

Copyright: The author/s

This work is licensed under a CC-BY 4.0 license

(*) Corresponding author

Original research article

DOI: <https://doi.org/10.20544/uklop.2026.629>

Received: 26.11.2025 • Accepted after revision: 18.01.2026 • Published: 09.05.2026



#UKLO
Annual **International**
Scientific Conference

DISINFORMATION AND DIGITAL TRANSFORMATION: IMPLICATIONS FOR THE EUROPEAN INTEGRATION OF NORTH MACEDONIA

Ana Sekulovska Jovkovska

Faculty of Informatics, University of Skopje, North Macedonia

ORCID: <https://orcid.org/0009-0007-4862-4380>

a.jovkovska@utms.edu.mk

Ilche Dimovski*

University "St. Kliment Ohridski" – Bitola, North Macedonia

ilce.dimovski@uklo.edu.mk

ABSTRACT

Introduction: This paper explores the dynamic relationship between digital transformation and disinformation, focusing on their implications for the European integration of North Macedonia. The study addresses the increased presence of disinformation, low levels of media literacy, and challenges in aligning national digital policies with European standards.

Methods: A combined theoretical and empirical approach is applied. The analysis highlights the European regulatory framework, with emphasis on the Digital Services Act and Digital Markets Act. Empirical data are collected through media content analysis, surveys, and semi-structured interviews with citizens and experts.

Results: Findings are expected to show that disinformation, especially as part of hybrid warfare, has significant influence on citizens' perceptions. Effective digital transformation and alignment with European regulations reduce institutional and societal vulnerability. Media literacy emerges as a central factor of resilience.

Discussion: The study confirms that disinformation erodes confidence in EU integration, whereas digital transformation and regulatory harmonization enhance resilience. Media literacy proves essential, though limitations remain. Future research should extend to regional comparisons and the role of algorithms in amplifying disinformation.

Keywords: Digital transformation, disinformation, European integration, Digital Services Act, media literacy, hybrid threats

1. INTRODUCTION

The rapid expansion of digital technologies has fundamentally reshaped the way individuals access and interact with information, positioning digital transformation as a key element of contemporary governance. While digital innovations enhance transparency, efficiency, and citizen engagement, they simultaneously expose societies to an increased volume of harmful content, including misinformation and disinformation amplified through fast-growing online ecosystems. These dynamics create a dual landscape—one defined by technological advancement, and another marked by new risks to public trust and democratic resilience.

In the context of the enlargement of the European Union (EU), digital governance has become strategically important, influencing both democratic consolidation and security. Candidate countries are expected to align their regulatory frameworks and digital capacities with EU standards. North Macedonia faces a particularly complex environment where efforts for digital modernization intertwine with political polarization, socio-economic challenges, and operations of external influence. Despite progress in digital public services and institutional interoperability, vulnerabilities in information integrity and media literacy remain significant.

Disinformation is deeply rooted in the national information sphere, driven by domestic political actors, foreign influence, and opportunistic digital manipulation. Narratives targeting the EU and its policies are among the most widespread, aiming to undermine public trust in institutions and decrease support for North Macedonia's Euro-Atlantic integration. Limited media literacy further increases citizens' susceptibility to manipulation, creating a feedback loop in which disinformation erodes trust, and low trust amplifies the effect of disinformation.

These conditions highlight the need to strengthen societal resilience by combining institutional digital capacity with enhanced public awareness and critical thinking. This study examines the interconnection between digital transformation, disinformation, and public perceptions of EU integration. It recognizes both the opportunities offered by digital governance and the threats posed by information manipulation in shaping political attitudes.

The research aims to explore how disinformation influences citizens' attitudes toward European integration and to assess the role of digital transformation and media literacy in mitigating such influences. The central research question investigates how the processes of digital transformation and the dynamics of disinformation affect public trust in North Macedonia's EU accession. The additional questions relate to:

1. the key actors and narratives driving EU-related disinformation;
2. the extent to which digital transformation enhances institutional and societal resilience; and
3. how media literacy shapes citizens' vulnerability to false content.

By integrating theoretical insights with empirical evidence, the study contributes to current academic and policy discussions on digital governance, information security, and Europeanization. Its findings aim to support national efforts to align digital policies with EU standards and to strengthen societal commitment to democratic integration.

2. Literature Review / Theoretical Framework

2.1. Digital Transformation: Definitions, Trends, and Public Sector Reforms

Digital transformation represents the integration of advanced digital technologies into societal and institutional processes, leading to changes in organizational structures, culture, and the way public services are delivered (Mergel et al., 2019; Goldkuhl, 2011). It is not limited solely to technological adoption but implies improving efficiency, transparency, and accountability, as well as greater citizen involvement in governance processes (Bannister & Connolly, 2020).

In the public sector, digital transformation is most commonly realized through the development of e-government, which offers faster and more accessible services, reduced bureaucracy, and the limitation of corrupt practices (United Nations, 2022; World Bank, 2021). E-services such as digital identity, electronic submission of documents, or online payments enable the administration to be more productive and more user-oriented (European Commission, 2020).

Contemporary trends shift the transformation from basic digitalization toward intelligent and proactive governance. Technologies such as artificial intelligence, data analytics, automation, and the Internet of Things create a foundation for personalized and predictive public services (Criado & Gil-García, 2019; Lindgren & van Veenstra, 2018). Open data platforms strengthen transparency and encourage collaboration between the public sector and civil society (European Commission, 2022).

Digitalization simultaneously opens significant risks related to cybersecurity, data misuse, and vulnerability of critical infrastructure. Therefore, national digital strategies increasingly focus on resilience and the responsible use of innovations (World Bank, 2021). In the European context, the regulatory frameworks DSA and DMA set standards for transparency, security, and platform accountability, which are also important for candidate countries (European Commission, 2023).

Although digital transformation has strong developmental potential, it can deepen the digital divide, which manifests as differences in access, skills, and the use of digital tools (Van Dijk, 2019). This divide is pronounced between urban and rural areas, generations, and economic groups, especially in transitional countries. Limited access to digital services reduces trust in institutions and increases citizens' susceptibility to manipulation and disinformation (Bannister & Connolly, 2020).

For many countries in transition, such as North Macedonia, the digital divide persists due to socio-economic inequalities, limited investment in digital education, and insufficient workforce capacity. Vulnerable groups, including older people, low-income households, and communities in remote areas, may remain excluded from digital progress. This exclusion is particularly problematic in the public sector, where digital public services risk deepening inequality if alternative access channels are not maintained.

Therefore, successful digital reforms must be inclusive and combine technological advancement with education, infrastructural investments, and protection from cyber risks. Only in this way can digital transformation contribute to democratic stability, equal access, and increased public trust.

2.2 Disinformation and Hybrid Threats

Disinformation represents deliberately constructed and disseminated inaccurate information with the aim to deceive, mislead, or psychologically influence the audience and to achieve political, ideological, or economic influence over the public (Wardle &

Derakhshan, 2017). Unlike misinformation, which results from unintentional mistakes, disinformation is characterized by a clear strategic intention and often constitutes an integral part of broader hybrid warfare operations.

In contemporary digital ecosystems, disinformation exploits the speed, scale, and algorithmic logic of social networks, enabling the rapid circulation of manipulative messages, especially in environments with low trust in institutions and limited media literacy (Bennett & Livingston, 2018). It thrives in contexts characterized by high social polarization, limited institutional trust, and low levels of media literacy—conditions particularly present in transitional democracies (Tucker et al., 2018).

The concept of hybrid warfare describes a strategic approach that combines conventional and unconventional means to achieve political and geopolitical goals without a formal declaration of conflict. At its core, hybrid warfare operates in the “grey zone” between peace and open armed confrontation, using political, informational, economic, cyber, and cultural instruments to destabilize the opponent (Hoffman, 2007; Lind, 1989; Nemeth, 2002).

The Russian doctrine describes this approach as “information confrontation,” where psychological operations, digital attacks, and media interventions are combined with traditional instruments of power (Gerasimov, 2013; Giles, 2016). Similarly, Chinese concepts of the “three wars”, psychological, media, and legal, indicate strategies of influence without direct confrontation (Chekinov & Bogdanov, 2013).

From a Western perspective, hybrid warfare is viewed as a synergistic combination of military and non-military means, including propaganda, cyber operations, political influence, and economic pressure (Hoffman, 2007). Examples such as the actions of Hezbollah in the Middle East illustrate the capabilities of non-state actors to employ hybrid tactics (Krieg & Rickli, 2019).

In the context of North Macedonia and the wider Western Balkans, hybrid warfare most often manifests through disinformation campaigns, cultural-religious influence, political mediation, and economic pressures with the aim of weakening pro-European orientations and destabilizing social cohesion (Galeotti, 2016; Raichev, 2023). Therefore, this study uses the term “hybrid warfare” instead of “hybrid threats,” because the concept of “threat” describes a potential or latent risk, while “warfare” indicates an active, intentional, and coordinated operation of influence. The analyzed examples in the Macedonian media and digital space fit more clearly within a model of hybrid warfare than within the more moderate concept of hybrid threats.

The structural characteristics of digital platforms additionally facilitate the spread of hybrid operations. Algorithms prioritize content that generates strong engagement, regardless of accuracy, creating echo chambers where false information can circulate unchallenged (Pariser, 2011; Bakshy et al., 2015). The rise of deepfake videos, altered historical narratives, and coordinated troll networks further complicates fact-checking (Chesney & Citron, 2019). New technologies advance rapidly, making disinformation tactics increasingly difficult to detect and regulate (Bradshaw & Howard, 2019).

Research shows that disinformation affects public perception through several mechanisms (Lewandowsky et al., 2017):

- agenda-setting and narrative shaping;
- emotional manipulation through fear, anger, and identity-based messages;
- delegitimization of institutions, especially in electoral contexts (Norris & Inglehart, 2019);
- creating uncertainty and confusion that weakens societal resilience (Paul & Matthews, 2016).

North Macedonia’s vulnerability to such operations is intensified by the fragmented media landscape and the high dependence on digital platforms as primary sources of information. Studies show that a significant portion of online content related to European

integration contains polarizing or misleading narratives (European Commission, 2022). The infodemic spread of contradictory information reduces the public's ability to distinguish credible sources from manipulative ones (WHO, 2020), and vulnerable groups, especially young people and individuals with lower levels of education, are disproportionately exposed (Guess et al., 2019).

Traditional media regulation faces difficulties in monitoring decentralized and encrypted digital communication spaces (Kello, 2017). Although fact-checking initiatives have expanded, they often have limited resources and insufficient reach compared to the viral spread of false content (Graves & Anderson, 2020). Responding to disinformation requires careful balancing to avoid risks of excessive censorship, political misuse, or undermining democratic standards and media pluralism (Roberts, 2019).

Experts clearly indicate that disinformation and hybrid operations represent central security challenges in the digital era (Hoffman, 2007; Giles, 2016).

Their capacity to undermine democratic legitimacy is amplified in contexts where digital transformation progresses faster than protective institutional, legal, and educational mechanisms.

2.3 Resilience and Media Literacy as Mitigating Factors

Resilience, in the context of information ecosystems and societal security, refers to the capacity of individuals, institutions, and communities to resist, adapt to, and recover from manipulations or disruptions caused by disinformation and hybrid threats (Pamment, 2020; NATO StratCom COE, 2020). With the accelerated digital transformation and the emergence of new risks, resilience becomes a fundamental requirement for protecting democratic processes, maintaining trust in governance, and ensuring informed civic participation (Van Dijck & Poell, 2018). A resilient society does not avoid exposure to harmful information but possesses the abilities and structural mechanisms for its timely recognition, challenge, and limitation (Ulmer, Sellnow & Seeger, 2022).

Resilience in information environments is multidimensional. Institutional resilience refers to the ability of public institutions, regulators, and security agencies to detect and respond in a timely manner to manipulative information (OECD, 2024). This requires modernized legal frameworks, cross-sector coordination, and proactive digital governance policies, such as the EU standards outlined in the DSA and DMA (European Commission, 2022). Increased transparency, platform accountability, and strengthened cybersecurity reduce institutional vulnerability and contribute to trust in the digital public sphere (Roberts, 2019).

Technological resilience implies the development of systems and tools for identifying and limiting disinformation (Helberger, 2020). This includes investments in artificial intelligence for content verification, secure digital identity solutions, and interoperable systems that enable secure communication in public networks (Floridi, 2018). Innovative responses from technological companies, civil society, and academia play a significant role in protecting against coordinated manipulative campaigns (Bradshaw & Howard, 2019). Societal resilience is the most critical layer, as citizens are the direct target of disinformation.

A key element is media literacy, defined as the ability to access, analyze, evaluate, and create information across different media formats (Pamment, 2020). Media literacy enables citizens to recognize manipulations, verify sources, and participate responsibly in public discourse (Koltay, 2011). In societies with information overload, media literacy becomes both an educational and a security necessity (Stoilova et al., 2020).

In North Macedonia, media literacy is gradually being integrated into national strategies, but it remains unevenly developed (MIM, 2022). Younger citizens, who primarily

receive information through social networks, often lack structured knowledge of critical thinking and digital responsibility (Tandoc et al., 2018). Older generations, meanwhile, face difficulties in evaluating digital content, creating intergenerational differences in vulnerability to disinformation (Olphert, and Damodaran, 2013) and influencing political perceptions and social cohesion (Groshek & Koc-Michalska, 2017).

Research shows a strong correlation between media literacy and resilience: citizens with higher critical digital skills have lower susceptibility to false narratives, higher trust in institutional sources, and greater support for democratic reforms and European integration (Jones-Jang et al., 2021; Vraga & Tully, 2021). Therefore, improving media literacy not only limits the spread of disinformation but also strengthens public stability and the strategic orientation of the state. Educational programs, public campaigns, and fact-checking platforms represent key elements in creating informed and resilient communities (Graves, 2018).

Despite progress, challenges remain. Efforts to build critical digital skills often lack sustainable funding and systematic integration into curricula (Frau-Meigs et al., 2017), and the shortage of trained educators limits effectiveness (Bulger, 2018). Furthermore, countermeasures against disinformation must balance protection with freedom of expression to avoid censorship or political misuse (Roberts, 2019).

For sustainable resilience-building, states must adopt a holistic approach that integrates institutional capacities, technological solutions, and civic competencies into a single system (OECD, 2024). In the case of North Macedonia, alignment with European standards for digital governance represents a critical path toward strengthening systemic resilience and advancing the process of European integration (European Commission, 2022).

3. The Context of European Policy: The Digital Services Act and the Digital Markets Act

The European Union has established a comprehensive framework for digital governance aimed at improving accountability, competition, and consumer protection across the entire online ecosystem (European Commission, 2020; 2022). Two central regulations, the Digital Services Act (DSA) and the Digital Markets Act (DMA), represent a significant step toward strengthening digital rights and addressing the risks posed by powerful online platforms (European Parliament & Council of the EU, 2022a; 2022b). Together, these acts define the obligations of digital intermediaries, ensuring that online spaces remain safe, secure, and competitive, while at the same time supporting the EU's democratic values.

3.1 Digital Services Act: Transparency, Safety, and Platform Accountability

The Digital Services Act introduces a new set of standards that regulate the removal of illegal content, transparency in content moderation, and the empowerment of users (European Commission, 2023a). Its implementation requires platforms to distinguish between illegal and harmful content while at the same time protecting freedom of expression (Keller & Leerssen, 2020).

The DSA places particular responsibility on very large online platforms (VLOPs), which serve as primary channels for the distribution of news and information. These platforms must conduct risk assessments, monitor algorithmic impacts, and cooperate with independent auditors to prevent the spread of harmful digital behavior (European Commission, 2023b).

Combating disinformation represents a core objective of the DSA. The regulation requires mechanisms that:

- ensure the traceability of digital advertisements,

- reduce the algorithmic amplification of harmful narratives, and
- facilitate improved cooperation with trusted fact-checking entities (European Commission, 2022b; NATO StratCom COE, 2021).

For EU candidate countries, such as North Macedonia, alignment with these standards is not only a formal requirement but also a critical tool for improving information security and democratic resilience (Tóth & Judit, 2022).

3.2 Digital Markets Act: Ensuring Fair Competition and Reducing Market Dominance

The Digital Markets Act (DMA) complements the Digital Services Act (DSA) by targeting the structural imbalances of the digital market and regulating the behavior of dominant technology companies. These companies, defined as “gatekeepers,” control key digital infrastructures such as app stores, search engines, and social networks, which enables them to exert significant influence over the online ecosystem (European Commission, 2020). Previous analyses show that such market power often leads to self-preferencing, data misuse, and restrictions on competition, problems that the DMA aims to address (Crémer, de Montjoye & Schweitzer, 2019).

The DMA aims to restrict market practices that reduce consumer choice and hinder competition, such as algorithms for self-preferencing, bundling of exclusive services, or the accumulation and monopolization of data (European Commission, 2020). By establishing obligations for interoperability, transparency, and fair access to data, the regulation creates equitable conditions for business operations in the digital environment (Martensand Zhao, 2021).

By preventing monopolistic behavior and encouraging fair competition, the DMA supports a diverse and innovative digital market that benefits both citizens and small and medium-sized enterprises. This is particularly relevant for the Western Balkans region, where digital entrepreneurship and local innovation depend on fair access to European digital markets and on stable competitive conditions (OECD, 2024).

3.3 North Macedonia’s Alignment with EU Digital Governance

North Macedonia has shown commitment to harmonizing its national legislation with the European digital agenda, however, progress is uneven. Policy initiatives, such as the National Cybersecurity Strategy, the creation of e-government portals, and the development of digital identity, signal significant steps towards modernization. However, several institutional and infrastructural gaps remain:

EU Requirement	Current Status in North Macedonia	Key Challenges
Platform accountability (DSA)	Partial adoption through media regulation updates	Limited platform oversight capacity
Transparency and content governance	Growing cooperation with fact-checkers and regulators	Lack of reliable monitoring systems
Fair digital market competition (DMA)	Legislative alignment underway	Slow adaptation for local SMEs
Cybersecurity standards	National strategies updated	Funding and workforce shortages

Figure. 1

Foreign influence and domestic political fragmentation continue to complicate the effective implementation of digital reforms. Moreover, the state’s ability to counter disinformation campaigns remains constrained by insufficient coordination among public

institutions, regulators, and civil society organizations. Although legislative alignment is strengthening, practical enforcement remains the primary barrier.

3.4 Toward a European-Integrated Digital Ecosystem

Alignment with the DSA and DMA holds transformative potential for North Macedonia, particularly through:

- improved digital economy competitiveness,
- enhanced transparency in the information environment,
- reduced vulnerability to hybrid threats, and
- strengthened public trust in democratic institutions.

Effective implementation will require coordinated efforts in capacity building, cross-border cooperation, and long-term policy investment. Strengthening digital literacy and cybersecurity must accompany regulatory reform to ensure that legal compliance translates into real-world societal protection.

In conclusion, the European regulatory framework provides a critical roadmap for digital transformation in North Macedonia. By adopting and enforcing DSA and DMA principles, the country can enhance democratic resilience while advancing toward EU membership. The alignment process thus represents both a compliance obligation and a strategic opportunity for safeguarding digital sovereignty and promoting European values.

4. Methodology

This study applies a mixed-method research design to examine the relationship between digital transformation, disinformation, and public perceptions of EU integration in North Macedonia. The combination of quantitative and qualitative techniques enables a multidimensional understanding of how digital information environments influence societal attitudes and democratic resilience. Data were collected through analytical documents, media content, anonymous questionnaires, and semi-structured expert interviews. Out of 850 distributed surveys across different regions of North Macedonia, 302 responses were obtained, with participants representing diverse demographic profiles. A total of 130 individuals from academic institutions, journalism, public administration, and political actors were invited, but only 20 agreed to be interviewed on the topic. Additionally, open-source databases and the digital resources were consulted, without the use of sensitive or classified material.

The methodological framework integrates several complementary research approaches. Case study analysis was used to observe selected political events and foreign policy processes, offering insight into mechanisms of influence on North Macedonia. Qualitative analysis of expert interviews and survey responses made it possible to identify perceptions regarding the role of external actors and the mediation carried out by domestic political elites. Comparative analysis served to contrast national strategies with EU-level strategies and to assess divergences affecting institutional stability. Content analysis provided a systematic examination of official documents, strategic reports, international publications, and media sources, facilitating objective tracking of narratives and channels of influence. Descriptive and analytic-synthetic reasoning supported the interpretation and integration of empirical and theoretical insights. Long-term observation and monitoring of political developments, media discourse, and diplomatic activity supplied updated contextual information and a nuanced understanding of how legislative reforms, public statements, and international reactions shape the broader environment.

Through this combination of methods, the study offers a layered and coherent analytical perspective on how external influences intertwine with domestic political dynamics and how political actors in North Macedonia interpret, adapt, or instrumentalize these influences within national decision-making processes.

4.1. Empirical Findings: Case of North Macedonia

The empirical analysis provides valuable insight into the digital information environment in North Macedonia, particularly in light of the European Union’s Digital Services Act (DSA), which emphasizes transparency, accountability, and systemic risk management within the online information ecosystem. The findings reveal structural patterns in how citizens consume international news, the extent of cross-border media influence, and the public’s ability to identify disinformation. These are critical elements for assessing national preparedness for implementing DSA standards.

International news was selected as an analytical category because foreign political and media narratives represent a main channel through which hybrid influences are carried out in North Macedonia. Research by the EU, NATO StratCom COE, and domestic fact-checking organizations shows that disinformation campaigns most frequently relate to international politics, geopolitical issues, and cross-border events, rather than to local news. Therefore, exposure to international news represents a more useful indicator for assessing the population’s vulnerability to hybrid operations.

4.1.1 Frequency of International News Consumption and Exposure to Digital Media

The survey results show that the majority of respondents (58%) follow news or international news daily, either several times a day or at least once a day, which indicates a high level of exposure to global information flows.

However, the depth and quality of engagement vary significantly across demographic groups. Although gender differences are minimal, age and education emerge as strong differentiating factors: older respondents (56–65) show lower engagement, with half of them reporting that they rarely consume international news, while younger and more educated respondents demonstrate higher levels of information consumption. This generational and educational divide reflects inequalities in digital literacy and media habits, which can directly influence resilience to online disinformation.

Geographical differences are also relevant. Respondents from urban areas tend to consume more news (37.5% several times a day), while those in rural areas report more limited exposure (38.5% only a few times per week). Such data suggest that digital access and infrastructure, as defined by DSA principles of equal access to online information, remain uneven across the country.

Ethnic differences further highlight patterns of selective exposure: Macedonian respondents (57.6%) are more frequent consumers of international news compared to respondents from other ethnic communities (55.5%), among whom nearly half acknowledge that they follow global news only occasionally. These results underscore a fragmented information landscape, where access to and trust in international media sources may vary along socio-cultural lines.

When it comes to gathering information about international relations and North Macedonia’s global position, respondents rely on a variety of sources. Most use media outlets (32.67%) and social networks (23.76%), indicating a significant influence of digital platforms. Scientific and professional literature also plays an important role, but other unspecified sources (12.87%) and personal experience (8.91%) are mentioned as well,

pointing to a mix of informal and official sources in shaping perceptions. They rely least on official government statements (4.95%), which suggests a degree of skepticism or a preference for independent sources of information. Younger demographic groups rely more heavily on social networks for information compared to older respondents.

Regarding this question, there are no major differences in the opinions of the interviewed experts.

4.1.2 Influence of Cross-Border Media on the Macedonian Media Space

A key dimension relevant to the DSA’s cross-border information regulation is the perceived influence of foreign digital content.

More than 70% of respondents believe that online content originating from Serbian media significantly influences both domestic news portals and public opinion in North Macedonia. This perception of influence remains consistent across gender, age, and place of residence, although it is slightly higher among women (75%) and urban respondents (71.6%). These findings reflect the regional interdependence of media ecosystems, where digital platforms transcend borders without adequate regulatory mechanisms. In the absence of strong domestic enforcement aligned with DSA obligations for very large online platforms (VLOPs) and media transparency, such external content can shape public narratives, spread bias, and potentially amplify disinformation (Tóth & Judit, 2022).

Education again emerges as a differentiating factor. Respondents with postgraduate qualifications (second cycle and above) show greater awareness of the influence of foreign media but are also more cautious in forming judgments (up to 44% expressing neutrality). This academic restraint suggests recognition of the complexity of hybrid information flows and an understanding that foreign content may influence not only information availability but also public trust in national media.

Most experts agree that disinformation is present but mainly originates from abroad and its influence is secondary, primarily affecting the country of origin. In this regard, they believe that domestic challenges such as corruption and political manipulation through fake news are more deeply rooted.

4.1.3 Public Awareness and Ability to Recognize Disinformation

Respondents were asked, “Does the public in North Macedonia know how to recognize disinformation and fake news?” to which 62.37% disagreed or strongly disagreed, revealing a significant gap in media literacy and critical information skills. Although divided, the experts also believe that the majority of the population, regardless of demographics, accepts unverified information as credible.

This aligns with the DSA’s risk assessment obligations, which require member states and platforms to address systemic risks such as disinformation, manipulation, and the erosion of civic trust.

The lack of ability to recognize credible sources was consistent across all genders and age groups, with more than 60% in each demographic category acknowledging difficulties in identifying false information. This indicates low resilience to manipulation and hybrid interference, especially in the digital sphere where algorithmic amplification and cross-border circulation of content are common (European Parliament & Council of the EU, 2022a).

Interestingly, respondents from rural areas showed greater confidence (53.85%) in their ability to recognize disinformation compared to respondents from urban areas (25%), which likely reflects overconfidence rather than actual skill. Educational differences confirm this pattern: individuals with higher levels of education (over 65%) were more likely to

acknowledge the challenge, while those with lower levels of education often underestimated the complexity of identifying disinformation.

Ethnic analysis reveals similar results—two-thirds of respondents from both Macedonian and non-Macedonian communities acknowledge that the public struggles to identify fake news. This widespread perception underscores the national vulnerability to coordinated disinformation campaigns, highlighting the urgent need for comprehensive digital literacy programs (Helberger, 2020).

It is important to note that both respondents and experts agree that politicians in North Macedonia produce fake news in order to achieve political advantage.

4.2. Implications in the Context of the Digital Services Act

The findings indicate that North Macedonia’s information environment mirrors many of the systemic risks that the DSA seeks to address, including algorithmic amplification of foreign content, lack of media transparency, and low user awareness of online manipulations.

In this context, the implementation of DSA-inspired standards could enhance national resilience through (European Parliament & Council of the EU, 2022a):

- **Transparency obligations for online platforms**, requiring them to disclose content sources, ownership, and moderation practices.
- **Mechanisms for countering disinformation**, such as verified media registries and fact-checking partnerships.

Table 1. Correlation Analysis of Key Variables Related to News Consumption and

<i>Variables</i>	<i>Frequency of News Consumption</i>	<i>Age</i>	<i>Gender</i>	<i>Education</i>	<i>Place of Residence</i>	<i>Ethnic Affiliation</i>	<i>Influence of Internet/Serbian Media</i>	<i>Ability to Recognize Disinformation</i>
<i>Frequency of News Consumption</i>	1.00	0.62	-0.05	0.48	0.37	0.29	0.12	0.21
<i>Age</i>	-0.62	1.00	0.03	-0.51	-0.08	-0.11	-0.15	-0.28
<i>Gender</i>	-0.05	0.03	1.00	0.06	0.02	-0.01	0.04	0.00
<i>Education</i>	0.48	0.51	0.06	1.00	0.22	0.18	0.33	0.42
<i>Place of Residence (Urban = 1)</i>	0.37	0.08	0.02	0.22	1.00	0.15	0.40	-0.26
<i>Ethnic Affiliation (Macedonian = 1)</i>	0.29	0.11	-0.01	0.18	0.15	1.00	0.09	0.10
<i>Influence of Internet / Serbian Media</i>	0.12	0.15	0.04	0.33	0.40	0.09	1.00	-0.54
<i>Ability to Recognize Disinformation</i>	0.21	0.28	0.00	0.42	-0.26	0.10	-0.54	1.00

Disinformation in North Macedonia

- **Promotion of media literacy** across all age and education groups to reduce susceptibility to false narratives.
- **Cross-border coordination** with EU and regional regulators to manage information influence from neighboring countries.

These steps would not only align North Macedonia with European regulatory frameworks but also strengthen its democratic information ecosystem, making it more resistant to manipulation and disinformation in the digital era.

The correlation matrix highlights several critical dynamics shaping North Macedonia's digital information landscape (Tóth, & Judit, 2022):

1. Education and digital literacy are the strongest protective factors against disinformation and online manipulation.
2. Age and exposure to cross-border media (especially Serbian platforms) are significant risk factors contributing to misinformation vulnerability.
3. Urban exposure correlates with both opportunity and risk—urban citizens consume more digital media but are also more exposed to manipulative online content.
4. The results reveal systemic challenges aligned with the EU Digital Services Act (DSA) priorities—particularly in the areas of transparency, user empowerment, and media accountability.

To enhance national resilience, DSA-aligned measures should focus on:

- Strengthening media literacy and critical digital education;
- Promoting cross-border content transparency and cooperation with regional regulators;
- Ensuring platform accountability and fact-checking obligations for major online services;
- Supporting inclusive access to reliable information across all demographic and geographic groups.

These findings collectively demonstrate that North Macedonia's information ecosystem reflects many of the systemic risks the DSA aims to mitigate, making its implementation a vital step toward a more transparent and trustworthy digital environment.

5. Empirical Findings, Correlation Analysis, and Policy Recommendations – Case of North Macedonia

This study examined the interconnected relationship between digital transformation, disinformation, and public perceptions of European integration in North Macedonia. The findings confirm that digital transformation provides major opportunities for more transparent and efficient governance; however, if not accompanied by adequate societal and institutional safeguards, it simultaneously increases vulnerability to disinformation and hybrid threats.

For EU candidate countries, this duality has a direct impact on political stability and strategic alignment, as information manipulation campaigns frequently seek to obstruct Euro-Atlantic integration processes.

Survey and media analysis results show that exposure to disinformation remains widespread, affecting more than half of the population weekly. Low trust in domestic media outlets and limited ability to distinguish between authentic and deceptive content further facilitate the spread of harmful narratives. These narratives often target EU-related reforms, portraying integration as a threat rather than an opportunity, which contributes to rising skepticism and reduced public confidence in the accession process. In this context, disinformation becomes both a security issue and an obstacle to democratic consolidation.

On the positive side, advancements in digital governance — including the expansion of e-government services and cybersecurity frameworks — demonstrate institutional willingness to modernize in line with EU expectations. Nevertheless, progress remains uneven, and enforcement capacities require substantial improvement. Alignment with the Digital Services Act (DSA) and Digital Markets Act (DMA) represents a crucial step toward

establishing resilient digital infrastructure and responsible platform governance in North Macedonia.

The study therefore concludes that three interdependent pillars are necessary for success in digital transformation and European integration:

- Strong and secure digital governance,
- High-quality and inclusive media literacy, and
- Effective regulation and accountability aligned with European standards.

Achieving balance among these pillars is essential for ensuring that technological progress reinforces rather than undermines democratic values.

5.1. Correlation Analysis and Key Findings

The correlation analysis underscores a multidimensional relationship between education, age, media exposure, and the ability to recognize disinformation in North Macedonia.

The findings indicate that digital inequalities, rooted in educational level, age, and geographic context, remain central to understanding public vulnerability to online manipulation. Specifically:

- Education and media literacy emerge as the most significant protective factors. Higher education correlates strongly with frequent news consumption and a greater ability to identify fake or misleading content.
- Older populations show lower levels of engagement with international news and limited awareness of digital risks, suggesting a generational gap in digital competencies.
- Urban populations are more exposed to online information flows, including foreign content, which increases both their access to diverse information and their exposure to potential disinformation.
- The perceived influence of Serbian media content on North Macedonia’s information space demonstrates the country’s exposure to cross-border information ecosystems, a key issue addressed under the DSA framework.
- The overall low confidence in recognizing disinformation reflects a systemic weakness in media literacy and a lack of institutional mechanisms for public education and verification of online information.

Taken together, these findings reveal that North Macedonia’s digital ecosystem faces structural challenges similar to those addressed by the EU Digital Services Act (DSA), particularly concerning transparency, algorithmic accountability, and systemic risk mitigation in online media environments.

5.2. Policy Recommendations

a. Strengthening Media and Digital Literacy

- Integrate media literacy and disinformation awareness modules into formal education (schools and universities) and lifelong learning programs for civil servants and citizens.
- Encourage collaboration between universities, civil society organizations, and public broadcasters to develop certified training in critical media consumption and digital ethics.
- Promote digital literacy campaigns in rural areas and among older citizens to bridge generational and regional divides.

b. Ensuring Transparency and Accountability of Online Platforms

- Adopt a national adaptation framework of the Digital Services Act, aligning domestic legislation with EU standards on platform transparency, data access, and algorithmic accountability.
- Require digital platforms and news portals to disclose ownership, funding sources, and editorial control structures.
- Establish a National Register of Verified Media Outlets to distinguish professional journalism from unverified or politically motivated online actors.

c. Managing Cross-Border Media Influence

- Strengthen regional cooperation mechanisms for monitoring and countering disinformation, especially from neighboring countries with overlapping language and media markets.
- Develop a cross-border transparency protocol for digital content sharing and ensure compliance with DSA provisions regarding very large online platforms (VLOPs) operating in the region.
- Encourage independent fact-checking networks to collaborate regionally and publish multilingual verification reports.

d. Building Institutional and Regulatory Capacity

- Create a National Digital Services Authority or expand the existing Media Agency's mandate to supervise platform compliance, risk assessment, and content moderation practices.
- Introduce periodic risk assessments of the information ecosystem, following DSA Article 34, to monitor algorithmic amplification, harmful content, and political manipulation.
- Support public-private partnerships promoting ethical standards in digital advertising, content recommendation, and data use.

e. Empowering Citizens and Protecting Public Trust

- Foster open data initiatives and improve access to verifiable government information to counter rumors and misinformation.
- Implement digital trust-building measures, such as verified digital identities and authentication of official online communication.
- Encourage civic participation through crowdsourced reporting of disinformation, enabling citizens to contribute to maintaining online integrity.

5.3. Strategic Outlook

The transition toward DSA-aligned governance in North Macedonia should not be viewed merely as a regulatory obligation but as a societal modernization process, one that strengthens public trust, democratic participation, and resilience against information manipulation.

Empirical evidence confirms that addressing education gaps, media accountability, and cross-border information risks is essential to ensuring a transparent, secure, and inclusive digital public sphere.

A national strategy combining policy harmonization with the DSA and citizen-centered digital empowerment can serve as a foundation for both European integration and democratic renewal in the digital era.

CONCLUSIONS

The conclusions show that digital transformation and disinformation dynamics are two parallel and mutually dependent axes that fundamentally shape North Macedonia's European integration. Although digital technologies create significant opportunities for improved governance, transparency, and civic participation, they simultaneously generate new vulnerabilities that amplify hybrid operations, political polarization, and institutional distrust. The empirical results of this research confirm that citizens are exposed to a considerable volume of disinformation, particularly through cross-border media content and social networks, with the lack of media literacy and low institutional trust being key factors that increase this vulnerability.

The data clearly indicate that digital transformation cannot be viewed solely as technological modernization, but as a systemic process that requires institutional coordination, cybersecurity mechanisms, and societal skills. In this context, harmonization with European regulations, particularly the Digital Services Act (DSA) and the Digital Markets Act (DMA), represents a critical prerequisite for strengthening security and democratic stability. These policies provide standards for transparency, platform accountability, protection from manipulative practices, and greater control over digital intermediaries, all of which are essential for states undergoing the accession process.

The research further shows that resilience is a multilayered concept that includes institutional, technological, and societal components. Among them, societal resilience (including media and digital literacy) stands out as the weakest point in the Macedonian context, yet at the same time as the greatest potential catalyst for stability and democratic participation. Increasing media literacy correlates with lower susceptibility to disinformation, higher trust in institutions, and greater support for European integration processes, confirming the necessary focus on educational policies and public campaigns.

In sum, the results indicate that, among other conditions of the Copenhagen criteria, the successful European integration of North Macedonia will depend on the state's ability to align digital transformation with EU regulatory standards while simultaneously strengthening society's capacity to address hybrid threats. A holistic approach that connects institutions, citizens, media, and technology companies is essential for building a resilient information environment and supporting the country's democratic and European perspectives. This study contributes analysis, evidence, and recommendations that can serve as a foundation for developing national strategies, enhanced digital regulation, and integrated resilience policies in the digital era.

REFERENCES

1. Bakshy, E., Messing, S., and Adamic, L. A. 2015. "Exposure to Ideologically Diverse News on Facebook." *Science* 348 (6239): 1130–1132.
2. Bannister, F., and Connolly, R. 2020. "The Future Ain't What It Used to Be: Forecasting the Impact of ICT on the Public Sphere." *Government Information Quarterly* 37 (1): 101410.
3. Bennett, W. L., and Livingston, S. 2018. "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication* 33 (2): 122–139.
4. Bradshaw, S., and Howard, P. N. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Oxford Internet Institute.
5. Bulger, M., & Davison, P. (2018). The Promises, Challenges and Futures of Media Literacy. *Journal of Media Literacy Education*, 10(1), 1-21.

6. Chekinov, S. G., and Bogdanov, S. A. 2013. “The Nature and Content of a New-Generation War.” *Military Thought* 22 (4): 12–23.
7. Chesney, R., and Citron, D. K. 2019. “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security.” *California Law Review* 107 (6): 1753–1820.
8. Crémer, J., de Montjoye, Y.-A., and Schweitzer, H. 2019. *Competition Policy for the Digital Era*. European Commission.
9. Criado, J. Ignacio, and J. Ramon Gil-García. 2019. “Creating Public Value through Smart Technologies and Strategies: From Digital Services to Artificial Intelligence and Beyond.” *International Journal of Public Sector Management* 32 (5): 438–450. <https://doi.org/10.1108/IJPSM-07-2019-0178>.
10. European Commission. 2020. *Shaping Europe’s Digital Future*. Brussels. ISBN 978-92-76-16362-6
11. European Commission. (2020). *Europe’s Digital Future: Digital Strategy*. Publications Office of the European Union. Available at: <https://digital-strategy.ec.europa.eu> (November 25, 2025)
12. European Commission. 2020. *eGovernment Benchmark 2020*. European Commission. Brussels. Available at: <https://digital-strategy.ec.europa.eu/en/node/674/printable/pdf> (November 25, 2025)
13. European Commission. 2022. *Digital Services Act Package*. Available at: <https://digital-strategy.ec.europa.eu> (November 25, 2025)
14. European Commission. 2022. *Open Data Maturity Report 2022*. DOI: 10.2830/70973
15. European Commission. 2022. *Western Balkans Media and Disinformation Resilience Report*. Available at: https://north-africa-middle-east-gulf.ec.europa.eu/document/download/9c142786-aeeb-4fb6-802a-04b126c0cfb1_en?filename=EU%20support%20to%20the%20media%20sector%20in%20the%20western%20balkans_factsheet.pdf (November 25, 2025)
16. European Commission. 2022. *European Media Freedom Act & European Democracy Action Plan*.
17. European Commission. 2022b. *Strengthening the Code of Practice on Disinformation*.
18. European Commission. 2023a. *Guidance on the Implementation of the Digital Services Act*.
19. European Commission. 2023b. *Designation and Supervision of Very Large Online Platforms under the DSA*.
20. Floridi, L. 2018. “Artificial intelligence, deepfakes and a future of ectypes.” *Philosophy & Technology* 31 (3): 317–321.
21. Frau-Meigs, D., Velez, I., and Michel, J. 2017. *Public Policies in Media and Information Literacy in Europe*. Routledge.
22. Galeotti, M. 2016. *Hybrid War or Gibridnaya Voina? Getting Russia’s Non-linear Military Challenge Right*. Mayak Intelligence.
23. Gerasimov, V. 2013. “The Value of Science Is in the Foresight.” *Military-Industrial Courier*.
24. Giles, K. 2016. *The Next Phase of Russian Information Warfare*. NATO StratCom COE.
25. Goldkuhl, G. 2011. “Design Research in Search for a Paradigm.” *European Design Science Symposium*, 84–95.
26. Graves, L. 2018. *Understanding the Promise and Limits of Automated Fact-Checking*. Reuters Institute.

27. Graves, L., and Anderson, C. W. 2020. Discipline and promote: Building infrastructure and managing algorithms in a “structured journalism” project by professional fact-checking group. *Sage Journals* Vol. 22, (2).
28. Groshek, J., and Koc-Michalska, K. 2017. “Helping populism win? Social media use, filter bubbles, and support for populist presidential candidates in the 2016 US election campaign” *Information, Communication & Society* 20 (9): 1389-1407.
29. Guess, A., Nagler, J., and Tucker, J. 2019. “Less than you think: Prevalence and predictors of fake news dissemination on Facebook.” *Science Advances* 5 (1): eaau4586.
30. Helberger, N. 2020. “The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power.” *Digital Journalism* 8 (6): 842-854.
31. Hoffman, F. G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute.
32. Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does media literacy help identification of fake news? Information literacy helps, but other literacies don't. *American Behavioral Scientist*, 65(2), 371–388. <https://doi.org/10.1177/0002764219869406>.
33. Keller, D., and Leerssen, P. 2020. “Facts and Where to Find Them: Empirical Foundations for Platform Regulation.” In *Social Media and Democracy*, edited by Persily & Tucker. Cambridge University Press.
34. Kello, L. 2017. *The Virtual Weapon and International Order*. Yale University Press.
35. Koltay, T. 2011. “The media and the literacies: media literacy, information literacy, digital literacy.” *Media, Culture & Society* 33 (2): 211–221
36. Krieg, A., and Rickli, J.-M. 2019. *Surrogate Warfare*. Georgetown University Press. <https://doi.org/10.2307/j.ctvf34hnd>
37. Lewandowsky, S., Ecker, U. K. H., and Cook, J. 2017. “Beyond Misinformation.” *Journal of Applied Research in Memory and Cognition* 6 (4): 353–369.
38. Lind, W. S., et al. 1989. “The Changing Face of War.” *Marine Corps Gazette* 73 (10): 22–26.
39. Lindgren, I., van Veenstra, A. F. 2018, “Digital government transformation: a case illustrating public-service development as part of public sector transformation”. *dgo '18 Proceedings of the 19th Annual International Conference on Digital Government Research*. <https://doi.org/10.1145/3209281.3209302>
40. Martens, B. and Zhao, B., 2021. *Data access and regime competition: A case study of car data sharing in China / Data access and competition in digital markets*. European Commission.
41. Mergel, I., Edelmann, N., and Haug, N. 2019. “Defining Digital Transformation.” *Government Information Quarterly* 36 (4): 101385.
42. MIM – Macedonian Institute for Media. 2022. *Media Literacy in University Study Programs in the Republic of North Macedonia*. USAID. IREX. MIM. ICS.YEF
43. NATO. 2021. *NATO 2030: United for a New Era*.
44. NATO StratCom COE. 2021. *Algorithms, Amplification and Accountability*.
45. Nemeth, W. J. 2002. *Future War and Chechnya: A Case for Hybrid Warfare*. Master's Thesis, Naval Postgraduate School.
46. Olphert, W. and Damodaran, L. 2013. “Older people and digital disengagement: a fourth digital divide?.” *Gerontology* 59(6):564-70. doi: 10.1159/000353630.
47. Norris, P., and Inglehart, R. 2019. *Cultural Backlash*. Cambridge University Press. ISBN:9781108595841

48. Stoilova, M., Livingstone, S., and Kelly, A. 2020. *Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy*. LSE.
49. OECD. 2024. *OECD Digital Economy Outlook (Volume 2) Strengthening Connectivity, Innovation and Trust*. DOI <https://doi.org/10.1787/3adf705b-en>
50. Pariser, E. 2011. *The Filter Bubble*. Penguin.
51. Paul, C., and Matthews, M. 2016. *The Russian “Firehose of Falsehood” Model*. RAND Corporation.
52. Pamment, J. 2020. “*The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework*.” Carnegie Endowment for International Peace.
53. Raichev, Y. (2023). Hybrid Wars and Hybrid Threats
54. Roberts, S. T. 2019. *Behind the Screen*. Yale University Press.
55. Tandoc, E. C., Lim, Z. W., and Ling, R. 2018. *Defining “Fake News”: A Typology of Scholarly Definitions*. Digital Journalism 6 137-153.
56. Tóth, A., and Judit, B. 2022. “EU Digital Services Act and Its Implications for Democracy and Platform Governance.” *Internet Policy Review* 11(4).
57. Tucker, J. A., et al. 2018. *Social Media, Political Polarization, and Disinformation*. Hewlett Foundation.
58. Ulmer, R. R, Sellnow, T. L., and Seeger, M. W.. 2022. *Effective Crisis Communication Moving From Crisis to Opportunity*.(Ed. 5). SAGE Publications, Inc
60. United Nations Department of Economic and Social Affairs. 2022. *United Nations E-Government Survey 2022*. DOI: <https://doi.org/10.18356/9789210019446>
61. Van Dijck, J., and Poell, T. 2018. *The Platform Society*. Oxford University Press.
62. Van Dijk, J. 2019. *The Digital Divide*. Polity Press.
63. Vraga, E. K., and Tully, M. 2021. “News literacy, social media behaviors, and skepticism toward information on social media.” *Information, Communication & Society* 24 (2): 150-166.
64. Wardle, G., & Hossein Derakhshan, H. 2017. Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI(2017)09
65. WHO. 2020. *Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation*. Available at: <https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation>. (November 25, 2025)
66. World Bank. 2021. *Digital Government Readiness Assessment*.
67. World Bank. 2021. *Cybersecurity Capacity Review*.