THE ROLE OF OPEN SOURCE INTELLIGENCE IN COUNTERING DISINFORMATION AND STRENGTHENING THE EUROPEAN UNION'S DIGITAL RESILIENCE

Yordan Terziev, PhD student,
Assoc. Prof. Velizar Shalamanov, PhD
Institute of Information and Communication Technologies,
Bulgarian Academy of Sciences

Abstract:

As the European Union confronts increasingly sophisticated campaigns of foreign information manipulation and interference, it must navigate the delicate balance between protecting democratic discourse and preserving fundamental rights. Unlike overt propaganda, modern disinformation efforts are subtle, often technically disguised, and designed to exploit the openness of the EU's media and political environment. In this context, Open Source Intelligence (OSINT) has emerged as a powerful too – not only for uncovering such operations, but for doing so in a way that aligns with the Union's legal and ethical commitments.

This paper[1] examines the evolving role of OSINT in the EU's disinformation response strategy, focusing on its methodological underpinnings, institutional adoption, and integration with emerging technologies like artificial intelligence. Drawing on concrete examples from recent threat reports, including the EEAS and France's VIGINUM, the analysis explores how OSINT contributes to a more resilient, transparent, and accountable model of digital defence. The article argues that for OSINT to remain both effective and legitimate, it must be embedded within a governance framework that prioritises proportionality, oversight, and public trust with a goal to maximize information resilience of our Alliance.

Keywords: OSINT, disinformation, information resilience, foreign interference, EU information policy

[1] The research on which this work is based has been funded by the National Research Program „Security and Defence“ under the framework agreement No ДСД-1/07.07.2022. for the execution of the National Research Program „Security and Défense“ between CNSDR-BAS and IICT-BAS, based on the Agreement No Д01-74/19.5.2022. between the Ministry of education and science and the defence Institute for the financing of the research program.

Introduction

In recent years, the information environment in Europe has undergone a transformation as rapid as it is destabilising. What was once a stable public sphere – anchored by national media systems and institutional gatekeepers – has given way to a fragmented and algorithmically mediated space, vulnerable to manipulation at scale. Nowhere is this vulnerability more apparent than in the context of foreign information manipulation and interference, or FIMI directly attacking our information resilience.[2] These activities, typically orchestrated by state-linked actors and networks of proxy operatives – including cybercriminal groups and ideologically aligned third parties, involve the deliberate use of deceptive tactics to influence public opinion, sow division, and erode institutional trust within EU Member States. The goal is not merely to mislead, but to shape the political terrain over time through repetition, misdirection, and strategic ambiguity[3].

Responding to this challenge requires more than reactive fact-checking or platform regulation. It demands the ability to anticipate, detect, and analyse disinformation campaigns as they unfold – before they cause political harm or polarise public debate beyond repair (it means to detect „weak signals" and monitor preparation activities in the attacking networks). This is where Open Source Intelligence has become increasingly valuable. By harnessing publicly available data – from social media posts and domain registries to satellite imagery and digital forensics – OSINT allows analysts to construct a clearer picture of how manipulation is orchestrated and disseminated. What distinguishes OSINT from more traditional intelligence approaches is not only the nature of its sources, but its transparency and replicability. It is, in effect, intelligence for open societies: observable, auditable, and consistent with democratic norms.

However, the integration of OSINT into policy and institutional frameworks is not without complications. While its potential for strengthening information resilience is considerable, its growing influence also raises legal, ethical, and methodological questions. Who decides which content is flagged? How can attribution be handled responsibly? And what safeguards ensure that surveillance does not masquerade as public interest research? As the EU moves to scale up its OSINT capacity, these questions become more than theoretical – they are foundational.

In the sections that follow, this paper traces the strategic evolution of OSINT within the EU, examining how it has been institutionalised and operationalised through tools like the DISARM framework and the FIMI Exposure Matrix. It

[2] European External Action Service (EEAS). (2023). *Foreign Information Manipulation and Interference: Threats and Policy Responses*. Brussels: EEAS.

[3] European External Action Service (EEAS). (2025). *Enhancing EU Information Resilience through FIMI Mapping and OSINT Integration*. Brussels: EEAS.

explores the interplay between human analysts and AI-assisted methods, drawing attention to the strengths and limits of automation in this domain. Case studies from recent EU elections, the MH17 investigation[4], and French-led initiatives such as Portal Kombat[5] provide a concrete basis for evaluating what OSINT can – and cannot – accomplish in the face of a complex and adversarial information landscape.

The Strategic Challenge of Foreign Information Manipulation

Foreign information manipulation and interference does not unfold as a singular event, nor can it be reduced to the spread of a false statement or image. Rather, it operates through layered, adaptive, and often transnational networks that blend technological infrastructure with strategic narrative design. These campaigns are rarely deployed in isolation. They are typically developed over time, often drawing from earlier patterns of manipulation, and are crafted to resonate with the local political and cultural environment of the targeted country.

What makes these operations particularly effective is their capacity to imitate and embed themselves within the legitimate information landscape. FIMI actors often appropriate the visual language, tone, and rhetorical structure of independent journalism, academic research, or citizen commentary. They create websites that mirror real news outlets, social media accounts that mimic credible individuals, and multimedia content that appears familiar and trustworthy. This capacity for mimicry, when combined with coordinated inauthentic amplification, allows disinformation to circulate widely before it is detected – if it is detected at all[6].

This complexity makes attribution especially challenging. Without specialised tools and interdisciplinary collaboration, it becomes nearly impossible to distinguish between an authentic citizen expression and a coordinated manipulation campaign. OSINT provides an entry point into this hidden architecture. Through domain tracing, digital fingerprinting, reverse image searches, and network analysis, investigators can reconstruct how narratives emerge, how they travel, and who is behind them. These methods are not speculative; they are grounded in verifiable data and can be peer-reviewed – a key feature that gives OSINT its institutional credibility.

The investigations conducted by VIGINUM into the disinformation networks dubbed „Portal Kombat" and „TigerWeb" offer an illustrative case. Analysts

[4] Bellingcat. (2015). *MH17 Investigation: Tracing the Trail of Buk Missile Launcher*. Retrieved from: https://www.bellingcat.com

[5] VIGINUM. (2025). *Annual Report on Foreign Digital Interference and FIMI Campaigns Targeting France*. Paris: Secrétariat général de la défense et de la sécurité nationale (SGDSN).

[6] VIGINUM. (2024). *Rapport d'activité 2023: Lutte contre les manipulations de l'information*. Paris: Service du Premier ministre - SGDSN.

uncovered a network of more than 190 websites, each designed to appear like a local or regional news outlet, but in reality, connected through shared design templates, hosting infrastructure, and content republishing patterns. These sites pushed coordinated narratives that aligned with Russian strategic interests – particularly regarding NATO, energy dependency, and the war in Ukraine. The exposure of this network was not based on leaks or classified data, but on open-source forensic techniques and public documentation[7].

Tools such as the DISARM framework[8] have further enabled analysts to categorise observed tactics in a consistent way. Developed by European researchers and fact-checkers, DISARM offers a standardised vocabulary for describing disinformation behaviours, including impersonation, narrative laundering, suppression, and distortion. Meanwhile, the FIMI Exposure Matrix goes beyond content analysis to include the infrastructural and behavioural indicators of manipulation – providing a structured lens through which to examine disinformation campaigns over time.

By moving beyond isolated content and focusing on structure, OSINT transforms disinformation analysis into something both forensic and strategic. It allows policymakers to identify not only what narratives are being pushed, but how they are operationalised and by whom. This knowledge, in turn, informs everything from diplomatic responses and platform engagement to public awareness campaigns and regulatory design.

From Concept to Capability: Institutionalising OSINT within the European Framework

The evolution of OSINT within the European Union has not been uniform. Initially, many of the most notable applications of open-source intelligence came from independent actors – investigative journalists, civil society analysts, and academics – working outside the confines of government institutions. However, as disinformation campaigns became more coordinated and technically sophisticated, so too did the need for a coherent, institutionally grounded response. What began as a decentralised, grassroots method has incrementally been integrated into formal structures of state and supranational governance.

A broader European framework has gradually developed to coordinate these efforts, encompassing regulatory, institutional, and collaborative elements. This co-regulatory framework includes instruments such as the Code of Practice on Disinformation, the Digital Services Act (DSA), and the European Democracy Action Plan (EDAP). The Code of Practice, in particular, serves as a key self-

[7] VIGINUM. (2025). *Portal Kombat: Une opération de manipulation de l'information d'origine russe*. Paris: SGDSN.

[8] EDMO & Fulde-Hardy, D. (2024). *DISARM Framework and FIMI Exposure Matrix: Analytical Tools for Disinformation Monitoring*. European Digital Media Observatory.

regulatory tool: developed initially in 2018 and strengthened in 2022, it brings together online platforms, civil society, and independent researchers to tackle disinformation[9]. Significantly, it requires signatories to produce regular transparency reports, which offer insight into detection mechanisms, content moderation, and data access – resources that OSINT practitioners increasingly rely on in their analyses.

In the Member States, for example, France's creation of the VIGINUM[10] agency in 2021 marked one of the earliest and most comprehensive national attempts to institutionalise OSINT as part of a broader strategy against foreign digital interference. Operating under the General Secretariat for Defence and National Security (SGDSN), VIGINUM was tasked with detecting, analysing, and publicly reporting on FIMI campaigns targeting French public debate. Its reports are methodologically transparent, accessible to the public, and anchored in open-source data – a combination that reinforces both credibility and democratic legitimacy.

At the EU level, the establishment of the European Digital Media Observatory (EDMO) has played a pivotal role in coordinating OSINT efforts across Member States. EDMO does not function as a top-down authority, but rather as a networked platform that links regional hubs, fact-checkers, academic researchers, and technical experts[11]. This decentralised model[12] reflects the Union's broader ethos of subsidiarity and respect for national diversity, while enabling common standards and interoperable methodologies. It is through EDMO, for example, that the DISARM framework gained traction as a shared reference point for coding disinformation behaviours across countries and languages.

Other initiatives embedded within the EU framework include the East StratCom Task Force (ESCTF) and the Rapid Alert System (RAS), both coordinated by the European External Action Service. The ESCTF, created in 2015, originally addressed Russian disinformation and has since evolved into a permanent fixture in the EU's strategic communication apparatus. The RAS complements these efforts by facilitating near real-time exchange of

[9] Yurukova, Mariya, Challenges to the Implementation of the European Approach to Countering Disinformation, Journal Diplomacy, February 29 / 2023, Diplomatic Institute, Ministry of Foreign Affairs, Republic of Bulgaria, issue:29, 2022, pages:140-150

[10] France SGDSN - VIGINUM. *Rapport d'activité 2024 - La lutte contre les ingérences numériques étrangères*. Paris: Secrétariat général de la défense et de la sécurité nationale (SGDSN), 2024.

[11] EDMO & Fulde-Hardy, J. *DISARM Framework: Harmonising the Detection of Disinformation*, European Digital Media Observatory, 2024.

[12] For Bulgaria and Romania as part of EDMO network under BROD project the regional approach is evolving and with the efforts of CIDC-AUBG to establish Balkan regional disinformation observatory the efforts are further enhanced. As of 2024 the established regional Sofia Information Integrity Forum for SEE and Black region provides a platform for consolidating various efforts around the base outlined by the EU.

intelligence related to foreign information manipulation and interference (FIMI), especially in times of crisis or elections[13].

Complementing these efforts, the G7 Rapid Response Mechanism (RRM) provides an international layer of coordination. Although not exclusively focused on the EU, the RRM has served as a valuable platform for sharing alerts and methodologies, particularly in the context of election security. It recognises that the vectors of FIMI are rarely confined to national borders and that robust response mechanisms must reflect this reality[14]. When disinformation narratives emerge in one jurisdiction, they often resurface – tweaked and translated in others. The ability to track these patterns in real time is essential for pre-emptive mitigation.

These institutional arrangements, while diverse in form, are unified by a common recognition: that disinformation is not simply a communicative nuisance, but a strategic threat to democratic stability. As such, it requires a response that is equally strategic – rooted not only in technical capability but in political will and shared responsibility (it is why a concept of the comprehensive approach to information resilience is getting traction). OSINT, when embedded within this framework, functions as more than a tool of detection. It becomes a lens through which institutions can understand their own vulnerabilities and develop a more resilient approach to public discourse.

This shift from fragmented initiatives to coordinated strategy marks a maturation of the EU's digital information security posture. Yet it also raises new questions about capacity, consistency, and control. How can Member States with differing levels of technical expertise contribute equally to a shared intelligence ecosystem? What mechanisms ensure that OSINT practices remain accountable across jurisdictions? And how can the EU maintain coherence without centralising authority to the point of eroding democratic flexibility?

Nonetheless, these challenges are addressed through increasingly interconnected governance mechanisms that balance EU-wide coordination with national flexibility. As the implementation of the DSA progresses and more Member States designate Digital Services Coordinators, there is growing momentum to incorporate OSINT findings into broader regulatory risk assessments and democratic resilience frameworks.

These tensions are not easily resolved. But they point to a necessary realisation: that the effectiveness of OSINT depends not only on what is seen, but on how institutions choose to respond. Intelligence, after all, is only as useful as the decisions it informs.

[13] Yurukova, M. (2024). Countering disinformation in EU Member States: the Importance of Not Going Back to Where We Started. In: Disinformation: Reloaded, Book Proceedings from the International Conference, University Press Sofia University „St. Kliment Ohridski“.

[14] G7 Rapid Response Mechanism. *Annual Report on Foreign Interference and Election Security*, 2022.

OSINT in Practice: Real-World Case Studies and Their Strategic Significance

The practical value of open-source intelligence becomes most evident when applied to real-world situations. While theoretical frameworks and institutional models are important, the credibility of OSINT rests on its performance under pressure. Over the past decade, several high-profile cases have demonstrated how open-source methods can meet – and at times exceed the evidentiary standards of more traditional intelligence operations. These cases also reveal OSINT's capacity not only to expose manipulation but to shift the political and legal response to it.

The investigation into the downing of Malaysia Airlines Flight MH17 over eastern Ukraine in 2014 remains one of the most widely cited examples of OSINT's power. In the absence of declassified government intelligence, independent researchers – most notably from Bellingcat – used satellite imagery, social media footage, vehicle identification techniques, and geolocation tools to reconstruct the movement of a Russian Buk missile launcher believed to be responsible for the attack. Their findings were detailed, independently verifiable, and cited in both journalistic and judicial proceedings[15]. What made the MH17 case particularly significant was not only its technical sophistication, but the fact that it emerged from public data and was made available for scrutiny. It demonstrated that even the most politically sensitive and technically complex investigations could be advanced through transparent, collaborative intelligence.

More recently, within the EU's own borders, OSINT has played a critical role in exposing election-related disinformation. In the lead-up to the 2024 European Parliament elections, analysts across several EU member states documented coordinated efforts to amplify false or misleading narratives targeting democratic institutions and political candidates. These campaigns blended authentic and deceptive content, often localised to match the cultural and political sensitivities of particular regions. They made strategic use of AI-generated imagery and text, pseudonymous personas, and carefully timed narrative deployment. What distinguished these operations from earlier forms of digital manipulation was their cross-platform design: disinformation would often originate on encrypted messaging apps or fringe websites, only to resurface on more mainstream platforms after being repackaged by sympathetic influencers or alternative news outlets[16].

OSINT practitioners were instrumental in tracing these campaigns across platforms and languages. Tools such as the DISARM codebook[17] and FIMI

[15] Bellingcat. *MH17 - Forensic Analysis and Open-Source Investigations*, 2015. Available at: https://www.bellingcat.com

[16] European External Action Service (EEAS). *Foreign Information Manipulation and Interference: Threat Report*, 2024.

[17] EDMO & Fulde-Hardy, J. *DISARM Framework and the FIMI Exposure Matrix: Methodologies for Tracking Disinformation Campaigns in the EU*, European Digital Media Observatory, 2024.

Exposure Matrix allowed analysts to classify tactics and infrastructure consistently, making it possible to compare events across countries and time periods. This standardisation, in turn, supported early warning systems and informed media literacy efforts aimed at debunking narratives before they reached critical mass.

Another case that illustrates the operational maturity of OSINT was the exposure of the Portal Kombat network by France's VIGINUM. This operation consisted of dozens of cloned websites designed to look like legitimate European news outlets, but in fact operated from servers registered through Russian-linked intermediaries. The sites distributed false or misleading stories, often mixing real events with manipulative framing, designed to undermine EU unity, cast doubt on Ukraine's sovereignty, and erode confidence in transatlantic alliance. VIGINUM's approach combined technical forensics with OSINT methodologies, such as link analysis, reverse image searches, and content correlation, to not only identify the fake domains, but also trace their connections to previously exposed Russian operations[18].

These case studies underscore OSINT's versatility. In moments of geopolitical tension, it can be a tool of strategic communication, reinforcing the EU's position with verifiable evidence. In legal or regulatory contexts, it can provide the documentation needed to justify sanctions or platform interventions. And in civil society, it empowers journalists and researchers to contest manipulation with facts. Yet each of these roles comes with different expectations and risks, reinforcing the need for clearly articulated norms and institutional guardrails.

What all these examples reveal is that OSINT is not simply a method of observing the digital world – it is a means of shaping how societies understand themselves in relation to it. Through its visibility, it creates accountability; through its openness, it strengthens legitimacy. And through its adaptability, it prepares democratic institutions to face a rapidly shifting information landscape.

Artificial Intelligence and OSINT: Expanding Capacity, Raising Questions

The integration of artificial intelligence into OSINT workflows has dramatically changed the scale and speed with which disinformation can be identified, mapped, and analysed. As the volume of digital content continues to grow exponentially, human analysts alone can no longer monitor, categorise, and assess manipulation campaigns in real time. AI offers the potential to filter signal from noise, to detect patterns across vast linguistic and cultural contexts, and to assist in generating timely responses. Yet this promise is tempered by

[18] France SGDSN - VIGINUM. *Rapport d'activité 2024 - La lutte contre les ingérences numériques étrangères.* Paris: Secrétariat général de la défense et de la sécurité nationale (SGDSN), 2025.

a range of limitations and ethical concerns that require careful governance. One of the most widespread uses of AI in OSINT today involves natural language processing (NLP). These systems can scan large volumes of text across multiple platforms and languages, identify common themes or emotional triggers, and flag content that fits predefined disinformation criteria. For example, during the 2024 European election monitoring period, OSINT analysts employed NLP models[19] to detect shifts in sentiment around key political issues, revealing how divisive narratives were being seeded in multiple languages but followed similar rhetorical patterns. In France, VIGINUM's work analysing thousands of political ads through Facebook's transparency tools demonstrated how NLP helped group content based on strategic framing, uncovering coordinated messaging clusters designed to stoke division and polarisation.

AI also supports visual OSINT through image recognition and deepfake detection. Given the growing use of synthetic media – particularly manipulated videos and AI-generated faces – such tools are essential for verifying authenticity. Visual similarity detection helps trace the origin of images and detect reuse or repurposing across contexts, allowing analysts to spot when old footage is recycled to present fabricated „evidence“ of current events. These capabilities, while powerful, are not infallible. They rely on training data and algorithms that may perform differently depending on the language, topic, or cultural context of the content they process.

Indeed, a major challenge identified in recent research is the uneven performance of AI systems across the EU's diverse linguistic landscape. The 2025 evaluation conducted by the International Network of AI Safety Institutes (INESIA) revealed that AI models demonstrated significantly lower accuracy when applied to languages with limited digital resources, such as Maltese or Latvian. These discrepancies pose a serious equity issue: if OSINT tools cannot reliably detect manipulation in all EU languages, some populations may be more exposed to interference simply because they are algorithmically underserved[20].

Moreover, the use of AI in OSINT raises urgent questions about explainability and accountability. Unlike traditional analytical processes, many AI systems – especially large language models – operate as „black boxes,“ producing results without clear pathways for understanding how those results were generated. This poses a risk in legal or regulatory settings where OSINT findings might inform policy decisions, content moderation, or even judicial action. Without transparent methodologies and human oversight, AI-generated intelligence may undermine rather than enhance institutional legitimacy.

To mitigate these risks, a hybrid approach has become increasingly important. Rather than replacing human analysts, AI should support them – enhancing

[19] France SGDSN - VIGINUM. *Rapport d'activité 2024 - La lutte contre les ingérences numériques étrangères*. Paris: Secrétariat général de la défense et de la sécurité nationale (SGDSN), 2025.

[20] INESIA (International Network of AI Safety Institutes). *Cross-Linguistic Evaluation of NLP and Disinformation Detection Systems in the European Union*, 2025.

their capacity while allowing for contextual judgement, critical reflection, and ethical oversight. This also calls for deeper investment in open, multilingual AI systems tailored to European values and linguistic diversity. If OSINT is to be a public good, the tools that power it must reflect that orientatio – not only in how they function, but in who benefits from them.

In sum, artificial intelligence holds enormous potential for enhancing OSINT. But that potential can only be fully realised if technical innovation is matched by thoughtful design, robust regulation, and a commitment to fairness and transparency. Otherwise, the tools meant to detect disinformation risk becoming opaque and unaccountable themselves – contributing to the very confusion they are meant to resolve.

Governing OSINT: Legal Limits and Ethical Imperatives

While OSINT offers a transparent and democratic approach to intelligence gathering, its growing influence in policy and security contexts calls for a clear and enforceable normative framework. Operating within the public domain does not exempt OSINT from legal and ethical scrutiny. On the contrary, its visibility and potential impact on public debate and rights protections demand a higher standard of care.

The General Data Protection Regulation (GDPR) remains the cornerstone of the EU's data governance regime, and its relevance to OSINT cannot be overstated. Even when information is publicly accessible, the act of aggregating, analysing, and interpreting it – particularly in ways that may profile individuals or communities – can trigger GDPR provisions[21].

For instance, linking metadata across platforms or inferring political or ethnic affiliations from behavioural data may constitute processing of sensitive data, which is tightly regulated under EU law. As such, any OSINT practice that touches on personal information must meet tests of necessity, proportionality, and legitimate interest, and must provide clear justification for its public utility.

In addition to the GDPR, other key legislative frameworks contribute to shaping the boundaries of responsible OSINT practice. The Digital Services Act (DSA)[22], in force since 2023, imposes obligations on very large online platforms to provide researchers – including OSINT analysts – with access to public data, risk assessments, and content moderation practices. This creates a legal basis for the use of platform data in scientific and investigative contexts.

[21] Nagendran, S. *GDPR and the Ethics of Open-Source Intelligence: Navigating Public Data and Private Rights*. Journal of Digital Law and Society, 2024.

[22] European Commission, *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*, 2023. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Similarly, the EU Artificial Intelligence Act (AI Act)[23] introduces requirements for transparency, human oversight, and ethical use of AI systems, including those applied in OSINT contexts. These instruments collectively promote responsible innovation and empower research while safeguarding against the misuse of personal and societal data.

Beyond data protection, the EU Charter of Fundamental Rights provides the normative foundation for all intelligence practices within the Union. Article 8 enshrines the right to the protection of personal data, while Article 11 guarantees freedom of expression and information. These rights are not absolute but must be balanced against each other. Any effort to track, categorise, or publicly attribute disinformation must be done in a way that does not chill legitimate speech or create a culture of over-surveillance. This is particularly relevant when OSINT is deployed in politically sensitive contexts, such as election monitoring, protests, or minority discourse.

To navigate these tensions, scholars and practitioners have called for dedicated ethical oversight of OSINT activity. Claire Benoit[24] and others have proposed the creation of OSINT ethics boards – independent bodies tasked with reviewing high-risk analyses, ensuring transparency in methodology, and advising on the proportionality of investigations. These bodies would not function as censors or compliance auditors, but as facilitators of responsible practice. Their presence would help ensure that OSINT remains a tool of public interest rather than a vector of institutional overreach.

More broadly, the rise of OSINT calls for a cultural shift in how intelligence is conceptualised in open societies. Intelligence should not be the exclusive domain of secrecy and coercion. When practised ethically and legally, OSINT represents a new model – an epistemology of democratic accountability. It brings visibility not only to threats but also to the processes of knowledge production itself. And in doing so, it invites scrutiny, participation, and dialogue, rather than reliance on authority alone.

The EU is uniquely positioned[25] to lead in this domain. With its strong legal foundations, commitment to digital rights, and diversity of media cultures, the Union has the normative architecture to define what ethical OSINT looks like in practice. But that leadership must be intentional. It requires investment in governance, training, and institutional reflexivity – not only to avoid misuse, but to model a form of intelligence that is worthy of the societies it aims to protect.

[23] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[24] Benoit, C. *Towards an Ethics Framework for OSINT: Transparency, Proportionality, and Oversight*. European Review of Intelligence Studies, 2023.

[25] At the same time in order EU to be effective is important to have level of maturity in each and every Member State in order to participate in the consultations and to reach well informed consensus-based decisions.

Conclusion: Open Intelligence for Open Societies / Open Source Intelligence as a Pillar of Democratic Resilience

In an era where information is contested, weaponised, and algorithmically amplified, the ability to see clearly – both technically and ethically – has become a strategic necessity. For the European Union, Open Source Intelligence is not merely a method of threat detection. It is a response to a deeper crisis: one in which the integrity of public discourse is under attack, and where trust in institutions cannot be defended through secrecy alone.

As this article has argued, OSINT enables the EU to confront foreign information manipulation not with suppression, but with exposure; not through centralized control, but through shared verification. It provides a toolkit for identifying disinformation, attributing its origins, and understanding its structural dynamics. But just as importantly, it offers a framework for democratic intelligence – one that is visible, contestable, and rooted in fundamental rights.

The examples examined – from the forensic reconstruction of MH17 to the coordinated defence of the 2024 EU elections – demonstrate that OSINT is more than a reactive instrument. It is proactive, strategic, and adaptable. It empowers not only institutions but citizens, researchers, and journalists to participate in the safeguarding of Europe's digital public sphere. And when combined with thoughtful regulation and ethical oversight, it serves as a bulwark against both disinformation and authoritarian overreach – helping to sustain the informational resilience that modern democracies depend on.

Yet OSINT's promise is not self-fulfilling. It must be continuously earned – through transparency in methodology, fairness in application, and humility in interpretation. As the Union expands its capabilities, it must also deepen its commitment to democratic principles. Artificial intelligence, multilingual coordination, and institutional integration are essential components, but none of them are sufficient without public trust.

In this sense, the future of OSINT is not only technical – it is political and cultural. It demands a vision of intelligence that is accountable to the public, responsive to pluralism, and anchored in law. The European Union has an opportunity to lead by example. Not simply by countering disinformation, but by showing how open societies defend themselves: not by closing down debate, but by insisting that truth matters, and that it can be pursued openly, together. OSINT will only succeed if it is thoughtfully embedded within a broader framework of information resilience – one that supports a comprehensive, coordinated, and principled approach to defending democratic discourse.

BIBLIOGRAPHY

- Benoit, C. (2023). *Bioethics and the Future of OSINT: Towards Normative Frameworks for Intelligence Transparency*.

- Bellingcat. (2015). *MH17: The Open Source Investigation*. Retrieved from https://www.bellingcat.com
- European Commission. (2024). *Political Guidelines 2024-2029*. Brussels.
- European External Action Service. (2023). *1st Report on Foreign Information Manipulation and Interference Threats*. Brussels: EEAS Strategic Communications Division.
- European External Action Service. (2024). *2nd Report on FIMI Threats: A Response Framework for Networked Defence*. Brussels: EEAS Data Team.
- European External Action Service. (2025). *3rd Threat Report: Exposing the Architecture of FIMI Operations*. Brussels: EEAS Data Team.
- European Commission (2023), *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*.
- European Commission (2021), *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*
- EDMO & Fulde-Hardy, M. (2024). *DISARM Elections Codebook: Typologies of Disinformation in EU Democratic Processes*. European Digital Media Observatory.
- France, SGDSN - VIGINUM. (2024). *Portal Kombat Network: Technical Report on Disinformation Infrastructure*. Paris.
- France, SGDSN - VIGINUM. (2025). *Annual Report: Information Threats and Electoral Protection in France*. Paris.
- G7 Rapid Response Mechanism. (2022). *Annual Report: Patterns of Strategic Information Manipulation*. Ottawa.
- INESIA. (2025). *Joint Testing Exercise: Evaluating AI Model Reliability in Multilingual OSINT Contexts*. Paris, London, Berlin.
- International Network of AI Safety Institutes. (2025). *Improving Methodologies for Model Evaluation Across Global Languages*.
- Nagendran, P. (2024). *Master's Thesis: The Ethics of OSINT in the AI Era*. University of Amsterdam.
- Pamment, J. (2024). *Resilience as a Framework for Deterrence in the Information Age: Lessons from Israel*. Hybrid CoE Report No. 10.
- VIGINUM. (2024). *Facebook Political Ads Audit Report*. Paris.
- VIGINUM. (2025). *Portal Kombat & TigerWeb: Mapping Russian Narrative Operations*. Technical Briefing.
- Yurukova, Mariya, Challenges to the Implementation of the European Approach to Countering Disinformation, Journal Diplomacy, February 29 / 2023, Diplomatic Institute, Ministry of Foreign Affairs, Republic of Bulgaria, issue:29, 2022, pages:140-150
- Yurukova, M. (2024). Countering disinformation in EU Member States: the Importance of Not Going Back to Where We Started. In: Disinformation: Reloaded, Book Proceedings from the International Conference, University Press Sofia University „St. Kliment Ohridski“