frontiers in Political Science

TYPE Original Research
PUBLISHED 27 October 2026
DOI 10.3389/fpos.2026.1897340

Check for updates

OPEN ACCESS

EDITED BY
Ilia Murtazashvili,
University of Pittsburgh, United States

REVIEWED BY
Ladislav Cabada,
Metropolitan University Prague, Czechia
Sundara Kashyap Vadapalli,
Heriot-Watt University, United Kingdom

*CORRESPONDENCE
Miloš R. Milenković
milos_milenkovic@hotmail.com

RECEIVED 01 June 2026
REVISED 10 September 2026
ACCEPTED 15 September 2026
PUBLISHED 27 October 2026

CITATION
Milenković MR and Miljković UG (2026) Societal resilience and total defence in the digital age: the cognitive dimension of disinformation and its implications for the national security of Serbia. *Front. Polit. Sci.* 8:1897340. doi: 10.3389/fpos.2026.1897340

COPYRIGHT
© 2026 Milenković and Miljković. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Societal resilience and total defence in the digital age: the cognitive dimension of disinformation and its implications for the national security of Serbia

Miloš R. Milenković* and Uroš G. Miljković

Strategic Research Institute, University of Defence in Belgrade, Belgrade, Serbia

This paper examines the cognitive dimension of disinformation and its implications for the national security of Serbia within the broader topic of societal resilience and total defence in the digital age. Under conditions of heightened hybrid threats and the strategic use of disinformation as a means of political and security pressure, the paper argues that enhancing cognitive resilience represents a crucial prerequisite for the effective implementation of the concept of total defence. The research is based on three complementary theoretical frameworks—social constructivism, network society theory and securitization theory. The empirical part of this study is based on research conducted among a sample of 202 adult respondents from Serbia using the Online Misinformation Susceptibility Scale (OMISS) and Perceived Media Information Environment Questionnaire (PMIEQ), which was specifically designed for this study. The results indicate that most respondents demonstrate a high level of susceptibility to online disinformation and uncritical acceptance of online content as a prevalent behavioral tendency. Moreover, the respondents perceive the media landscape in Serbia as an arena of competing external influences, identifying Russia and China as the most prominent foreign actors, while expressing a strong need for an institutional government response to the spread of disinformation. The concluding part of the paper presents recommendations aimed at enhancing cognitive resilience, which is considered a functional component of total defence and national security in the digital age.

KEYWORDS
cognitive resilience, disinformation, hybrid threats, media literacy, national security of Serbia, societal resilience, total defence

1 Introduction

The contemporary security landscape cannot be understood solely through category of the use of military force and physical threat to territory and state sovereignty. We are now living in a digital age, with societies showing a high level of dependence on information flows and network platforms through which information is transmitted at high speed. In this context, information has, among other things, become an instrument of strategic competition with the

capacity to shape the reality, due to the fact that it enables state and non-state actors to influence global processes, quickly attract attention and direct perceptions to their own advantage (Joint Chiefs of Staff, 2018). Precisely for that reason modern disinformation campaigns increasingly operate as repeated, sustained efforts to influence public opinion; their aim extends beyond simple persuasion: they seek to confuse audiences, erode institutional trust, and make it more difficult for citizens to distinguish accurate information from manipulated content (Paul and Matthews, 2016). This process is further intensified by the emergence of cognitive warfare, which does not merely aim to control the flow of information, but seeks to influence the very mechanisms of perception, interpretation, and decision-making, at both the individual and societal level (Cluzel, 2020; Claverie and du Cluzel, 2021; Deppe, 2023; Deppe and Schaal, 2024). This means that disinformation and similar forms of information operations are not merely matters of media and political communication, but constitute immediate security issues that affect the public sphere and influence societal stability, institutional effectiveness, and the legitimacy of government.

Under such conditions, security today depends less on reacting to crises and more on the state's capacity to prepare, respond, and maintain core functions while ensuring rapid recovery once a crisis subsides. For this very reason the concept of resilience is becoming increasingly prominent in academic debates and official state policies. RAND Corporation's synthetic definition of a societal resilience is "society's ability to be prepared for, resist, absorb and/or achieve a new state of equilibrium after a disruption" (Nederveen et al., 2024, p. 17), while NATO additionally operationalizes this concept as the capability to prepare for, withstand, and rapidly recover from strategic shocks and disruptions (NATO, 2022, p. 7). Furthermore, resilience is not restricted to critical infrastructure, supply chains or continuity of government, but also extends to institutional trust, strategic communication, social cohesion and citizens' readiness to operate in a coordinated manner during a crisis (European Union, 2022, p. 34). This is precisely where societal resilience merges with the concept of total defence, which implies the integrated engagement of state authorities, local communities, economy and citizens. It must be emphasized that total defence in the digital age is not complete if it encompasses only material and organizational resources. It must also include cognitive resilience of the citizens, primarily their capacity to recognize manipulation, preserve trust and avoid paralysis in decision-making and collective response.

To better understand the significance and findings of this paper, it is necessary to briefly explain Serbia's geopolitical and security position. The Republic of Serbia is a continental state located in the central part of Southeast Europe, whose geographical position determines its geopolitical, transit, and security significance. Serbia is a militarily neutral state and does not seek membership in NATO, nor in any other military alliance. It is surrounded mainly by NATO member states and has institutionalized cooperation with the Alliance, primarily within the Partnership for Peace program (NATO, 2026). At the same time, EU membership is Serbia's officially declared strategic goal (Ministry of Foreign Affairs of the Republic of Serbia, 2026). The Republic of Serbia seeks to simultaneously pursue the process of European integration, preserve its policy of military neutrality, and maintain developed relations with states belonging to different centers of power (Republic of Serbia, 2019a). Its security situation is further complicated by the unresolved status of its southern province of Kosovo and Metohija, which is now predominantly inhabited by ethnic Albanians. This territory, which has been under the protectorate of international military forces—KFOR (Kosovo Force), since 1999, as well as the civilian missions UNMIK (United Nations Interim Administration Mission in Kosovo) and EULEX Kosovo (European Union Rule of Law Mission in Kosovo), unilaterally declared independence in 2008. This declaration remains officially unrecognized by Serbia and several other states, while it has been recognized by others, including most states of the so-called political West. Serbia's security landscape is also shaped by complex regional relations with the states that once lived together in the Yugoslav federation (Republic of Serbia, 2019a).

The Republic of Serbia has traditionally maintained a strong historical, cultural, and religious relationship with the Russian Federation, as well as political and economic ties, particularly in the energy sector. Alongside this relationship, Serbia is developing a comprehensive strategic partnership with the People's Republic of China, while also being strongly oriented, economically, institutionally, and politically, towards the European Union and, in political and security terms, towards the United States of America. Among regional states, Turkey exerts the most significant influence. Taken together, these overlapping ties and interests shape Serbia's geopolitical position and overall security environment, leading the country to apply a distinctive strategy of balancing, or hedging; this involves cooperating with EU states, traditional partners, and non-European actors, while remaining on its European path and preserving its military neutrality (Nikolic, 2023; Belloni, 2024; Jović-Lazić, 2025; Stekić and Mitić, 2025; Đurić, 2026). This complex interplay of foreign interests, together with Serbia's aspiration not to align itself with either side, creates favorable conditions for various actors to pursue their own agendas. As a result, any attempt by these actors to exert influence through the digital and media sphere could potentially have a direct impact on Serbia's security status.

Given the specific geopolitical and security position of Serbia described above, it can be argued that the cognitive dimension of disinformation and societal resilience in the digital age are particularly important for Serbia, because its security interests and strategic concept evolve under the conditions of military neutrality, high exposure to external information influence, and significant domestic dependency on public trust in institutions. National Security Strategy of the Republic of Serbia does not define national security exclusively as objective protection of values and interests, but as "subjective sense of security of the citizens" (Republic of Serbia, 2019a, p. 1) as well. In other words, disinformation does need not to cause immediate physical damage in order to produce relevant security consequences; it is sufficient to create a subjective perception of threat. In assessing the security environment, National Security Strategy of the Republic of Serbia recognizes the fact that "spreading false news and disinformation within the concept of hybrid and information warfare may have negative impact on the functioning of defence system elements" and therefore the strategic concept of Serbian defence system is based on the model of Total defence[1] (Republic of Serbia, 2019b, p. 2).

1 Serbia's experience with the concept of Total defence dates back to the time when it was part of a larger state, the Socialist Federal Republic of Yugoslavia (SFRY). A pivotal moment in the development of the Yugoslav concept of total defence was the intervention of Warsaw Pact forces in Czechoslovakia in 1968. This event significantly accelerated the

In the light of the fact that disinformation, as deliberately false information intended to cause harm (Wardle and Derakhshan, 2017), is addressed in European Union documents, to which Serbia aspires to accede, alongside hybrid threats, cyber-attacks and foreign information manipulation (European Union, 2022), it becomes clear why it is necessary to investigate its cognitive dimension in the context of the national security of Serbia. In addition, state borders do not represent an obstacle to the impact of (dis)information, given its ability to operate both within and beyond the country of origin.

In accordance with the previously stated, this paper aims to answer the following questions:

(1) What is the level of Serbian citizens' susceptibility to online disinformation?
(2) What are the perceptions of Serbian citizens regarding the media and information landscape, the prevalence of false and misleading information and the role of foreign actors in shaping media content?
(3) What are the implications of these findings for the development of cognitive resilience within the concept of Total defence and Serbia's national security?

2 Theoretical framework

The most appropriate theoretical framework for the analysis of societal resilience and total defence in the digital age comprises three social and security theories; social constructivism, network society theory, and securitization theory. All three theories achieved their full affirmation at the end of the 20th century and continued to be further developed and empirically validated in the 21st century, which makes them relevant today. Social constructivism should assist us in gaining a better understanding of *what is happening*, network society theory of *how it is happening*, and securitization theory of *what security implications these processes have*. Although the concepts of societal resilience and total defence belong to the domain of practical politics rather than to a theoretical framework in the strict sense, they play a practical and important role in understanding the cognitive dimension of disinformation within the context of national security.

The first theory is social constructivism, which implies that national security should not be viewed narrowly through institutional mechanisms and material resources, but more broadly, through rules, social norms, identities, and meanings. The creators of the theory, Berger and Luckmann, argue that "reality is socially constructed" (Berger and Luckmann, 1991, p. 13), while Nicholas Onuf, continuing this line of thought, writes that "people always construct, or constitute, social reality" (Onuf, 1989, p. 1). This means that social and political reality is not pre-established, but is constantly shaped through practice, language and interaction. Alexander Wendt speaks similarly when it comes to international relations (Wendt, 1999). Social constructivism is important for this topic because it shows that disinformation should be understood as an attempt to reshape meanings of threat, trust, legitimacy and collective identity, i.e., as an intervention directed to the very process of social construction of security reality.

Constructivist security studies start from the notion that security threats, interests and identities are determined by intersubjective meanings and social practices, rather than being merely the result of material factors (Farrell, 2002). In that sense, the cognitive dimension becomes a core element of modern security landscape, because it is the very domain in which perceptions of threat, trust and social cohesion are created and reproduced. The thesis is that different political systems, ideologies, religions and world views are determined by certain narratives (Kubálková et al., 1998). Wendt's analysis of identity and the perception of *self* and *other* additionally suggests that threats do not have fixed and objective meaning, but that they are understood based on the way they are socially interpreted (Wendt, 1992). Taking all that into consideration, it can be argued that disinformation in the digital age operates predominantly in cognitive and symbolic spheres, because it strives to subvert the existing norms, undermine trust in institutions, and change perceptions of threat, thereby exerting influence on national security. Applied to the Serbian context, this means that the narratives created by leading media in Serbia shape a perception of enemies and dangers, i.e., a sense of (in)security. Social constructivism speaks precisely to the fact that this sense need not necessarily be grounded in real facts and actual danger; it is sufficient to know how citizens perceive and predominantly understand these phenomena, processes and actors.

The second theory is network society theory, which provides an answer to how the cognitive dimension actually functions. It starts from the premise that modern society is not any longer predominantly organized through stable hierarchical relations and territorially limited institutions, but through digital networks and information flows. According to Castells, one of the principal theorists of network society, this form of social structure stems from the interaction between a new technological paradigm and social organization, whereby digital communication networks become its infrastructural backbone (Castells, 2005). Subsequently, this idea acquires broader social formulation, reflected in the assertion that networks constitute the new social structure (Castells, 2010). Thus, the mechanism of this order is not based solely on faster spreading of information, but on the fact that, thanks to their capacity for reconfiguration, global reach and networking logic, networks are becoming the dominant form of coordination of production, experience, power and culture (Castells, 2010; Castells, 2009). Through the network society theory, Castells explains the so-called *instant war*, that is, the characteristics of war which may be acceptable to that modern society. Such war is, inter alia, designed to be perceived as "clean," which is, in addition to the use of precision weaponry that reduces civilian casualties, achieved through media control of public opinion via selection of information and manipulation (Castells, 2010; Starčević and Milenković, 2023). Precisely for this reason, disinformation in network society does not operate solely as false content, but as an intervention aimed at influencing action, cohesion and the dynamics of the society itself. Those who control the flows, interfaces and communication codes, possess the ability to influence the societal perceptions of threat, trust, crisis, and security.

Research has shown that the internet is reshaping social relations toward networked individualism, i.e., it is shifting them

institutionalization of its own doctrine of General People's Defence and Social Self-Protection (ONO and DSZ) and strengthened the Yugoslav leadership's conviction that the defence of the country must rest on broad societal involvement and the capacity for prolonged resistance to a potential aggressor (Torkar and Polnar, 2023).

from closely related and clearly delineated groups to looser, more flexible and partially bounded networks which enable intensive and frequent communication. Broadband and continuous connectivity, personalization and global reach enable the communication to be directed to an individual (Wellman et al., 2003). According to van Dijk, network society is an infrastructure of social and media networks at all levels; however, those networks are becoming increasingly coded, selective, and exclusionary, while their vulnerability is not only technical but also deeply social, because dependence on networks can produce new inequalities, marginalization, and systemic instability (van Dijk, 2006). For the topic of societal resilience and total defence, this is of the utmost importance, because in the digital age, resilience is not only a matter of the protection of infrastructure or refuting individual falsehoods, but also the capacity of society to preserve reliable communication channels, trust in institutions, a shared worldview, and a shared understanding of its surroundings.

Contemporary security studies have gradually shifted their focus from exclusively state-centric understanding of security, in which the main threats were military and interstate in nature, towards a broader understanding in which political, social, economic and information phenomena can be presented as security issues if they are articulated as threats to survival of a particular reference object (Buzan et al., 1998). This brings us to the third theory—theory of securitization, which is founded on the thesis that the security is principally a "speech act," i.e. that an issue is introduced into the field of security once an authorized actor presents it as an existential threat and the audience accepts it as such, thereby creating space for the implementation of emergency measures (Wæver, 1995; Buzan et al., 1998). For the topic of this work it is important to point out that disinformation is not a security issue in itself, but becomes one when it is recognized as a threat to societal stability, the maintenance of trust, and the functioning of institutions. In contemporary environment, information warfare is increasingly acquiring a form of a race for domination of the information landscape, whereby important goals are directed not only at information sources but also at shifting the way of thinking and behavior of an opposing party (Miljković, 2025). Disinformation and propaganda become particularly relevant for the national security when they precede or accompany a broader strategy of coercion, destabilization and an escalation of a latent conflict, as demonstrated in the case of the Russia-Ukraine war, in which information operation was recognized as an important element in the preparation for the armed conflict itself (Vuletić and Milenković, 2023).

As noted earlier, disinformation is characterized by the presence of deliberate intent to deceive, distinguishing it from misinformation, which refers to false content lacking such intent (Wardle and Derakhshan, 2017). Tsang (2026) argues that authorial intent should not be the primary basis for classifying false information and instead proposes a typology grounded in how content is constructed—distinguishing fabrication and manipulation, which typically involve deliberate deception, from misinterpretation and the provision of incomplete information, which may result from honest error rather than malicious intent. Damage caused by disinformation most often occurs in the form of deception, manipulative or biased content and negative impact on public opinion (Lazer et al., 2018). It is also important to note that disinformation in practice is not easily discerned; it often takes the form of partially accurate, contextually manipulated or strategically conceived deceiving content, which further complicates its recognition and verification (Wardle and Derakhshan, 2017; Broda and Strömbäck, 2024).

For that very reason, the empirical part of this work is not limited to disinformation in the strict sense, but it encompasses the broader phenomenon of false and misleading information, that is, content whose intent may not always be verified, but whose impact on the public opinion, trust in institutions and citizens' perception of security is equally detrimental.

3 Findings from previous research in Serbia and the region

Within implementation of Serbia's Media Strategy, officially entitled Strategy for the Development of the Public Information System in the Republic of Serbia for the period 2020–2025 (Government of the Republic of Serbia, 2020), a study was conducted with the support of the OSCE Mission to Serbia and the European Union. The research was conducted in 2025 via telephone survey, on a two-stage stratified representative sample of 800 respondents aged 18–75, with a particular focus on the critical dimension of media literacy and on how citizens use media, verify information, and recognize harmful content (Matović et al., 2025). Research findings show that television still dominates in Serbia and it is watched by 96.7% of the respondents; it is followed by different messaging applications, used by 81.5% and radio with 66.3%, while social media are consumed by 57.5% of the respondents. At the same time, 77.4% of the respondents stated that they do not read print media and 43.5% do not follow any online information portals. For the topic of cognitive resilience, the findings that 27.6% of the respondents rarely or never recognize false news, 51.5% do not recognize conspiracy theories, and 71.9% never identify AI-generated content are particularly important. Additionally, 68.6% of respondents often or on a daily basis feel overwhelmed by media content, while 58.3% are often exposed to content which triggers strong negative emotions. Regarding information checking, almost half of the respondents (47.9%) rarely or never cross-check information across different sources, 65.8% rarely or never read post comments, while 90.3% rarely or never use fact-checking sites (Matović et al., 2025). It is particularly telling that respondents most often verify the truthfulness of news with "someone they know" (89.7%), and cite friends, relatives, and colleagues as the most reliable source of information (68.5%), while the confidence in institutional media is significantly lower; for instance—36.9% of respondents trust television, 11.7% online portals and only 3.7% print media (Matović et al., 2025).

A recent study, conducted in 2026 by the Center for Free Elections and Democracy (CeSID)[2] in cooperation with Regulatory Authority for Electronic Media (REM),[3] was published in the Report

2 The Center for Free Elections and Democracy (CeSID) is a Serbian non-governmental and non-partisan organization, founded in 1997 in Belgrade. Its main areas of activity include monitoring electoral processes, procedures and campaigns, as well as legislation, training observers, and conducting public opinion research (CeSID, 2026a).

3 The Regulatory Authority for Electronic Media (REM) is an independent

on Media User Preferences in Serbia. It was carried out within the project Protecting Freedom of Expression and of the media in Serbia (PROFREX), supported by the European Union and the Council of Europe. The quantitative part was conducted through face-to-face interviews on a random representative sample of 1,000 adult citizens, while the qualitative part encompassed three online focus groups with 22 participants (young people, older adults, and members of national minorities), providing both insights into statistical trends and explanations for them (CeSID, 2026b). This research showed that citizens spend, on average, on a daily basis, 144 min watching television, 113 min listening to the radio, around 102 min on social networks and 68 min following information portals, which indicates a parallel coexistence of digitization and the enduring power of the television format. Data on trust are particularly important: television stations with national broadcasting licences enjoy 28% trust, but also 39% distrust, which is clearly indicative of polarization; internet portals have only 16% trust, while social media receive even lower ratings, depending on the platform. At the same time, more than two-thirds of respondents believe that propaganda, fake news, disinformation, and spin are present in domestic media, while 67% of respondents consider television the dominant source of such content (CeSID, 2026b). Regarding trust, the qualitative part of the research shows that all surveyed groups express a high level of skepticism, but distribute it differently: young people place greater confidence in "what they see," for instance videos, live streams, and investigative journalism; older people still attribute a minimum level of institutional responsibility to traditional media; and members of minority groups seek reliable and linguistically accessible local sources. In the chapter on harmful content, participants from all groups state that they are faced with disinformation, hate speech and propaganda, almost on a daily basis. Older adults particularly point to national television channels and tabloids, while younger people highlight social media comments and manipulation in show-based formats; members of minority groups highlight local instances of sensationalism and panic in connection with socially sensitive topics (CeSID, 2026b).

These national-level findings should also be situated within a broader regional pattern. Disinformation has been identified as a constant feature of politics throughout the Western Balkans, including Serbia, with research suggesting that it functions primarily as a symptom, rather than the cause, of deeper breakdowns in social cohesion and democratic governance (Greene et al., 2021). Research further suggests that in political environments characterized by limited political competition and pronounced polarization, disinformation may disproportionately reflect and reinforce dominant political narratives (Greene et al., 2021). This pattern is consistent with the domestic findings on cognitive vulnerability and weak information-verification habits and practices reported above (Matović et al., 2025; CeSID, 2026b).

regulatory body established by law, which exercises public authority in Serbia in the field of electronic media, primarily television, radio and other audiovisual media services. Under the Serbian Law on Electronic Media, REM's tasks include, among other things, analyzing the media market and contributing to the protection of media pluralism, freedom of expression, the public interest, and the rights of media service users (Regulatory Authority for Electronic Media (REM), 2026).

4 Empirical research on misinformation susceptibility and perceptions of the media information environment in Serbia

4.1 Research design and sample characteristics

A cross-sectional survey design was employed to examine participants' susceptibility to online misinformation and their perceptions of the media information environment. This study included a total sample of $N = 202$ adult participants; 57.9% identified as female and 42.1% as male. Participants' ages ranged from 18 to 69 years, with a mean age of $M = 37.7$ ($SD = 11.7$). Regarding educational level, the majority of the sample held a university degree, with 57.4% ($n = 116$) had completed graduate or master's studies and 25.7% ($n = 52$) of participants had completed secondary education. The remaining participants were equally distributed between those with a doctoral degree or specialization (8.4%, $n = 17$) and those with a higher vocational school degree (8.4%, $n = 17$).

Prior to data analysis, specific inclusion criteria were applied to ensure the relevance of the data: only individuals who reported maintaining active profiles on social media platforms were included in the final sample. This criterion was considered essential, as online platforms serve as the primary environments in which users encounter news from both official media outlets and various unofficial sources. Consequently, all participants who did not meet this requirement were excluded from the study.

4.2 Data collection instruments

4.2.1 Online misinformation susceptibility scale

To assess participants' susceptibility to online misinformation, the Online Misinformation Susceptibility Scale (OMISS) was utilized (Katsiroumpa et al., 2025a). The OMISS was selected because the central concern of this study is not whether participants possess factual knowledge about disinformation, but rather how they habitually behave when encountering (dis)information in online environments. Unlike measures of factual knowledge about misinformation, the OMISS captures general behavioral tendencies related to evaluation of online content; the scale consists of nine items, measuring how frequently individuals critically evaluate online content encountered on social media or websites. Each item is rated on a five-point Likert scale, ranging from 1 (*always*) to 5 (*never*), with higher total scores indicating greater susceptibility to online misinformation. Total scores range from 9 to 45, and authors propose that the participants scoring ≥ 23 are classified as having high misinformation susceptibility (Katsiroumpa et al., 2025b). In the present study, internal consistency of the instrument was 0.87 Cronbach α. The OMISS has been proposed as valid measure, applicable across multiple domains in which online misinformation poses a significant challenge, including healthcare, news media, politics, and science (Katsiroumpa et al., 2025a). Behavioral tendencies—such as whether individuals verify sources, cross-check information, or critically evaluate online content—are more directly relevant to the security implications examined in

this paper than declarative knowledge about the phenomenon itself.

4.2.2 Perceived media information environment questionnaire

Participants' perceptions of and attitudes toward the media information environment were assessed using the Perceived Media Information Environment Questionnaire (PMIEQ), developed for the purposes of this study. The questionnaire consists of 11 items covering five conceptually related domains: (1) perceived reliability and credibility of news on digital platforms; (2) self-reported exposure to suspected false or misleading information; (3) perceived prevalence of disinformation across different media sources and different areas; (4) attitudes toward geopolitical determinants of media reporting, and (5) views on responsibility for and institutional responses to the spread of false and misleading information. In line with the rationale outlined in the theoretical framework, the questionnaire deliberately employs the formulation "false and misleading information" rather than "disinformation" specifically, in order to minimize response bias associated with the intentionality connotations of the latter term. Items employ categorical response formats tailored to each construct, including four-point Likert-type scales, frequency scales, and nominal response options. Content validity was established through expert review, confirming that the items adequately represent the theoretical domains that the questionnaire was designed to assess and measure. The questionnaire was designed and administered in Serbian language. English translations of item wording are provided in the Results section.

4.2.3 Sociodemographic questionnaire

A brief sociodemographic questionnaire was administered to collect background information on participants, including gender, age, educational level and social media use.

4.3 Conducting the empirical research

The study was conducted by the paper authors as part of the "Assumptions of the Optimal Implementation of the Total Defence Concept in the Republic of Serbia" project, which is implemented by the Institute for Strategic Research of the University of Defence in Belgrade. Participants were recruited from across the entire territory of the Republic of Serbia. Data collection took place during April 2026, via an online survey platform (Google Forms). To reach a diverse range of respondents, a convenience sampling strategy was employed, further supplemented by a snowball technique, using various social media platforms and professional networks. Participants were encouraged to share the survey within their own networks to ensure that populations from different Serbian regions were represented. The study was conducted in accordance with ethical standards, which required all participants to provide informed consent before accessing the research instruments. All instruments were administered consecutively within a single online session. Participation was voluntary and unpaid, and participants were informed that they could withdraw from the study at any time without consequence. Given the anonymous and non-mandatory nature of the survey, the absence of any personally identifiable or sensitive information, and the minimal-risk nature of the research involving the general adult population, the study presented no ethical risks warranting formal committee approval.

4.4 Data analysis procedure

Data were analyzed using IBM SPSS Statistics 25. Descriptive statistics were computed for all study variables; frequencies and percentages were calculated for categorical variables, while means and standard deviations were computed for continuous variables. Given the exploratory nature of the study, the analysis was intentionally limited to descriptive statistics, with the aim of providing an initial overview of the research problem, complemented by a preliminary correlation analysis to examine key sociodemographic relationships. Internal consistency of the OMISS was assessed using Cronbach's alpha coefficient.

5 Empirical findings and statistical analysis

The results are presented in two sections. First, findings from the OMISS are reported, providing an initial baseline of individual susceptibility to online misinformation within our sample. These results are followed by participants' perceptions of the broader media information environment, providing context for understanding how individual susceptibility is situated within the wider informational landscape that participants encounter in their daily lives.

As shown in Table 1, OMISS total scores ranged from 9 to 45 ($M = 25.48$, $SD = 7.17$), with the average participant scoring above the established cut-off value of 23. Accordingly, the majority of participants (60.9%, $n = 123$) were classified as having high susceptibility to misinformation.

As shown in Table 2, no statistically significant correlation was found between OMISS scores and age, ($\rho = 0.027$, $p = 0.706$), suggesting that susceptibility to misinformation was not significantly

TABLE 1 Descriptive statistics and susceptibility classification for the Online Misinformation Susceptibility Scale (OMISS).

OMISS total score	n	%	M	SD	Min	Max
	202	100.0	25.48	7.17	9	45
Susceptibility classification						
Low susceptibility (OMISS_total < 23)	79	39.1				
High susceptibility (OMISS_total ≥23)	123	60.9				

Susceptibility classification is based on the proposed cut-off score of 23 (Katsiroumpa et al., 2025b).

associated with age within the present sample. In contrast, a weak but statistically significant negative correlation was found between OMISS scores and educational level ($\rho = -0.172$, $p = 0.014$), indicating that higher education was associated with somewhat lower susceptibility to misinformation.

The majority of respondents expressed skepticism toward news published on digital platforms, with 70.3% rating such content as reliable only to a lesser extent. A smaller proportion considered digital news either largely reliable (14.4%) or not reliable at all (14.4%), while only 1.0% viewed it as completely reliable. These findings suggest a generally cautious attitude toward online news among the sampled population (Table 3).

As shown in Table 4, the majority of respondents (42.6%) reported encountering information on digital platforms suspected to be false and misleading several times a week ("Often"). The second largest group consisted of participants who noticed such information once a week ("Occasionally"), accounting for 31.7% ($n = 64$) of the sample. The smallest proportion of the sample (9.4%) reported rarely encountering suspected false or misleading information.

When asked whether they consider false and misleading information to have the power to threaten national security, the largest proportion of respondents (40.6%) indicated that it does so to a greater extent (Table 5). Additionally, nearly a quarter of the sample (24.8%, $n = 50$) stated that false and misleading information threatens national security completely or to a critical extent. In contrast, 31.7% of the participants felt that this threat exists only to a lesser extent, while a minimal proportion of the sample (3.0%, $n = 6$) reported that false and misleading information does not threaten national security at all.

Respondents were asked to assess the extent to which media ownership and foreign and international actors exert greater influence over reporting than professional ethics. With regard to media ownership, responses were strongly skewed toward agreement: nearly half of the respondents completely agreed with this view, and an additional 38.6% agreed to a greater extent, with only 12.9% expressing any degree of disagreement. Perceptions of the influence of foreign and international actors were more moderate, with responses more evenly distributed across categories. Although a combined majority agreed that such actors exert greater influence than professional ethics, the largest single group agreed only to a lesser extent, and complete disagreement remained minimal (Table 6).

Table 7 and Figure 1 represent respondents' perceptions of false and misleading news across six different types of media sources.

For *public service media*, responses are relatively evenly distributed across the moderate, substantial, and high categories, with the largest single proportion of respondents estimating the share of false and misleading news to be substantial. Specifically, 22.3% of respondents estimated that 41–60% of the news shared by public service media is false or misleading.

Pro-regime media received the highest predominant ratings across all media sources, with 36.6% of respondents estimating that between 81 and 100% of its informative content are false and misleading information. An additional 9.4% placed it in the high category (61–80%), while 18.3% in the substantial category (41–60%). Only 13.4% of respondents estimated a minimal proportion of false news (1–20%) in pro-regime media, while 4.0% perceived none.

For *pro-opposition media*, 6.4% of respondents estimated that between 81 and 100% of its content consists of false and misleading news, while 9.4% placed it in the high category (61–80%). The largest proportion of respondents assigned it a substantial rating (33.2%), followed by moderate (28.7%) and minimal (20.8%) categories. Only 1.5% of respondents perceived no false news coming from this source.

TABLE 2 Correlations between OMISS total score and age and educational level of respondents (*N = 202*).

Variable	Spearman correlation	
	r	*p*
Age	0.027	0.706
Education level	−0.172	**0.014***

Spearman's rank correlation coefficient was used for both variables, given the ordinal nature of the education variable and the borderline distributional normality of the OMISS total score. r denotes Spearman's rho (ρ). *Correlation is significant at the $p < 0.05$ level (2-tailed).

TABLE 3 Respondents' assessments of the reliability and credibility of news published on digital platforms.

Response	n (%)
Not reliable at all	29 (14.4%)
Reliable to a lesser extent	142 (70.3%)
Reliable to a greater extent	29 (14.4%)
Completely reliable	2 (1.0%)

TABLE 4 Perception of encountering suspected false or misleading information on digital platforms in the past month.

Response	n (%)
Rarely (once or twice)	19 (9.4%)
Occasionally (once a week)	64 (31.7%)
Often (several times a week)	86 (42.6%)
Every day	33 (16.3%)

TABLE 5 Respondents' views on whether false and misleading information has the power to threaten national security.

Response	n (%)
Not at all	6 (3.0%)
To a lesser extent	64 (31.7%)
To a greater extent	82 (40.6%)
Completely (to a critical extent)	50 (24.8%)

TABLE 6 Respondents' views on media ownership and the influence of foreign and international actors on media reporting.

Response	Media owner	Foreign and international actors
	n (%)	n (%)
Strongly disagree	10 (5.0%)	13 (6.4%)
Agree to a lesser extent	16 (7.9%)	75 (37.1%)
Agree to a greater extent	78 (38.6%)	73 (36.1%)
Completely agree	98 (48.5%)	41 (20.3%)

The perceptions of *foreign media and independent analysts* showed very similar patterns, with both distributions peaking in the moderate category (21–40%). Specifically, 34.2% of respondents attribute a moderate share of false news to foreign media, while 33.7% do the same for independent analysts. For both sources, only a small proportion of respondents perceive the presence of misleading news to be predominant (3.5 and 2.5%, respectively).

For *influencers and public figures*, 12.4% of respondents estimated that between 81 and 100% of their content consists of false and misleading news, and 19.3% placed them in the high category (61–80%). The moderate category received the largest proportion (25.7%), followed by substantial (22.3%) and minimal (17.8%). Only 2.5% of respondents perceived no false news in content produced by influencers and public figures (Table 7; Figure 1).

Table 8 and Figure 2 presents the respondents' perceptions regarding the prevalence of false and misleading news across seven distinct thematic areas. The findings reveal contrasting patterns in the perceived prevalence of misinformation depending on the topic in question.

A high perceived prevalence of misinformation is evident in domains related to politics and security. For *domestic politics*, the distribution is concentrated toward the highest levels of presence, with nearly half of the sample (47.0%) perceiving false and misleading news to be present to an extremely large or dominant extent, and an additional 39.1% reporting it to a greater extent.

Similar distributions are observed for *international politics and security* and *national security*, where the largest proportion of respondents indicated that misinformation is present to a greater extent (50.5 and 49.5%, respectively), while approximately a quarter of the sample perceived it as dominant (25.2 and 26.7%, respectively). In all three domains, fewer than 2.0% of participants reported that false and misleading news was not present.

The domain of *economy and finance* also followed a high-prevalence pattern, with 42.1% of participants reporting the presence of misleading information to a greater extent and 32.7% identifying it as dominant.

More moderate perception of misinformation is observed in the areas of *health* and *science and technology*. In the health domain, responses were nearly equally distributed between the lower and higher categories, with 40.1% reporting the presence of false and misleading news to a lesser extent and 38.1% reporting it to a greater extent. Meanwhile, the distribution for science and technology was concentrated around the lower-middle spectrum, with a clear majority of respondents (64.4%) stating that misleading news was

TABLE 7 Respondents' perceptions of false and misleading news across different media sources.

Media source	Perception of false and misleading news (n/%)					
	None	Minimal	Moderate	Substantial	High	Predominant
Public service	10 (5.0%)	43 (21.3%)	44 (21.8%)	45 (22.3%)	32 (15.8%)	28 (13.9%)
Pro-regime media	8 (4.0%)	27 (13.4%)	37 (18.3%)	37 (18.3%)	19 (9.4%)	74 (36.6%)
Pro-opposition media	3 (1.5%)	42 (20.8%)	58 (28.7%)	67 (33.2%)	19 (9.4%)	13 (6.4%)
Foreign media	5 (2.5%)	58 (28.7%)	69 (34.2%)	43 (21.3%)	20 (9.9%)	7 (3.5%)
Independent analysts	12 (5.9%)	56 (27.7%)	68 (33.7%)	41 (20.3%)	20 (9.9%)	5 (2.5%)
Influencers / public figures	5 (2.5%)	36 (17.8%)	52 (25.7%)	45 (22.3%)	39 (19.3%)	25 (12.4%)

Values represent the percentage of respondents (%) who assigned each rating category to the respective media source. Response categories reflect respondents' estimated proportion of false and misleading news within each source: None (0%), Minimal (1–20%), Moderate (21–40%), Substantial (41–60%), High (61–80%), Predominant (81–100%); total $N = 202$. Visual representation of data is shown in Figure 1.

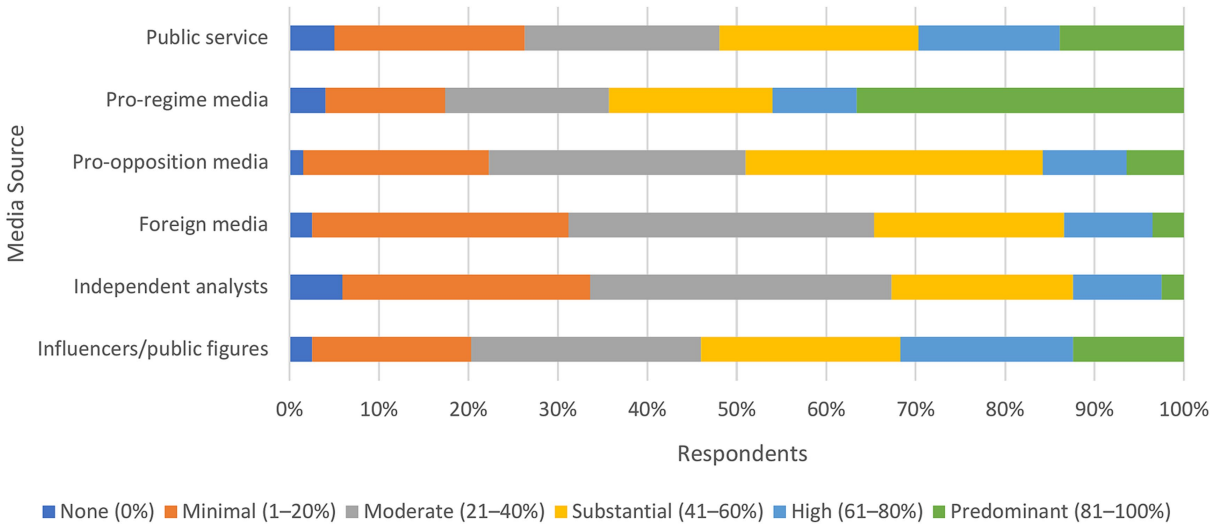


FIGURE 1
Visual overview of the distribution of perceptions of false and misleading news by media source.

present only to a lesser extent, while only 2.5% perceived it as dominant.

Finally, *sports* domain stood out as the thematic area perceived to be least affected by misinformation. The largest group of respondents reported that false and misleading news is present only to a lesser extent (43.1%), closely followed by 41.1% of the sample who stated that it is not present at all.

Table 9 and Figure 3 represent respondents' perceptions of the extent to which Serbian media are used as platforms for promoting the interests of foreign actors.

Respondents expressed moderate concern regarding *NATO's* influence, with 38.6% estimating that Serbian media promote NATO interests to a greater extent, and 17.3% to an extremely large extent. However, 36.1% perceived this influence to be present only to a lesser extent, while 7.9% perceived none at all.

Next, the *EU* received somewhat higher ratings, with 43.1% of respondents estimating that Serbian media promote EU interests to a greater extent, and 24.8% to an extremely large extent. Only 3.0% perceived no such influence.

Perceptions of *US* influence followed a similar pattern, with 45.5% of respondents estimating that Serbian media promote US interests to a greater extent, and 20.8% to an extremely large extent. Only 4.0% perceived no such influence.

China received one of the highest ratings, with 47.0% of respondents estimating that Serbian media promote Chinese interests to a greater extent, and 27.7% to an extremely large extent. Only 2.5% perceived no such influence, indicating a relatively high perceived level of Chinese media presence.

Russia received the highest proportion of extremely large extent category across all foreign actors, with 35.6% of respondents placing it in this category. An additional 43.6% estimated Russian influence to be present to a greater extent, while only 2.5% perceived no such influence at all. This made Russia the foreign actor most frequently perceived as having an influence on Serbian media.

In contrast, *Turkey* received somewhat different ratings compared with other foreign actors. The largest proportion of respondents estimated its influence to be present only to a lesser extent (46.0%), while 21.8% perceived no influence at all. Only 7.9% rated Turkish influence as extremely large, suggesting that respondents perceived Serbian media as substantially less oriented toward promoting Turkish interests (Table 10).

Finally, *regional states*, referring to neighboring countries, received moderate ratings, with 42.1% of respondents estimating their influence to a lesser extent and 17.3% perceiving no influence at all. Only 10.4% rated their influence as extremely large.

The largest proportion of respondents attributed primary responsibility for preventing the spread of false and misleading information to the state and its institutions (40.6%), followed by media editors (26.2%) and journalists or individuals who publish such content (22.8%). Educational institutions were considered the least responsible (2.0%), while only 8.4% of respondents attributed primary responsibility on consumers themselves.

The majority of respondents expressed support for the establishment of an official state body responsible for identifying and exposing false and misleading news. Specifically, 50% completely agreed with this statement, while an additional 27.2% agreed to a greater extent, indicating that a combined 77.2% of respondents expressed a high or complete level of agreement with this proposition. Only 19.3% agreed to a lesser extent, while 3.5% completely disagreed (Table 11).

6 Interpretation of the empirical findings in the context of Serbia's national security

The present study aimed to examine Serbian citizens' susceptibility to online misinformation and their perceptions of the broader media information environment within the context of societal resilience and national security. The following section discusses the findings in relation to the three research questions outlined in the introduction, the theoretical framework, existing empirical evidence, and their implications for national security policy and the development of cognitive resilience in Serbia.

The results obtained using the Online Misinformation Susceptibility Scale (OMISS) indicate a relatively high level of susceptibility to online disinformation in the present sample, given the fact that majority of the respondents (60.9%) were classified into the

TABLE 8 Respondents' perception of the prevalence of false and misleading news across thematic areas.

Thematic area	Perception of prevalence of false and misleading news across thematic areas (n/%)			
	Not present	Present to a lesser extent	Present to a greater extent	Present to an extremely large extent (dominant)
International politics and security	4 (2.0%)	45 (22.3%)	102 (50.5%)	51 (25.2%)
Domestic politics	1 (0.5%)	27 (13.4%)	79 (39.1%)	95 (47.0%)
National security	4 (2.0%)	44 (21.8%)	100 (49.5%)	54 (26.7%)
Economy and finance	1 (0.5%)	50 (24.8%)	85 (42.1%)	66 (32.7%)
Science and technology	34 (16.8%)	130 (64.4%)	33 (16.3%)	5 (2.5%)
Health	9 (4.5%)	81 (40.1%)	77 (38.1%)	35 (17.3%)
Sports	83 (41.1%)	87 (43.1%)	24 (11.9%)	8 (4.0%)

Values represent the percentage of respondents (%) who assigned each rating to the respective thematic area ($N = 202$). Response categories reflect respondents' subjective assessment of the extent to which false and misleading news are present in each area, ranging from "Not present" to "Present to an extremely large extent (dominant)." Percentages sum to 100% for each area; total $N = 202$. Visual representation of data is shown in Figure 2.

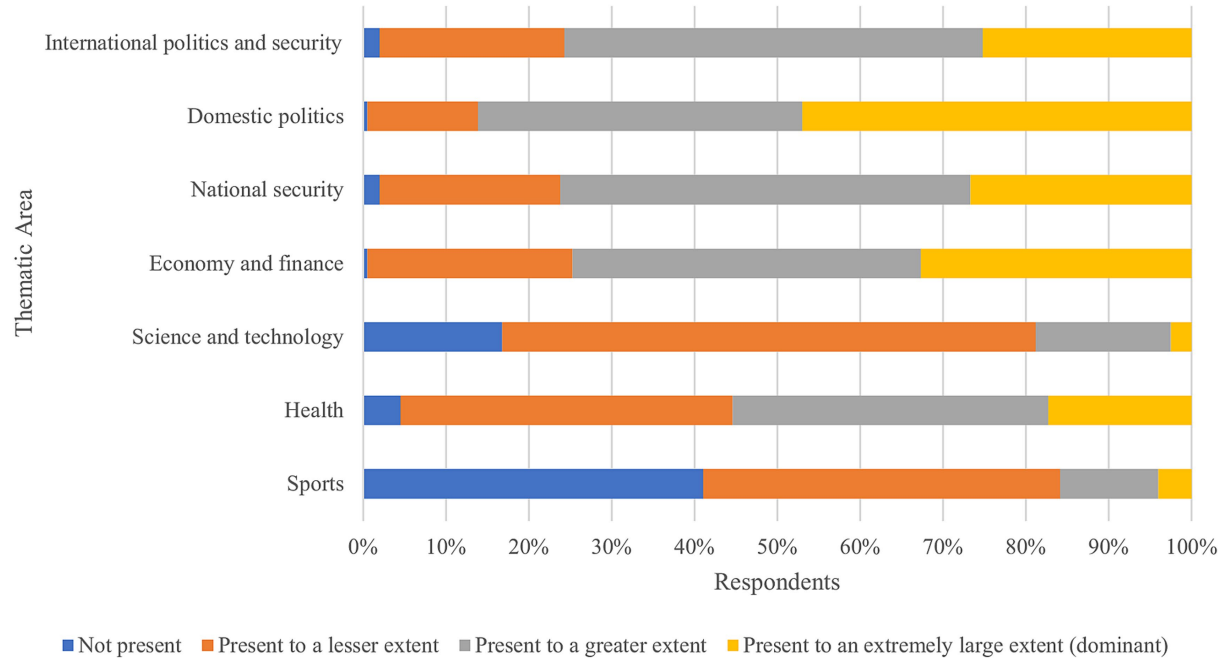


FIGURE 2
Visual overview of the distribution of respondents' perceptions of false and misleading news prevalence across thematic areas.

TABLE 9 Respondents' perceptions of the extent to which Serbian media are used as platforms for promoting foreign interests.

Foreign interest	Perceived extent of foreign influence			
	Not at all	To a lesser extent	To a greater extent	To an extremely large extent
NATO	16 (7.9%)	73 (36.1%)	78 (38.6%)	35 (17.3%)
EU	6 (3.0%)	59 (29.2%)	87 (43.1%)	50 (24.8%)
USA	8 (4.0%)	60 (29.7%)	92 (45.5%)	42 (20.8%)
China	5 (2.5%)	46 (22.8%)	95 (47.0%)	56 (27.7%)
Russia	5 (2.5%)	37 (18.3%)	88 (43.6%)	72 (35.6%)
Turkey	44 (21.8%)	93 (46.0%)	49 (24.3%)	16 (7.9%)
Regional states	35 (17.3%)	85 (42.1%)	61 (30.2%)	21 (10.4%)

Values represent the percentage of respondents (%) who assigned each rating to the respective foreign interest ($N = 202$). Response categories reflect respondents' subjective assessment of the extent to which Serbian media are used as platforms for promoting foreign interests, ranging from "Not at all" to "To an extremely large extent." Percentages sum to 100% for each foreign interest; total N = 202. Visual representation of data is shown in Figure 3.

category of high susceptibility. These findings are particularly significant due to the fact that OMISS does not measure respondents' factual knowledge of disinformation, but rather their general cognitive and behavioral habits when evaluating and verifying digital content. This does not necessarily mean that the respondents are unable to recognize inaccurate information; rather, it suggests that substantial proportion of them do not apply mechanisms for critical evaluation, analytical questioning, and content verification often enough when encountering online content. This finding is particularly interesting given the educational structure of our sample, which largely consisted of respondents with higher or postgraduate education.

Our data support, to some extent, the thesis that susceptibility to misinformation is not solely a consequence of a lower educational level. This interpretation is further supported by correlational analysis: no statistically significant correlation was found between OMISS scores and age ($\rho = 0.027$, $p = 0.706$), whereas a weak but statistically significant negative correlation was found between OMISS scores and educational level ($\rho = -0.172$, $p = 0.014$). Given the weak strength of this association, higher education level appears to provide only limited protective effect against susceptibility to misinformation. This finding is consistent with the observation that the majority of respondents in this predominantly highly-educated sample were nonetheless classified as highly susceptible. Although formal education may contribute to the development of critical thinking skills, research suggests that even highly educated individuals can be influenced by factors such as the objective tone of online content and the professional appearance of internet websites, which may obscure the absence of adequate sources or supporting evidence for the information they publish (Sultan et al., 2024; Breakstone et al., 2022).

Although the aforementioned correlations (weak for educational level and non-significant for age) should not be overinterpreted as

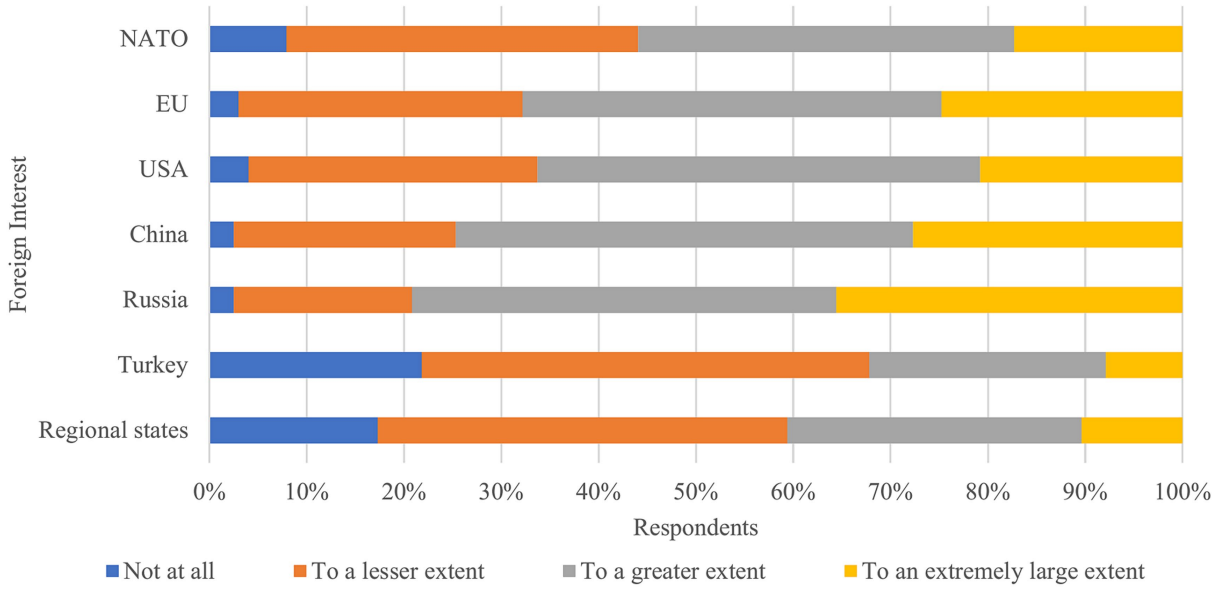


FIGURE 3
Visual overview of the distribution of respondents' perceptions of the extent to which Serbian media are used as platforms for promoting foreign interests.

TABLE 10 Respondents' views on who bears the greatest responsibility for preventing the spread of false and misleading information.

Response	n (%)
The state and its institutions	82 (40.6%)
People who consume them	17 (8.4%)
Journalists / individuals who publish them	46 (22.8%)
Educational institutions	4 (2.0%)
Media editors	53 (26.2%)

TABLE 11 Respondents' agreement with the statement that an official state body should be responsible for identifying and exposing false and misleading news.

Response	n (%)
Completely disagree	7 (3.5%)
Agree to a lesser extent	39 (19.3%)
Agree to a greater extent	55 (27.2%)
Completely agree	101 (50.0%)

evidence of widespread cognitive vulnerability, the observed pattern may still be relevant to consider in a broader societal context. From a national security perspective, this behavioral tendency among respondents may represent a relevant vulnerability; namely, if individuals do not develop consistent habits of verifying information encountered in their online environments, this may facilitate the dissemination of disinformation campaigns and influence operations (Deppe, 2023). This issue is particularly relevant in the context of contemporary hybrid conflicts, in which information operations may precede or accompany broader political, security, and geopolitical processes (Hoffman, 2007; Mitrović, 2018; Dov Bachmann et al., 2023). With regard to the respondents' perception of the reliability and accuracy of the news to which they are exposed, the results show that substantial majority (84.7%) perceived such news as credible only to a lesser extent or not credible at all. This finding is consistent with previous research indicating relatively low levels of trust in the media in Serbia (Matović et al., 2025; CeSID, 2026b). This pattern may be understood through the concept of a "distrust mindset," a cognitive orientation characterized by a tendency to spontaneously consider alternative explanations rather than accepting information at face value. While such a mindset can act as a safeguard against uncritical acceptance of misinformation, it may paradoxically also lead individuals to embrace alternative and potentially false narratives (Mayo, 2024). In other words, heightened skepticism toward established information sources coexists with, and may even facilitate, greater openness to unverified or alternative claims. At the same time, more than a half of the respondents (58.9%) state that they encounter suspicious or deceiving information several times a week or every day. These finding indicate that respondents are functioning in the media landscape which they perceive as highly risky, informationally unstable and potentially manipulative. However, it is important to remark that low trust in digital content does not necessarily imply higher resilience to disinformation. Recent research suggests that high exposure to false news erodes general trust in news and fuels overconfidence in to discern truth from falsehood, without actually improving accuracy in distinguishing between the two (Altay et al., 2025). Accordingly, the continuous exposure to suspicious information reported by respondents in the present sample, even when they are aware of its potential unreliability, may be interpreted as a contributor to informational fatigue, and a weakened ability to distinguish credible from untrustworthy sources, rather than to greater resilience against disinformation.

It is encouraging that a majority of respondents are aware of the connection between disinformation and national security. More than two thirds of the respondents (65.4%) believe that false and misleading information threaten national security to a greater, critical, or complete extent. This finding is consistent with broader international

trends: a cross-national survey conducted by Pew Research Center found that a median of 72% of adults across 25 countries considered the spread of false information online a major threat to their country (Pew Research Center, 2025). This finding suggests that respondents do not perceive disinformation merely as an issue of media ethics or inaccurate reporting, but also as a phenomenon which they associate with broader social, political and security consequences. This interpretation is consistent with the theory of securitization, insofar as a substantial proportion of respondents recognize high exposure to false and misleading information as a potential security problem capable of affecting national security.

According to respondents' perceptions, the editorial policy in Serbian media is not primarily guided by professional ethical standards, but is influenced by the interests and positions of media owners, as well as by foreign and international actors. A vast majority of the respondents believed that media owners have a greater influence on editorial policy and media content than professional ethics (87.1%), whereby almost half of the respondents (48.5%) expressing complete agreement with this statement. The perceived influence of media owners may be associated with political and economic interests, including the indirect influence of political actors and concentrated economic capital. The observed distribution of responses appears consistent with an information environment in which private and political interests may at times prevail over journalistic ethics, potentially reflecting broader challenges to media social responsibility. This is consistent with the political economy of communications, whereby corporate control over key communication channels shapes a value system that prioritizes commercial and entertainment content over public accountability (Kljajić, 2023). In this context, Bennett and Uldam (2024) warn that a media system subordinated to the interests of owners creates structural vulnerability across the entire information ecosystem, leaving it susceptible to external pressures and the strategic dissemination of disinformation.

At the same time, most respondents believed that both foreign and international actors have an important influence on media reporting in Serbia (56.4%), while 20.3% of respondents completely agreed with that statement. These perceptions may partly reflect Serbia's specific geopolitical position in the central Balkans, situated at the crossroads of different political, economic, and security interests of global and regional actors. Within Serbian public discourse, the media landscape has long been perceived as an arena of competing influences from the East and the West, which is further intensified by global geopolitical tensions and the increasing use of information and hybrid operations. As Vučković and Radeljić (2024) argue, Serbia functions as a small state balancing between competing geostrategic realms without committing definitively to either side, an approach that leaves it vulnerable to being perceived as unreliable by both East and West. This issue is particularly relevant in the context of Serbia's military neutrality amid the largest armed conflict in Europe since the Second World War. Under such circumstances, maintaining a position of neutrality can become increasingly difficult when competing sides exert pressure not to remain uninvolved, but to take sides.

The findings concerning respondents' perceptions of false and misleading news across different media sources reveal two important elements with potential implications for national security. First, they support the previously discussed perception that all types of media are viewed as potential spaces for the dissemination of false and misleading news. Second, the findings indicate a pronounced perception of political polarization within the Serbian media environment. Respondents express the highest level of distrust toward pro-regime media, with slightly more than a third (36.6%) believing that false and misleading news is present to a dominant extent, while an additional 27.7% assessed its presence as high or substantial. At the same time, pro-opposition media were not perceived as the space without manipulative content either: more than 40% of respondents believed that the level of misleading news in these media was substantial or high. The distribution of our results is broadly consistent with recent empirical results on asymmetries in reporting within the Serbian media environment. The research showed that there is a significant difference in the reporting of the so-called "pro-regime" and "opposition" media, which is reflected in the way of reporting on current events (Džunić and Golubović, 2026). According to the Fragile States Index (FSI), Serbia has traditionally received a relatively unfavorable score on the Factionalized Elites indicator, which concerns societal cohesion—that is, divisions among social and political elites, among which political divisions tend to dominate (The Fund for Peace, 2024). These circumstances may have implications for societal resilience and the implementation of the concept of Total defence, given that both concepts emphasize societal cohesion and coordinated action across society during crisis and wartime conditions.

The fact that influencers and public figures were perceived as relatively risky channels for spreading misleading content is particularly significant, and it implies the transformation of the information environment toward increasingly networked and personalized forms of communication. Indeed, findings from the Digital News Report 2025 indicate that online influencers and domestic politicians are now perceived as the most prominent sources of false or misleading information worldwide (Newman et al., 2025). These findings support the understanding that contemporary cognitive influence is no longer exerted exclusively through traditional media, but increasingly through digital and hybrid communication networks, where the boundaries between information, political mobilization, propaganda, and entertainment are becoming progressively blurred.

This pattern can be interpreted within the framework of Castells' theory of the network society, which points to the transformation of the traditional model of mass communication and the growing significance of decentralized, interactive, and networked communication flows. Particularly relevant is his concept of mass self-communication, which describes a communication environment in which individuals and other non-state actors can independently produce and distribute content to a potentially mass audience, while simultaneously operating within broader digital communication networks (Castells, 2009).

At the same time, the relatively moderate level of distrust of foreign media and independent analysts may indicate that some segments of the Serbian public sphere perceive alternative or foreign actors as more credible than the domestic, politically polarized media environment. Consequently, as these audiences migrate toward alternative news sources, recent research highlights the potential for increased political polarization, greater susceptibility to misinformation, and heightened belief in conspiracy theories (Mourão and Robertson, 2019).

From the perspective of societal resilience and total defence, this finding is significant because it suggests that media institutions that might otherwise serve as important channels of communication between the state and citizens during crises may face a degree of public distrust. Conversely, greater perceived credibility of purportedly independent and foreign information sources may create a potential vulnerability if these channels of communications are used during a crisis

to disseminate disinformation capable of destabilizing national security and defence.

The analysis of the thematic areas in which false and misleading news is perceived as most prevalent showed that respondents do not perceive such content as evenly distributed across topics. Instead, they perceive its greatest prevalence in politically and security-sensitive domains. The highest perceived prevalence was recorded in domestic politics, where a substantial majority of respondents considered false and misleading news to be present to a greater or extremely large extent. Cross-cultural research conducted in eight countries that are considered democratic and developed, has demonstrated that the trust in politicians is relatively low (Bodas et al., 2022), suggesting that political trust represents a broader international challenge rather than a phenomenon specific to Serbian society. A similar pattern was observed in the areas of international politics and security, as well as in the area of national security, where approximately three-quarters of respondents perceived a high prevalence of false and misleading news. These findings are particularly relevant to the present study because they suggest that respondents perceive disinformation as most closely tied to domains in which political attitudes and perceptions of security threats are formed. Viewed through the prism of cognitive warfare, domestic politics, national security, and international relations represent strategically important targets for disinformation campaigns because information operations in these areas may influence public opinion, undermine trust in institutions, and contribute to social polarization (Cluzel, 2020; Deppe and Schaal, 2024). At the same time, the distribution of responses indicates that the respondents distinguish between areas perceived as carrying higher and lower risks. While politics, security, and the economy are perceived as domains with a high prevalence of false and misleading information, science and technology, and particularly sports, are perceived as domains with substantially lower levels of such content. This distinction is important because it suggests that respondents do not hold uniformly negative perceptions of all media content; rather, they appear to recognize that misinformation may be particularly prevalent in areas characterized by significant political, economic, or security interests. This finding is relevant to societal resilience and total defence because, if the greatest informational risks are perceived in the very domains in which attitudes toward the state, security, international relations, and economic stability are formed, the development of citizens' cognitive resilience becomes an important component of national security.

A further analysis of the results indicates that respondents perceive the Serbian media landscape as an arena in which the interests of great powers and geopolitical actors clash. It is notable that Russia and China were perceived as actors whose interests are promoted to the greatest extent in the Serbian media, with Russia receiving the highest percentage of responses in the "extremely large extent" category (35.6%). This finding may be interpreted in light of the historically strong political, cultural, and religious ties between Serbia and Russia, as well as the broader media and geopolitical context following the outbreak of the war in Ukraine. Within part of Serbian public opinion, Russia continues to be perceived as a traditional ally and a counterbalance to Western political influence, potentially creating favorable conditions for the presence of pro-Russian narratives in the domestic information environment. This perception is corroborated by independent content analysis of the Serbian media landscape, which found that Serbian media outlets—despite relying predominantly on Western news agencies as sources—portrayed the EU and the United States considerably more negatively than positively. In contrast, coverage based on Russian agency reports portrayed Russia predominantly in a positive light (Centre for Research, Transparency and Accountability [CRTA], 2022). At the same time, the high perceived level of Chinese influence may be associated with the intensification of economic, infrastructural, and technological cooperation between Serbia and China over the past decade, as well as to the visible media presentation of Chinese investments, the policy of "steel friendship," and cooperation within the framework of "The Belt and Road" initiative. It is also significant that the United States and the European Union were perceived as actors whose interests are promoted in Serbian media to a great or extremely large extent. This suggests that respondents do not perceive the media environment as being oriented exclusively toward one geopolitical pole, but rather as a space in which competing global centers of power seek to project their interests. In the Serbian context, such perceptions may also reflect broader social and political polarization between pro-Western, including pro-American and pro-European, and pro-Eastern, including pro-Russian and pro-Chinese, orientations that have been evident in public discourse for decades. It should be noted that the broader geopolitical context serves as a framework for interpretation rather than as a direct empirical result of this research; however, since the paper addresses implications in the field of security and defence, engaging with this geopolitical context remains necessary for a fuller understanding of the findings.

The fact that the respondents did not assess all foreign actors in the same way, but differentiate between global and regional actors, is also noteworthy. While Russia, China, the United States, and the EU were perceived as having a relatively strong presence in the media environment, Turkey and countries of the region received substantially lower ratings. This difference may indicate that respondents primarily associate media influence with actors possessing significant geopolitical, economic, or security capacities to shape strategic narratives in Serbia.

This does not mean that public discourse lacks information about regional actors that could have negative implications for Serbia's national security. For example, it is no secret to the public that Turkey is one of the main sponsors of the Kosovo Security Force, the armed formation of the so-called state of Kosovo, which Serbian authorities, in accordance with international law and UN Security Council Resolution 1,244, considers to be its own territory (United Nations Security Council, 1999; Reuters, 2025; Karović, 2025; Ministry of Defence of the Republic of Serbia, 2025). A similar issue concerns the signing of a declaration on defence cooperation between Croatia, Albania, and the so-called Kosovo, which Serbian officials have interpreted as a potential factor of regional destabilization and a signal of the emergence of new lines of confrontation (Ministry of Defence of the Republic of Croatia, 2025; Čolić, 2025; Kosovo Online, 2026). Evaluating the objective nature or severity of these threats is beyond the scope of the present study. Nevertheless, it is relevant that Serbian officials consistently raise such concerns within the public narrative. This interpretation by Serbian officials is consistent with the theory of social constructivism, according to which the very perception of a threat represents a sufficient condition for feelings of insecurity and for undertaking measures to counter the perceived threat. Despite these concerns, respondents perceived Serbian media as being used to a lesser extent, or not at all, as platforms for promoting the interests of Turkey and regional actors. Our findings suggest that, although perceptions of these threats are present in official public discourse, they do not necessarily translate into dominant media themes.

The relatively moderate, but still significant perception of NATO influence on media content in Serbia is particularly interesting in the context of collective memories of the NATO aggression and bombing of 1999 and the enduring presence of anti-NATO sentiment among part of the Serbian public. Although NATO is a formal partner of Serbia within the "Partnership for Peace" program, historical experience and political sensitivities continue to shape how some citizens interpret media narratives concerning the organization, security, and geopolitics. These results are relevant to the present study because they indicate that respondents do not perceive the information environment as politically neutral, but rather as a space of ongoing competition over influence, the interpretation of reality, and the formation of public opinion. In this sense, the cognitive dimension of contemporary security threats involves not only the dissemination of disinformation but also the long-term formation of political and identity orientations through competing foreign-policy and media narratives. Consequently, strengthening societal resilience requires the development of citizens' capacity to critically evaluate media content and recognize potential forms of foreign influence, as well as efforts to strengthen the resilience of the national information environment as a means of preserving its sovereignty amid intensive geopolitical competition.

The prevention and containment of the spread of false and misleading news were perceived by respondents primarily as responsibilities of state institutions and professional actors rather than exclusively as responsibilities of individuals. The largest proportion of respondents believed that the state and its institutions should bear the main responsibility for preventing the spread of disinformation (40.6%), followed by media editors (26.2%) and journalists or individuals who publish such content (22.8%). At the same time, more than three-quarters of respondents (77.2%) supported the establishment of an official state body responsible for identifying and exposing false and misleading news. Serbia already has the Regulatory Authority for Electronic Media (REM), but previous research indicates insufficient public trust that this institution can fully respond to such challenges (CeSID, 2026b; Blagojev et al., 2023). The responses to these two questions indicate a relatively high level of acceptance of the securitization of the information environment, that is, a willingness among part of the public to treat disinformation as a matter of national security, which may justify institutional and, potentially, emergency response measures. At the same time, these findings raise an important democratic question concerning the balance between security, media freedom, and state intervention in the information environment. Any such measures would therefore need to operate within clear legal safeguards and respect the principles of media pluralism and freedom of expression.

It is also noteworthy that only a small proportion of respondents identified citizens themselves as bearing primary responsibility (8.4%), despite the fact that individuals are often the creators or sharers of unverified information, rather than merely passive consumers of content produced by established media organizations. Educational institutions received the lowest proportion of responses (2.0%) in terms of perceived responsibility. Although educational institutions play an important role in developing critical thinking, media literacy, and social responsibility, they were not perceived as the primary actors responsible for preventing the spread of false and misleading news and information. This does not mean that they are unimportant for strengthening societal resilience; on the contrary, their potential role may be particularly important in developing the cognitive dimension of resilience over the longer term.

Finally, several limitations of the study that should be acknowledged. First, the sample was convenience-based, and that participants were not equally balanced across all sociodemographic characteristics; most notably, more than 65% of the participants held a graduate, master's, or doctoral degree. The sample therefore deviates from national demographic characteristics, and this imbalance may have influenced the findings. Second, respondents were recruited primarily through social media platforms and professional networks, which limits the representativeness of the sample and the generalizability of the findings to the broader Serbian population. Third, the data analysis was largely restricted to descriptive statistics; consequently, the findings should be interpreted as exploratory rather than confirmatory. Fourth, although the OMISS scale is designed as a general-context measure applicable across domains (Katsiroumpa et al., 2025a), the cut-off score used to classify respondents was derived from a general Greek sample (Katsiroumpa et al., 2025b). Because its cross-cultural validity in Serbia has not yet been independently established, the resulting categories (Table 1) should therefore be interpreted with caution. Finally, all data were collected through self-report instruments, which are inherently susceptible to socially desirable responding other forms of response bias. This represents a potential source of bias that should be considered when interpreting the findings. Future research should address these limitations through probability-based sampling, more balanced samples across sociodemographic characteristics, and the use of inferential statistical methods.

7 Conclusion and recommendations

Before turning to the broader implications, it should be emphasized that, in light of the sample characteristics discussed above, the following conclusions should be regarded as preliminary indicators that warrant confirmation through a nationally representative follow-up study. In this sense, our findings provide exploratory insight into the cognitive dimension of disinformation as an issue relevant to Serbia's national security, underscoring that this remains a significant yet insufficiently researched aspect of the field.

Respondents in this study operate within a media environment that they perceive as highly saturated with false and misleading information originating from various media sources. These perceptions may plausibly extend beyond the sampled population, given that this media environment is shared across the national information space; however, such extrapolation cannot be confirmed by the present study's design. In addition, respondents perceive the Serbian media environment as an arena of competing foreign influences, particularly those of major geopolitical actors. At the same time, the findings indicate a relatively high level of susceptibility to online misinformation among the surveyed participants, as reflected in their reported tendency to insufficiently verify the information to which they are exposed. Taken together, these findings point to potential vulnerabilities that merit closer examination through more representative research, particularly given their possible implications for societal resilience under crisis conditions.

It is encouraging that the findings indicate that respondents recognize false and misleading information as a national security threat requiring an institutional response. However, the security risk is not exclusively associated with the existence of false and misleading information itself; it may also arise from the erosion of trust in media and institutions and the weakening of their perceived authority and credibility. Therefore, for the successful implementation of the Total Defence concept, the cognitive resilience of citizens should increasingly be recognized as a functional component of national security rather than merely as a matter of media literacy.

Contemporary disinformation and propaganda campaigns can affect social cohesion, trust in institutions, and the capacity for collective action during crises. Consequently, the information environment should be incorporated into broader security and defence planning. With the aim of strengthening national security in the digital age, and taking into account the findings and conclusions of this study, the authors propose several recommendations intended to contribute to strengthening societal resilience and supporting the effective implementation of the Total Defence concept. Although these recommendations are primarily applicable to Serbia, some of them may also be relevant to other countries facing similar challenges. The recommendations are as follows:

1. Institutional recognition of information security and cognitive resilience

Within the concept of total defence, it is necessary to institutionally recognize and define "information security" and "cognitive resilience" as important components of national security. Regulations at various levels, starting with the National Security Strategy and the Defence Strategy, through laws and lower-level legal acts, should be adapted to the contemporary conditions of the digital age. In particular, these documents should clearly define the roles and responsibilities of relevant security institutions, while also improving how citizens are informed about reliable sources of information during crises.

2. Strengthening the civilian component of total defence

The civilian component of defence, as part of total defence, must necessarily encompass the cognitive, informational, and social dimensions of security. Research shows that security risks arise not only from the existence of disinformation, but also from declining trust, fragmentation of the public information space, and the erosion of the perceived authority of media and institutions. Accordingly, within the concept of total defence, particular attention should be devoted to strengthening citizens' trust in accountable institutions and credible sources of information, through which citizens can obtain reliable guidance on how to act appropriately during crises or situations involving heightened security risk. Public service media, given their broad reach and public mandate, should play an important role in this process.

3. Systematic development of media and information literacy

Given the relatively high susceptibility to false and misleading information observed in the present sample (operationalized through the OMISS score), media and information literacy should be systematically developed at all levels of education, from primary and secondary education to higher education, as well as through lifelong learning programs. Special emphasis should be placed on developing critical thinking, understanding mechanisms of digital manipulation, evaluating the credibility of information sources, and verifying online content. These competencies represent important foundations of societal resilience in the digital age. It is also necessary to develop special educational programs and training for different social groups, including civil servants, members of the security system, teachers, journalists, youth and the elderly population. Different generational and educational groups use different media platforms and may consequently encounter different forms of manipulative content. Measures aimed at strengthening societal resilience should therefore be adapted to the needs and media habits of specific target groups, Concrete measures could include introducing media literacy as part of the existing curricula, conducting public awareness campaigns during periods of heightened security risk, and integrating digital literacy and media literacy modules into teacher training programs.

4. Strengthening the role and credibility of public service media

Given that our research indicates a relatively high perception of foreign influence across the media landscape, we propose that, in addition to providing timely and accurate reporting, public service media should play a more significant role in strengthening societal resilience through the production of educational and informational content focused on media literacy, recognition of disinformation, and the responsible use of digital platforms. In that process, cooperation among public service media, universities, research institutions, and independent fact-checking organizations should be encouraged, particularly in the development of media literacy programs and the verification of information during crises. At the same time, the state and its institutions must strengthen safeguards to protect public service media from political, financial, and other forms of undue influence that could compromise editorial independence, professional journalism, and the credibility of public service media as a reliable source of information.

5. Development of national capacities for the early detection of information operations

It is necessary to develop national capacities for the early detection of coordinated disinformation campaigns and hybrid information operations, particularly during crisis and periods of heightened security risk. At the same time, the mechanisms for countering such threats must remain subject to democratic oversight, transparent procedures, and the principles of freedom of expression, media freedom, and pluralism. In this regard, the responsible use of artificial intelligence and other advanced analytical tools should be explored as a means of supporting the detection of disinformation. Such tools can assist in processing large volumes of media content, recognizing coordinated patterns of information dissemination, analyzing recurring narratives, and detecting potentially manipulative or synthetically generated content. However, automated systems should complement, not replace, human assessment and should include safeguards for transparency, accountability, privacy, and fundamental rights.

Author's note

This paper is part of project entitled "Assumptions of the Optimal Implementation of the Total Defence Concept in the Republic of

Serbia (ISI-DH/1/26-28)," which is implemented by the Institute for Strategic Research of the University of Defence in Belgrade and which is financed by the budget of the Republic of Serbia.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

The study was conducted in accordance with local legislation and institutional requirements and, given the anonymous and voluntary nature of the survey, did not require formal ethics committee approval. The participants provided their written informed consent to participate in this study.

Author contributions

MM: Conceptualization, Methodology, Writing – original draft, Writing – review & editing. UM: Conceptualization, Methodology, Writing – original draft, Writing – review & editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. This work was supported by the budget of the Republic of Serbia, as part of the project 'Assumptions of the Optimal Implementation of the Total Defence Concept in the Republic of Serbia' (ISI-DH/1/26-28), implemented by the Institute for Strategic Research of the University of Defence in Belgrade.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Altay, S., Lyons, B. A., and Modirrousta-Galian, A. (2025). Exposure to higher rates of false news erodes media trust and fuels overconfidence. *Mass Commun. Soc.* 28, 301–325. doi: 10.1080/15205436.2024.2382776

Belloni, R. (2024). Serbia between east and west: ontological security, vicarious identity and the problem of sanctions against Russia. *Eur. Secur.* 33, 284–302. doi: 10.1080/09662839.2023.2290048

Bennett, W. L., and Uldam, J. (2024). Corporate social responsibility in the disinformation age. *Manag. Commun. Q.* 38, 864–896. doi: 10.1177/08933189241261717

Berger, P. L., and Luckmann, T. (1991). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. London: Penguin Books Original work published 1966.

Blagojev, T., Medić, D., and Sejdinović, N. (2023). *Strategy for the Development of the Media System of Serbia (2020–2025) and its Implementation: Knowledge, Attitudes and Proposals of Media Workers*. Belgrade: Association of Media, Association of Online Media, Independent Journalists' Association of Vojvodina, Independent Journalists' Association of Serbia, Local Press, and Slavko Ćuruvija Foundation.

Bodas, M., Peleg, K., Stolero, N., and Adini, B. (2022). Understanding societal resilience — cross-sectional study in eight countries. *Front. Public Health* 10:883281. doi: 10.3389/fpubh.2022.883281

Breakstone, J., Smith, M., Ziv, N., and Wineburg, S. (2022). Civic preparation for the digital age: how college students evaluate online sources about social and political issues. *J. High. Educ.* 93, 963–988. doi: 10.1080/00221546.2022.2082783

Broda, E., and Strömbäck, J. (2024). Misinformation, disinformation, and fake news: lessons from an interdisciplinary, systematic literature review. *Ann. Int. Commun. Assoc.* 48, 139–166. doi: 10.1080/23808985.2024.2323736

Buzan, B., Wæver, O., and De Wilde, J. (1998). *Security: A new Framework for Analysis*. Boulder, Colorado: Lynne Rienner Publishers.

Castells, M. (2005) in *The Network Society: From Knowledge to Policy*, eds. M. Castells and G. Cardoso (Washington DC.: Johns Hopkins Center for Transatlantic Relations), 3–22.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press.

Castells, M. (2010). *The rise of the Network Society*. 2nd Edn Chichester: Wiley-Blackwell.

Centre for Research, Transparency and Accountability [CRTA] (2022). *Tracking the Propaganda and Disinformation about Foreign Influence in Serbia: Case Study: Serbian media on the Ukraine war*. Belgrade: CRTA.

CeSID (2026a) Ko smo mi? Available online at: https://www.cesid.rs/o-nama/ko-smo-mi/ (Accessed May 15, 2026)

CeSID (2026b). *Report on the Needs of Media Service Users in Serbia*. Belgrade: Regulatory Authority for Electronic Media of the Republic of Serbia (REM), Council of Europe, European Union.

Claverie, B., and du Cluzel, F. (2021). *The Cognitive Warfare Concept. NATO ACT Innovation Hub*, 1–11. Virginia: Norfolk.

Cluzel, F.D. (2020) Cognitive Warfare. NATO Allied Command Transformation Innovation Hub. Available online at: https://innovationhub-act.org/wp-content/uploads/2023/12/20210122_CW-Final.pdf (Accessed May 02, 2026)

Čolić, N. (2025). *New Balkan Military pact: What lies behind the Croatia–Kosovo–Albania Alliance and is it Directed at Serbia?* Belgrade: NIN.

Deppe, C. (2023). Disinformation in cognitive warfare, foreign information manipulation and interference, and hybrid threats. *Defence Horizon J.* doi: 10.5281/zenodo.10005172

Deppe, C., and Schaal, G. S. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Front. Big Data* 7:1452129. doi: 10.3389/fdata.2024.1452129

Dov Bachmann, S.-D., Putter, D., and Duczynski, G. (2023). Hybrid warfare and disinformation: a Ukraine war perspective. *Glob. Policy* 14, 858–869. doi: 10.1111/1758-5899.13257

Đurić, M. (2026). *Why Serbia Chooses Balancing in Foreign Policy*. Belgrade: NIN.

Džunić, M., and Golubović, N. (2026). Regenerating democracy in a captured media environment: student protests and hypermedia mobilization in Serbia. *Front. Polit. Sci.* 8:1776544. doi: 10.3389/fpos.2026.1776544

European Union (2022). *A Strategic Compass for Security and Defence*. Brussels: EU/ EEAS.

Farrell, T. (2002). Constructivist security studies: portrait of a research program. *Int. Stud. Rev.* 4, 49–72. doi: 10.1111/1521-9488.00229

Government of the Republic of Serbia (2020) Strategy for the Development of the Public Information System in the Republic of Serbia for the Period 2020–2025 (Official Gazette of the Republic of Serbia, No. 11/2020). Available online at: https://pravno-informacioni-sistem.rs/eli/rep/sgrs/vlada/strategija/2020/11/1 (Accessed August 10, 2026)

Greene, S., Asmolov, G., Fagan, A., Fridman, O., and Gjuzelov, B. (2021). *Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them*. Brussels: Policy Department for External Relations, Directorate-General for External Policies, European Parliament.

Hoffman, F. G. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Arlington, Virginia: Potomac Institute for Policy Studies.

Joint Chiefs of Staff (2018). *Joint Concept for Operating in the Information Environment*. Washington, DC: Joint Chiefs of Staff.

Jović-Lazić, A. (2025). On the edge: Serbia between the west, Russia, and its own course. *Međunarodni problemi / Int. Problems* 77, 409–438. doi: 10.2298/MEDJP2503409J

Karović, B. (2025). *Turkey in the Balkans: When Soft power Becomes harder – Ankara Increasingly Present in the region*. Belgrade: NIN.

Katsiroumpa, A., Moisoglou, I., Gallos, P., Galani, O., Tsiachri, M., Lamprakopoulou, K., et al. (2025b). Online misinformation susceptibility scale: determination of an optimal cut-off point. *Int. J. Caring Sci.* 18, 1164–1170.

Katsiroumpa, A., Moisoglou, I., Mangoulia, P., Konstantakopoulou, O., Gallos, P., Tsiachri, M., et al. (2025a). The online misinformation susceptibility scale: development and initial validation. *Health* 13:2252. doi: 10.3390/healthcare13172252

Kljajić, N. P. (2023). The importance of media literacy for members of the military. *Vojno Delo* 75, 46–59. doi: 10.5937/vojdelo2304046K

Kosovo Online (2026) *Vucic: The Greatest Threat to Serbia is the Military Alliance of Zagreb, Pristina and Tirana – Someone has given the "green light"*. Zvečan.

Kubálková, V., Onuf, N., and Kowert, P. (1998). *International Relations in a Constructed World*. New York: Routledge.

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., et al. (2018). The science of fake news. *Science* 359, 1094–1096. doi: 10.1126/science.aao2998

Matović, M., Milojević, A., Milin Perković, S., Tomašević, A., and Josifović, S. (2025). *Media Literacy of Citizens of Serbia: Survey Research Report*. Belgrade: Faculty of Political Sciences, University of Belgrade and OSCE Mission to Serbia.

Mayo, R. (2024). Trust or distrust? Neither! The right mindset for confronting disinformation. *Curr. Opin. Psychol.* 56:101779. doi: 10.1016/j.copsyc.2023.101779

Miljković, U. G. (2025). Psychological resilience to propaganda in the contemporary information space. *Vojno delo* 77, 59–80. doi: 10.5937/vojdelo2504059M

Ministry of Defence of the Republic of Croatia (2025) *Joint Declaration (Albania–Croatia–Kosovo)*. Zagreb.

Ministry of Defence of the Republic of Serbia (2025) *Chief of General Staff Meets with new KFOR Commander*. Belgrade.

Ministry of Foreign Affairs of the Republic of Serbia (2026) *Political Relations between Serbia and the EU*. Belgrade.

Mitrović, M. (2018). Genesis of propaganda as a strategic means of hybrid warfare concept. *Vojno Delo* 70, 34–49. doi: 10.5937/vojdelo1801034M

Mourão, R. R., and Robertson, C. T. (2019). Fake news as discursive integration: an analysis of sites that publish false, misleading, hyperpartisan and sensational information. *J. Theol. Stud.* 20, 2077–2095. doi: 10.1080/1461670X.2019.1566871

NATO (2022) *NATO 2022 strategic concept*. Brussels.

NATO (2026) *NATO on the map*. Brussels.

Nederveen, F., Hoorens, S., Frinking, E. J., and Soest, H. (2024). *Weerbaarheid becijferd: Een methode om weerbaarheid tegen dreigingen voor de nationale veiligheid inzichtelijk te maken [Resilience quantified: A method for mapping resilience against threats to national security]*. California: RAND Corporation.

Newman, N., Ross Arguedas, A., Robertson, C. T., Nielsen, R. K., and Fletcher, R. (2025). *Digital news Report 2025*. Oxford: Reuters Institute for the Study of Journalism.

Nikolic, K. (2023). Serbia hedging its bets between west and east. *J. Balkan Stud.* 3, 59–90. doi: 10.51331/A037

Onuf, N. G. (1989). *World of our Making: Rules and rule in social Theory and International Relations*. South Carolina: University of South Carolina Pres.

Paul, C., and Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda model: Why it Might work and Options to Counter it*. California: RAND Corporation.

Pew Research Center (2025) *International Opinion on Global Threats*. Washington, DC.

Regulatory Authority for Electronic Media (REM) (2026) *Activity Reports*. Belgrade.

Republic of Serbia (2019a). National Security Strategy of the Republic of Serbia. Official Gazette of the Republic of Serbia, No. 94/2019. Available online at: https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/strategija/2019/94/2 (Accessed May 2, 2026)

Republic of Serbia (2019b). Defence Strategy of the Republic of Serbia. Official Gazette of the Republic of Serbia, No. 94/2019. Available online at: https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/strategija/2019/94/1 (Accessed April 27, 2026)

Reuters (2025). *Kosovo to Boost Defence Spending by 60%, Plans drone, Ammunition Production, PM Says*. London: Reuters.

Starčević, S., and Milenković, M. (2023). Instant war in the theory of network society. *Vojno Delo* 75, 1–12. doi: 10.5937/vojdelo2303001S

Stekić, N., and Mitić, A. (2025). Perspectives on Serbia's China–EU hedging strategy: resilient to de-hedging? *Međunarodni problemi / Int. Problems* 77, 193–223. doi: 10.2298/MEDJP2502193S

Sultan, M., Tump, A. N., Ehmann, N., Lorenz-Spreen, P., Hertwig, R., Gollwitzer, A., et al. (2024). Susceptibility to online misinformation: a systematic meta-analysis of demographic and psychological factors. *Proc. Natl. Acad. Sci. USA* 121:e2409329121. doi: 10.1073/pnas.2409329121

The Fund for Peace (2024). *Fragile States Index Annual Report 2024*. Washington, DC: The Fund for Peace.

Torkar, B., and Polnar, S. (2023). The impact of the 1968 Prague spring on Czechoslovak and Yugoslav military doctrines. *Acta Histriae* 31, 307–332. doi: 10.19233/AH.2023.14

Tsang, S. J. (2026). Misinformation, disinformation, and fake news? Proposing a typology framework of false information. *Journalism* 27, 719–739. doi: 10.1177/14648849241304380

United Nations Security Council (1999). *United Nations Security Council Resolution 1244 (1999) on the Situation Relating to Kosovo. S/RES/1244 (1999), Adopted on 10 June 1999*. New York: United Nations Security Council.

van Dijk, J. A. G. M. (2006). *The Network Society: Social Aspects of new media*. 2nd Edn London: Sage.

Vuletić, D., and Milenković, M. R. (2023). "Information warfare as an introduction to Russia-Ukraine armed conflict," in *Strategic Intersections: The new Architecture of International Security*, eds. M. Subotić and Ş. Cioculescu (Strategic Research Institute; Institute for Political Studies of Defence and Military History), 185–197.

Vučković, C., and Radeljić, B. (2024). You are either with us, or against us: the small state of Serbia between domestic ambition and external pressures. *Cogent Social Sciences*, 10. doi: 10.1080/23311886.2024.2389479

Wæver, O. (1995). "Securitization and desecuritization," in *On Security*, ed. R. D. Lipschutz (New York: Columbia University Press), 46–86.

Wardle, C., and Derakhshan, H. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe.

Wellman, B., Quan-Haase, A., Boase, J., Chen, W., Hampton, K., Díaz de Isla Gómez, I., et al. (2003). The social affordances of the internet for networked individualism. *J. Comput.-Mediat. Commun.* 8. doi: 10.1111/j.1083-6101.2003.tb00216.x

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *Int. Organ.* 46, 391–425.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.