DOI: https://doi.org/10.26642/sas-2025-2(8)-61-71
УДК 32:316.77:004.738.5:351.74

Garaschuk Dmytro
PhD student
Zhytomyr Polytechnic State University
https://orcid.org/0009-0004-9878-4110

Serhieiev Viacheslav
doctor habilitated in political science, docent
Zhytomyr Polytechnic State University
https://orcid.org/0000-0001-7859-0408

Infodemics and Populism in the Digital Age: Threats to Political Stability and Security Challenges

Abstract. The article explores the interplay between infodemics and populism in the digital age, highlighting their profound impact on political stability and democratic institutions. It examines how misinformation and disinformation, amplified through digital platforms, contribute to the rise and consolidation of populist movements. The study identifies key mechanisms such as algorithmic content curation, echo chambers, and cognitive biases that facilitate the spread of populist narratives and deepen political polarization.

The research delves into the role of digital media in reshaping political communication, illustrating how populist actors exploit social networks, messaging apps, and targeted digital strategies to construct alternative political realities. Moreover, the transformation of traditional electoral strategies due to the widespread use of misinformation-driven mobilization is discussed, with a particular focus on case studies of electoral interference and mass political radicalization.

Additionally, the article evaluates the security implications of digital populism, considering how disinformation campaigns erode trust in democratic institutions, manipulate public perception, and create vulnerabilities that can be exploited by foreign and domestic actors. The effectiveness of countermeasures—ranging from media literacy initiatives and fact-checking mechanisms to platform regulations and AI-driven content moderation—is critically assessed, emphasizing the challenges of combating disinformation without compromising free speech.

The findings underscore the urgent need for interdisciplinary research to address the threats posed by digital populism. Prospects for further study include developing comprehensive strategies to counteract manipulative digital technologies, refining regulatory frameworks, and enhancing democratic resilience against the destabilizing effects of infodemics. The study contributes to the broader discourse on information integrity, political stability, and the evolving landscape of digital governance in democratic societies.

Keywords: populism in the digital age; infodemic; disinformation; undermining democratic institutions; security challenges.

Relevance of the topic. The intersection of infodemics and populism has become a critical global challenge, influencing political stability, democratic resilience, and national security. The rapid spread of misinformation through digital platforms intensifies political polarization, undermines trust in institutions, and affects electoral processes. As digital communication evolves, populist actors exploit information disorders to advance their agendas.

This topic is significant due to its wide-ranging effects on governance, social cohesion, and international security. Disinformation is no longer confined to fringe groups but now shapes mainstream political discourse. From contested elections to public health crises, false narratives mobilize social movements, distort public perception, and sometimes incite violence. Beyond political instability, infodemics pose security risks by enabling foreign interference, fueling radicalization, and weakening civic engagement.

Understanding how digital populism and infodemics function is crucial for developing countermeasures. Despite fact-checking, media literacy programs, and regulations, disinformation strategies continue to adapt. Social media algorithms and cognitive biases reinforce echo chambers, complicating efforts to curb misinformation.

The geopolitical impact further highlights the urgency of this issue. State and non-state actors weaponize disinformation to destabilize governments and undermine electoral integrity. Addressing this challenge requires a multidisciplinary approach integrating political science, technology studies, and security analysis.

Analysis of recent research and publications. The study of infodemics and populism in the digital age has gained significant scholarly attention, particularly in the context of their influence on political stability, democratic governance, and societal polarization. Researchers have examined the mechanisms through which misinformation spreads, the role of digital platforms in amplifying populist rhetoric, and the challenges posed by algorithmic content selection. Scholars such as Bradshaw and Howard [3] have explored the role of social media in enabling coordinated disinformation campaigns, highlighting how state and non-state actors exploit digital platforms to manipulate public opinion. Their research underscores the growing sophistication of misinformation networks and their impact on political discourse. Tucker, Guess, and Barbera [28] analyze the consequences of online political misinformation, emphasizing its role in deepening partisan divides and reducing trust in democratic institutions.

A key area of investigation has been the effectiveness of countermeasures. Graves and Cherubini [17] discuss the rise of fact-checking initiatives, examining their capacity to mitigate misinformation. While fact-checking has shown positive effects on public knowledge, its reach remains limited, particularly in polarized environments where misinformation thrives. The influence of social media algorithms in shaping political narratives has also been extensively studied. Faddoul, Chaslot, and Farid [13] investigate YouTube's recommendation system, demonstrating how algorithmic curation can facilitate the spread of conspiracy theories. On a broader scale, Roberts [22] examines digital censorship and state control of information, contrasting democratic and authoritarian approaches to managing online discourse. The European Commission [12] presents regulatory responses such as the Digital Services Act, which aims to impose obligations on large platforms to curb misinformation. While these measures reflect growing recognition of the problem, challenges remain in balancing regulation with free speech protections.

Finally, Starbird, Arif, and Wilson [26] investigate disinformation as a form of collaborative work, revealing how misinformation ecosystems evolve and sustain themselves through digital networks. Their findings suggest that addressing infodemics requires a systemic approach that integrates technological solutions, policy interventions, and media literacy efforts. The collective insights from these studies highlight the multifaceted nature of digital populism and infodemics. Future research must continue to refine strategies for countering misinformation, assess the long-term implications of algorithmic governance, and explore ways to safeguard democratic institutions in an era of digital disruption.

The primary objective of this article is to analyze the relationship between infodemics and populism in the digital age, with a particular focus on their impact on political stability, democratic governance, and security. By examining the mechanisms through which digital platforms facilitate the spread of misinformation and amplify populist rhetoric, this study seeks to provide a comprehensive understanding of how these phenomena shape contemporary political realities. This article aims to identify and assess the key strategies employed by populist actors to leverage digital disinformation for political gain. It explores how social media algorithms, cognitive biases, and targeted messaging contribute to the dissemination and reinforcement of misleading narratives. Additionally, it evaluates the extent to which these processes erode public trust in institutions, polarize societies, and influence electoral outcomes.

Another critical goal of this research is to assess the effectiveness of existing countermeasures, including fact-checking initiatives, media literacy programs, platform regulation, and algorithmic adjustments. By analyzing both the successes and limitations of these approaches, the study aims to provide insights into how democratic societies can better protect themselves against the threats posed by digital populism and infodemics.

Finally, the article seeks to contribute to the broader academic and policy discussions on information integrity and democratic resilience. By integrating perspectives from political science, media studies, and security analysis, it aspires to offer recommendations for mitigating the negative effects of digital misinformation while preserving fundamental democratic values and freedoms.

Presentation of the research material and its main results. The digital age has ushered in unprecedented information abundance and new modes of political communication. While the ready availability of information can empower citizens, it has also given rise to infodemics – overwhelming floods of information (both true and false) that spread rapidly online [35]. At the same time, resurgent populist movements have exploited social media to propagate simplified, emotive narratives that often blur truth and falsehood. This report examines the intersection of infodemics, populism, and security, focusing on how social media-fueled misinformation and disinformation contribute to electoral interference and political instability.

The term “infodemic” is a portmanteau of “information” and “epidemic”. It refers to a rapid, far-reaching spread of information (including both accurate and inaccurate content) on a particular issue, akin to the viral spread of a disease [32]. David Rothkopf originally coined the term in 2003 during the SARS outbreak to describe how an “information epidemic” can amplify a crisis. In essence, an infodemic is “too much information” – especially false or misleading information – circulating in the digital and physical environment, which causes confusion and undermines effective responses. Crucially, an infodemic encompasses more than isolated instances of falsehood; it is characterized by information overload, high velocity of spread, and difficulty distinguishing credible facts from misinformation. This distinguishes it from traditional

misinformation and disinformation in both scale and context. “Misinformation” refers to false information that is spread without malicious intent – for example, an individual unknowingly sharing an incorrect rumor. “Disinformation”, by contrast, denotes false information deliberately created and disseminated with the intent to deceive or cause harm. As the World Health Organization notes, misinformation is often circulated by well-meaning people who believe the content is true, whereas disinformation is purposefully manufactured to advance an agenda and can be “dangerous” in its effects [36]. An infodemic may contain both misinformation and disinformation, along with true information, all intermingled in a chaotic torrent. The defining feature of an infodemic is thus the scale, speed, and saturation of information – a “flood” that complicates the discernment of truth. In the digital age, social media and constant connectivity have greatly magnified this phenomenon, allowing rumors, conspiracy theories, and propaganda to proliferate globally in minutes.

Populism is generally defined in political science as a thin-centered ideology that separates society into two antagonistic camps – “the pure people” versus “the corrupt elite” – and asserts that politics should express the general will of the people [19]. Populist rhetoric is moralistic and Manichean: populists claim an exclusive moral representation of “the people” and portray elites (political establishment, mainstream media, experts) as selfish and corrupt. This core definition (after Cas Mudde) highlights that populism is not a full ideology on its own, but a flexible frame that can attach to various left or right host [20]. In practice, contemporary populist movements exhibit anti-establishment, anti-pluralist tendencies and often attack institutions of liberal democracy (such as independent media or courts) as betrayers of the “real” people’s will.

The digital age has transformed populism, providing new tools and channels for populist leaders and movements. Social media in particular enables what scholars call a “social media-populism nexus” [25] – an alignment between the algorithmic dynamics of online platforms and populist communication strategies. Populists thrive on direct, unmediated communication with supporters, and platforms like Twitter, Facebook, and YouTube allow them to bypass traditional gatekeepers (e.g. mainstream press) and broadcast their messages directly to the public. In doing so, they often spread emotionally charged, simplistic narratives that resonate with feelings of grievance or mistrust. Many of these narratives lean on misinformation. For example, populist politicians frequently dismiss any critical news as “fake news” and propagate their own alternative facts. This strategy undermines the credibility of independent media while rallying supporters around the populist as the sole source of “truth.” Empirical research shows that when populist leaders accuse the media of lying or spreading fake news, it erodes public trust in journalism and bolsters trust in the populist figure among their followers [27]. In other words, populists weaponize misinformation accusations as well as misinformation itself.

Several characteristics of digital-age populism stand out:

- Anti-Media Agitation: Populist actors routinely label the mainstream press as biased or untrustworthy (“enemy of the people”), which primes their base to discount independent verification. This creates a ready audience for misinformation that flatters populist narratives. A survey experiment found that populist attacks on media as “fake news” significantly reduced audiences’ trust in those media outlets, especially among people with strong populist attitudes [27]. By chipping away at the credibility of traditional information gatekeepers, populists can more freely disseminate their preferred narratives.
- Direct Social Media Outreach: Populists heavily utilize Facebook, Twitter, WhatsApp, YouTube and other platforms to communicate simple, emotive messages. These messages often feature “us-vs-them” tropes, conspiracy theories, or sensational claims that drive engagement. For instance, former U.S. President Donald Trump harnessed Twitter to spread unverified claims (such as about election fraud or crime statistics) at an unprecedented scale, while Brazil’s Jair Bolsonaro relied on WhatsApp groups to circulate inflammatory content about his opponents [2]. This direct outreach plays into populists’ anti-elite ethos – they present themselves as speaking for “the people” against institutions, and social media provides an ostensibly democratic megaphone.
- Narratives of Crisis and Conspiracy: Populist communication frequently frames political issues in terms of existential crisis or conspiracy (e.g. “the election is being rigged by globalist elites,” or “the media is hiding the truth about X”). Such narratives both justify the populist’s challenge to the status quo and lend themselves to the spread of disinformation. During the COVID-19 pandemic, for example, some populist leaders disseminated conspiracy theories about the virus or vaccines (denouncing scientific experts as elitists imposing harmful rules) to reinforce their political stance [30]. These false narratives can catch fire online, contributing to a broader infodemic.

Social media has supercharged populism by restructuring the public sphere in ways that favor populist styles of communication. Traditional journalism’s gatekeeping and fact-checking functions are diminished, while sensational content can go viral with few checks. Social media often tends to benefit populists and is conducive to their agenda because it rewards provocative, polarizing discourse and undermines the shared knowledge basis of democratic debate [7]. Digital populism is thus both a driver and a beneficiary of the infodemic age: populist actors inject streams of misleading content into the online ecosystem, and the fragmented, high-volume information environment in turn makes citizens more susceptible to populist narratives.

Far from being passive victims of misinformation, many populist actors actively exploit infodemics as a political strategy. Recent research indicates that the proliferation of false or misleading information in the online

sphere is often not random or evenly distributed, but concentrated around certain political actors – notably radical populists. In a cross-national study of millions of social media posts, Törnberg et al. found that radical right-wing populist parties are strongly associated with spreading misinformation, far more than other political groups [27]. In other words, misinformation online is frequently "strategic", deliberately driven by populist politicians and activists to gain traction. By sowing doubts, stoking outrage, and reinforcing "us-versus-them" narratives, populists use misinformation to rally their base and convert grievances into electoral support.

The motivation for populists to leverage infodemics is clear: sensational falsehoods or conspiracy claims can drive engagement and cement in-group loyalty. Populist campaigns often rely on emotionally resonant claims that may not be true but feel true to their supporters (for example, overstating immigration threats or painting opponents as corrupt criminals). These claims, when amplified in an infodemic environment, create a sense of popular knowledge – a worldview shared by the populist's followers that may diverge sharply from verified reality. By dominating the narrative within echo chambers (discussed below), populists can create a self-reinforcing cycle: misinformation strengthens their political message, and their message in turn lends credibility to the misinformation [14]. This deliberate undermining of shared facts is a form of information warfare in domestic politics, one that populists wield to discredit opponents (labeling them as liars or part of a sinister plot) and to appear as the sole truthful voice of the people.

A critical mechanism enabling populists' informational strategy is the architecture of social media itself. Major platforms use algorithms optimized for engagement – they prioritize content likely to draw attention, clicks, and shares. Unfortunately, misinformation and extreme partisan content often outperform sober, factual content in capturing attention, due to human psychological biases (people gravitate toward novel, emotionally-charged news) [16]. This creates an inadvertent alignment between populist propaganda and algorithmic promotion. As Brady et al. noted, there is a "misalignment between the objective of social media algorithms – to boost engagement – and the functions of human psychology," which leads to increased polarization and misinformation online [4]. Algorithms are essentially "engagement-maximizing recommendation engines". They tend to amplify posts that trigger strong reactions (outrage, fear, enthusiasm), which often includes the inflammatory or divisive claims populists make. The result is that populist misinformation not only spreads organically via supporters, but is further amplified by platform algorithms into ever-wider circulation.

Under these conditions, cognitive biases further propel the infodemic. One key bias is confirmation bias – people's tendency to seek and accept information that confirms their prior beliefs and to discount information that contradicts them. Echo chambers result from people's tendency to prefer congenial information and disregard uncongenial information [14]. Populist misinformation exploits this: it usually aligns with the audience's grievances or worldview ("what they want to hear"). For instance, a populist claim that "the mainstream media lies to you" finds fertile ground among those already distrustful of media; any contradictory evidence can be dismissed as coming from the very source deemed untrustworthy. Another bias at play is the illusory truth effect – repeated exposure to a claim, even if false, can instill a sense of familiarity that people mistake for truth. In the cacophony of social media, false stories often get repeated and forwarded many times. By sheer repetition across memes, tweets, and videos, a baseless claim (e.g. a conspiracy that a vote tally was changed by a secret server) can begin to feel familiar and plausible to individuals encountering it over and over.

Additionally, emotional biases are leveraged: content that provokes anger or fear tends to stick in memory and get shared. Populist disinformation often uses moral-emotional language ("outrageous," "treason," "threat") that triggers indignation. Studies have found that false news with high emotional valence spreads faster and deeper on Twitter than neutral news [4]. This is partly because users are more likely to share posts that shock or anger them. Populists intuitively craft messages to hit these emotional buttons, and the algorithmic systems boost such content to more users, creating a vicious cycle of amplification.

The strategic synergy between populist messaging and social media algorithms means that infodemics are not random accidents; they are often actively stoked and amplified. Populist actors inject misleading or incendiary claims into the information stream. These claims find eager sharers in partisan communities and are magnified by algorithms tuned to engagement. Within like-minded networks, misinformation gets continuously reinforced (few disagreeing voices penetrate), exploiting human biases toward confirmation and emotional reasoning. Over time, whole alternative narratives can take root, forming the basis for populist political mobilization.

The spread of infodemics poses a direct threat to core democratic institutions and public trust in governance. Healthy democracies depend on an informed citizenry, a shared base of factual knowledge, and trust in processes like elections and the rule of law. Infodemics undercut each of these pillars. When false or misleading information runs rampant, citizens may lose trust in official information channels, including electoral authorities, legislatures, and the press [15]. Widespread belief in conspiracy theories or fake news leads segments of the public to doubt even well-established democratic procedures. For example, if voters are bombarded on social media with false claims that an upcoming election will be rigged or that voter fraud is widespread, they may begin to suspect the legitimacy of the vote before it even occurs.

Disinformation and populist narratives also seek to delegitimize the independent media and other oversight bodies (judges, election boards) that check power. As noted earlier, populist leaders label unfavorable coverage

as “fake” – a tactic that not only rallies their base but corrodes the overall credibility of media in the public eye. Over time, constant exposure to such rhetoric and related falsehoods leads to a “trust crisis”: people no longer know whom or what to believe. A longitudinal study in the U.S. found that exposure to online fake news was associated with “lower trust in mainstream media across party lines” [21]. In democracies worldwide, trust in journalism and expert authorities has declined in the past decade, in part due to relentless misinformation attacks. This atmosphere of doubt benefits authoritarian-leaning populists, as it becomes easier to dismiss factual criticism or push untruths without accountability. It also weakens democratic accountability itself – if citizens disbelieve critical reporting or fact-based evidence of government wrongdoing, it is difficult to mobilize corrections or punish malfeasance.

Furthermore, infodemics polarize societies, making consensus or compromise harder and governance more dysfunctional. When different segments of the population live in divergent informational worlds (one side, for instance, convinced of completely false narratives about the other), polarization deepens into “pernicious polarization” where each camp views the other as illegitimate. This can lead to political paralysis or the election of extreme candidates who capitalize on the distrust. In some cases, the legitimacy of democratic outcomes themselves comes under attack, leading to instability and even violence (as case studies will illustrate). As the World Economic Forum warned, widespread digital misinformation is acting as an accelerant to the erosion of social cohesion and can “destabilize trust in information and political processes” [37]. The net effect is that infodemics chip away at the “soft infrastructure” of democracy – shared truths, informed debate, and institutional credibility – creating a more volatile and fragile political environment.

Analysis of case studies on election-related infodemics and digital populism, includes the 2016 U.S. elections, Brexit, Brazil 2022, and other instances where misinformation campaigns, algorithmic manipulation, and populist rhetoric influenced governance, electoral integrity, and public trust in democratic institutions:

- United States 2016: The U.S. presidential election of 2016 is a seminal case of electoral interference via social media infodemics [29]. Here, a combination of foreign influence and domestic misinformation created a storm of false or misleading narratives that arguably affected voter perceptions. Russian state-backed actors (particularly the Internet Research Agency, IRA) orchestrated a massive disinformation campaign on U.S. social media platforms. Using troll accounts and bots masquerading as Americans, the IRA posted divisive propaganda on Facebook, Twitter, Instagram, and YouTube, aiming to exacerbate social fractures (race, religion, regional divides) and to either boost Donald Trump or suppress turnout for Hillary Clinton. The scale of this campaign was enormous – Facebook later revealed that Russia-linked pages had reached up to 126 million users on its platform with some 80,000 posts from 2015 to 2017 [31]. To put that in perspective, 126 million people is over half of the U.S. voting population. Many of these posts pushed false stories or conspiratorial content (for example, claims linking Clinton to criminal acts, or stoking fears about immigrants and crime). On Twitter, approximately 36,000 automated bot accounts linked to Russia generated 1.4 million election-related tweets, which were viewed 288 million times. This foreign disinformation barrage operated in tandem with a domestic infodemic: viral false news articles (often from “fake news” websites with partisan agendas) flooded Facebook feeds in the final months of the campaign. Notably, analysis by Silverman (BuzzFeed News) found that fake election news stories (e.g. the Pope had endorsed Trump, or Clinton sold weapons to ISIS) outperformed mainstream news stories on Facebook in terms of shares and engagement in the weeks before voting. The consequence of this environment was a confused electorate and a deeply poisoned information sphere. While it is difficult to quantify the exact impact on vote choices, subsequent investigations concluded that the Russian social media campaign “sought to interfere in the 2016 election” by manipulating U.S. public opinion. The U.S. intelligence community and Senate reports concurred that this infodemic of disinformation contributed to mistrust and polarization surrounding the election outcome. Indeed, the 2016 election marked for many Americans the beginning of a “post-truth” era in politics [11].
- Brexit 2016**:** The United Kingdom’s 2016 referendum on EU membership (Brexit) similarly saw a wave of misinformation and external interference that illustrate infodemic dynamics. The Leave campaign frequently used dubious or misleading claims – the most infamous being the slogan that the UK sent “£350 million a week” to the EU (implying that money could fund the National Health Service instead). This figure was widely debunked as an exaggeration, yet it was relentlessly repeated in campaign materials and social media, becoming an emotionally potent pseudo-fact for many voters. Additionally, xenophobic rumors (such as Turkey imminently joining the EU, sending millions of migrants – false) were circulated to stoke fear [9]. Social media platforms, especially Facebook, were used extensively for micro-targeted political ads, and questions later arose about data analytics firms (e.g. Cambridge Analytica) harvesting user data to target voters with tailored messages, possibly including misleading ones. Beyond domestic actors, evidence of automated bot involvement and foreign influence emerged. Researchers discovered networks of thousands of Twitter bots that pumped out pro-Brexit messages in the run-up to the vote [5]. One study by City University of London identified a sudden appearance of 13,000 suspected bots that posted predominantly Leave-supporting content, then disappeared shortly after the referendum [1]. Separately, an analysis by Swansea University and UC Berkeley found around 150,000 Twitter accounts linked to Russia that were tweeting about Brexit around the time of the

referendum [34]. While these accounts' exact impact is debated, a working paper for the National Bureau of Economic Research estimated that automated accounts could have been responsible for a non-trivial 1.76 percentage point increase in the Leave vote share by amplifying certain messages. Given the Brexit referendum passed with 51.9% voting Leave, even small influences might have been decisive. Regardless of precise effect, the Brexit experience showcased how infodemic conditions (widespread misleading claims, social media echo chambers, and possible foreign disinformation) can contribute to a historic political outcome. The aftermath in Britain was marked by contentious debate over false campaign information and a noted deterioration of trust – both between citizens and in institutions, as the country grappled with implementing a decision many felt was swayed by lies.

- Brazil 2022: The Brazilian general election of 2022 (and the turbulent period around it) provides a recent case of how populist-driven infodemics can threaten electoral integrity and political stability. The contest pitted incumbent President Jair Bolsonaro – a right-wing populist – against former President Luiz Inácio Lula da Silva. Even before the election, Brazil had been dealing with heavy misinformation, much of it spread via WhatsApp groups (which are extremely popular in Brazil for political communication). Bolsonaro's camp frequently used these messaging apps in the 2018 election and continued in 2022 to disseminate misleading content, such as doctored videos and false claims painting Lula as linked to organized crime or communist plots. More alarmingly, as the 2022 vote neared, Bolsonaro openly attacked the credibility of Brazil's electronic voting system, claiming without evidence that it was rigged or prone to fraud. These claims, amplified by his supporters online, constituted an open disinformation campaign from the top – the sitting president priming his base to reject any result not in his favor [23]. Bolsonaro lost the October 2022 election by a narrow margin. In the weeks that followed, an infodemic of election denial spread among his most ardent supporters on social networks and messaging apps, echoing the false belief that the vote was stolen. This culminated on January 8, 2023, when thousands of Bolsonaro supporters – radicalized by online disinformation – stormed the Brazilian Congress, Supreme Court, and presidential palace in Brasília, in an eerie parallel to the U.S. Capitol riot of January 6, 2021 [24]. Thus, the 2022 Brazil elections demonstrated that disinformation can have violent consequences: falsehoods from an illiberal incumbent led a segment of the population to outright reject a democratic election and engage in insurrectionary behavior. Beyond the immediate violence, the infodemic undermined Brazil's democratic stability – trust in the electoral authority (TSE) was shaken among millions of Bolsonaro voters, and the incoming Lula administration faced a hardened opposition convinced by conspiratorial narratives. Studies of the 2022 Brazil infodemic found that belief in electoral misinformation was strongly associated with participation in partisan online groups and low trust in institutions. In other words, the more people steeped themselves in the Bolsonaro-aligned digital ecosystem, the more likely they were to believe the election was illegitimate. The Brazilian case underscores how populist disinformation can push a democracy to the brink, by delegitimizing a fundamental process (free elections) and spurring extra-legal action [6].

Beyond discrete election events, persistent infodemics strain the day-to-day functioning of democratic governance. Policymaking becomes more challenging when large portions of the public hold misinformed views on policy issues due to online falsehoods. For instance, during the COVID-19 pandemic, many governments struggled to enact health policies because of widespread misinformation about the virus and vaccines [30]. Mask mandates and vaccination drives were met with resistance fueled by conspiracy theories (often spread by populist or anti-establishment actors) that COVID was a hoax or that vaccines were dangerous. This not only had public health consequences but also political ones: it created another axis of polarization and hampered evidence-based decision-making. Likewise, on issues like climate change, immigration, or economic reform, infodemics can distort public perception – voters act on the basis of sensational claims rather than factual data, pressuring politicians to follow suit or adopt populist narratives themselves. In the long term, the routine use of disinformation erodes the capacity for rational policy debate. Officials and experts may face harassment or disbelief when presenting factual information that contradicts the myths entrenched in social media discourse. We have seen scientists and public officials in multiple countries vilified as part of "elite conspiracies" when they try to correct false narratives (whether about election integrity or vaccine efficacy) [8]. This creates a chilling effect and a governance environment driven more by viral narratives than by deliberation.

The spread of infodemics undermines democracy by corroding the informational foundation on which democratic institutions rely. Elections – the mechanism for translating popular will – lose legitimacy if swaths of citizens believe, without evidence, that they are rigged. Democratic governments lose authority if citizens come to trust misinformation more than official communications. And the media's role as the fourth estate is crippled if "fake news" accusations persuade people that no independent arbiters of truth exist. The result is often political instability: disputed elections, mass protests or violence based on false beliefs, and a general climate of democratic backsliding. Countries like the U.S., UK, Brazil (and others such as India, Poland, the Philippines, etc.) have all experienced elements of this destabilization in the past decade, correlating with the rise of social-media-fueled populism.

Beyond domestic politics, infodemics and digital populism pose significant national security and global security risks. The deliberate manipulation of information online can weaken a nation from within and also serve as a weapon in geopolitical rivalry.

Several authoritarian states have recognized that sowing misinformation in rival countries is a cheap and effective form of asymmetric warfare. Russia, in particular, has integrated information operations into its military doctrine – sometimes described as the Gerasimov Doctrine or "hybrid warfare," where cyber attacks and propaganda complement conventional force. We saw this in the 2016 U.S. election interference, and Russia has employed similar tactics in Europe (e.g. propaganda campaigns around elections in France, Germany, and the Brexit referendum). Foreign state actors and their proxies (bots, troll farms, state-sponsored media) use social media to spread false narratives that amplify existing divisions in target societies. The goal is often to destabilize democratic societies by fueling polarization, confusion, and distrust. U.S. intelligence officials have warned that Russia, China, Iran and others continue to meddle in online discourse – from spreading false news about candidates to stoking extremist movements – as a means to weaken their adversaries internally without firing a shot [33]. This represents a national security threat: an infodemic induced or guided by a hostile power can undermine the integrity of a country's political system and societal cohesion.

Moreover, digital populism can itself lead to security issues. Populist leaders with authoritarian tendencies might incite internal conflict or erode rule of law, as seen in cases where they refuse electoral outcomes or encourage vigilante behaviors. The January 6, 2021 Capitol attack in the U.S. and the January 8, 2023 Brasília attack in Brazil are examples where misinformation-driven populist movements turned violent, effectively challenging the state's authority. These events had national security ramifications – they exposed vulnerabilities in protecting institutions and the potential for domestic extremist groups (fired up by propaganda) to engage in insurrection. Intelligence agencies are increasingly attentive to such domestic terrorism risks born from online radicalization and conspiracies.

A distinctive feature of the digital infodemic phenomenon is the role of automated and coordinated inauthentic behavior. Propagators of disinformation often deploy "bots" – automated social media accounts – and organized "troll farms" (teams of human operators managing fake personas) to magnify their reach. These bots and trolls can rapidly spread false content, make it trend, or create the illusion that a certain viewpoint has massive support. For example, during elections, a small group can use thousands of bots to swarm hashtags, boosting a misleading narrative to prominence. This not only directly injects misinformation to many users, but also can trick platform algorithms (which might interpret trending activity as genuine user interest, further promoting the content). As noted, tens of thousands of bots were identified in both the U.S. 2016 and Brexit cases, and they likely appear in most major political events now [31, 34].

The broader geopolitical implications of unchecked infodemics are concerning. Liberal democracies worldwide face what some analysts call a crisis of "epistemic security" – the security of knowledge and truth in public discourse. When hostile powers or transnational extremist networks spread conspiracies (for example, QAnon originated in the U.S. but spread to Europe and elsewhere), they create trans-border communities of the misinformed. This can weaken alliances and democratic solidarity. NATO and EU officials have cited disinformation as a major hybrid threat. For instance, during the COVID-19 pandemic, Russian and Chinese outlets pushed anti-Western vaccine narratives in Europe, aiming to undermine trust in Western vaccines and institutions, which could translate into slower recovery or public unrest – a strategic win for authoritarian competitors [10].

Public Health and Economic Stability: Infodemics do not only affect political arenas – they can also jeopardize public health and economic stability, which are components of national and human security. The COVID-19 infodemic is illustrative. As the "Journal of Medical Internet Research" noted, the pandemic's infodemic "significantly affected public health" by causing confusion, mistrust in health authorities, and widespread noncompliance with health guidelines [18]. When misinformation (like false cures, anti-vaccine rumors, or claims that the virus is a hoax) spreads, people may engage in risky behaviors, refuse vaccines or masks, and even resort to harmful "treatments". This not only costs lives but also can prolong a crisis, straining healthcare systems and economies. The WHO has warned that the COVID-19 infodemic undermines the public health responseand can intensify outbreaks. From a security standpoint, a population mired in health misinformation is less able to respond to biological threats – whether natural or man-made. Enemies could even introduce specific health-related disinformation to amplify the damage of a bioterror attack or simply to wreak havoc (imagine disinformation that causes people to reject a needed antidote or prophylactic measure during an emergency).

Economically, disinformation can also have tangible impacts. Modern economies depend heavily on information flows and investor confidence. False information in financial markets – such as rumors spread on Twitter or deepfake news – can move stock prices. A striking example occurred in May 2023, when an AI-generated fake image of an explosion at the Pentagon went viral on social media, briefly causing panic and a dip in the stock market before it was debunked [37]. This incident showed that "AI fakes shared on social media have the potential to cause short-term investor panic and long-term reputational damage". As generative AI

makes it easier to create realistic fake videos or audio, the risk grows that a well-timed piece of disinformation could spark a financial crisis or be used as economic sabotage. On a larger scale, if a country's politics are destabilized by infodemics, that instability will deter investment, disrupt markets, and damage economic prospects. For example, prolonged election disputes or civil unrest fueled by misinformation (like in the U.S. 2020-2021 or Brazil 2022-2023) create uncertainty that can affect currency value, capital flight, or trade. Thus, economic security is intertwined with informational integrity.

Finally, transnational issues require factual cooperation, which infodemics impede. Climate change, for instance, is an area where disinformation (often industry-backed or ideologically driven) has stalled policy responses for years by seeding public doubts about scientific consensus. In a sense, climate misinformation is a global security risk, as it delays action on an existential threat. Similarly, during international crises or conflicts, disinformation can warp decision-making – consider how quickly false stories can spread during a conflict, potentially leading to miscalculations or escalation. We now see militaries incorporating counter-disinformation tasks as part of defense.

Addressing the intertwined threats of infodemics and digital-age populism requires a multi-faceted approach involving governments, technology companies, media, and civil society. Over the past decade, various countermeasures have emerged, including fact-checking initiatives, media literacy campaigns, platform moderation strategies, and regulatory responses. While these efforts have had varying degrees of success, ongoing adaptation is necessary to mitigate the evolving threats posed by disinformation.

Fact-checking organizations such as PolitiFact and Snopes play a crucial role in countering misinformation by systematically verifying claims and disseminating corrections [17]. Studies indicate that fact-checking can improve factual accuracy, although its effectiveness depends on the timing of corrections and audience receptivity. However, fact-checking often struggles to keep pace with the rapid dissemination of falsehoods, particularly in polarized environments where misinformation reinforces preexisting biases.

Social media companies have implemented various countermeasures to curb misinformation, including content moderation policies, algorithmic adjustments, and partnerships with fact-checking organizations. Platforms like Facebook and Twitter have introduced warning labels, downranked misleading content, and removed coordinated disinformation campaigns [3]. During major political events and public health crises, these interventions have helped limit the reach of false claims, though enforcement has often been inconsistent.

Algorithmic interventions aim to reduce the virality of misinformation. Platforms have adjusted recommendation systems to deprioritize low-quality sources, while Twitter has experimented with friction mechanisms to slow the spread of unverified content [28]. YouTube revised its algorithm to limit the reach of conspiracy theories, reporting a decline in views of misleading videos [13]. However, critics argue that profit-driven engagement models incentivize platforms to prioritize virality over accuracy, complicating efforts to curb misinformation effectively.

Democratic governments have pursued various regulatory approaches to balance free speech with combating misinformation. The European Union's "Digital Services Act" (DSA) imposes obligations on large platforms to mitigate systemic misinformation risks [12]. Germany's "NetzDG" law requires social media companies to remove illegal content within 24 hours, while France has implemented election-specific regulations to counter false claims. In contrast, the U.S. has focused on promoting transparency in online political advertising and platform accountability rather than direct content regulation [28].

Conversely, authoritarian regimes frequently use misinformation laws as tools for censorship and political control. Russia's 2019 "fake news" law criminalizes information contradicting state narratives, while China's digital policies enable strict online discourse regulation [22]. These regimes also engage in external disinformation campaigns, leveraging state-affiliated media and social media networks to influence public opinion globally [26].

Conclusions and Prospects for Further Research. The intersection of infodemics and populism in the digital age presents a profound challenge to political stability, democratic governance, and global security. This study has demonstrated that the rapid spread of misinformation and disinformation via digital platforms not only amplifies populist narratives but also erodes trust in institutions, distorts electoral processes, and fosters political polarization. The mechanisms driving this phenomenon (algorithmic amplification, cognitive biases, and targeted digital manipulation) underscore the urgent need for a multi-dimensional response that involves policymakers, technology companies, media organizations, and civil society.

A key takeaway from this research is that digital populism does not merely exploit existing societal divisions; it actively deepens them by creating alternative realities in which fact-based discourse becomes secondary to emotionally charged and strategically crafted narratives. This manipulation of information ecosystems undermines rational deliberation, leading to the deterioration of democratic norms and fostering environments in which authoritarian tendencies can take root. The case studies analyzed illustrate that infodemics have the capacity to incite real-world actions, from electoral interference to mass protests and even violent insurrections. These events serve as stark reminders that digital disinformation is not a passive phenomenon but an active force shaping political landscapes globally.

Despite efforts to counteract the spread of falsehoods (ranging from fact-checking initiatives and media literacy programs to platform moderation and regulatory interventions) substantial gaps remain. The scalability of fact-checking, the persistence of algorithmically driven echo chambers, and the increasing sophistication of disinformation tactics present ongoing challenges. While some governments have introduced regulatory frameworks to mitigate the spread of false information, these measures often struggle to balance free speech protections with the need to curb harmful content. Moreover, authoritarian regimes have weaponized anti-misinformation laws to suppress dissent rather than enhance information integrity.

Looking ahead, several critical areas warrant further research. First, there is a need for deeper empirical analysis of the effectiveness of current countermeasures. Understanding which interventions yield tangible reductions in misinformation consumption and belief, and under what conditions, can inform more targeted policy responses. Second, research should explore the role of artificial intelligence in both exacerbating and mitigating disinformation. The advent of deepfakes, automated bot networks, and AI-generated narratives introduces new layers of complexity that demand proactive regulatory and technological solutions.

Another promising avenue for research lies in the study of public resilience to infodemics. Investigating how different societies, demographic groups, and political cultures respond to digital misinformation can reveal insights into strategies for enhancing collective resistance. Comparative analyses of countries that have successfully mitigated the effects of infodemics (such as Finland's media literacy initiatives) could offer valuable lessons for broader global application. Additionally, interdisciplinary approaches that integrate political science, cognitive psychology, and data science can provide more comprehensive models for understanding and addressing the dynamics of digital disinformation.

Finally, future research should consider the geopolitical dimensions of infodemics. As state and non-state actors increasingly engage in coordinated disinformation campaigns to destabilize rival nations, understanding the transnational impact of digital populism is essential. The intersection of cybersecurity, strategic communication, and democratic resilience must be further explored to develop robust international frameworks for countering information manipulation.

In conclusion, while digital infodemics and populism present significant challenges to democratic governance and political stability, they are not insurmountable. By advancing research on effective countermeasures, fostering interdisciplinary collaboration, and strengthening global cooperation, it is possible to build a more resilient information ecosystem that safeguards democratic values in the digital age.

References:

1. Ball, J. (2017), «A Suspected Network Of 13,000 Twitter Bots Pumped Out Pro-Brexit Messages In The Run-Up To The EU Vote», *BuzzFeed*, [Online], available at: https://www.buzzfeed.com/jamesball/a-suspected-network-of-13000-twitter-bots-pumped-out-pro
2. Bobba, G. (2021), «Digital Populism: How the Web and Social Media Are Shaping Populism in Western Democracies», *Political Populism*, in Heinisch, R., Holtz-Bacha, C., Mazzoleni, O. (ed.), Nomos Verlagsgesellschaft mbH & Co, KG, pp. 457–468.
3. Bradshaw, S. and Howard, P. (2019), «The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation».
4. Brady, W.J., Jackson, J.C., Lindström, B. and Crockett, M.J. (2023), «Algorithm-mediated social learning in online social networks», *Trends in Cognitive Sciences*, Vol. 27, pp. 947–960, doi: 10.1016/j.tics.2023.06.008.
5. Burgess, M. «Here's the first evidence Russia used Twitter to influence Brexit», *Wired*, [Online], available at: https://www.wired.com/story/brexit-russia-influence-twitter-bots-internet-research-agency/
6. Centner, R. and Nogueira, M. (2024), «Geographies of entitled anger: Revanchist populism in Brazil and beyond», *Environment and Planning C: Politics and Space*, Vol. 42, pp. 501–508, doi: 10.1177/23996544241254249.
7. Chatterje-Doody, P.N. and Crilley, R. (2019), «Populism and Contemporary Global Media: Populist Communication Logics and the Co-construction of Transnational Identities», *Populism and World Politics*, in Stengel, F.A., MacDonald, D.B., Nabers, D. (ed.), Springer International Publishing, Cham, pp. 73–99.
8. Christner, C. (2022), «Populist attitudes and conspiracy beliefs: Exploring the relation between the latent structures of populist attitudes and conspiracy beliefs», *Journal of Social and Political Psychology*, Vol. 10, pp. 72–85, doi: 10.5964/jspp.7969.
9. Clarke, H.D., Goodwin, M. and Whiteley, P. (2017), «Why Britain Voted for Brexit: An Individual-Level Analysis of the 2016 Referendum Vote», *Parliamentary Affairs*, Vol. 70, pp. 439–464, doi: 10.1093/pa/gsx005.
10. Cosentino, G. (2023), *The Infodemic: Disinformation, Geopolitics and the Covid-19 Pandemic*, Bloomsbury Publishing Plc, London.
11. Dempsey, S., Li, J., Witkovsky, B. et al. (2024), «Manufacturing January 6: How Republican County Parties Mobilized Anger to Promote #StopTheSteal», *Politics & Society*, Vol. 53, Iss. 1, doi: 10.1177/00323292241279671.
12. European Commission (2023), *Digital Services Act: application of the risk management framework to Russian disinformation campaigns*, Publications Office, LU.
13. Faddoul, M., Chaslot, G. and Farid, H. (2020), «A Longitudinal Analysis of YouTube's Promotion of Conspiracy Videos», *Computers and Society*, doi: 10.48550/arXiv.2003.03318.

14. Garaschuk, D.V. (2024), «Digital echo chambers: amplifying populist rhetoric in the age of social media», *Current Problems of Philosophy and Sociology*, No.46, pp. 152–157, doi: 10.32782/apfs.v046.2024.26.
15. Garaschuk, D.V. (2024), «TRUTH DECAY AND POPULISM: ERODING DEMOCRACY IN THE 21ST CENTURY», *International and Political Studies*, No. 37, pp. 65–78, doi: 10.32782/2707-5206.2024.37.6.
16. Garaschuk, D.V. and Serhieiev, V.S. (2024), «Fact-Checking Challenges of Digital Populism in the «Truth Decay» Era», *Filosofiia ta publichni komunikatsii: informatsiinyi prostir suchasnoi kultury*, Liha-Pres, pp. 22–26.
17. Graves, L. and Cherubini, F. (2016), *The rise of fact-checking sites in Europe*, Reuters Institute for the Study of Journalism.
18. Kisa, S. and Kisa, A. (2024), «A Comprehensive Analysis of COVID-19 Misinformation, Public Health Impacts, and Communication Strategies: Scoping Review», *Journal of Medical Internet Research*, Vol. 26, doi: 10.2196/56931.
19. Mudde, C. (2004), «The Populist Zeitgeist», *Government and Opposition*, Vol. 39, pp. 541–563, doi: 10.1111/j.1477-7053.2004.00135.x.
20. Mudde, C. and Kaltwasser, C.R. (2013), «Exclusionary vs. Inclusionary Populism: Comparing Contemporary Europe and Latin America», *Government and Opposition*, Vol. 48, pp. 147–173, doi: 10.1017/gov.2012.11.
21. Ognyanova, K., Lazer, D., Robertson, R.E. and Wilson, C. (2020), «Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power», *Harvard Kennedy School Misinformation Review*, Vol. 1, Iss. 4, doi: 10.37016/mr-2020-024.
22. Roberts, M.E. (2018), *Censored: Distraction and Diversion Inside China's Great Firewall*, Princeton University Press, Princeton, N.J.
23. Rossini, P., Mont'Alverne, C. and Kalogeropoulos, A. (2023), «Explaining beliefs in electoral misinformation in the 2022 Brazilian election: The role of ideology, political trust, social media, and messaging apps», *Harvard Kennedy School Misinformation Review*, Vol. 4, Iss. 3, doi: 10.37016/mr-2020-115.
24. Savarese, M. (2024), «How Brazilian police say Bolsonaro plotted a coup to stay in office», *AP News*, [Online], available at: https://apnews.com/article/bolsonaro-brazil-coup-legal-woes-report-43bae30906925a8dc04e319b901488f8
25. Siles, I., Tristán, L. and Carazo, C. (2021), «Populism, media, and misinformation in Latin America», *The Routledge Companion to Media Disinformation and Populism*, in Tumber, H., Waisbord, S. (ed.), 1st ed., Routledge, pp. 356–365.
26. Starbird, K., Arif, A. and Wilson, T. (2019), «Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations», *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3, pp. 1–26, doi: 10.1145/3359229.
27. Törnberg, P. and Chueri, J. (2025), «When Do Parties Lie? Misinformation and Radical-Right Populism Across 26 Countries», *The International Journal of Press/Politics*, doi: 10.1177/19401612241311886.
28. Tucker, J.A., Guess, A.M., Barberá, P. et al. (2018), «Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature», doi: 10.2139/ssrn.3144139.
29. Zhang, H., Afzaal, M. and Liu, C. (2020), «American Populism in Digital Era: Strategies of Manipulation in Donald Trump's Election Tweets», *Revista Argentina de Clínica Psicológica*, Vol. 29, No. 3, pp. 1273–1280, doi: 10.24205/03276716.2020.957.
30. Zubčić, M.-L. and Giacomini, G. (2025), «Beyond «Infodemic»: Complexity, Knowledge and Populism in COVID-19 Crisis Governance», *Social Epistemology*, Vol. 39, pp. 56–76, doi: 10.1080/02691728.2024.2356528.
31. «Facebook: Up to 126 million people saw Russian-planted posts» (2017), *POLITICO*, [Online], available at: https://www.politico.com/story/2017/10/30/facebook-russian-planted-posts-244340
32. «Infodemic» (2024), *Wikipedia*, [Online], available at: https://en.wikipedia.org/wiki/Infodemic
33. «Promoting Free Speech While Exposing Manipulation of Fact» (2024), *Voice of America*, [Online], available at: https://editorials.voa.gov/a/promoting-free-speech-while-at-same-time-exposing-manipulation-of-fact/7819036.html
34. «Russian interference in the 2016 Brexit referendum» (2025), *Wikipedia*, [Online], available at: https://en.wikipedia.org/wiki/Russian_interference_in_the_2016_Brexit_referendum
35. «Infodemic», *World Health Organization*, [Online], available at: https://www.who.int/health-topics/infodemic#tab=tab_1
36. «Let's flatten the infodemic curve», *World Health Organization*, [Online], available at: https://www.who.int/news-room/spotlight/let-s-flatten-the-infodemic-curve
37. «The rising risk of misinformation and disinformation», *Zurich Insurance Group*, [Online], available at: https://www.zurich.com/knowledge/topics/global-risks/the-rising-risk-of-misinformation-and-disinformation

---

Гаращук Д., Сергєєв В.

Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики

Анотація. Стаття досліджує взаємозв'язок між інфодеміями та популізмом у цифрову епоху, підкреслюючи їхній суттєвий вплив на політичну стабільність і демократичні інститути. Аналізується, як дезінформація та маніпулятивний контент, поширюваний через цифрові платформи, сприяють зростанню і консолідації популістських рухів. Визначено ключові механізми, такі як алгоритмічна селекція контенту, інформаційні бульбашки та когнітивні упередження, що полегшують поширення популістських наративів і поглиблюють політичну поляризацію.

Дослідження розглядає роль цифрових медіа у трансформації політичної комунікації, демонструючи, як

популістські актори використовують соціальні мережі, месенджери та таргетовані цифрові стратегії для побудови альтернативних політичних реальностей. Також розглядається трансформація традиційних виборчих стратегій під впливом масштабного використання дезінформаційних кампаній, із акцентом на випадки втручання у вибори та масової політичної радикалізації.

Окремо оцінюються безпекові аспекти цифрового популізму, зокрема його вплив на довіру до демократичних інституцій, маніпуляцію суспільною думкою та створення вразливостей, що можуть використовуватися як зовнішніми, так і внутрішніми акторами. Критично аналізується ефективність заходів протидії—від програм медіаграмотності та механізмів фактчекінгу до регулювання платформ та модерації контенту на основі штучного інтелекту, наголошуючи на викликах боротьби з дезінформацією без обмеження свободи слова.

Отримані результати підкреслюють нагальну потребу у міждисциплінарних дослідженнях для протидії загрозам цифрового популізму. Перспективи подальших досліджень включають розробку комплексних стратегій протидії маніпулятивним цифровим технологіям, удосконалення нормативно-правових рамок і посилення демократичної стійкості перед дестабілізуючими наслідками інфодемій. Це дослідження сприяє ширшій дискусії щодо інформаційної безпеки, політичної стабільності та змін у сфері цифрового управління у демократичних суспільствах.

Ключові слова: популізм у цифрову епоху; інфодемія; дезінформація; підрив демократичних інститутів; безпекові виклики.

Стаття надійшла до редакції 26.03.2025.