Assessing Geopolitical Risk: How OSINT Tools Can Address Current Intelligence Challenges

Key Takeaways

- Open source intelligence (OSINT) is valuable for public sector intelligence applications. Publicly available information (PAI) supports geopolitical assessments by providing insights often unavailable through classified sources—like on-the-ground activity, real-time alerts, and broader trends in areas of interest.
- OSINT provides a lot of data, but analysts lack the resources to process and analyze it efficiently. OSINT also raises privacy concerns for governments, who are still navigating the laws, policies, and governance required to optimize public data.
- OSINT tools aren't a silver bullet solution for these challenges. But procuring easy-to-use OSINT software with adequate regional coverage and real-time data is crucial for timely, accurate intelligence.
- These three pillars—ease of use, global data coverage, and real-time access—are valuable for current geopolitical applications like the Russia-Ukraine crisis.

Assessing Geopolitical Risk in the Modern Information Environment

Geopolitics evolve rapidly. For government agencies, keeping pace with new developments is becoming a greater challenge: information is abundant, but resources are scarce.

The public sector has quickly realized the value of open-source intelligence (OSINT) in the last few years. Combined with classified intelligence sources, this public information provides immense value for intelligence applications like assessing geopolitics. The problem is that open sources only add to data overload issues faced by analysts.

In the United States, activities in a range of geographies—from global powers like China and Russia to unstable regions like Afghanistan and Syria—all have potential impacts on US persons and interests.[1] Transnational issues, like COVID-19, climate change, migration, terrorism, and organized crime also intersect US interests.

Governments need to understand strategic environments, anticipate potential threats, and support ongoing and planned operations in these regions.[2] Without the ability to produce accurate, timely information, decision-makers could jeopardize national interests, physical assets, and public safety.

To address data overwhelm and nascent OSINT practices in government, intelligence leaders must invest in easy-to-use OSINT tools that prioritize real-time data and regional coverage. This resource explains the current OSINT values and challenges faced by intelligence teams for geopolitical monitoring. It also recommends three key OSINT tool capabilities to address current challenges.

[1] Office of the Director of National Intelligence: "Annual Threat Assessment of the US Intelligence Community," April 9, 2021.
[2] Office of the Director of National Intelligence: "National Intelligence Strategy of the United States of America," 2019, P. 9.

OSINT Gaining Precedence

The explosion of social media and other online channels gives analysts an abundance of information for geopolitical use cases. Open source intelligence (OSINT) is by no means a new practice—but this designated "INT" has gained priority for intelligence professionals over the last few years. Why?

Now that over half the world's population[3] is active internet users, the web provides data sets with great intelligence value for geopolitical assessments. Technological, economic, and military actions also can no longer solely guarantee national security as adversaries leverage information environments to achieve their goals. Publicly available data is now required to better understand adversary capabilities and protect national interests.

In February 2021, the CSIS Technology and Intelligence Task Force called for OSINT to be upgraded to "core" intelligence alongside other classified INT's, like SIGINT. The Defense Intelligence Agency—which relies on unclassified, open sources for 80% of its reports—has also been designated as the lead agency for OSINT.[4] Open sources include mainstream and fringe social media, regional networks, deep and dark websites, and surface web content like maps, public records, and satellite imagery.

WHY OSINT IS A CORE "INT"

Provides insights unavailable from other sources like classified INT's	Doesn't just focus on key targets—also shows broader trends in areas of interest	Improves speed-to-information for breaking events

[3] Ying Lin: "10 Internet Statistics Every Marketer Should Know in 2021," Oberlo, May 9, 2021.
[4] Byron Tau: "Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data," The Wall Street Journal, Dec. 10, 2021.

OSINT Challenges for National Security

OSINT's value doesn't come without challenges. As demand for OSINT has increased in government and military, this sector struggles with:

- **Data overload.** Open source data provides valuable insights, but its sheer volume means that analysts are overwhelmed and can't process and analyze relevant data efficiently. According to cross-industry research, less than half of an organization's structured data is utilized, and less than 1% of its unstructured data (which open sources often produce) is used.[5] To put "data abundance" in perspective, the US military contractor MAG Aerospace can gather over ten terabytes of data on a three-hour mission.[6]
- **Privacy and compliance standards.** Using open-source data for government surveillance and investigation has raised privacy concerns. For example, domestic mobile data has been monitored by the Defense Intelligence Agency without a warrant, which has been criticized by privacy advocates.[7] Privacy issues may become a greater concern as regional legislation, like the GDPR, evolve.
- **Lagging adoption strategies.** OSINT practices have been evolving in the commercial sector for some time. However, the national security community was not prepared for PAI's increased demand. This means that government intelligence operations are still catching up in terms of the technologies, laws, policies, and governance required to optimize OSINT.[8] Open source data risks becoming underutilized, which could cause information gaps and minimize OSINT's value.

> *"SIGINT, GEOINT and HUMINT reporting, for example, is well understood by analysts, has established tradecraft, and is supported by a deep bench of specialists… In the world of open source, the lack of common tradecraft and reach-back support… makes evaluating the accuracy and validity of PAI/CAI challenging, and all-source analysts may be understandably reluctant to use that reporting."* [9]

[5] Leandro DalleMule & Thomas H. Davenport: "What's Your Data Strategy?" Harvard Business Review, May-June 2017.
[6] Loren Blinde: "Solving the Problem of Data Overload," Intelligence Community News, April 20, 2021.
[7] Byron Tau: "Military Intelligence Agency Says It Monitored U.S. Cellphone Movements Without Warrant," The Wall Street Journal, Jan. 22, 2021.
[8] Bob Ashley and Neil Wiley: "How the Intelligence Community Can Get Better at Open Source Intel," Defense One, July 16, 2021.
[9] Bob Ashley and Neil Wiley: "How the Intelligence Community Can Get Better at Open Source Intel," Defense One, July 16, 2021.

OSINT Tools for Geopolitical Monitoring

Intelligence leaders can address some of these issues by collaborating with commercial technology providers. Commercial OSINT solutions help analysts streamline data overload, address privacy concerns, and establish OSINT tradecraft for national security.

OSINT tools include software that helps analysts collect, process, and analyze open source data more efficiently. There are a variety of commercial OSINT tools available, but not every solution is designed to address public sector requirements. By prioritizing the following features, intelligence leaders can procure solutions that address common challenges and improve the accuracy and timeliness of geopolitical assessments.

REAL-TIME DATA

OSINT tools need to collect and display data in real-time (or as close to real-time as possible) to ensure timely delivery. For example, many OSINT tools ingest public social media data, but not all tools provide real-time access. While one tool may render a post within a few seconds of it showing up online, others may take several hours.

Intelligence professionals can avoid this lag by verifying latency times with technology vendors, prioritizing solutions with real-time or near real-time data. This is valuable for geopolitical applications because open sources often provide the earliest indicators of new developments and breaking events.

REGIONAL DATA COVERAGE

If an analyst is assigned to a specific area, OSINT has immense value. Social media, news, and fringe networks utilized in a target area can illuminate public sentiment, on-the-ground activities, and media manipulation more accurately than sources external to the region. However, this insight is easily overlooked by analysts who are unfamiliar with regional information sources.

Intelligence teams tasked with monitoring global regions should procure OSINT solutions from providers who prioritize global data coverage. This gives analysts access to covert information sources relevant in specific areas, like Russia, Asia-Pacific, the Americas, Europe, the Middle East, and Africa.

SOFTWARE USABILITY

Analysts are more likely to recommend tools based on their usability over their perceived usefulness.[10] Some commercial intelligence products are powerful but have steep learning curves. This is not ideal when analysts are already inundated with data and inexperienced with OSINT tradecraft.

Intuitive OSINT software has a simple UI, an intuitive workflow, avoids click-heavy processes, and only displays relevant information, reducing noise and false positives. This helps address data overwhelm and increases tool adoption and usage. These features are necessary to familiarize analysts with OSINT tradecraft and optimize its value.

ADDRESSING PRIVACY AND COMPLIANCE CONCERNS

Geopolitical applications require public data generated by global populations. This could raise concerns around data privacy, especially in regions governed by privacy legislation. Privacy-focused software vendors understand global privacy legislation, have relationships with mainstream data providers, and update software features to align with current privacy standards. This addresses privacy issues that agencies may encounter when accessing data themselves. Partnering with these vendors also helps fill current gaps in laws, policies, and governance preventing the public sector from optimizing OSINT.

[10] Mandeep K. Dhami: "A Survey of Intelligence Analysts' Perceptions of Analytic Tools," Nov. 13, 2017.

Example: Monitoring the Russia-Ukraine War With OSINT

> "The rules of war have cardinally changed... The effectiveness of non-military tools in achieving strategic or political goals in a conflict has exceeded that of weapons."
>
> *— Valery Gerasimov, Russian General of the Army* [11]

Situation

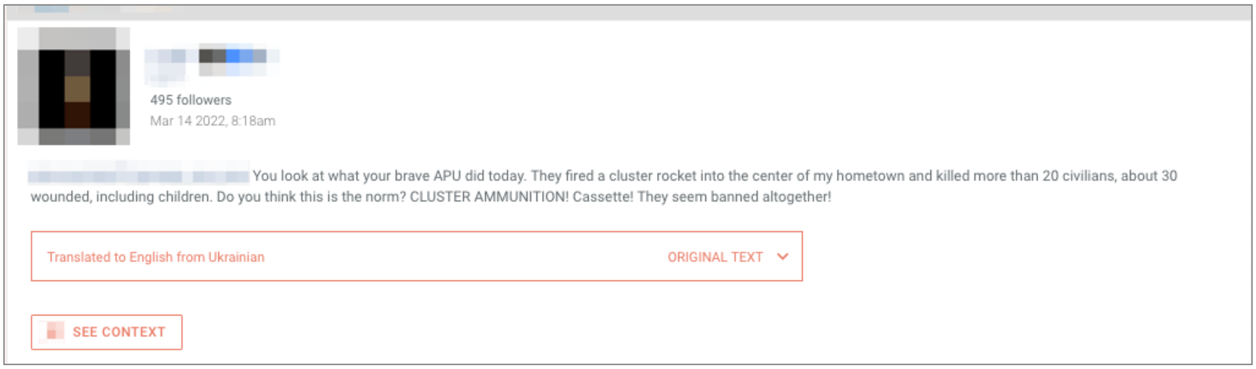
Russian activity in Ukraine has raised concerns from Western governments since the Crimean Peninsula's annexation in 2014. Skirmishes continued intermittently, but tensions renewed in spring 2021 and again in fall 2021 when significant Russian military buildup near Ukraine's border sparked fears of a potential invasion—which was launched on February 24, 2022.

OSINT played a significant role in the conflict on two fronts: the physical battlefield and the information space. Open-source data, largely from social media and satellite imagery, were widely used by NATO states and OSINT experts to monitor on-the-ground activities and fact-check narratives.

[11] Michael Bernard: "A Method to Assess Sociocultural and Geopolitical Responses to Concurrent Infrastructure, Information & Economic Attacks," Sandia National Laboratories Department of Energy, June 13, 2019, P. 2.

ON-THE-GROUND ACTIVITIES

For example, some experts claim that Google's public traffic data helped predict the Russian invasion on February 24th.[12] Satellite imagery helped monitor the progress of Russian vehicles, indicating setbacks and advances. Open-source photos and videos also determined more accurate casualty numbers, as well as the use of specific military tactics like cluster munitions.[13]



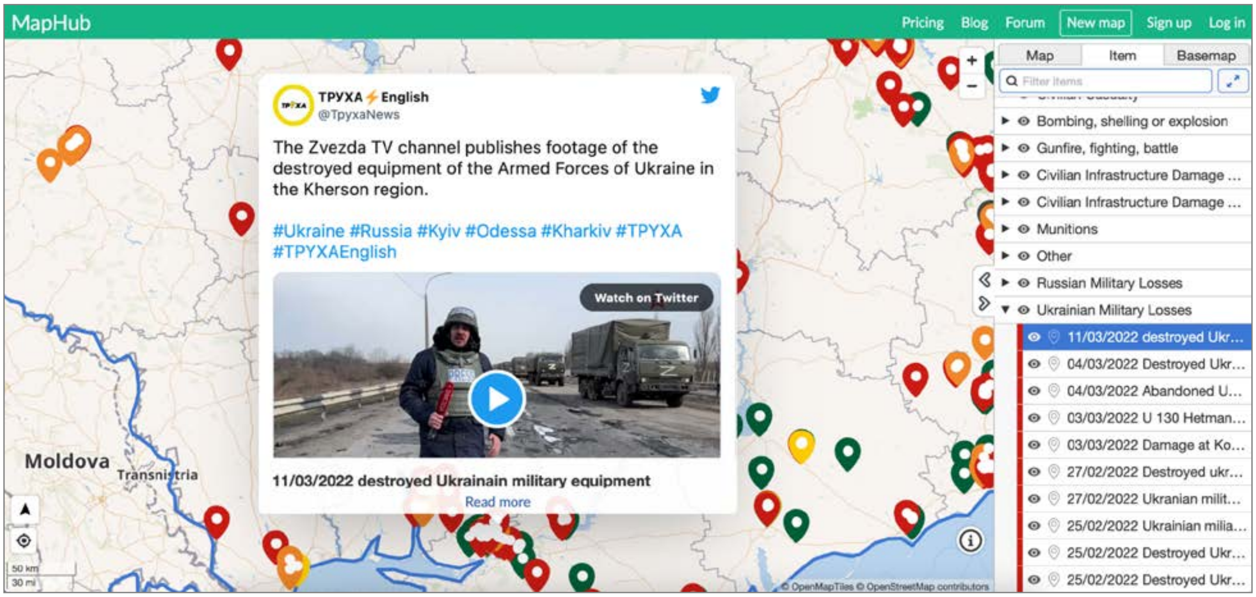
[redacted]

495 followers
Mar 14 2022, 8:18am

[redacted] You look at what your brave APU did today. They fired a cluster rocket into the center of my hometown and killed more than 20 civilians, about 30 wounded, including children. Do you think this is the norm? CLUSTER AMMUNITION! Cassette! They seem banned altogether!

A social media user reports the use of cluster munitions targeting civilians in their hometown on March 14, 2022 (post translated from Ukrainian)—discovered using the Echosec Platform.

Widespread social media use means that anyone with a phone essentially becomes a battlefield sensor in a conflict zone. As users post photos and videos from the ground, analysts can monitor attacks and assess damage in real-time. Social media content can also precisely locate these activities, either through geotagging or image-based location analysis.



TPYXA⚡English
@TpyxaNews

The Zvezda TV channel publishes footage of the destroyed equipment of the Armed Forces of Ukraine in the Kherson region.

#Ukraine #Russia #Kyiv #Odessa #Kharkiv #TPYXA #TPYXAEnglish

11/03/2022 destroyed Ukrainain military equipment

MapHub
Pricing
Blog
Forum
New map
Sign up
Log in
Map
Item
Basemap
Filter items
Bombing, shelling or explosion
Gunfire, fighting, battle
Civilian Infrastructure Damage ...
Civilian Infrastructure Damage ...
Munitions
Other
Russian Military Losses
Ukrainian Military Losses
11/03/2022 destroyed Ukr...
04/03/2022 Destroyed Ukr...
04/03/2022 Abandoned U...
03/03/2022 U 130 Hetman...
03/03/2022 Damage at Ko...
27/02/2022 Destroyed ukr...
27/02/2022 Ukranian milit...
25/02/2022 Ukrainian milia...
25/02/2022 Destroyed Ukr...
25/02/2022 Destroyed Ukr...
Watch on Twitter
Read more
Moldova
Transnistria
50 km
30 mi
© OpenMapTiles © OpenStreetMap contributors

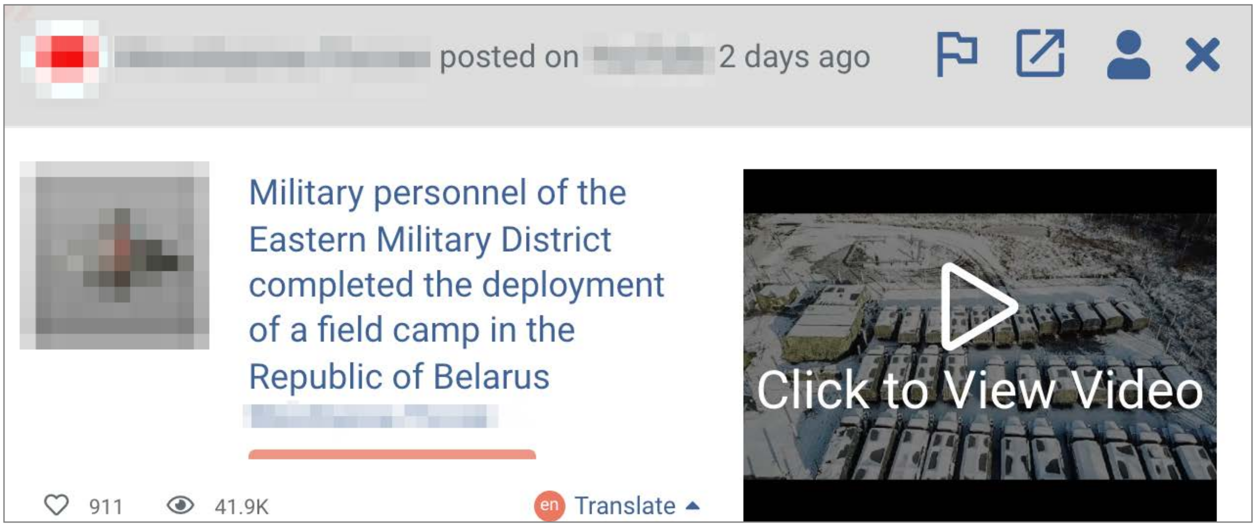
OSINT investigations have generated tools like the Russia-Ukraine Monitor Map above, a crowdsourced effort to track and verify military activities.[14]

[12] Aardon Gordn and Matthew Gault: "Google Maps Live Traffic Showed the Russian Invasion of Ukraine," Vice, February 24, 2022.
[13] Bellingcat: "Invasion of Ukraine: Tracking use of Cluster Munitions in Civilian Areas," February 27, 2022.
[14] Centre for Information Resilience, Bellingcat, Conflict Intelligence Team: "Russia-Ukraine Monitor Map," March 2022.

INFORMATION WARFARE

Russia has been known for dominating information warfare for several years—from leveraging QAnon conspiracies in the United States to justifying military actions in Syria and Georgia. But Russia's invasion of Ukraine was different: by the time of the invasion, governments and social media companies understood these tactics well enough to predict and counter their influence more effectively.

Ukraine and its allies were proactive in identifying and verifying Russian narratives. Even before the invasion, analysts countered the Kremlin's denial of a military buildup by widely sharing images of the scale of Russian border activities. Ukraine and its network of allies also effectively predicted and debunked Russian claims, using social media analysis to verify narratives.[15]



[redacted] posted on [redacted] 2 days ago

Military personnel of the Eastern Military District completed the deployment of a field camp in the Republic of Belarus

[redacted]

♡ 911 41.9K

Social media content shows an increase in military activity in Belarus in early February 2022, visualizing the scale of escalation in eastern Europe (post translated from Russian).

SOLUTION

REAL-TIME DATA	GLOBAL DATA COVERAGE	USABILITY
Conflicts like the Ukraine-Russia war evolve daily. Real-time data improves speed-to-information and ensures that analysts understand new developments as soon as they surface on public channels like social media.	There are dozens of OSINT sources unique to the Russia-Ukraine region, including social networks like VK, fringe forums like Dvach, and state media outlets. Comprehensive regional coverage minimizes information gaps created by sticking to familiar networks.	An easy-to-use OSINT tool helps analysts work more efficiently, address data overload, and optimize the value of open-source content.

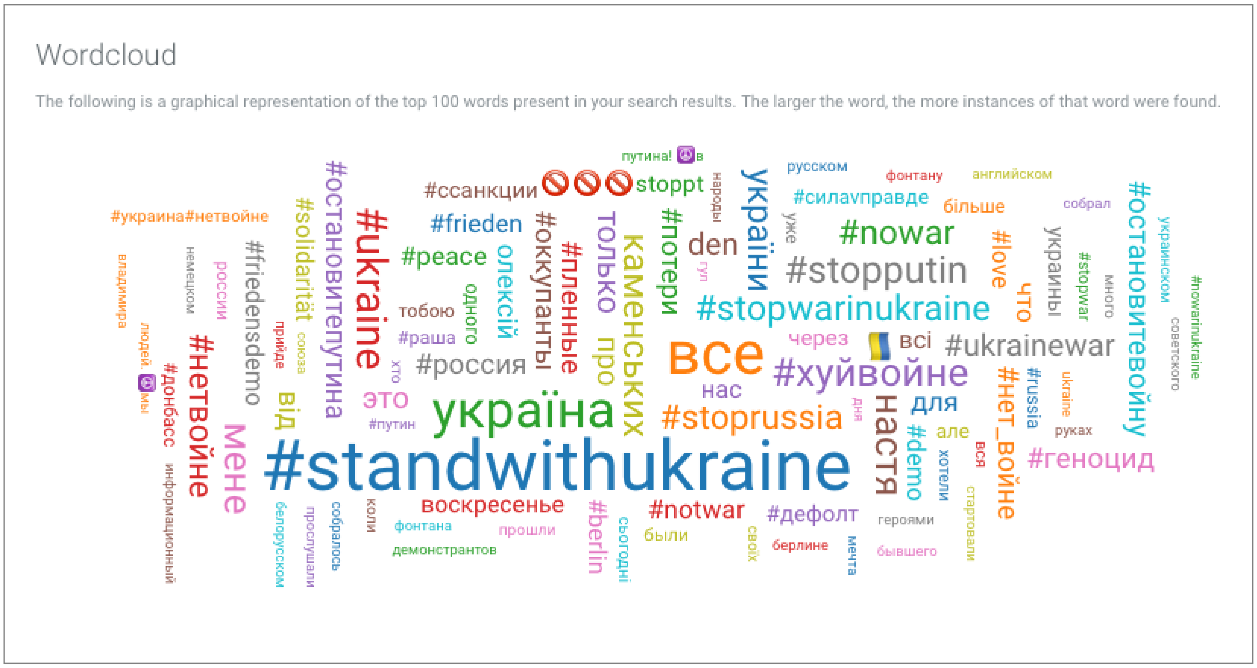
[15] Bellingcat: "Dubious & debunked claims," February 22, 2022.

For Ukraine and its allies, evaluating open-source data was crucial—both to assess military actions and information tactics on both sides. Through the conflict, the world witnessed the value of OSINT experts in analyzing ground-truth information and fact-checking adversarial narratives.

OSINT tools support this effort and were valuable in the Russia-Ukraine war for several reasons:

- **Data sources that are mainstream in the West**—like Twitter, Instagram, and Facebook—are not mainstream in Russia. Advanced OSINT software provides access to networks relevant in Russia, like OK.ru, VK, local forums, and alternative news outlets.
- **Analysts need to understand how public sentiment changes within Russia.** This can be hard to assess from the outside, especially when major social media is blocked for Russian citizens.[16] OSINT platforms covering Russian data sources can provide more accurate insights.
- **Advanced functionality like geofencing and AI is necessary** to efficiently gather insights in a rapidly evolving situation.
- **OSINT tools will enable future researchers** to study the conflict and investigate war crimes, storing relevant data even after it is deleted from its original source.

OSINT tools that prioritize real-time access, global coverage, and usability are central to producing accurate and timely intelligence for this geopolitical use case.



Wordcloud

The following is a graphical representation of the top 100 words present in your search results. The larger the word, the more instances of that word were found.

A word cloud representing VK and OK.ru (popular Russian networks) content using the hashtag #standwithukraine. OSINT tools were valuable for generating analytics to assess Russian public sentiment in response to the war.

[16] Shirin Ghaffary: "Russia continues its online censorship spree by blocking Instagram," March 11, 2022.

OUTCOME

A proactive OSINT strategy can have several impacts on a war's fallout. For one, states are better poised to predict, understand, and neutralize an adversary's information tactics before they go viral. During Russia's invasion of Ukraine, Ukraine's counter-information strategy also put pressure on foreign countries to increase support. This strategy boosted morale, encouraged volunteer fighters, and gained backing from Russian nationals. These support channels could have significant impacts on a war's timeline and outcome.

Regional data coverage and real-time access also give governments a faster, more accurate picture of new developments. In other words, robust OSINT tools can help drive more informed, efficient policies and decision-making in response to war.

According to The Washington Post, "Western policymakers seem to finally recognize not only that the Kremlin instigated and continues the war in Ukraine, but that the Kremlin treats the information ecosystem as an active front in any conflict."[17]

OSINT tools are crucial to this evolution in modern warfare as public data sources democratize the accessibility of battlefield information—on both digital and physical fronts.

[17] Nina Jankowicz and Ross Burley: "The West has gotten savvier about Russian disinformation. Will that help Ukraine?" The Washington Post, Jan. 22, 2022.

Does your team monitor global information environments?

Flashpoint provides intuitive OSINT software to improve analyst usage, expand global data coverage, and ensure real-time access. Contact us to find out if our solutions are right for you.

Contact Us