States. A total of 34 documents (311 provisions) for 2015-2024 were analysed: regulations, EU directives, national laws and implementing acts. The main selection criteria were:

- regulation of digital platforms, media and online content;
- presence of cybersecurity provisions;
- obligations of states to monitor disinformation.

Sources: EUR-Lex, legislative bases of the Council of the EU and national bulletins.

2. National law enforcement practice. A total of 12 Member States (Germany, France, Italy, Spain, Poland, Romania, Hungary, Sweden, Estonia, Czech Republic, Greece, and Netherlands) were selected based on:

- regional representation;
- diversity of legal systems;
- level of impact of information operations;
- presence or absence of national strategies.

This ensured comparative legal variability and the possibility of generalizing the results.

3. *International agreements and analytical reports*. The sample covered 21 documents, including:

- recommendations of the Council of Europe (CE), UNESCO, OSCE;
- analysis of NATO StratCom COE and EEAS.

Criteria: relevance to the topics of disinformation, hybrid threats, cyber resilience and mention in official strategic documents.

4. Statistical and socio-legal sources. Over 280 datasets were used:

- Eurobarometer survey on media literacy;
- national statistical services (INSEE, Statistisches Bundesamt, CSO Poland);
- annual reports of Computer Emergency Response Teams (CERT) and EU cybersecurity agencies (ENISA);
- judicial statistics of the European Commission for the Efficiency of Justice (CEPEJ).

The main criterion is the officiality of the source and the coverage of the topics of digital threats, institutional capacity and public perception of risks (2015-2024).

3.3. Methods

To achieve the objectives of the study, four complementary legal methods were applied, which correspond to the sample structure:

1. Legal dogmatics. Applied to EU regulations (in particular Regulation (EU) 2022/2065 and Directive 2016/1148) and EEAS strategic documents. The method allowed for a systematic interpretation of provisions on countering disinformation, platform liability, and state obligations. The analysis used a unified legal matrix with blocks (1) detection of disinformation, (2) enforcement mechanisms, (3) scope and mandates.

2. Comparative law. Applied to the analysis of legal approaches in 12 Member States. A four-level coding was used: legal form; institutional powers; implementation mechanisms; compliance with EU law. This made it possible to assess the level of harmonisation and the impact of the subsidiarity principle.

3. Legal monitoring. Legislative changes in the field of information security were tracked: parliamentary initiatives, decrees, government strategies. A monitoring dashboard using API was created to record changes in EU legislation and national legal frameworks. Key indicators: emergence of cyber units; introduction of media literacy programmes; changes in the regulatory framework.

4. Socio-legal method. Used to assess the social impact of the regulation based on official statistics and sociology. In particular:

- frequency of cybercrimes (phishing, blackmail, fraud);
- data from national CERTs;
- results of sociological surveys on trust in the media, digital literacy, and perception of external influence.

The obtained quantitative data were normalized using z-scores and aggregated into the Disinformation Vulnerability Index. A cross-tabulation was performed between this index and the incidence rate indicators by country. Correlation analysis was performed using Pearson's r coefficient, and the level of statistical significance was defined as $\alpha = 0.05$.

The construction of the Disinformation Vulnerability Index (DVI)

The construction of the Disinformation Vulnerability Index (DVI), in order to provide an explanation of how it was developed, was completed by way of a multi-step analytical process that combined indicators based on legal, institutional, and socio-legal indicators obtained from over 280 official and peer-reviewed sources.

The DVI was created as a means to measure the comparative vulnerability of the EU Member States to threats posed by disinformation within their national information security systems.

All collected data was initially categorized by one of four dimensions for analysis:

(1) Regulatory Capacity: National Legal Frameworks - The existence and scope of national laws implementing EU Counter-Disinformation and Cybersecurity Norms;

(2) Institutional Capacity: Competent Authorities, CERTs, Supervisory Bodies - Whether the entities exist, are specialized in their function, and whether they have sufficient resources to perform their functions;

(3) Technological Resilience: Tools & Mechanisms - Monitoring tools; Incident Response capabilities; and Cybersecurity measures implemented within organizations;

(4) Societal Resilience: Media Literacy; Public Trust Indicators; Exposure to Disinformation Campaigns.

Each of these dimensions was further broken down into operationalized indicators based upon available information from official statistics (Eurobarometer, ENISA, CEPEJ), national reports, and documented practices of law enforcement agencies. In addition to quantitative statistics, qualitative legal assessments were developed into ordinal variables that could be compared across countries through use of a standard coding methodology.

All of these indicators were standardized at the second stage using the Z-transformation method to remove measurement scale effects and minimize statistical bias. The transformed data for each indicator was then combined within each analytical factor based on an equal-weighted scheme. This approach is consistent with the hypothesis that regulatory, institutional, technological and social factors are equally important and functionally interdependent in shaping disinformation vulnerabilities and therefore the degree to which institutions are capable of enforcing regulations related to regulation.

The last step involved aggregating the four individual factor-based composite dimension scores into a single index of regulatory completeness and enforcement capacity (with values ranging from 0 to 100), indicating increased regulatory effectiveness and decreased vulnerability to disinformation as the value of the index increases. Following this aggregation, the developed index was compared to country-specific incidence rates of disinformation-related cyber attacks and Pearson's r

coefficient was calculated (α=0.05) to determine the level of correlation between legal and institutional capacity and observed security results.

4. Results

4.1. Legal-dogmatic analysis of EU regulatory instruments

Legal-Dogmatic Analysis - Legal dogmatics examined 34 Regulatory Acts of the European Union (EU) that were developed from 2015 through 2024 and contained 311 normative provisions related to preventing disinformation and protecting Information Security. The provisions were grouped based on a thematic classification system similar to the one described above in the "Methods" section as follows: Disinformation Detection; Platform Responsibility; National Coordination (See Table 1).

Table 1. Breakdown of legal provisions by thematic area in EU regulations on countering disinformation (2015–2024)

Thematic block	Number of provisions	Percentage (%)
Disinformation detection	118	38.2
Platform responsibility	97	31.4
National coordination	96	30.4
Total	311	100

Source: developed by the authors based on the data from De Hert and Penedo,[29] EUR-LEX - 52024IE0014 - EN - EUR-LEX,[30] European Court of Auditors,[31] Council of Europe[32]

The research shows that nearly 40 percent of the analyzed legal measures are based on detection mechanisms. In these cases, digital service providers have to monitor their services; report to regulatory bodies about their activities; perform risk assessments for potential dangers related to disinformation. This is a clear example of the EU's preventive approach, as expressed in the Digital Services Act and in the way it focuses on identifying system-wide risks related to the spread of disinformation at an

[29] DE HERT, Paul and PENEDO, Andrés Chomczyk. A democratic alternative to the Digital Services Act's handshake between States and online platforms to tackle disinformation. *EU Law Analysis.* 2022. Available from: https://eulawanalysis.blogspot.com/2022/01/a-democratic-alternative-to-digital.html?utm

[30] EUR-LEX - 52024IE0014 - EN - EUR-LEX. 2025. Available from: https://eur-lex.europa.eu/eli/C/2024/4052/oj?utm

[31] EUROPEAN COURT OF AUDITORS. Special report No 9/2021: Combating disinformation: Role of the EU response to safeguard the internal market and citizens' rights (SR 21 09). Publications Office of the European Union. 2021. Available from: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf

[32] COUNCIL OF EUROPE. Principles for media and communication governance: Recommendation CM/Rec (2022)11 and explanatory report. 2022. Available from: https://edoc.coe.int/en/media/11117-principles-for-media-and-communication-governance-recommendation-cmrec202211-and-explanatory-report.html

early stage. The legal obligations regarding the liability of platforms (i.e., 31.4 percent) support the same principle by obligating online platforms to take care of the quality of the data they collect and transmit; to provide the public with transparent information about their services; and to be accountable in case they do not fulfill these obligations. The remaining 30.4 percent of the provisions deal with the coordination among Member States concerning the national implementation of EU information security policies. At the same time, however, the study also demonstrated how often there were normative inconsistencies in the legal measures studied, primarily with respect to the definition of "disinformation" and how it is distinguished from other dangerous forms of content. The inconsistencies mentioned above were also found in existing literature. They resulted in overlapping competence areas for the EU institutions and the national authorities in charge of enforcing the provisions. This led to differences in the way the provisions are enforced nationally, and it provides direct background knowledge for the comparative and empirical results presented below.

4.2. Comparative analysis of national legal and institutional capacity

The distribution of the Disinformation Vulnerability Index is illustrated in Figure 2 for twelve selected EU Member States. The index operationalizes the combined legal, institutional, technological and societal dimensions of counter-disinformation capacity as described in the methodological section.

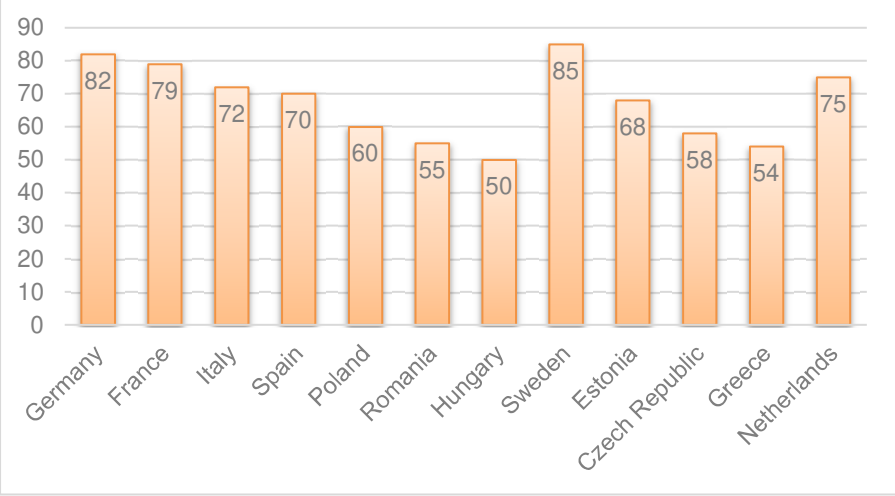

Figure 2. Coverage of disinformation regulation and enforcement mechanisms by country (index scale 0–100)

Source: developed by the authors based on the data from Kalniņa-Lukaševica,[33] Freedom House,[34] KPMG,[35] European Centre for Press and Media Freedom[36]

The EU Member States scoring highest on this Index (75-85) - for example, Sweden, Germany, France and The Netherlands – show a large degree of regulatory completeness and institutional specialisation. In the EU Member States showing the highest scores, National Strategies which are aligned with EU Legal Standards and well-funded Supervisory Authorities and CERT structures have been established in order to ensure that EU Instruments are effectively complemented by national Legislation, thus making it possible to enforce Proactively and to translate Supranational Norms into Effective Domestic Practice.

In contrast, the EU Member States with scores in the middle range (60-74), such as Italy, Spain, Estonia and Poland, show an incomplete alignment with the Regulatory Objectives set out in EU Law. Although there has been almost complete Formal Transposition of EU Law, Enforcement Capacity and Inter-Agency Coordination in these jurisdictions remains uneven and the Resource Constraints and Fragmentation of Institutional Mandates restrict the Effectiveness of Counter-Disinformation Measures despite Compliance with EU Legal Requirements.

The EU Member States which score lowest on this Index (50-59), such as The Czech Republic, Romania, Greece and Hungary, demonstrate Underdeveloped Regulatory and Institutional Frameworks, which are often Fragmented. The Vagueness of Legal Definitions, the Limited Specialisation of Enforcement Bodies and the Lack of Comprehensive National Strategies in these Jurisdictions create Vulnerability to Disinformation Campaigns. The Findings of this Study therefore confirm the Central Hypothesis of the Study, namely that Harmonisation of Laws within the EU does not Automatically Translate into Uniform Security Outcomes.

[33] KALNIŅA-LUKAŠEVICA, Zanda. Foreign interference: A threat to democratic security in Europe (Doc. 16131). *Parliamentary Assembly of the Council of Europe*. 2025. Available from https://pace.coe.int/en/files/34179/html?utm

[34] FREEDOM HOUSE. Freedom on the Net 2024: Digital booklet. 2024. Available from: https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

[35] KPMG. KPMG network and information security directive (NIS 2). 2023. Available from: https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2023/10/kpmg-network-and-information-security-directive-nis2.pdf

[36] EUROPEAN CENTRE FOR PRESS AND MEDIA FREEDOM. 1,117 media freedom alerts in the past year: MFRR Monitoring Report 2023. 2024. Available from: https://www.ecpmf.eu/1117-media-freedom-alerts-in-the-past-year-mfrr-monitoring-report-2023/

4.3. Legal monitoring and dynamics of regulatory adaptation

Legal Monitoring Results reveal a rising level of legal enactments on information security from 2015 until 2024 (see Figure 3). As such, there has been an increase in the average number of enacted or revised legal documents per year — from 1.2 between 2015 – 2017 to 3.8 between 2021 – 2024. Trends of this nature are consistent with the adoption and implementation of major EU instruments, specifically the Digital Services Act and the NIS2 Directive.

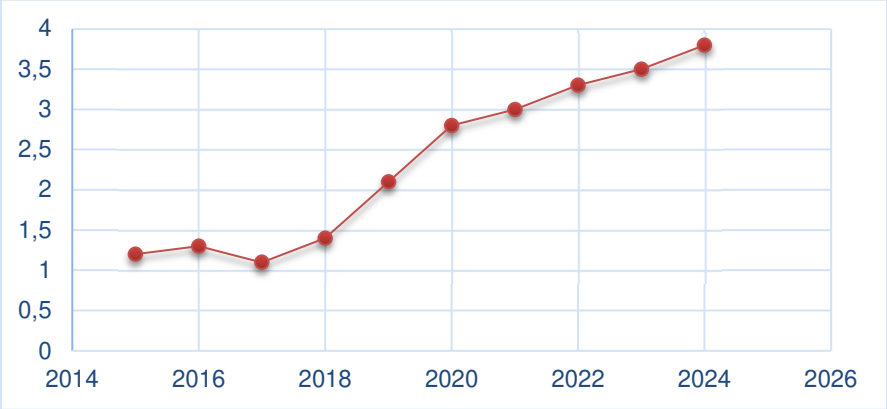

Figure 3. Annual number of legislative acts related to disinformation and information security in EU Member States (2015–2024)

Source: developed by the authors based on the data from European Economic and Social Committee,[37] European Commission Eurobarometer,[38] European Parliament & Council of the European Union[39]

The first phase of relatively low legislative activity is reflective of the developmental stages of the EU's policy making process that were being implemented prior to 2017 — where disinformation was addressed by means of soft law regulations. In the second phase that started after 2017, an accelerated legislative response was made relative to disinformation identified as a hybrid threat. The third phase that peaked in 2023 – 2024 — reflected growing levels of geopolitical tension and the obligatory regulatory requirements for the EU's member states.

[37] EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. Opinion of the European Economic and Social Committee – Safeguarding democracy against disinformation (own-initiative opinion). Official Journal of the European Union, C/2024/4052. 2024. Available from: https://eur-lex.europa.eu/eli/C/2024/4052/oj

[38] EUROPEAN COMMISSION. Standard Eurobarometer 102 – Autumn 2024 [Data set]. Directorate-General for Communication, European Commission. 2024. Available from https://europa.eu/eurobarometer/surveys/detail/3215

[39] EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, pp. 1–102. 2022. Available from: https://eur-lex.europa.eu/eli/reg/2022/2065

These three phases indicate an evolution from responding to disinformation in an uncoordinated fashion to creating a framework of regulations that although still not uniform throughout all EU member states — will be more cohesive than previously had been the case.

4.4. Socio-legal indicators and empirical security outcomes

Empirical data (surveys/statistics) between 2017–2024 show mixed results toward social resilience and empirically based security according to research studies on law and sociology.

A clear increase (12%) in average media literacy shown in Table 2 as a direct result of educational programs and EU awareness campaigns indicates a positive upward trend in social resilience regarding disinformation.

Table 2. Trends in media literacy and trust in institutions (2017-2024)

Year	Average media literacy score (%)	Trust in institutions (%)
2017	58	47
2020	64	50
2024	70	53

Source: developed by the authors based on the data from European Regulators Group for Audiovisual Media Services, Action Group 3.,[40] European Commission,[41] Noerr,[42] European University Institute[43]

Although there was a six percent increase in the percentage of public trust in institutions over the last seven years, this increase is very small and could indicate that while educational and regulatory measures have been successful at reducing disinformation; the long-term ramifications of numerous efforts to disseminate disinformation and the increase in political division within society will be difficult to overcome. Additionally, the success of these measures will also depend upon the ability of each country to implement them.

The number of cyber incidents involving disinformation increased by 50 percent from 2018 through 2023 at an average rate of 8.4 percent per year (See Figure 4).

[40] EUROPEAN REGULATORS GROUP FOR AUDIOVISUAL MEDIA SERVICES, ACTION GROUP 3. Report on Media Literacy [ERGA-AG3-2021-Report-on-Media-Literacy]. 2021. Available from https://erga-online.eu/wp-content/uploads/2021/12/ERGA-AG3-2021-Report-on-Media-Literacy.pdf

[41] EUROPEAN COMMISSION. European media information and communication community. 2025. Available from https://media-board.europa.eu/index_en

[42] NOERR. NIS 2 update for Europe. 2025. Available from https://www.noerr.com/en/insights/nis-2-update-for-europe-march-2025

[43] EUROPEAN UNIVERSITY INSTITUTE. Media ownership monitor. 2025. Available from: https://media-ownership.eu

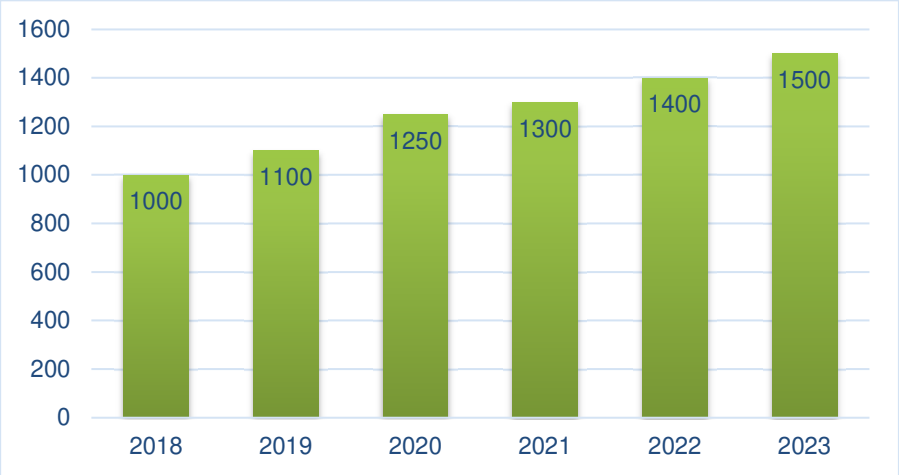

Figure 4. Annual number of cybercrime incidents related to disinformation in EU Member States (2018–2023)

Source: developed by the authors based on the data from European Union Agency for Cybersecurity,[44] European Parliament & Council of the European Union,[45] European Commission[46]

A significant increase occurred in 2020 which correlates to the COVID-19 pandemic and the resulting infodemic. However, as demonstrated by the continuing increase in the years that followed, this represents the development of disinformation into part of a larger hybrid threat strategy. More than 60 percent of the identified incidents involved the critical information infrastructure of various entities such as media organizations, health care providers and election processes.

Although the regulatory environment has strengthened with the adoption of the DSA and NIS2, there was no year that evidenced a stabilizing or declining trend in incidence. These findings indicate a consistent disparity between regulatory norms and actual cybersecurity performance across all EU Member States, but particularly among those states that have less developed institutional and technological capacities. The findings reinforce that legal reforms are necessary; however, they must be complemented with law enforcement activities, allocation of resources and cross border cooperation to demonstrate measurable reduction in vulnerabilities.

[44] EUROPEAN UNION AGENCY FOR CYBERSECURITY. Threat Landscape. *ENISA*. 2024. Available from: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[45] EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union,* L 333, pp. 80–152. 2022. Available from:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[46] EUROPEAN COMMISSION. Europe's digital decade: Digital targets for 2030 (COM(2020) 784 final). 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0784

4.5. Synthesis of results

When considered collectively, the study's results indicate that EU anti-disinformation policies have also brought about an increase in the degree of legal unity and clarity among European Union member states' regulations. In contrast, empirical data collected show significant differences in both the application and effectiveness of these policies across member states. The research shows a higher correlation between the levels of index scores obtained by each member state and their institutional strength and relative vulnerability; whereas countries with less robust systems for enforcing compliance are continually at risk from both existing and developing forms of misinformation. This will establish a solid base for the analysis of the strategic implications of this study and for further development of anti-disinformation policy in the next section.

5. Discussion

This research confirms the original hypothesis that the European Union's legal framework regarding counteracting disinformation is a strong institutional and normative basis to enhance the information security in all the member states of the European Union. EU has created an architecture of governance at different levels based on a combination of legislation (Digital Services Act; Directive (EU) 2021/836 (NIS2); a non-legislative instrument (Code of Practice on Disinformation); institutional inter-communication; and technical innovations. This multilevel framework represents a transition from reactive responses to the regulatory system as being preventative and risk-based. However, the empirical evidence indicates that the effectiveness of this framework depends on the unequal capacity of EU Member States.

The comparative analysis shows that differences in regulatory enforcement; institutional specialization; and technological preparedness directly impact on the European Union's overall position in a strategic sense. The EU member states with an advanced framework for law and institutions exhibit both a reduced risk of being vulnerable to disinformation as well as act as a stabilizing anchor within the EU's information security system. On the other hand, those member states whose enforcement capacity is limited or have a fractured governance structure are structural weak spots and as such can be manipulated through cross border information operations from outside of the EU. As a result this creates an asymmetry that reduces

the cohesion of the EU's common response to these types of threats and in addition reduces the deterrent impact of the EU's regulatory regime at the geopolitical level.

Zvozdetska's conceptualization of disinformation as an existential threat to both national and collective security is supported by these results, however, they extend upon her research by illustrating how member state vulnerabilities converge to form Union wide strategic risk[47]. Likewise, the above-mentioned work by Sheremet et al., on the effects of information warfare support the necessity for the EU to have a collective response to hybrid threats; similarly, the current research supports that such collective action cannot occur solely due to legal conformity, but rather due to operational capacity convergence[48]. Therefore, EU information security can be viewed as a shared, but indivisible public good, in which each members states deficiency will result in decreased Union wide information security.

In addition to legal dogma, the study's legal-dogmatic analysis shows how the EU has made a considerable amount of progress regarding addressing the previously mentioned regulation fragmentation through increased accountability for platforms and national coordination mechanisms with the Digital Services Act (DSA) and the NIS2 Regulation. The legal-dogmatic study also illustrates that enhanced supervisory responsibilities are confirmed by an evident increase in legislative activities as well as institutional adaptations post-2022. However, the continued occurrence of high numbers of disinformation-related cyber-incidents illustrate that legal-compliance does not immediately equate to successful prevention of cyber-incidents. This gap can be seen most clearly in those Member States, where the competent authorities have insufficient funds, knowledge, or political independence to put EU law into practice.

Counter-disinformation strategies and free speech continue to be an important problem as far as the norms of what is acceptable are concerned. Hueso's fears about the potential of excessive regulation are somewhat confirmed by the differing ways that countries have implemented their definitions of harmful content and obligations for platforms[49]. On the other hand, this study confirms Machowicz's statement that freedom of expression requires a minimum quality of information in the public sphere;

[47] ZVOZDETSKA, Oksana. Disinformation as a threat to the EU National security: Issues and approaches. *Modern Historical and Political Issues*, 2021, vol. 43, pp. 30–39. https://doi.org/10.31861/mhpi2021.43.30-39

[48] SHEREMET, Oleg S., et al. Political and legal aspects of the information warfare. *Revista Amazonia Investiga*, 2021, vol. 10, no. 45, pp. 31–41. https://doi.org/10.34069/ai/2021.45.09.3

[49] HUESO, Lorenzo C. Who, how and what to regulate (or not regulate) in the face of disinformation. *Teoría Y Realidad Constitucional*, 2022, vol. 49, pp. 199–238. https://doi.org/10.5944/trc.49.2022.33849

therefore, there should be no obligation of platforms to provide such information[50]. The proportionality principle contained in EU law creates a common law foundation that can be used to reconcile conflicting goals of counter-disinformation and freedom of expression, however, it will only be effective if consistently applied among EU member states. Differing national approaches to content moderation and enforcement can create different areas of the internal market for digital services and weaken the legitimacy of regulatory actions taken under the authority of the EU.

The results of this research support a strategic approach to understanding that disinformation will be included as part of hybrid threats to critical infrastructure, election processes and public trust. The evidence from the empirical data supports the relationship between Information Security (Information Governance) and Cybersecurity Governance and highlights how disinformation campaigns have been successfully combined with cyberattacks to achieve an objective. This is positive in that it represents a step toward the integration of Information Security and Cybersecurity Governance by the EU under NIS2, but the differences in implementation among Member States limit the EU's ability to demonstrate strategic resilience on the global stage.

There could be a number of positive factors in regard to the use of Artificial Intelligence (AI) technologies, such as AI-based tools that can detect Coordinated Inauthentic Behaviour, to improve the EU's Counter-Disinformation capacity. The findings from this research are consistent with Çağlayan & Négyesi's views on the benefits of AI-based tools for detecting Disinformation, however, they also support the necessity for EU legislation to ensure adequate protection against a harmful or unjustified impairment of Fundamental Rights[51][52]. The lack of common standards for Algorithmic Accountability and Transparency will likely exacerbate the existing disparities among EU Member States and will not mitigate them.

In general the discussion shows that the effectiveness of EU counter-disinformation policy cannot be determined by the degree of normative coherence with

[50] MACHOWICZ, K. (2022). The impact of the quality of information on the use of freedom of expression. Studia Iuridica Lublinensia, 31(3), 189–201. https://doi.org/10.17951/sil.2022.31.3.189-201

[51] ÇAĞLAYAN, Mehmet U. Review of some recent European cybersecurity research and innovation projects. *Infocommunications Journal*, 2022, vol. 14, no. 4, pp. 70–78. https://doi.org/10.36244/icj.2022.4.10

[52] NÉGYESI, Imre. Possibilities of using artificial intelligence in EU and UN peacekeeping activities. *Revista Academiei Forţelor Terestre*, 2024, vol. 29, no. 1, pp. 11–19. https://doi.org/10.2478/raft-2024-0002

EU law alone, nor by the amount of legislation passed. The EU counter-disinformation policy's effectiveness will depend on whether it is able to reduce the empirical vulnerability of the EU as well as increase the overall strategic posture of the EU as a whole within a growing number of conflicting and highly competitive information environments. The EU should develop the capacity to close the gap in counter-disinformation policy effectiveness, (i.e., to move from the legal framework towards operationalization), through developing capabilities for cross border coordination, as well as building institutional and social capacity to ensure long term resilience. Developing such capacities and taking such actions are essential for ensuring that EU counter-disinformation policy will serve both the internal market regulation of the EU and contribute to the overall geopolitical stability and democratic legitimacy of the EU as an entity.

5.1. Limitations

This study has limitations related to its focus on EU policies, which may not capture all the specifics of implementation and enforcement practices in individual Member States. Furthermore, the rapid variability of disinformation tactics makes it difficult to comprehensively assess the long-term effectiveness of existing regulatory mechanisms.

5.2. Recommendations

Further research should be complemented by a comparative analysis of domestic responses of EU Member States. This will contribute to a more complete assessment of the effectiveness of policies at the supranational level. Policymakers should be encouraged to more actively support cross-border cooperation and invest in adaptive technological solutions. This approach will allow for more effective counteraction to modern threats of disinformation, while ensuring respect for fundamental rights.

Furthermore, it is appropriate to introduce specific policy instruments, in particular national media literacy programmes, which can be co-financed and coordinated by the European Commission. Such programmes can be piloted or adapted in EU candidate countries, in particular in Ukraine and Serbia. This will create conditions for testing scalable solutions in different institutional settings and will promote harmonization with EU requirements in the field of information security in the context of the European integration process.

6. Conclusions

This research found that disinformation is now considered a system-wide threat to both information security as well as democratic stability and strategic resilience for the European Union. This research also demonstrated that the various policy initiatives (such as the Digital Services Act, the NIS2 Directive and related strategic tools) have created a comprehensive regulatory framework designed to counter disinformation by establishing legal obligations to institutional coordination and technology-based safeguards to help bolster the Union's ability to respond to hybrid threats in a contested information space.

The empirical data also indicate that, the impact of EU counter-disinformation policies is inconsistent for member states of the EU. Legal integration, while significant, differs considerably from country to country. The varying level of implementation of EU norms into national law; and the degree of national enforcement vary significantly among EU member states. Countries with a highly developed institutional system (i.e., an agency or department), which has specialized oversight responsibilities and/or a high level of digital governance have a more robust ability to resist disinformation threats than those countries without these capabilities. Similarly, some countries lack sufficient technology to support efforts to combat disinformation. In addition, some countries do not have clear institutional mandates related to enforcing EU norms, which also diminishes their ability to effectively enforce EU counter-disinformation policies. Overall, the disparity in the ability of countries to implement and enforce EU norms weakens the resilience of the EU's information environment, as well as its ability to provide a coordinated strategic response to disinformation threats.

A continuing normative conflict exists at the heart of this research regarding the balance to be struck between protecting and regulating free speech versus protecting society from the harmful effects of false or misleading information. The research finds that such conflicts may be resolved through the use of the principle of proportionality within the EU's legal structure if those regulations being implemented are clear, open, and consistently enforced. Therefore, the implementation of regulations designed to protect citizens from disinformation must be viewed not as a limitation on democratic rights but rather as a means to ensure that they are exercised effectively in the virtual space.

Strategically, the convergence of cyber attacks against the critical infrastructure of European Union member states with campaigns of disinformation has established a

new dimension of dependency between the two areas of governance and security. The NIS2 Directive is a significant development in terms of integrating the two areas of governance. However, the lack of a common level of operational capacity among all EU member states will limit the directive's practical effectiveness. The development of technology-based tools (such as AI based detection systems) offers significant opportunities to develop better early warning systems and responses to disinformation campaigns. However, these technologies must be used in conjunction with strong legal protections to prevent the violation of individuals' rights.

This study's relevance to practice is demonstrated by the contributions it can make toward developing policies that are based upon evidence. The Disinformation Vulnerability Index will serve as a comparative analytical tool for identifying structural vulnerabilities and for establishing priorities for building capacity (at both the country and regional levels). The results of the study indicate the necessity for targeted assistance at the EU-level, improved transnational cooperation (such as through the exchange of best practices), and better-coordinated media literacy programs across all EU member states in order to decrease the differences in disinformation vulnerability among them. Enhancing national level institutional capacity is important for enhancing the EU's internal security; however, it is equally important for reinforcing the EU's overall geopolitical position and democratic legitimacy.

In future studies, researchers should investigate the long-term effects of regulations aimed at reducing disinformation, how new technologies are being used for information operations, and how EU counter-disinformation policy impacts the behavior of external actors' strategic actions. The most effective way to ensure sustainable information security within the EU is through an adaptable and holistic approach (including harmonizing laws, enhancing operational capacity, and increasing societal resilience) to the issues surrounding disinformation.

REFERENCES

ANTIPOVA, Olha. Strategic communications as a component of state information security. Law *Journal of the National Academy of Internal Affairs*, 2023, vol. 13, no. 1, pp. 44-52. https://doi.org/10.56215/naia-chasopis/1.2023.44

BARHOUMI, Ouala. NIS 2: Where are European countries in transposing the directive? *Wavestone*. 2024. Available from https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive/

ÇAĞLAYAN, Mehmet U. Review of some recent European cybersecurity research and innovation projects. *Infocommunications Journal*, 2022, vol. 14, no. 4, pp. 70–78. https://doi.org/10.36244/icj.2022.4.10

COUNCIL OF EUROPE. Principles for media and communication governance: Recommendation

CM/Rec (2022)11 and explanatory report. 2022. Available from: https://edoc.coe.int/en/media/11117-principles-for-media-and-communication-governance-recommendation-cmrec202211-and-explanatory-report.html

DE HERT, Paul and PENEDO, Andrés Chomczyk. A democratic alternative to the Digital Services Act's handshake between States and online platforms to tackle disinformation. *EU Law Analysis.* 2022. Available from: https://eulawanalysis.blogspot.com/2022/01/a-democratic-alternative-to-digital.html?utm

EUR-LEX - 52024IE0014 - EN - EUR-LEX. 2025. Available from: https://eur-lex.europa.eu/eli/C/2024/4052/oj?utm

EUROPEAN CENTRE FOR PRESS AND MEDIA FREEDOM. 1,117 media freedom alerts in the past year: MFRR Monitoring Report 2023. 2024. Available from: https://www.ecpmf.eu/1117-media-freedom-alerts-in-the-past-year-mfrr-monitoring-report-2023/

EUROPEAN COMMISSION. Code of practice on disinformation. Digital strategy. 2025. Available from https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

EUROPEAN COMMISSION. Europe's digital decade: Digital targets for 2030 (COM(2020) 784 final). 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0784

EUROPEAN COMMISSION. European media information and communication community. 2025. Available from https://media-board.europa.eu/index_en

EUROPEAN COMMISSION. Standard Eurobarometer 102 – Autumn 2024 [Data set]. Directorate-General for Communication, European Commission. 2024. Available from https://europa.eu/eurobarometer/surveys/detail/3215

EUROPEAN COURT OF AUDITORS. Special report No 9/2021: Combating disinformation: Role of the EU response to safeguard the internal market and citizens' rights (SR 21 09). Publications Office of the European Union. 2021. Available from: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf

EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. Opinion of the European Economic and Social Committee – Safeguarding democracy against disinformation (own-initiative opinion). Official Journal of the European Union, C/2024/4052. 2024. Available from: https://eur-lex.europa.eu/eli/C/2024/4052/oj

EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION. Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, pp. 1–102. 2022. Available from: https://eur-lex.europa.eu/eli/reg/2022/2065

EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. *Official Journal of the European Union,* L 333, pp. 80–152. 2022. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

EUROPEAN REGULATORS GROUP FOR AUDIOVISUAL MEDIA SERVICES, ACTION GROUP 3. Report on Media Literacy [ERGA-AG3-2021-Report-on-Media-Literacy]. 2021. Available from https://erga-online.eu/wp-content/uploads/2021/12/ERGA-AG3-2021-Report-on-Media-Literacy.pdf

EUROPEAN UNION AGENCY FOR CYBERSECURITY. Threat Landscape. *ENISA*. 2024. Available from: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

EUROPEAN UNIVERSITY INSTITUTE. Media ownership monitor. 2025. Available from: https://media-ownership.eu

FREEDOM HOUSE. Freedom on the Net 2024: Digital booklet. 2024. Available from: https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf

HUESO, Lorenzo C. Who, how and what to regulate (or not regulate) in the face of disinformation. *Teoría Y Realidad Constitucional*, 2022, vol. 49, pp. 199–238. https://doi.org/10.5944/trc.49.2022.33849

KALNIŅA-LUKAŠEVICA, Zanda. Foreign interference: A threat to democratic security in Europe (Doc. 16131). *Parliamentary Assembly of the Council of Europe*. 2025. Available from https://pace.coe.int/en/files/34179/html?utm

KPMG. KPMG network and information security directive (NIS 2). 2023. Available from: https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2023/10/kpmg-network-and-information-security-directive-nis2.pdf

LEROY, Iryna and ZOLOTARYOVA, Iryna. Critical infrastructure defense: Perspectives from the EU and USA cyber experts. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 2023, vol. 5,

pp. 165–170. https://doi.org/10.33271/nvngu/2023-5/165
MACHOWICZ, K. (2022). The impact of the quality of information on the use of freedom of expression. Studia Iuridica Lublinensia, 31(3), 189–201. https://doi.org/10.17951/sil.2022.31.3.189-201
MARTINS, Bruno. O. and JUMBERT, Maria G. EU Border technologies and the co-production of security 'problems' and 'solutions.' *Journal of Ethnic and Migration Studies*, 2020, vol. 48, no. 6, pp. 1430–1447. https://doi.org/10.1080/1369183x.2020.1851470
MELNYK, Dmytro S., et al. Practice of the Member States of the European Union in the field of anti-corruption regulation. *Journal of Financial Crime*, 2022, vol. 29, no. 3, pp. 853-863. https://doi.org/10.1108/JFC-03-2021-0050
MINITAB. Data analysis, statistical & process improvement tools. 2025. Available from https://www.minitab.com/en-us/
MUNKØE, Malthe and MÖLDER, Holger. Cybersecurity in the era of hypercompetitiveness: Can the EU meet the new challenges? *Revista CIDOB D Afers Internacionals*, 2022, vol. 131, pp. 69–94. https://doi.org/10.24241/rcai.2022.131.2.69
NÉGYESI, Imre. Possibilities of using artificial intelligence in EU and UN peacekeeping activities. *Revista Academiei Forţelor Terestre*, 2024, vol. 29, no. 1, pp. 11–19. https://doi.org/10.2478/raft-2024-0002
NOERR. NIS 2 update for Europe. 2025. Available from https://www.noerr.com/en/insights/nis-2-update-for-europe-march-2025
SEMENETS-ORLOVA, Inna, et al. Human-centered approach in new development tendencies of value-oriented public administration: Potential of education. *Economic Affairs* (New Delhi), 2022, vol. 67, no. 5, pp. 899-906. https://doi.org/10.46852/0424-2513.5.2022.25
SHEREMET, Oleg S., et al. Political and legal aspects of the information warfare. *Revista Amazonia Investiga*, 2021, vol. 10, no. 45, pp. 31–41. https://doi.org/10.34069/ai/2021.45.09.3
STASIUK, Nadiia. Particular aspects of legal prevention and counteraction to domestic violence in Ukraine. *European Political and Law Discourse*, 2020, vol. 7, no. 4, pp. 185–189. https://doi.org/10.46340/eppd.2020.7.4.28
THE NIS 2 DIRECTIVE. 2025. Available from https://www.nis-2-directive.com
VANDEZANDE, Niels. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 2023, vol. 52, 105890. https://doi.org/10.1016/j.clsr.2023.105890
ZVOZDETSKA, Oksana. Disinformation as a threat to the EU National security: Issues and approaches. *Modern Historical and Political Issues*, 2021, vol. 43, pp. 30–39. https://doi.org/10.31861/mhpi2021.43.30-39

Data de submissão do artigo: 15/08/2025

Data de aprovação do artigo: 09/12/2025

Edição e propriedade:
Universidade Portucalense Cooperativa de Ensino Superior, CRL
Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto
Email: upt@upt.pt