NARRATIVE WARFARE & COGNITIVE SECURITY IN EDUCATION AN OSINT-CENTRIC CURRICULUM FOR COMMUNICATION RESILIENCE (CASE ROMANIA 2024–2025)

Nicolae Ovidiu VOINEA, Lecturer Ph.D., Hyperion University
Alexandru Daniel CRIȘAN, Ph.D. Candidate in Administrative Science, SNSPA

https://doi.org/10.66793/tituecir19proceeding20

Abstract

This paper designs and evaluates a university-level "Cognitive Security & Narrative Analytics" curriculum that blends open-source intelligence (OSINT) methods, discourse analysis, and ethical communication to counter foreign disinformation operations in Romania's hybrid media ecosystem. Using 2024–2025 case studies – including deepfakes, coordinated inauthentic behavior, and cross-platform narrative cascades – we introduce a practical lab model encompassing data collection (open sources), rigorous source vetting, narrative mapping, and development of rapid-response communication playbooks for public institutions and civil society. We present assessment rubrics and sample assignments (e.g. fact-checking sprints, influence-network mapping), and a minimal-tooling stack accessible to non-technical students. Our findings suggest that embedding "narrative forensics" (the analysis of malign narratives and their spread) into higher education builds durable civic competence, strengthens public diplomacy, and aligns with knowledge-based society goals. The paper offers a replicable template for Romanian universities and partners (media, NGOs, government) to fortify cognitive security through education.

***Keywords*:** *Education, Asymetric Warfare, Disinformation, Cognitive Security*

1. Introductory Aspects

Misinformation and influence campaigns today represent a serious security threat, eroding public trust and destabilizing societies. The World Economic Forum's Global Risks Report 2025 warns that "misinformation and disinformation" rank among the top short-term global risks, fueling instability and undermining trust in governance[1]. Modern adversaries engage in "narrative warfare," weaponizing stories and false narratives to influence beliefs and perceptions on a large scale. In NATO's analysis, the cognitive domain, the realm of human thought, has effectively become a new battlefield: "In cognitive warfare, the human mind becomes the battlefield. The aim is to change not only what people think, but how they think and act."[2] This so-called cognitive warfare incorporates multiple vectors such as cyber, information, social and psychological engineering tactics to influence or disrupt human perception and cognition. As a result, securing the cognitive domain of society, often termed cognitive security, is increasingly recognized as vital to national resilience[3]

Romania, as an Eastern European democracy and NATO/EU member, faces intense information challenges in the current hybrid threat environment. Its proximity to the war in Ukraine and internal socio-political fractures make it a prime target for foreign influence operations. Indeed, declassified documents by Romanian intelligence in late 2024 described "aggressive hybrid actions" during the presidential election campaign that suggested Russian interference.

[1] ***, *Global Risks Report 2025: Conflict, Environment and Disinformation Top Threats, World Economic Forum*, 2025
[2] Aronhime, L. (coord), *Countering cognitive warfare: awareness and resilience,* Johns Hopkins University & Imperial College London, 20th of May 2021.
[3] Rickli, J.M.; Knappe, T, *Enhancing Cognitive Security and Societal Resilience to Counter Cognitive Warfare*, Geneva Center for Security Policy, 7th of October 2025.

In a stunning turn of events, a previously little-known far-right candidate, Călin Georgescu, unexpectedly won the first round of the November 2024 election, driven in part by a massive surge of coordinated activity on TikTok and other platforms[4]. Georgescu's "TikTok Messiah" phenomenon (as media dubbed it) saw him trending among the top global topics on TikTok at the peak of the campaign. Security services assessed that Russian hybrid actions on social media helped explain his sudden success[5]

TikTok alone removed some 66,000 fake Romanian accounts after the election, at which point **7** *million* false "likes" vanished, along with 10 million bot followers that had artificially inflated his popularity.[6]

Hundreds of paid influencers were enlisted to amplify his content. In response to these revelations, Romania's Constitutional Court took the unprecedented step of annulling the election results and canceling the scheduled runoff, which is safe to say highly vulnerabilized the image of the Romanian institutions on both sides of the political spectrum. To the Pro-Georgescu camp the election seemed stolen in a silent coup and for the Pro-European camp the State seemed impotent and incapable of tackling the challenges of a hostile actor seeking to influence their electoral process.

The Georgescu case is but one example in a wave of foreign information manipulation and interference (FIMI) that Romania and its neighbors confronted in 2024–2025. Another case involved a deepfake-driven malvertising campaign: security researchers observed malicious actors using AI-generated video news anchors in deceptive YouTube ads targeting Romanian users, which spread false information while also dropping malware**7**. This hybrid threat combined a deepfake video (to mislead viewers with synthetic human "newscasters") and a cyber element (malicious links embedded in the ads), illustrating a form of "cognitive hacking", essentially hacking the human mind via digital means. Meanwhile, Meta (Facebook) reported disrupting a Romania-based network in early 2025 that comprised 658 fake Facebook accounts (plus 14 Pages and 2 Instagram accounts) engaged in coordinated inauthentic behavior[8]

Against this backdrop, building resilience in the information environment has become a strategic priority. Traditional approaches like fact-checking and platform moderation, while important, are not sufficient on their own. A complementary "whole-of-society" approach is needed, one that empowers citizens at all levels to critically analyze and respond to malign information[9].

Furthermore one must take into account a number of factors and approaches such digital skills involved in an eventual countereffort against disinformation as well as the ethical and integrity considerations of such tools.

Education is increasingly seen as the cornerstone of such resilience[10]. NATO and EU experts emphasize that non-military instruments, education, media literacy, critical thinking training, support for quality journalism, are among the primary tools to achieve cognitive security for society. In practice, countries with strong educational interventions in this arena tend to fare better: Finland, for example, is consistently ranked Europe's most resilient nation against fake news, thanks in part to embedding media literacy and anti-disinformation training into school curricula from an early age. Practices of moral leadership from the private sector could also represent a flagstone concerning such new endeavours.[11].

---

[4] Goury-Laffont, V., *Report ties Romanian liberals to TikTok campaign that fueled pro-Russia candidate,* Politico EU - December 21, 2024

[5] ***, *Romanian court annuls presidential vote after Russian interference claims Calin Georgescu won the first round of the election after being propelled by TikTok. Romania's security services pointed to "Russian hybrid actions,* The Washington Post, December 6, 2024

[6] Mutler, A., *Romania's 'TikTok Messiah' Is Gone But Admirers Live On The country's extreme right is prospering ahead of re-run presidential elections despite extensive evidence of continuing Russian subversion*, Center for European Policy Analysis (CEPA), March 27, 2025

[7] Bârgăoanu, A.; Pană, M., *Cyber Influence Defence: Applying the DISARM Framework to a Cognitive Hacking Case from the Romanian Digital Space*, Applied Cybersecurity & Internet Governance Journal, 2024

[8] Lakshmanan, R, *Meta Disrupts Influence Ops Targeting Romania, Azerbaijan, and Taiwan with Fake Personas, The Hacker News*, May 30, 2025

[9] Grigorescu A.; Alistar, T.V.; Lincaru, L., *Digital Skills, Ethics, and Integrity—The Impact of Risky Internet Use, a Multivariate and Spatial Approach to Understanding NEET Vulnerability Systems 2025*, Volume 13, Issue 8, 649, https://doi.org/10.3390/systems13080649

[10] Roozenbeek, J.; van der Linden, S.; Nygren, T., *Prebunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures*, Misinformation Review, Harvard Kennedy School, The Harvard Kennedy School, January 2020, Volume 1, Issue 2, https://doi.org/10.37016//mr-2020-008

[11] Vaduva, S.; Alistar, V.; Thomas, A..; Lupiţu, C.; Neagoie, D.; *Moral Leadership in Business: Towards a Business Culture of Integrity*, 10.1007/978-3-319-42881-9, 2016

By contrast, Romania ranks near the bottom in Europe for media literacy (32 points in the 2023 Media Literacy Index, second-lowest in the EU),[12] reflecting a vulnerability that adversaries have exploited. Romanian educators and sociologists have begun to voice the need for formal instruction on fake news and disinformation phenomena in classrooms. In recent years, pilot lessons on debunking and digital literacy have been gradually introduced in some schools, focusing on raising awareness of the dangers of fake news among pupils and students. This paper situates itself at the intersection of security studies and education, proposing a concrete educational solution to Romania's cognitive security challenge. We design and evaluate a university-level curriculum titled "Cognitive Security & Narrative Analytics," aimed at senior undergraduates or graduate students in fields like communications, international relations, or security studies. The proposed curriculum is explicitly OSINT-centric, meaning it emphasizes open-source intelligence techniques, the same methods used by investigative journalists and intelligence analysts to gather and verify information from publicly available sources. By blending OSINT with narrative theory, discourse analysis, and strategic communication, the program teaches students to systematically dissect information threats (such as those illustrated by the cases above) and to craft informed countermeasures. Students learn not only to debunk falsehoods, but to understand the underlying narratives and influence techniques at play, a skillset we refer to as "narrative forensics." The goal is to produce graduates who can serve as "cognitive security" specialists in various sectors (public institutions, media, NGOs), thereby extending Romania's capacity to detect and counter information warfare at the grassroots level.

In the sections that follow, we first review the conceptual foundations of narrative warfare, cognitive security, and the role of OSINT in countering disinformation (Section 2). We then outline the curriculum design (Section 3). By bridging the gap between security strategy and education, this work demonstrates an innovative approach to inoculating an open society against information threats. In essence, it treats the classroom as the new frontline in narrative warfare, a training ground for the next generation of "infowarriors" who fight not with censorship or propaganda, but with critical thinking, open-source evidence, and ethical communication.

2. Conceptual Framework: Narrative Warfare, Cognitive Security and OSINT

Narrative Warfare refers to the strategic use of stories, framing, and messaging to influence perceptions, attitudes, and behaviors in a target audience. The concept builds on the understanding that humans make sense of complex reality through narratives; hence, controlling the narrative means shaping how people interpret events. Adversarial actors – from state propaganda machines to extremist groups – engage in narrative warfare by spreading malicious narratives (e.g. conspiracy theories, disinformation campaigns) that advance their interests. These narratives often tap into identities and emotions, creating compelling (if false) explanations that can motivate action or sow division. In the digital era, narrative warfare has been amplified by social media, where virality can rapidly propagate a story worldwide before it can be debunked. A narrative cascade occurs when a particular framing or story spreads explosively across platforms and communities, effectively "going viral" and potentially overshadowing factual discourse. For instance, a rumor or fake news story might emerge on a fringe forum, get picked up by influential accounts on Twitter or Facebook, then receive coverage on mainstream news,[13] accumulating credibility and audience with each step.

The 2024 Romanian election interference described earlier is a prime example: a fringe candidate's narrative ("Romania needs a nationalist savior," etc.) was boosted by coordinated online agents until it became a dominant story in the public sphere.

Cognitive Security is the flip side, the effort to protect and strengthen the public's cognitive domain against such manipulative narratives. One can define cognitive security as a state (and process) in which malign influence or manipulation is unable to significantly alter human cognition or decision-making. In practice, achieving cognitive security means building a society's immunity to misinformation and propaganda. This aligns closely with the idea of societal resilience, the capacity of communities to withstand and bounce back from disruptions. NATO's framework for resilience now explicitly includes the information sphere; as one NATO publication noted, the Alliance must "move beyond countering disinformation at the surface level and instead focus on building orientation resilience" at every level of society[14]. In other words, rather than only reacting to each falsehood (the "whack-a-mole" approach), it is crucial to strengthen the population's overall ability to discern truth from falsehood, to orient themselves correctly in a sea of information. This concept evokes deterrence by denial: instead of (or in addition to) deterring adversaries through punishment, we deter them by

[12] Radu, A.F.; Petcu, I., The education system, the way to fight fake news, National Institute for Research and Development in Informatics – ICI Bucharest, Romania. Vol. 1: Security Above All!, 2024

[13] Alvarez, I. et all, *OSINT for analyzing fake news, a guide for journalists, investigators, and law enforcement* ISBN 978-973-0-37583-1, DOI: 10.19107/OSINT-4-FAKE-NEWS, 2023

[14] Thoreau, H.D., *Cognitive Warfare, Applied Cognitive Effects Newsletter, Perception*, Vol 1, Issue 2, October 2025

denying the success of their influence operations. If a population is highly skeptical of and resistant to fake narratives, then the adversary's effort yields little to no result.

A whole-of-society approach is widely advocated to enhance cognitive security, this means governments, educational institutions, media organizations, tech platforms, and civil society all have roles to play in fortifying the information environment. Our focus here is on the educational dimension. Traditional media literacy and information literacy programs are an important starting point, teaching students how to verify sources, recognize bias, and think critically about the media they consume. Countries like Finland have shown that integrating media literacy early (in primary and secondary school) correlates with citizens who are better at discerning online falsehoods

However, as information threats grow more complex, some scholars argue we must go "beyond media literacy" to what might be called cognitive security education. This involves not just analyzing content at face value, but understanding the tactics and strategies of malign influence. A human-factors approach to cognitive security education suggests focusing on how people process information, including psychological biases and emotional triggers that make disinformation appealing. In other words, the curriculum should train students to recognize why certain narratives are persuasive or how they exploit fears, identities, and cognitive biases.

Our proposed curriculum builds on media literacy foundations but adds a strong element of OSINT and analytic tradecraft as used in security and intelligence contexts. Open-Source Intelligence (OSINT) traditionally refers to collecting and analyzing information from freely available sources (social media posts, news articles, databases, etc.) in a systematic way, often to produce actionable intelligence. Within the disinformation fight, OSINT skills allow an analyst (or student) to investigate the origin and spread of a suspicious story, to verify (or debunk) viral content, and to map out networks of accounts or websites that are pushing a narrative. For example, using OSINT tools one can perform reverse image searches to find where else an image has appeared (useful for spotting recycled or doctored images), query domain registration records to discover who likely operates a given "news" site, analyze metadata from videos, or track the social media amplification of a hashtag. The Romanian infosec community has recognized OSINT's value in this realm: the Romanian Association for Information Security Assurance (RAISA), with support from the U.S. Embassy, developed an "OSINT for Analyzing Fake News" guide (2023) containing step-by-step techniques and tools to help analysts and the public dissect false online content. The guide covers content verification methods (e.g. using browser extensions, blacklist checkers, or domain analysis to vet websites) and social media intelligence tools for platforms like Facebook, TikTok, and YouTube, as well as image and video analysis tools.

Such initiatives underscore how OSINT bridges technical investigation with media literacy. They also illustrate the concept of information laundering, showing how disinformation originating on social media can, if left unchecked, penetrate mainstream media and the entire public conversation.

Furthermore, structured analytic frameworks like DISARM (Disinformation Analysis and Risk Management) have been applied alongside OSINT to dissect influence campaigns. A recent case study by Romanian researchers (Bârgăoanu & Pană, 2024) matched the DISARM framework with evidence gathered via OSINT to analyze a cognitive hacking incident (the YouTube deepfake ads case). This study demonstrated, step by step, how open-source evidence, e.g. data from online ad libraries, social network analysis, etc. , can be used to attribute hostile influence actions and to anticipate their impact. By teaching such methodologies in an academic setting, we give students a taste of real-world narrative analytics: identifying the "who, what, how, and why" of an influence operation. It is essentially training students to be information detectives, combining data literacy, investigative curiosity, and understanding of geopolitical context.

Another key component is discourse analysis and narrative theory. While OSINT provides the factual verification and "follow the trail" skills, discourse/narrative analysis provides tools to decode the content and messaging itself. This means examining the language of propaganda or fake news: What frames are being used? What emotional appeals or rhetorical techniques appear? Who are the heroes, villains, victims in the story being told? What deeper cultural myths or conspiracy tropes does a given narrative tap into? For instance, in the Irish far-right disinformation context, researchers used narrative concept mapping to chart how different themes (COVID-19 conspiracies, anti-immigrant "Great Replacement" theory, anti-LGBTQ tropes, etc.) interconnected and reinforced a broader worldview[15]. In summary, the curriculum's conceptual backbone integrates security and educational perspectives: security studies contribute concepts like cognitive warfare, hybrid threats, influence tactics, and analytic frameworks (e.g. kill-chain analysis of information ops), while communication/media studies contribute pedagogy for critical thinking, media literacy principles, and social science methods of content analysis. By uniting these, we address both the "supply" and "demand" sides of disinformation – the supply side being the hostile actors and their methods (which students learn to investigate and anticipate), and the demand side being the public's susceptibility (which students learn to mitigate through awareness and communication

[15] Dunne, S.A.; Siapera, E., *Narrative Connections: Using Narrative concept Mapping to Understand the Irish Far-Right,* UCD Centre for Digital Policy, 2021

strategies). The next section translates these ideas into the concrete design of the "Cognitive Security & Narrative Analytics" course.

3. Curriculum design and pedagogy

In order to keep the pace with the current challenges in this particular vector of communicational warfare, the proposed structure of a mitigative curriculum is the following: "Cognitive Security & Narrative Analytics" runs one semester (14 weeks) at upper-undergraduate/Master's level, piloted (by a authorized Unuversity) at University X, Bucharest. It is co-taught by Communication Studies and Security Studies, 6 ECTS, with weekly 2h lecture + 2h lab, class size 20–30 for intensive practice.

Learning objectives. By course end, students can: (1) distinguish misinformation, disinformation, malinformation, propaganda, and "cognitive hacking," with recent RO/CEE examples; (2) apply OSINT to verify content, trace sources, and map narrative diffusion; (3) deconstruct narratives (frames, actors, appeals, intents); (4) vet source credibility rigorously; (5) design rapid-response and prebunking/counter-messaging playbooks; (6) act ethically (avoid amplifying falsehoods; respect legal/privacy bounds; balance counter-influence with free expression).

Modules and content.

- **Module 1 — The information environment & cognitive threats.** Hybrid/FIMI landscape; key definitions; global exemplars plus Romanian anchors (e.g., 2024 "TikTok Messiah" election interference). Readings draw on NATO/EU/academic work on cognitive warfare and the weaponization of public opinion. *Assignment:* classify a recent incident (propaganda/hoax/coordinated disinfo), outline harms and likely vectors.
- **Module 2 — OSINT fundamentals for info-ops.** Tradecraft analysis pipeline (plan–collect–analyze–report); hands-on with **reverse image search**, InVid keyframes, basic geolocation, WHOIS and web archives, advanced social search / light scraping (Twint/snscrape), simple network graphs (Gephi/Kumu). Minimal, free toolchain tailored to RO context, using RAISA's **OSINT for Analyzing Fake News** and companion materials (raisa.org; cyberlearning.ro). Method emphasis via **SIFT** (Stop, Investigate the source, Find better coverage, Trace claims) for real-time verification (clark.libguides.com; library.pugetsound.edu). *Lab:* team fact-check sprint on a viral item; document earliest seed, asset provenance, amplifiers, and confidence assessment in an analyst note.
- **Module 3 — Narrative analysis & mapping.** Frameworks to parse message architecture: central claim, frames, heroes/villains/victims, affective levers, myths, calls-to-action. Concept-mapping of families of narratives (e.g., Kremlin "declinism," anti-vax tropes) and **information-laundering** pathways from fringe to mainstream; cross-platform cascade detection (Telegram ↔ Facebook ↔ YouTube/X). *Assignment:* select a live storyline; map origin chain, thematic links, audience segmentation, and propose a counter-narrative.
- **Module 4 — Counter-influence & ethical communication.** Evidence-based **prebunking** and **debunking**; messenger strategy; timing (fill the information void), format (inoculation messaging), and harm-minimizing wording (avoid myth repetition). Build **rapid-response playbooks** and escalation trees; survey newsroom fact-checking partnerships and government/NGO StratCom cells using templates from IFES *Crisis Communication & Combating Disinformation Playbook*. Ethics: transparency, proportionality, legality, and avoiding retaliatory disinfo. *Group task:* 24–48h response plan for a pre-election smear: channels, core lines, spokespeople, outreach to vulnerable cohorts, and metrics.
- **Module 5 — Capstone simulation & policy links.** Multi-day **information-crisis simulation** (e.g., viral presidential deepfake): teams (GovComms, media/fact-check, civil society, platform liaison) verify with OSINT, perform rapid narrative forensics, coordinate takedown requests, issue public guidance, and brief decision-makers. Debrief ties to national/EU policy and cross-sector cooperation lessons drawn from the 2024 Romanian case (intelligence, platforms, law enforcement, EU scrutiny of platform conduct: globalwitness.org; globalwitness.org). Discuss needs for a formal RO hybrid/cognitive security strategy and university–NGO–state pipelines.

The curriculum translates cognitive security from concept to classroom by fusing OSINT tradecraft, narrative forensics, and ethical communication in a lab-centric, minimal-tooling design. Its five-module arc—foundations of the information environment, hands-on verification methods, narrative mapping, counter-influence playbooks, and a capstone crisis simulation, builds progressively from individual analytic rigor to coordinated response. Active learning (weekly "Disinfo Digests," team sprints) and cross-disciplinary teaching (communications + security studies) ensure students can verify provenance, decode persuasive frames, and communicate responsibly under time pressure in Romania's hybrid media ecosystem.

Scalable and cost-efficient, the model is readily portable across Romanian universities and partner institutions (media, NGOs, public bodies), strengthening "deterrence by denial" through a growing cadre of narrative-aware, OSINT-capable practitioners. By institutionalizing clear rubrics, ethical standards, and policy-facing simulations, the course creates an immediate pipeline for StratCom support while remaining future-proof via annually refreshed casework. In short, it equips graduates not only to spot and neutralize malign narratives, but to reinforce trust-preserving communication, an essential capability for democratic resilience.

4. Conclusions

This paper argued that cognitive security must be treated as a core educational objective, not merely a crisis-response function. The proposed Cognitive Security & Narrative Analytics curriculum operationalizes this shift by integrating OSINT tradecraft, narrative forensics, and ethical communication into a coherent, lab-centric program that is feasible within existing university constraints. Its primary role is twofold: first, to develop verifiable analytic competence at the individual level (source vetting, provenance tracing, narrative mapping); second, to institutionalize coordinated response capacity at the organizational level (rapid-response playbooks, cross-sector simulations, ethical guardrails). The added value lies in combining a minimal-tooling stack with rigorous method—lowering barriers for non-technical learners while preserving professional standards of evidence—thereby creating a scalable pipeline of practitioners who can serve media, public institutions, and civil society.

Beyond skill formation, the curriculum strengthens "deterrence by denial" in Romania's contested information space. By normalizing prebunking, fast verification, and trust-preserving messaging, universities can push resilience upstream, before malign narratives harden into beliefs. The capstone simulation connects academic learning to policy and practice, familiarizing students with platform transparency tools, government–NGO coordination, and crisis timing. Ethically, the program reinforces transparency, proportionality, and legality, countering the twin risks of cynicism ("everything is propaganda") and overreach (heavy-handed takedowns that erode civil liberties). The emphasis on reflective practice, short debriefs on cognitive biases, emotional triggers, and digital wellbeing, helps sustain performance in high-toxicity monitoring roles.

If such initiatives are not adopted, the risks compound. Narrative cascades will continue to exploit low media-literacy baselines and platform affordances, converting fringe frames into mainstream discourse at pace. Institutions face accelerated trust erosion: false claims about elections, public health, or national security can polarize communities, depress turnout, and delegitimize lawful outcomes. Operationally, public bodies remain reactive and tool-dependent, outsourcing verification to opaque vendors and losing tempo to adversaries who iterate narratives daily. Strategically, Romania forfeits an inexpensive resilience lever—education, while adversaries scale synthetic media, paid influence networks, and cross-platform laundering. The opportunity cost is profound: every cohort that graduates without verification fluency enlarges the addressable audience for hostile disinformation operations.

Implementation is straightforward. Universities can host the course jointly between communication and security studies; embed assessment rubrics that privilege evidence over opinion; refresh casework annually; and formalize pathways to practice via internships with StratCom units, newsrooms, and NGOs. A light-footprint "Narrative Security Lab" can anchor continuous monitoring, faculty–student research, and open briefings, turning universities into civic early-warning nodes. To guard against failure modes, politicization of curricula, performative fact-checking, or inadvertent censorship, the program should keep governance plural (academic + civil society advisory), publish methods, and separate analysis from advocacy in all student outputs.

In sum, the curriculum offers a replicable, cost-efficient template to harden Romania's cognitive domain by design. It equips graduates to verify faster, communicate cleaner, and coordinate better, converting classrooms into resilience multipliers and aligning higher education with democratic security. The alternative is to remain structurally behind the threat curve, paying in public trust what could be invested now in method, ethics, and people.

BIBLIOGRAPHY:

1. Alvarez, I. et all, *OSINT for analyzing fake news, a guide for journalists, investigators, and law enforcement* ISBN 978-973-0-37583-1, DOI: 10.19107/OSINT-4-FAKE-NEWS, 2023
2. Aronhime, L. (coord), *Countering cognitive warfare: awareness and resilience,* Johns Hopkins University & Imperial College London, 20th of May 2021
3. Bârgăoanu, A.; Pană, M., *Cyber Influence Defence: Applying the DISARM Framework to a Cognitive Hacking Case from the Romanian Digital Space*, Applied Cybersecurity & Internet Governance Journal, 2024
4. Dunne, S.A.; Siapera, E., *Narrative Connections: Using Narrative concept Mapping to Understand the Irish Far-Right,* UCD Centre for Digital Policy, 2021
5. Goury-Laffont, V., *Report ties Romanian liberals to TikTok campaign that fueled pro-Russia candidate,* Politico EU - December 21, 2024
6. Grigorescu A.; Alistar, T.V.; Lincaru, L., *Digital Skills, Ethics, and Integrity—The Impact of Risky Internet Use, a Multivariate and Spatial Approach to Understanding NEET Vulnerability Systems 2025*, Volume 13, Issue 8, 649, https://doi.org/10.3390/systems13080649

7. Lakshmanan, R, *Meta Disrupts Influence Ops Targeting Romania, Azerbaijan, and Taiwan with Fake Personas, The Hacker News*, May 30, 2025
8. Mutler, A., *Romania's 'TikTok Messiah' Is Gone But Admirers Live On The country's extreme right is prospering ahead of re-run presidential elections despite extensive evidence of continuing Russian subversion*, Center for European Policy Analysis (CEPA), March 27, 2025
9. Radu, A.F.; Petcu, I., The education system, the way to fight fake news, National Institute for Research and Development in Informatics – ICI Bucharest, Romania. Vol. 1: Security Above All!, 2024
10. Rickli, J.M.; Knappe, T, *Enhancing Cognitive Security and Societal Resilience to Counter Cognitive Warfare*, Geneva Center for Security Policy, 7th of October 2025.
11. Roozenbeek, J.; van der Linden, S.; Nygren, T., *Prebunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures*, Misinformation Review, Harvard Kennedy School, The Harvard Kennedy School, January 2020, Volume 1, Issue 2, https://doi.org/10.37016//mr-2020-008
12. Thoreau, H.D., *Cognitive Warfare, Applied Cognitive Effects Newsletter, Perception*, Vol 1, Issue 2, October 2025
13. Vaduva, S.; Alistar, V.; Thomas, A..; Lupiţu, C.; Neagoie, D.; *Moral Leadership in Business: Towards a Business Culture of Integrity*, 10.1007/978-3-319-42881-9, 2016
14. ***, *Global Risks Report 2025: Conflict, Environment and Disinformation Top Threats, World Economic Forum*, 2025
15. ***, *Romanian court annuls presidential vote after Russian interference claims Calin Georgescu won the first round of the election after being propelled by TikTok. Romania's security services pointed to "Russian hybrid actions,* The Washington Post, December 6, 2024