UDC 321.7:351.751.5]:352.07(477)"364"

Avery J. Kachmarsky,
Seton Hall University
ORCID ID: 0009-0008-9568-4834

WAR, INFORMATION, AND DEMOCRACY: UKRAINE'S APPROACH TO DECENTRALIZED TRANSPARENCY

Abstract. This essay explores the development of decentralized, citizen-led digital transparency networks in Ukraine, from their origins in post-Soviet governance challenges to their expansion during the ongoing war with Russia. The analysis examines how open-source intelligence communities and anti-corruption platforms have strengthened democratic accountability by improving access to information, supporting independent verification, and increasing public participation. The essay also examines how these systems challenge authoritarian governance by limiting control over information and exposing misinformation. In addition, the essay considers the limitations of these networks, including issues of misinformation, ethical concerns, and long-term sustainability. This examination highlights how Ukraine's use of digital transparency contributes to broader state-building processes while demonstrating the resilience of democratic governance during conflict.

Introduction

Ukraine's development of decentralized, citizen-led digital transparency networks reflects broader efforts to address long-standing governance challenges while adapting to the pressures of ongoing conflict. Since gaining independence in 1991, the country has faced persistent issues related to corruption, weak institutional trust, and uneven democratic consolidation. In response, both state institutions and civil society actors have increasingly turned toward transparency to improve accountability, particularly using digital tools and open data systems. These efforts have become significantly more visible during the war with Russia, where access to information and the ability to verify events in real time have taken on greater importance.

The expansion of Open-Source Intelligence (OSINT) networks and public transparency platforms has reshaped how information is produced, shared, and evaluated, allowing citizens to play a more active role in monitoring both government actions and wartime developments. At the same time, these systems have contributed to strengthening democratic accountability by increasing visibility and limiting the ability of actors to control information. However, while these networks offer clear advantages, they also introduce new challenges related to misinformation, ethical concerns, and sustainability.

Origins of digital transparency in Ukraine

Ukraine's system of digital transparency developed gradually in response to structural governance challenges that emerged after the collapse of the Soviet Union, particularly the concentration of political and economic power among elites and the resulting lack of public trust in state institutions. Throughout the post-Soviet period, corruption remained a persistent issue, shaping both domestic politics and public perceptions of legitimacy, as Ukraine continued to face

"a lack of political will, poor governance, corruption, military weakness, and dysfunctional law enforcement" *(Iryna Solonenko, 2015).*

These conditions contributed to growing dissatisfaction with formal institutions and created an opportunity for civil society organizations to push for reforms that emphasized openness, accountability, and citizen involvement, particularly during key political moments such as the Orange Revolution and the Euromaidan protests. These movements highlighted the limitations of formal democratic structures and reinforced the idea that legitimacy depended not only on elections, but also on sustained public oversight. Over time, new forms of digital participation began to change how accountability could work in practice, as "the online community is filming, posting and resharing evidence of Russian war crimes… in the hope that someday, victims might hold the guilty to account" *(Jack Crawford and Andrea Ricci, 2024).*

One of the most significant outcomes of these reform efforts was the introduction of digital governance tools, especially open-data platforms designed to increase transparency. The establishment of ProZorro in 2016 marked a major institutional shift, operating on "the main principle of eProcurement system: 'Everyone can see everything.'" *(Nadiia Konashchuk, 2016).*

This system enabled public access to procurement processes, allowing journalists, watchdog organizations, and citizens to monitor state spending, as the platform "publishes the structured date online… [and] these achievements represent an outstanding opening in the area of access to information…[and] progress in civic participation…" *(Open Government Partnership).*

Procurement reform made it easier for people to see how public money and other assets are being used and spot potential corruption. By embedding transparency into formal systems, Ukraine moved toward a model in which accountability is supported by both institutional structures and public engagement.

Early forms of OSINT began to emerge, especially following Russia's illegal annexation of Crimea in 2014. These networks relied on publicly available data, including satellite imagery and social media content, to track developments and verify events. OSINT is defined as "intelligence produced by collecting, evaluating and analyzing publicly available information with the purpose of answering a specific intelligence question," often outside traditional state-controlled frameworks *(Ritu Gill, 2023).*

Through this, information gathering became more decentralized, allowing non-state actors to contribute directly to analysis and verification processes.

Expansion during wartime conditions

The full-scale, illegal Russian invasion of Ukraine in 2022 accelerated the expansion of decentralized transparency networks, as the need for timely and reliable information increased under conditions of conflict. As state institutions faced operational pressure, citizen-led initiatives expanded rapidly, filling gaps in information collection and verification. OSINT communities became central to documenting the war, using techniques such as geolocation, satellite analysis, and cross-referencing digital evidence to track developments in real time. This transformation has been described as the emergence of a "transparent battlefield," in which conflicts are increasingly visible through publicly accessible data *(Nicholas Romanow, 2025).*

The structure of these networks reflects a high degree of decentralization, with a wide range of actors contributing to information gathering and analysis. Rather than relying on a single institutional framework, this system draws from multiple streams of publicly available data, as

"these public sources can range from… unencrypted radio messages [to] public social media posts." *(Vanessa Smith-Boyle, 2022).*

This variety of inputs allows different actors, including journalists, investigators, civil society organizations, and volunteers, to participate in collecting and interpreting information, strengthening the overall depth and reliability of available intelligence. As a result, these networks can respond quickly and flexibly to developments, with verification and analysis occurring across multiple channels rather than through a centralized authority. Citizen participation has played an important role in this expansion, as individuals contribute images, videos, and firsthand accounts that are then analyzed within larger networks. As a result, citizens have become active participants in documenting the conflict, rather than just passive observers.

Strengthening democratic accountability

Decentralized transparency networks have strengthened democratic accountability in Ukraine by increasing visibility into state actions and reducing the likelihood that misconduct can remain hidden. Unlike traditional oversight methods that rely primarily on centralized institutions, these systems distribute monitoring capabilities across a range of actors, making it more difficult to suppress information. This shift has contributed to a more open political environment, where information can be independently verified and widely shared. Independent verification represents one of the most significant functions of these networks, particularly in a conflict setting where competing narratives are common. OSINT investigators have used digital evidence to confirm events such as missile strikes and troop movements, ensuring that "the auditing and verification of all digital items… can be carried out by referring to the third-party record holders (*Starling Lab, 2023).*

This approach allows claims to be tested against independently preserved evidence rather than relying solely on official statements or single sources. By combining web archives, metadata, and field documentation, investigators create an evidence base that is more resistant to manipulation or distortion, since having multiple sources makes it much harder for false information to go unchecked. This ability to systematically verify information strengthens trust in reporting and reduces the influence of misinformation, particularly in fast-moving conflict environments where false narratives can spread quickly.

In addition to improving verification, these systems have expanded opportunities for civic participation by allowing individuals to contribute directly to monitoring and reporting processes. This reflects key democratic principles that emphasize the importance of public engagement in governance. Recently, this has taken the form of distributed investigative efforts and documentation of Russia's ongoing strikes on Ukraine's infrastructure, including civilian missile impacts, Iranian Shahed drone attacks on energy facilities, and damage to urban areas in cities such as Kharkiv and Odesa. Civilians and volunteer investigators frequently share videos and images of these incidents, which are then cross-referenced with satellite imagery and archived to confirm timing, location, and impact. Documentation of civilian killings in Bucha used satellite imagery from Maxar Technologies alongside open-source material to challenge Russian narratives about what happened and when. John Scott-Railton, a senior researcher with the Citizen Lab at the University of Toronto, stated that OSINT has been "an unprecedented amount of information, and [it is] making the… operation of Russia's propagandists a lot harder," as there used to be no widely available way of contradicting with factual evidence false narratives *(Kazi Stastna, 2022).*

These examples demonstrate the necessity of civilian participation and collaboration with fellow civilians and larger groups to track down information and holding individuals or groups accountable. By fostering ongoing participation, rather than limiting involvement to periodic democratic processes, decentralized transparency networks strengthen the relationship between citizens and the state while reinforcing accountability.

Challenging authoritarian governance

The rise of decentralized transparency networks in Ukraine also challenges governance models that rely on tightly controlled information environments. In such systems, authority is often maintained by limiting access to information, shaping what can be publicly seen, and controlling how events are presented. Ukraine's wartime information environment makes this harder by allowing multiple, independent ways of collecting and sharing evidence that do not depend on official sources and continue to exist alongside state or military communications.

This has been seen in the documentation of forced deportations and filtration practices in occupied territories, where satellite imagery, transport logs, and leaked administrative records have been combined to reconstruct civilian movement patterns. In doing so, this documentation directly challenges authoritarian governance by limiting the ability of authorities to conceal or selectively present what is happening on the ground. For instance, open-source investigators tracked transit routes from Mariupol to filtration sites in Russia-occupied regions by aligning train schedules with Telegram posts and commercial satellite captures *(Dean Kirby, 2023).*

Similarly, analysts monitoring the early years of the expanded war have examined recovered battlefield components to understand evolving strike capabilities. The components have included "'universal planning and correction' modules… (UMPK)… can be attached to Russian FAB-250 or FAB-500 general purpose air-dropped munitions to increase their range and add an element of guidance… 'dumb' bombs..." *(Conflict Armament Research).*

These findings show that verification becomes distributed across many independently maintained datasets, reducing the ability of any one authority to fully define the narrative.

The resilience of these networks is also supported by their presence across multiple platforms. Information related to battlefield developments is frequently shared across messaging applications, mapping tools, and satellite databases, making it difficult for any single actor to fully remove or control it. Because information is not managed by one central source, this structure limits the ability to shape or restrict narratives in the same way as centralized systems. As a result, transparency develops through the accumulation of independently verified pieces of evidence, rather than through a single controlled channel.

Limitations and ongoing challenges

Despite their advantages, decentralized transparency systems still face several ongoing challenges. One major issue is that different investigative groups often use different methods to verify information, which can lead to inconsistent results. For example, during the July 2024 attack on a pediatric hospital in Kyiv, "which killed over 35 people…, injured another 190 "OSINT investigators" in Ukraine, and further afield were quick to identify the make and composition of the Kh-101 missile that hit the hospital, denying Russia the opportunity to mask the attack *(Crawford and Ricci, "Puzzling Pieces").*

Another challenge is the growing use of disinformation within open data spaces. False or manipulated content, including AI-generated images and altered drone footage, has increasingly

been used to confuse or mislead users. In some cases, fake material has circulated alongside real evidence, making it harder to distinguish what is accurate. As a result, investigators have had to rely on more advanced methods, such as checking metadata or analyzing visual details like shadows, to confirm authenticity.

Ethical concerns have also become more important as these practices expand. For instance, reconstructing attack timelines in heavily populated areas like Kherson can raise questions about whether sharing detailed, location-based information might unintentionally put civilians at risk. In response, some groups have started delaying the release of sensitive information or removing certain details to balance transparency with safety. Finally, maintaining these systems over time remains a challenge. The amount of data collected, from satellite imagery to drone footage and civilian uploads, is extremely large and continues to grow. This creates pressure on storage systems and makes it difficult to organize and analyze information efficiently. Some organizations are beginning to test new ways of storing and backing up data, but these solutions are not yet widely adopted, making long-term sustainability an ongoing concern. Overall, while decentralized digital transparency networks experience challenges, they have become a key part of how accountability, information sharing, and public participation function in Ukraine and aim to limit the role of propaganda from authoritarian regimes.

References

Conflict Armament Research. "Russia Develops Guidance Modules for Air-Dropped Munitions." ArcGIS StoryMaps. December 2023. https://storymaps.arcgis.com/stories/e4f0a90ddd7d4cd6b1d889704f6b2396.

Crawford, Jack, and Andrea Ricci. 2024. "Puzzling Pieces: OSINT and War Crime Accountability in Ukraine." The Royal United Services Institute. September 26, 2024. https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine.

Gill, Ritu. 2023. "What Is Open-Source Intelligence?" SANS Institute. February 23, 2023. https://www.sans.org/blog/what-is-open-source-intelligence.

Kirby, Dean. 2023. "Open-Source: Finding Russia's Filtration Camps." The Centre for Investigative Journalism. June 28, 2023. https://tcij.org/summer-conference-event/open-source-finding-russias-filtration-camps/.

Konashchuk, Nadiia. 2016. "eProcurement System ProZorro." Observatory of Public Sector Innovation. October 29, 2016. https://oecd-opsi.org/innovations/eprocurement-system-prozorro/.

Open Government Partnership. "Open Public Procurement (UA0064)." Open Government Partnership. n.d. https://www.opengovpartnership.org/members/ukraine/commitments/ua0064/.

Romanow, Nicholas. 2025. "The Transparency Trap: Risks of Deception in the Age of OSINT." U.S. Naval Institute. January 2025. https://www.usni.org/magazines/proceedings/2025/january/transparency-trap-risks-deception-age-osint.

Smith-Boyle, Vanessa. 2022. "How OSINT Has Shaped the War in Ukraine." American Security Project. June 22, 2022. https://www.americansecurityproject.org/osint-in-ukraine/.

Solonenko, Iryna. 2015. "Ukrainian Civil Society from the Orange Revolution to Euromaidan: Striving for a New Social Contract." Institut für Friedensforschung und Sicherheitspolitik (IFSH). February 20, 2015. 219. *https://www.ifsh.de/file-CORE/documents/yearbook/english/14/4_DD_IFSH_OSCE_Yearbook_2014_1749-1_Freigabe.pdf.*

Starling Lab. 2023. "New Evidence Techniques Document Bombed Ukrainian Schools For ICC." The Starling Lab for Data Integrity. 2023. *https://www.starlinglab.org/new-evidence-techniques-document-bombed-ukrainian-schools-for-icc/.*

Stastna, Kazi. 2022. "The Smartphone War: Soldiers, Civilians and Satellites Give the World a Window onto Russian Invasion." CBC NEWS. April 8, 2022. *https://www.cbc.ca/news/world/ukraine-osint-war-1.6410037.*