

Disinformation as a Security Challenge for the European Union in a Time of Deteriorating Geopolitical Situation

Vladimír Andrassy^{1*}, Monika Vavříková¹

¹Armed Forces Academy of the General M. R. Štefánik, Demänová 393, 031 01 Liptovský Mikuláš, Slovak Republic

Correspondence: *vladimir.andrassy@aos.sk

Abstract

Disinformation is becoming one of the most serious security challenges for the European Union, especially in the context of the deteriorating geopolitical situation. In recent years, disinformation has evolved from a marginal phenomenon to a systematically used tool of influence and manipulation, which disrupts the functioning of democratic societies, undermines trust in democratic values, principles and institutions and destabilizes social cohesion. Both state and non-state actors use disinformation to achieve their political, ideological, security and economic goals without direct military confrontation. The European Union is responding to these threats with comprehensive political, legislative and strategic measures, including the European Democracy Action Plan, the Digital Services Act and the Strategic Compass for Security and Defence, among others. Strengthening societal resilience through the development of media and digital literacy, critical thinking and pluralistic public discourse also plays a key role. The analysis shows that an effective and efficient fight against disinformation necessarily requires a coordinated and broad-spectrum response that respects democratic principles and values, but at the same time minimizes the space for abuse of the information environment.

KEY WORDS: *Disinformation, democratic society, threat, challenge, manipulation.*

Citation: Andrassy, V.; Vavříková, M. Disinformation as a Security Challenge for the European Union in a Time of Deteriorating Geopolitical Situation. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, [https://doi.org/ 10.47459/cndcgs.2026.44](https://doi.org/10.47459/cndcgs.2026.44)

1. Introduction

The security situation in the world has been changing dramatically in recent years. The global and regional security environment is marked by instability, variability, power competition, and frequent disruption of the rules-based international order. A significant increase in security incidents, growing tensions in several parts of the world, ongoing Russian aggression in Ukraine, as well as deteriorating relations between democratic countries and authoritarian regimes such as Russia, China or Iran, confirm that a profound geopolitical transformation with far-reaching consequences for democratic societies is taking place. In this context, the use of unconventional tools, which go beyond the scope of classic open military confrontation, is gaining increasing importance. One of these is disinformation [1,2].

The spread of untrue, false, misleading, or distorted information in the form of disinformation is no longer just a side phenomenon occurring in contemporary society. In recent years, it has become a systematically used tool of manipulation, serving to destabilize democratic societies, undermine public trust in democratic rules, principles and institutions, and disrupt social cohesion [3,4] therefore, it constitutes a unique challenge requiring effective crisis management [5]. The use of information space – mainly social networks and their platforms – for spreading various disinformation, conspiracy theories, hoaxes and fake news is proving to be a very cost-effective, difficult-to-attribute and highly effective tool of hybrid influence [6,7]. From this perspective, disinformation is a non-military asymmetric security threat primarily targeting open, pluralistic and democratic societies, including the European Union (EU) and its member states [8,4].

The political and security structures of the EU, as well as the expert community, are increasingly aware that the fight against disinformation cannot be reduced to a technical or media problem. It is a very demanding and complex challenge that requires strategic political, security, legislative, technological and societal solutions, coordinated at national and supranational levels. The efforts of authoritarian regimes to revise the global order based on rules, including norms of journalism, accountability and trust in truth, inevitably necessitate an adequate and value-anchored response from

democratic institutions [9]. The worsening geopolitical situation thus has a direct impact not only on the internal security of the EU as a whole, but also on its member states, especially in terms of protecting the democratic order, the integrity of public debate, elections and social cohesion [10]. Disinformation strikes at the core values of democratic societies [1]. For this reason, it is increasingly perceived as a first-category security threat, which is also reflected in relevant documents, such as the EU Strategic Compass for Security and Defence, the European Democracy Action Plan or in regulatory instruments such as the Digital Services Act.

The theoretical framework of this paper is based on a concept that reflects the changing character of security threats and challenges in the conditions of global transformation. The basic premise is the understanding of security as a broad, multidimensional phenomenon that transcends the traditional military understanding of threat and includes political, societal, informational, economic, technological, environmental, legislative and other aspects [11]. In accordance with this, disinformation is perceived as one of the key tools of hybrid influence, whose goal is not only to influence public opinion, but systematically to disrupt democratic processes, order, social trust and the legitimate authority of institutions [7,12].

From a methodological point of view, the article is based on a qualitative analysis of secondary sources, especially academic literature, official EU documents, research reports and political and security strategies, concepts and initiatives. The analytical-synthetic method, content, critical and comparative analysis are mainly applied, with an emphasis on the logical connection between actors, measures and effects in the fight against disinformation. Attention is also paid to aspects of normative discourse, primarily in connection with the role of the EU as a value-anchored actor within the existing international system.

The aim of the paper is to analyse disinformation as a security challenge for the EU in the current period of deteriorating geopolitical situation. The emphasis is placed mainly on the connection between the strategic goals of authoritarian regimes, the exposure of democratic societies to disinformation influence, external interference and manipulations, and the Union's responses in the form of political, security, legal, social and other measures.

2. Disinformation as a Tool of Geopolitical Competition

In the current era, amidst increasing geostrategic competition between democratic and authoritarian states, information operations and manipulation of public discourse are gaining increasing importance [13]. Within the framework of so-called hybrid conflicts, disinformation is becoming one of the main tools of power projection in the information space – their goal is to weaken the resilience of target, primarily democratic societies, disrupt their functioning, undermine the democratic foundations and pillars on which they are built, question the credibility of democratic institutions, and disturb their political stability without the use of military force [6,7]. State and non-state actors – in order to achieve their predetermined political, ideological, security, economic, and other goals – use disinformation as an asymmetric form of struggle that is very cost-effective, difficult to attribute, and extremely effective, especially in pluralistic democratic societies. By using purposefully spread false, misleading, altered, or distorted information, they strive to polarize public opinion, promote religious, ethnic, and racial intolerance, and disrupt social cohesion. This tactic allows them to achieve strategic advantages without direct military confrontation [14,1].

The term "disinformation" itself, in the context of European institutions, refers to demonstrably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and which may cause harm to the public interest [15,16]. It is important that this is a targeted activity, often related to external interference and influencing democratic processes – such as elections, referendums, or legislative initiatives – through the manipulation of public opinion. Disinformation thus differs from misinformation, which arises unintentionally, and is part of the strategic communication of state and non-state actors who pursue their own geopolitical, ideological, security, or economic goals [17,9].

Russia represents the most active state actor in conducting systematic disinformation operations aimed against the European Union as a whole and its member states. Russian activity is characterized by its long-term nature, sophistication, and adaptability. The main goals of Russian disinformation strategy include undermining unity within the Union, weakening transatlantic cooperation, supporting extremist and pro-Russian forces in member states, and questioning the values of democracy, the rule of law, and human rights. Key tools include state-backed media like RT and Sputnik, as well as extensive networks of bots, trolls, and fake accounts on social networks [18,19]. A typical example of these activities was the Russian disinformation campaign during the coronavirus pandemic, which purposefully spread narratives about the ineffectiveness of Western vaccines, the alleged dictatorship of hygienic measures in the EU, and at the same time glorified the Russian Sputnik V vaccine [20]. Another area was the war in Ukraine, where Russia used a massive disinformation machine to relativize its responsibility, justify aggression, and accuse the West of escalating the conflict. These narratives were often adopted by extremist and disinformation websites even within EU member states [21,22].

China has historically avoided open disinformation campaigns, but in recent years has adopted some techniques of so-called discursive confrontation. China invests in information influencing through state-controlled media, diplomatic communication, and strategic presence on platforms like Twitter, TikTok, YouTube, and others [23]. Its goal is primarily to shape a positive global image of China, question the Western model of democracy, and legitimize authoritarian capitalism as an alternative. In connection with the coronavirus pandemic and the war in Ukraine, China spread pro-Russian and anti-American narratives, thereby contributing to the disruption of unified discourse in the EU [24,25].

Other state actors like Iran use disinformation as part of a broader ideological conflict with the West. Iranian campaigns focus mainly on inciting antisemitism, anti-Americanism, and anti-Zionism, as well as supporting Islamist

narratives. The activity of non-state actors connected to states is also significant in this context – for example, hacking groups or so-called proxy organizations that serve as tools for state-controlled information operations to circumvent direct links [26].

Besides Russia, China, and Iran, other countries also spread disinformation. The specificity of this phase of geopolitical conflict is that the disinformation activities of individual states often overlap, complement each other, or coordinate, creating multipolar disinformation pressure on democratic societies [27,18]. The EU therefore faces a challenge not only in terms of detecting and attributing these activities, but also in terms of creating an effective and coordinated response framework that respects democratic principles while minimizing the space for abusing the information environment [28,29].

In addition to state actors, non-state actors also play a significant role in these activities, in the form of various extremist groups, ideologically motivated organizations, so-called "alternative media," but also commercially motivated platforms for which gaining attention is a commodity. Many of these entities thus profit from disinformation not only ideologically, but also economically, through monetization of clicks, product sales, or building influence on social networks [30]. The result is a complex disinformation ecosystem where the political, ideological, security, and economic interests of foreign powers, extremist groups, and opportunistic entrepreneurs converge.

Democratic societies are inherently open, pluralistic, and based on trust – be it in institutions, media, science, or civic participation. However, precisely these values, which represent the foundation of liberal democracy, also become a source of their vulnerability in the context of disinformation campaigns. Unlike authoritarian regimes, which have strongly centralized control of the information space and limited access to a plurality of opinions, democratic states are forced to respect freedom of expression, privacy protection, and the openness of information flows, which disinformation actors exploit for their own purposes [31].

One of the main weaknesses of democratic systems is their high degree of exposure to external interference. European and national elections, referendums, and other political processes are repeatedly targeted by manipulative operations whose goal is either to reduce voter turnout or to increase support for extremist and Eurosceptic entities. In the period before elections in the member states of the Union or to the European Parliament, security institutions recorded systematic attempts at interference by foreign actors, including the dissemination of false narratives about migration, religion, sexual minorities, or the loss of sovereignty of member states [32].

Furthermore, democratic societies also face internal polarization, which reduces their resilience to disinformation. Information fragmentation, the creation of so-called echo chambers and information bubbles, as well as growing distrust towards traditional media and institutions, create an environment conducive to the spread of manipulative content [33]. In this context, a weakness in media literacy and critical thinking is also evident, especially among socially and digitally vulnerable population groups [34]. The technological dimension of this vulnerability is related to the dominance of global digital platforms, whose business model is based on maximizing interaction and exploiting attention as a commodity [30]. Algorithms that prioritize sensations, emotionally charged content, and controversy naturally increase the visibility of disinformation narratives – especially if they are supported by paid advertising, coordinated bot networks, and micro-targeting [35]. The EU's legal and regulatory framework is only gradually catching up with the speed of innovation in this area, which creates a time window for those actors who exploit information asymmetry to their advantage.

3. Political, Legislative, and Strategic Responses of the EU

Given the increasing scale, frequency, sophistication, and strategic nature of disinformation campaigns, the EU has had to fundamentally re-evaluate its perception of the information space in recent years and proceed with building a comprehensive framework aimed at building resilience against these threats. Gradually, several tools have been created and a number of political, security, legislative, and strategic measures and initiatives have been adopted, which today form the basis of European anti-disinformation policy. In doing so, the EU strives to reconcile the need for protection against manipulation through disinformation with the protection of fundamental rights, such as freedom of expression, assembly, information, and privacy.

One of the fundamental pillars of this policy is the European Democracy Action Plan (EDAP), which the European Commission adopted in December 2020. This document sets out three strategic areas: (a) strengthening the integrity of electoral processes, (b) promoting media pluralism and media independence, and (c) combating disinformation. EDAP – within the framework of combating disinformation – introduces requirements for greater platform transparency, cooperation with fact-checkers, building literacy, and supporting science and research. It significantly supports a participatory approach that connects public authorities, civil society, research institutions, and technological platforms. EDAP also envisages the creation of a common framework for responding to hybrid threats, including those in the information sphere [36].

Even before the adoption of EDAP, the EU attempted to create mechanisms for self-regulation and cooperation with online platforms – the result was the Code of Practice on Disinformation, which was established in 2018 and revised in 2022. This is the first such tool of its kind in the world that obliges technology companies such as Google, Meta, Twitter (X), TikTok, Microsoft, and others to adopt voluntary measures in the area of demonetizing disinformation content, advertising transparency, cooperation with fact-checkers, publishing algorithmic rules, and improving user literacy. It should be noted that it was originally a voluntary mechanism. However, the European Commission has taken a significant step towards strengthening its regulatory approach to mitigating online disinformation. On February 13, 2025, the

Commission officially integrated its voluntary Code of Practice on Disinformation into the framework of the Digital Services Act (DSA). This is not just a procedural update; it is a strategic shift that places the Code in the position of a 'relevant reference point' for platform compliance. Effective from July 1, 2025, this change transforms the Code from a voluntary agreement into a cornerstone of the DSA, with potential consequences for enforcement measures against online platforms that do not comply with its provisions [37].

From the above, it follows that the Digital Services Act (DSA) has become a key legislative instrument of the EU in the field of digital space regulation. This legal act creates a uniform framework for the functioning of online platforms, digital service providers, and social media, introducing binding rules for content responsibility, algorithmic decision-making, advertising transparency, and user protection. In the area of disinformation, the DSA plays a fundamental role by establishing obligations for online platforms, including preventing systematic risks to public discourse, public health, and security [38] and this role is particularly crucial in pandemic situations [39].

One of the main innovative elements of the DSA is its emphasis on risk assessments and independent audits of algorithms, which are intended to reveal the extent to which recommendation and content distribution systems facilitate the spread of harmful narratives. Platforms are obliged to cooperate with national and European regulatory authorities, as well as to make data necessary for the analysis of digital threats available to researchers. In case of violations of obligations, fines of up to 6% of global turnover are threatened, which represents the toughest law enforcement mechanism in the history of digital regulation in the EU [40].

In addition to legislative measures, the EDMO (European Digital Media Observatory) platform plays an important role. The European Commission launched it in 2020 as an independent network of research centres, fact-checkers, universities, and experts. EDMO performs several functions: it analyses disinformation campaigns and narratives, develops methodologies for their detection, supports media literacy, and provides recommendations for public policy-making. EDMO also acts as a bridge between academia, civil society, and public institutions, thereby contributing to the creation of evidence-based responses to information threats [41].

A fundamental shift in the understanding of disinformation as a security threat occurred in 2022 with the adoption of the Strategic Compass for Security and Defence, which defines the main trajectory of the development of the EU's Common Security and Defence Policy until 2030. In this strategy, disinformation, information operations, and hybrid threats are clearly identified as key security challenges that require a comprehensive and multidisciplinary response [42]. The Strategic Compass emphasizes the need to strengthen the resilience of society, critical infrastructure, and institutions against hybrid attacks, including those conducted in the digital and information space. One of the key measures is the creation of the EU Hybrid Toolbox – a set of tools that enable a rapid response to hybrid incidents, including disinformation campaigns. This tool includes diplomatic, cyber, economic, and communication means to help member states detect, attribute, and neutralize hybrid threats [43].

In the area of strategic communication and defence against information interference, the importance of the EEAS StratCom Division – a specialized unit of the European External Action Service (EEAS), which was established already in 2015 – is increasing. StratCom operates through regional units and ensures the monitoring, analysis, and counter-information of disinformation campaigns. An important output of this activity is the EUvsDisinfo database, which documents specific cases and narratives, thereby providing an empirical basis for political decision-making and research.

Other documents contributing to the EU's strategic response framework include: the EU cybersecurity strategy [44], the EU Security Union Strategy 2020-2025 [45] and the Joint Communication on strengthening resilience against hybrid threats from 2016 and its updates [46]. These documents take into account the growing interconnectedness between the physical, digital, and information spaces and emphasize the need for a common value framework for responding to hostile influence [46].

An important aspect of the strategic framework is also the link between internal and external security, which is reflected in initiatives such as an integrated approach to security, linking diplomatic, military, cyber, and communication tools. Disinformation, in this logic, is perceived as a threat that transcends the boundaries of individual sectors, and therefore necessarily requires a coordinated response from all relevant EU policies – including defence, foreign policy, internal affairs, the digital agenda, and education.

Effective combat against disinformation requires not only high-quality political and legislative tools, but also functional, coordinated, and inclusive inter-institutional cooperation across the entire EU. The European Union has therefore, over the last decade, created a network of bodies, platforms, and working groups that ensure both vertical and horizontal communication, information exchange, and synergy among actors with different remits and professional focuses.

The key coordinating actor is the already mentioned European External Action Service (EEAS), which includes the aforementioned StratCom Division. This unit not only analyses disinformation campaigns but also cooperates with member states, NATO, and other partners in strategic communication, including narrative building and supporting credible sources. The EEAS also provides expert input for the political decision-making of the EU Council and the European Commission in the fight against...

In the area of expertise and recommendation-making, the High-Level Expert Group on Fake News and Online Disinformation (HLEG), established by the Commission in 2018, plays an important role. HLEG consists of experts from academia, media, technology companies, and civil society, and it forms the basic framework for subsequent political and regulatory measures, including the already mentioned Code of Practice and the DSA. HLEG recommended an approach focused on transparency, accountability, strengthening literacy, and supporting quality journalism [15].

An important function is also performed by ERGA (European Regulators Group for Audiovisual Media Services) – a network of national regulatory authorities for audiovisual services, which supports the uniform implementation of European regulations, including measures against harmful content and disinformation. ERGA cooperates with platforms, governments, and researchers in formulating recommendations concerning content moderation, algorithmic accountability, and strengthening pluralism [47].

Other important institutional initiatives include: the Rapid Alert System (RAS) for information exchange among member states during electoral periods, the Task Force Against Disinformation within the EEAS and the European Commission, networks of fact-checkers and research centres connected to EDMO, and a growing number of national strategies and agencies that implement common EU principles in the fight against disinformation. These mechanisms represent the basis of a co-regulatory model, in which public authorities, private companies, and civil society cooperate with the aim of protecting public discourse, the integrity of democratic processes, and information security. Coordination, interoperability, and knowledge sharing among these actors are essential for the timely detection, response, and prevention of disinformation threats in a rapidly changing and technologically very demanding environment.

4. The Need to Strengthen the Resilience of European Society

One of the most effective and, at the same time, long-term sustainable tools in the fight against disinformation is strengthening society's resilience through education, the development of critical thinking, and media literacy [1,48]. In an environment where information flows are not filtered by traditional gatekeepers—such as editors, professional journalists, or academic authorities—an individual's ability to recognize manipulative content, evaluate the trustworthiness of sources, and analyse argumentative structures plays a crucial role in protecting public discourse.

Media literacy encompasses not only the ability to effectively use information technologies but also the ability to interpret, deconstruct, and critically reflect on media as social constructs that can carry ideological, political, or commercial intentions. In this sense, media literacy is fundamentally important not only for individual decision-making but also for the collective resilience of a democratic society against manipulation and polarization [49].

However, in many EU member states, the level of media literacy remains uneven. Differences exist not only between countries but also between generations, social groups, and regions. Studies indicate that low media literacy correlates with a higher degree of susceptibility to disinformation and a greater propensity for conspiracy theories [50]. It follows that media literacy should be considered a strategic component of the EU's defence capability, similar to cybersecurity or the defence of critical infrastructure.

Particularly important is the implementation of systematic media and information literacy programs into school curricula at primary and secondary education levels. In this regard, the European Commission recommends developing national strategies, supporting pedagogical innovations, and training teachers, who play a key role in cultivating critical thinking from an early age. Beyond formal education, it's also necessary to develop non-formal learning methods through libraries, public media, and civic initiatives [51].

Another challenge is the dynamics of information behaviour in the digital environment, where user habits are shaped by interaction with algorithm-designed content. In this context, it's crucial to link media literacy with digital literacy so that individuals understand how their behaviour influences the selection of displayed content and how this creates a predisposition to information cocoons [30].

Modern disinformation campaigns heavily rely on the specific functioning of social networks and digital platforms, whose algorithms determine what content is displayed to users. In an effort to maximize user engagement and time spent online, these algorithms often prioritize emotionally charged, controversial, or polarizing content—providing disinformation actors with ideal conditions for spreading manipulative narratives [7].

One of the most serious consequences of this dynamic is the emergence of so-called echo chambers—homogeneous online environments where users mutually confirm their views and are not confronted with differing perspectives. Simultaneously, information bubbles are created, within which algorithms tailor content to individual preferences, leading to a personalization of truth and a fragmentation of public discourse [52]. These phenomena significantly weaken a common reality, which is a fundamental prerequisite for the functioning of democracy.

Research has shown that in such environments, users are more susceptible to believing false information that confirms their prior beliefs, while their willingness to fact-check or change their minds based on new evidence decreases. This creates cognitive closure, which is very advantageous for propagandistic actors—their goal is not to convince everyone, but to activate and radicalize a certain group of the audience that will become a carrier of disinformation content within their community [53,54].

It is also important to realize that social networks are not just neutral platforms; they act as active information intermediaries—their business model is based on selling attention and data, not on guaranteeing the truthfulness of content [30]. Therefore, the EU, through tools like the DSA (Digital Services Act) and EDMO (European Digital Media Observatory), insists on introducing transparency of algorithmic recommendations, enabling independent research into their effects, and supporting alternative platform environment designs that would consider the public interest. Increasing societal resilience cannot therefore be reduced solely to the individual user level—it is a systemic issue of technological design, digital policy, and social architecture.

Societal resilience to disinformation does not solely depend on individuals' ability to recognize false content, but more broadly, on the quality of public discourse that allows for the exchange of opinions, the inclusion of diverse

perspectives, and respect for facts. Pluralistic discourse is a fundamental pillar of democratic societies, but in recent years, it has been increasingly disrupted by polarization, emotional escalation, and a loss of trust in traditional institutions. Therefore, it is crucial to create conditions for quality public discussion, not only through professional media but also by supporting civic initiatives, community platforms, and participatory projects that strengthen a sense of belonging, shared values, and critical reflection. Such forms of public engagement play a key role in increasing collective immunity to manipulation [55].

Fact-checking organizations play a specific role, verifying statements, articles, and campaigns, thereby strengthening the trustworthiness of the information environment. Within the EU, several reputable entities (e.g., Corrective, Demagog, AFP Fact Check) are involved in the EDMO network and collaborate with online platforms and national regulators. These activities have not only technical but also societal value—they demonstrate that the public is not defenceless against manipulation but can respond expertly, transparently, and independently [56,57].

In this context, it is also important to ensure that pluralistic discourse is not perceived as a synonym for "relativism" or "post-truth," but rather firmly grounded in common methodological and ethical norms of knowledge and argumentation. This requires investment in education, support for investigative journalism, public service media, and open science, all of which can serve as stabilizing pillars of the public sphere [58].

From the above, it's clear that building resilience against disinformation is, first and foremost, a long-term societal project that goes beyond reactionary security measures. The most effective long-term strategy is early and systematic education that develops critical thinking skills, media and digital literacy, as well as civic awareness and value rootedness. Therefore, formal education plays a crucial role in preventing the spread of manipulative and false information.

Educational institutions should not be seen merely as places for transmitting knowledge, but also as spaces for cultivating democratic competencies, the ability to conduct reasoned discussions, and to understand the complexity of social phenomena. European recommendations in this area emphasize the need to integrate media and information literacy across subjects, support an interdisciplinary approach, introduce practical exercises with information analysis, and ensure continuous teacher training [59].

In this context, it's also important to mention non-governmental organizations (NGOs), which play an indispensable role in complementing and expanding educational activities to the general public. Their flexibility, grassroots presence, and ability to communicate specifically with particular communities allow them to effectively supplement the efforts of the state and institutions. Many of these organizations conduct workshops, campaigns, digital games, and analytical publications that have both an educational and an activating dimension [60]. Such activities help build local networks of resilience that can react quickly and flexibly to new disinformation threats.

Given the complexity and constant variability of disinformation threats, it is clear that the EU's response must be not only effective and efficient but also systemic, adaptive, and legally anchored. The current fragmentation of approaches among member states, the diversity of national strategies, and differing regulatory capacities can weaken the overall coherence and effectiveness of European efforts in this area. Therefore, there is increasingly intensive discussion about the need for a more centralized, coordinated, and long-term sustainable framework that would include legislative, technological, educational, and strategic aspects.

Such a framework should meet several basic criteria: it should primarily be (a) value-anchored in the principles of democracy, the rule of law, and the protection of fundamental rights, (b) technologically flexible to respond to new types of threats, including generative AI and deepfakes, (c) multi-institutional, thus connecting European institutions, member states, research organizations, platforms, and civil society, and (d) internationally compatible, so that the EU remains a relevant actor in shaping global standards in digital security [61].

One of the key aspects of a future strategy is also balancing security imperatives with the protection of freedom of expression. Overly repressive measures can jeopardize the free exchange of opinions, while an insufficiently regulated environment provides space for the dissemination of harmful content. Therefore, it is necessary to build normatively sensitive policies that will be able to distinguish between legal plurality of opinions and coordinated manipulative campaigns aimed at destabilizing democratic processes [62].

Another challenge is the sustainability of measures over time. Many strategies and initiatives in the area of disinformation have arisen reactively—in response to specific crises—such as the coronavirus pandemic, the Russian invasion of Ukraine, or election interference. To ensure true resilience, however, it is necessary to create long-term mechanisms for funding, political support, and institutional capacity that will allow for the continuity and accumulation of knowledge and experience even outside immediate crisis periods.

Conclusion

Democracy is one of the fundamental values of the European Union. It is at the core of open and transparent societies. In the European Union, citizens can freely express their opinions, participate in democratic life, and elect their political representatives. However, in recent years, there has been an increase in false, misleading, distorted, or altered information that can affect various aspects of our lives: health, public safety, trust in democracy, climate and environment, migration, and the fundamental rights and values that underpin our societies.

The analysis presented in this paper shows that disinformation is no longer a fringe phenomenon and is increasingly emerging as a strategic security challenge for the European Union and its member states, especially in the context of a deteriorating geopolitical situation. The rise of authoritarian regimes attempts to revise the international order,

and technological transformations in information technologies create a new dynamic of asymmetrical security threats, where the ability to control the information space is as important as traditional military or economic tools of power.

The findings from individual chapters indicate that disinformation is deliberately used by both state and non-state actors to weaken the EU's internal cohesion, undermine citizens' trust in democratic institutions, and influence public opinion in critical areas—from elections and vaccination to military conflicts. Particular attention is required for targeted disinformation campaigns, primarily conducted by Russia and China, as well as the misuse of misleading information and populist narratives in hybrid operations.

The European Union has responded to these challenges with a fairly wide range of political, legislative, and strategic measures, among which the most notable are the European Democracy Action Plan, the Digital Services Act, the strengthened Code of Practice on Disinformation, as well as the Strategic Compass for Security and Defence and its connection to the hybrid threats agenda. Inter-institutional mechanisms such as EEAS StratCom, HLEG, and EDMO also play a significant role.

At the same time, it is becoming increasingly clear that strengthening societal resilience—both at the transnational, EU level and at the national level—is a necessary prerequisite for successfully managing disinformation campaigns. Key factors include the development of media and digital literacy, critical thinking, pluralistic public discourse, and the networking of civil society actors, including educational institutions, non-governmental initiatives, and fact-checkers.

At the transnational level, cooperation with the North Atlantic Alliance (NATO) and other democratic partners is also extremely important, as is the reflection of the challenges of the digital era—especially in connection with generative AI, deepfakes, and automated content dissemination. These trends show that information security is becoming an inseparable part of ensuring the security and defence not only of the EU as a whole and its member states, but also of other democratic societies worldwide, and requires a strategic, long-term, and multidisciplinary response.

References

1. **Ivančík, R.** *Dezinformácie. Teoretické východiská ich skúmania*. Praha: Leges, 2025. 188 p. ISBN 978-80-7502-769-6.
2. **Colomina, C.** The world in 2025: ten issues that will shape the international agenda. In *Barcelona Centre for International Affairs*, 2025. Retrieved from: <https://www.cidob.org/en/publications/world-2025-ten-issues-will-shape-international-agenda>
3. **Woolley, S. C. & Howard, P. N.** *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press, 2019. ISBN 978-0-190-93140-7.
4. **Ivančík, R., Müllerová, J.** Disinformation, Propaganda, and Fake News as Non-Military Security Threats for Contemporary Modern Human Society. In *Security Dimensions*, 2022, No. 40, pp. 116-132. ISSN 2353-7000. Retrieved from: <https://securitydimensions.publisherspanel.com/resources/html/article/details?id=2288402582-5194>
5. **Brezina, D. & Kompan, J.** Evaluation of Modern Approaches to Crisis Management. In *Challenges to National Defence in Contemporary Geopolitical Situation*, 2024, pp. 397-402. Retrieved from: <https://doi.org/10.3849/cndcgs.2024.397>
6. **Pamment, J.** The EU's Role in Fighting Disinformation: Taking Back the Initiative. In *Carnegie Europe*, 2020. Retrieved from: <https://carnegieeurope.eu/2020/06/22/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82124>
7. **Ivančík, R. & Nečas, P.** On disinformation as a hybrid threat spread through social networks. In *Entrepreneurship and Sustainability Issues*, 2022, Vol. 10, No. 1, pp. 344-357. ISSN 2345-0282. Retrieved from: [https://doi.org/10.9770/jesi.2022.10.1\(18\)](https://doi.org/10.9770/jesi.2022.10.1(18))
8. **Flore, M., Balahur, A., Podavini, A. & Verile, M.** *Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda*. Luxembourg: Publications Office of the European Union, 2019. 94 p. ISBN 978-92-76-03320-2. Retrieved from: <https://doi.10.2760/919835>
9. **EEAS.** Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). In *European External Action Service*, 2025a. Retrieved from: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
10. **Castaldi, R.** European defence for security and peace. In *Foundation for European Progressive Studies*, 2025. Retrieved from: <https://feps-europe.eu/wp-content/uploads/2025/03/European-Defence-for-Security-and-Peace.pdf>
11. **Brezina, D. & Martaus, T.** Extremism in the Armed Forces of the Slovak Republic. In *Journal of Electrical Systems*, Volume 20, no. 5 p. 1467-1479. ISSN 1112-5209. Retrieved from: <https://journal.esrgroups.org/jes/article/view/2478>
12. **D'Andrea, A., Fusacchia, G. & D'Ulizia, A.** Policy Review: Countering Disinformation in the Digital Age - Policies and Initiatives to Safeguard Democracy in Europe. In *Information Policy*, 2025, Vol. 30, No. 1, pp. 82-91. ISSN 1875-8754. Retrieved from: <https://doi.org/10.1177/15701255251318900>
13. **Vilmer, J.-B., Escorcía, A., Guillaume, M. & Herrera, J.** *Information Manipulation: A Challenge for Our Democracies*. Paris: The Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research of the Ministry for the Armed Forces 2018. ISBN 978-2-11-152607-5. Retrieved from: https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

14. **Rosenbach, E. & Mansted, K.** Can Democracy Survive in the Information Age? In *Belfer Center for Science and International Affairs of the Harvard Kennedy School*, 2018. Retrieved from: <https://www.belfercenter.org/publication/can-democracy-survive-information-age>
15. **European Commission.** Final report of the High-Level Expert Group on Fake News and Online Disinformation. In European Commission, 2018. Retrieved from: <https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation>
16. **EEAS.** Countering disinformation and building societal resilience. In *European External Action Service*, 2024a. Retrieved from: https://www.eeas.europa.eu/eeas/countering-disinformation-and-building-societal-resilience_en
17. **European Commission.** Strategic communication and countering information manipulation. In *European Commission*, 2024a. Retrieved from: https://commission.europa.eu/topics/countering-information-manipulation_en
18. **Hood, L.** Disinformation campaigns are undermining democracy, In *The Conversation*, 2023. Retrieved from: <https://theconversation.com/disinformation-campaigns-are-undermining-democracy-heres-how-we-can-fight-back-217539>
19. **Odarchenko, K.** The Fight Against Disinformation: A Persistent Challenge for Democracy. In Foreign Policy Research Institute, 2021. Retrieved from: <https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/>
20. **European Commission.** Tackling coronavirus disinformation. In *European Commission*, 2021. Retrieved from: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_en
21. **EUvsDiSiNFO.** Ukraine. In *European External Action Service*, 2025. Retrieved from: <https://euvsdisinfo.eu/ukraine/>
22. **FMI.** Disinformation related to the Russian war of aggression against Ukraine. In *Federal Ministry of the Interior*, 2025. Retrieved from: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/disinformation-related-to-the-russian-war-of-aggression-against-ukraine.html>
23. **Cook, S.** Beijing's Global Media Influence: Authoritarian Expansion and the Power of Democratic Resilience. In *Freedom House*, 2021. Retrieved from: <https://freedomhouse.org/report/beijings-global-media-influence>
24. **Gimbals.** China's Information Operations Strategy: Controlling Narratives and Shaping Global Perceptions. In *3Gimbals*, 2024. Retrieved from: <https://3gimbals.com/insights/chinas-information-operations-strategy-controlling-narratives-and-shaping-global-perceptions/>
25. **Osavul.** How Chinese Narratives Affect the World. In *OSavul*, 2025. Retrieved from: <https://www.osavul.cloud/blog/how-chinese-narratives-affect-the-world>
26. **Greenblatt, J.** State Hate: How Iran's Press TV Uses Social Media to Promote Anti-Jewish Hatred. In *Center for Countering Digital Hate*, 2025. Retrieved from: <https://www.adl.org/resources/report/state-hate-how-irans-press-tv-uses-social-media-promote-anti-jewish-hatred>
27. **Odarchenko, K.** The Fight Against Disinformation: A Persistent Challenge for Democracy. In Foreign Policy Research Institute, 2021. Retrieved from: <https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/>
28. **EEAS.** 3rd EEAS Report on Foreign Information Manipulation & Interference (FIMI). In *European External Action Service*, 2025b. Retrieved from: <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3rd-ThreatReport-March-2025-05-Digital-HD.pdf>
29. **Majchút, I.** Contemporary Civil-Military Relations. *Challenges to National Defence in Contemporary Geopolitical Situation: Proceedings of the 4th International Scientific Conference*, 2024. Retrieved from: <https://doi.org/10.3849/cndcgs.2024.124>
30. **Ivančík, R., Nečas, P. & Ilaščíková, L.** Attention as a Commodity in the World of Disinformation and Social Media. In *Entrepreneurship and Sustainability Issues*, 2024, Vol. 12, no. 2, p. 176-192. ISSN 2345-0282. Retrieved from: <https://doi.org/10.9770/k7393698996>
31. **Bridgman, A., Gehringer, F., Owen, T. & Romanishyn, A.** Countering Foreign Information Manipulation and Interference - Lessons from the 2024 European Elections. In *Konrad Adenauer Stiftung*, 2025. Retrieved from: https://www.kas.de/documents/d/canada/eu-kas-report_fimi-and-european-elections
32. **EEAS.** 2nd EEAS Report on Foreign Information Manipulation & Interference (FIMI). In *European External Action Service*, 2024b. Retrieved from: https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf
33. **Flaxman, S., Goel, S. & Rao, J. M.** Filter Bubbles, Echo Chambers, and Online News Consumption. *Public Opinion Quarterly*, 2016, Vol. 80, No. 1, pp. 298-320. ISSN 0033-362X. Retrieved from: <https://doi.org/10.1093/poq/nfw006>
34. **Tucker, J. A.** Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. In *Hewlett Foundation*, 2018. Retrieved from: <https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf>
35. **Bradshaw, S. & Howard, P. N.** Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. In *University of Oxford*. 2018. Retrieved from: <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf>
36. **European Commission.** European Democracy Action Plan: making EU democracies stronger. In *European Commission*, 2020. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

37. **Jahangir, R.** The EU's Code of Practice on Disinformation is Now Part of the Digital Services Act. What Does It Mean? In *Tech Policy Press*, 2025. Retrieved from: <https://www.techpolicy.press/the-eus-code-of-practice-on-disinformation-is-now-part-of-the-digital-services-act-what-does-it-mean/>
38. **European Union.** Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act). In *Official Journal of the European Union*, 2022. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>
39. **Brezina, D. & Kompan, J.** Capability of the Armed Forces of the Slovak Republic to provide logistical support for a pandemic crisis response. In *Transportation Research Procedia*, 2026, Vol 93, pp. 1026-1033. Retrieved from: <https://doi.org/10.1016/j.trpro.2025.12.038>
40. **EDPS.** EDPS Opinion on the European Commission's proposal for a Digital Services Act. In *European Data Protection Supervisor*, 2021. Retrieved from: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en
41. **European Commission.** European Digital Media Observatory (EDMO). In *European Commission*, 2024b. Retrieved from: <https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>
42. **European Council.** Strategic Compass for Security and Defence. In *European Council*, 2022. Retrieved from: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>
43. **Lasoen, K.** Realising the EU Hybrid Toolbox: opportunities and pitfalls. In *Clingendael – the Netherlands Institute of International Relations*, 2022. Retrieved from: https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf
44. **European Commission.** The Cybersecurity Strategy. In *European Commission*, 2025. Retrieved from: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>
45. **European Union.** Communication from the Commission on the EU Security Union Strategy. In *Official Journal of the European Union*, 2020. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605>
46. **European Union.** Joint Framework on countering hybrid threats. A European Union response. In *Official Journal of the European Union*, 2016. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018>
47. **ERGA.** European Regulators Group for Audiovisual Media Services. In <https://erga-online.eu>, 2025. Retrieved from: <https://erga-online.eu>
48. **Conte, M. M., Roman, F., Sacchet, M., Spinello, E., Molnár, A., Attias, S., Tudorache, P., Kompan, J., Dolan, A.** Students' perception of international collaboration and cultural understanding in digitally driven education. In *Proceedings of the International Conferences on e-Learning and Digital Learning 2024*, ELDL 2024; Sustainability, Technology and Education 2024, STE 2024, pp. 145-153.
49. **Caled, D. & Silva, M. J.** Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. In *Journal of Computational Social Science*, 2022, Vol. 5, No. 1, pp. 123-159. ISSN 2432-2725. Retrieved from: <https://doi.org/10.1007/s42001-021-00118-8>
50. **EDJN.** Mapping media literacy practices and activities in the EU. In *The European Data Journalism Network*, 2022. Retrieved from: https://www.europeandatajournalism.eu/cp_data_news/mapping-media-literacy-practices-and-activities-in-the-eu/
51. **Rojas-Estrada, E. G., Aguaded, I. & García-Ruiz, R.** Media and Information Literacy in the Prescribed Curriculum: A Systematic Review on its Integration. In *Education and Information Technologies*, 2024, Vol. 29, pp. 445–472. ISSN 1573-7608. Retrieved from: <https://doi.org/10.1007/s10639-023-12154-0>
52. **Diaz Ruiz, C.** Disinformation on digital media platforms: A market-shaping approach. In *New Media & Society*, 2023, Vol. 27, č. 4, pp. 188-211. ISSN 1461-7315. Retrieved from: <https://doi.org/10.1177/14614448231207644>
53. **Nickerson, R. S.** Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. In *Review of General Psychology*, 1998, Vol. 2, No. 2, pp. 175-220. ISSN 1939-1552. Retrieved from: <https://doi.org/10.1177/00027642221118264>
54. **Chadwick, A., Vaccari, C. & Kaiser, J.** The Amplification of Exaggerated and False News on Social Media: The Roles of Platform Use, Motivations, Affect, and Ideology. In *American Behavioral Scientist*, 2022, Vol. 69, No. 2, pp. 113-130. ISSN 1552-3381. Retrieved from: <https://doi.org/10.1177/00027642221118264>
55. **Hammonds, W.** Enabling civil society to combat mis- and Disinformation. In *Ecorys Policy Brief*, 2024. Retrieved from: <https://doi.org/10.1177/00027642221118264>
56. **Graves, L. & Cherubini, F.** The Rise of Fact-Checking Sites in Europe. In *Reuters Institute for the Study of Journalism*, 2024. Retrieved from: <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/The%2520Rise%2520of%2520Fact-Checking%2520Sites%2520in%2520Europe.pdf>
57. **García-Gordillo, M., Rivas-de-Roca, R. & de-Lima-Santos, M.** The Fact-Checking Initiatives in the EU: A Diverse Ecosystem Against Disinformation. In *Media and Communication*, 2025, Vol. 13, Article 9421. Retrieved from: <https://doi.org/10.17645/mac.9421>
58. **Tryggvason, Á., Öhman, J. & Van Poeck, K.** Pluralistic environmental and sustainability education – a scholarly review. In *Environmental Education Research*, 2023, Vol. 29, č. 10, pp. 460-485. ISSN 1469-5871. Retrieved from: <https://doi.org/10.1080/13504622.2023.2229076>

59. **UNESCO.** Media and information literacy curriculum for teachers. In *United Nations Educational, Scientific and Cultural Organization*, 2024. Retrieved from: <https://www.unesco.org/en/articles/media-and-information-literacy-curriculum-teachers>
60. **Dziegiel, W. & Pawlik, K.** Combating climate disinformation is in the interest of all EU member states and NATO allies. In Casimir Pulaski Foundation, 2025. Retrieved from: <https://pulaski.pl/en/combating-climate-disinformation-is-in-the-interest-of-all-eu-member-states-and-nato-allies/>
61. **Botero Arcila, B. & Griffin, K.** Social media platforms and challenges for democracy, rule of law and fundamental rights. In *European Parliament, Directorate-General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs*, 2023. Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743400/IPOL_STU\(2023\)743400_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/743400/IPOL_STU(2023)743400_EN.pdf)
62. **Bayer, B. & Katsirea, I., Batura, O., Holznagel, B., Hartmann, S. & Lubianec, K.** The fight against disinformation and the right to freedom of expression. In *European Parliament, Directorate-General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs*, 2021. Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU\(2021\)695445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2026 and/or the editor(s). CNDCGS 2026 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.