carahsoft The Trusted Government IT Solutions Provider®

OSINT Buyer's Guide **for Government**

Discover Data Intelligence Solutions to Address Evolving Information Needs and Navigate New Policy Development

FEATURING: ***Use Cases*** • ***Success Stories*** ***Contract Vehicles*** • ***OSINT Policies*** • ***Upcoming Events***

carahsoft

OSMOSISCon 2024

October 20-22 | Las Vegas, NV

Scan to **learn more** & **Register**

Welcome to the OSINT Buyer's Guide

Open-Source Intelligence (OSINT) is a crucial element of modern government operations as it enables agencies to gather and analyze public information for informed decision-making.

However, effectively leveraging OSINT presents several significant challenges. One major issue is the vast amount and variety of data available. With the internet and social media generating an enormous volume of information daily, agencies struggle to sift through and identify relevant content. Data is collected from various sources, including social media, news websites, public records and more, which complicates the collection and analysis processes. Ensuring the quality and reliability of data is another major hurdle, as misinformation and disinformation are widespread, making it difficult to determine the credibility of sources.

Carahsoft's OSINT portfolio addresses these challenges with a comprehensive suite of solutions tailored to government needs. It features advanced AI and machine learning technologies that process large volumes of data quickly and accurately, identifying relevant information and patterns. Real-time monitoring tools provide timely and actionable intelligence. The portfolio is built for seamless integration with existing IT infrastructures, supporting standardized data formats and protocols to enhance compatibility and interoperability. To ensure data quality and reliability, Carahsoft's solution portfolio includes verification tools to authenticate sources and rigorous quality control measures. Privacy and compliance are top priority, with all process's adherent to relevant laws and ethical guidelines.

While OSINT is not new to the government, the standardization of the practice is becoming increasingly prominent and necessary in today's rapidly changing world.

Michael Shrader
Vice President of Intelligence & Innovative Solutions
Carahsoft

Table of Contents:

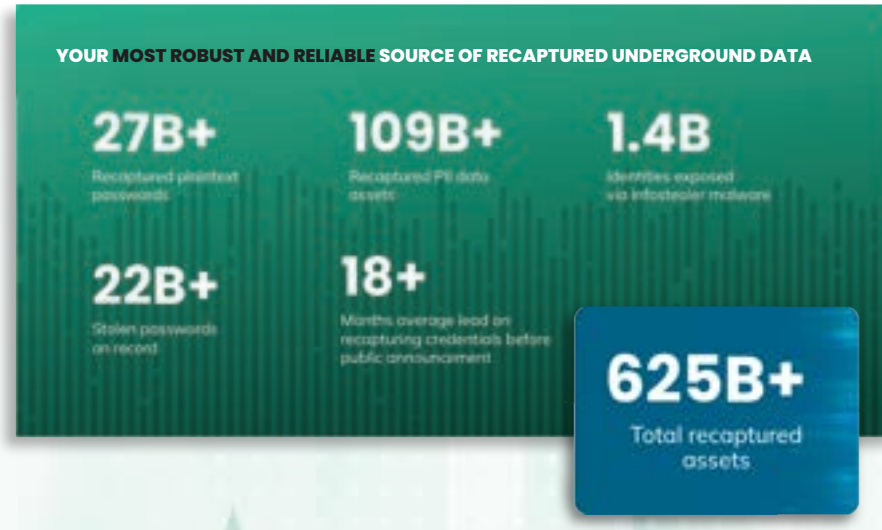
SpyCloud

TAKE CONTROL OF THE DIGITAL DOMAIN WITH

SpyCloud Identity Intelligence

SpyCloud's industry-leading government cybersecurity solutions are powered by ***the most reliable set of open-source Identity Intelligence data from the criminal underground***, supporting the full spectrum of cyber operations and offering a deeper understanding of bad actors' intentions.

- **Most comprehensive and current** global identity intelligence data collection
- Data is **clean and organized** to simplify analysis
- Analytics **easily identify connections** to build a target profile
- Data delivery via portal, API, on-premise, and analyst services



Learn more about how SpyCloud can help support your intelligence gathering and targeting efforts.

spycloud.com/federal

TRUSTED CYBER INTELLIGENCE PARTNER FOR GOVERNMENT AGENCIES

U.S. AIR FORCE · FBI · IRS · U.S. DEPARTMENT OF ENERGY

Cellebrite | Justice Accelerated

Smart Search.

Uncover Hidden Digital Footprints in Minutes!

Investigators face the daunting task of sifting through vast amounts of fragmented and dispersed data across multiple platforms. Manual searches are time-consuming, maintaining anonymity is challenging and it is hard to consolidate information from various sources.

Cellebrite Smart Search is the ultimate solution to these challenges. This intuitive online tool gathers open-source data, analyzing social media, public records and web mentions, and provides a comprehensive view of a person's digital footprint. With Smart Search, investigators can:

- Conduct simultaneous searches across multiple sources.
- Aggregate social media and online data beyond public records
- Validate information or generate investigative leads
- Identify patterns and connections to accelerate investigations
- Reduce backlogs in intelligence requests

If you know how to use a search engine, you can use Smart Search
There's no expertise required and it delivers actionable insights effortlessly.

Every crime leaves a digital footprint.

Equip your team with Smart Search to speed up investigations and enhance public safety.
Scan the QR code to learn more or visit:

Use Cases

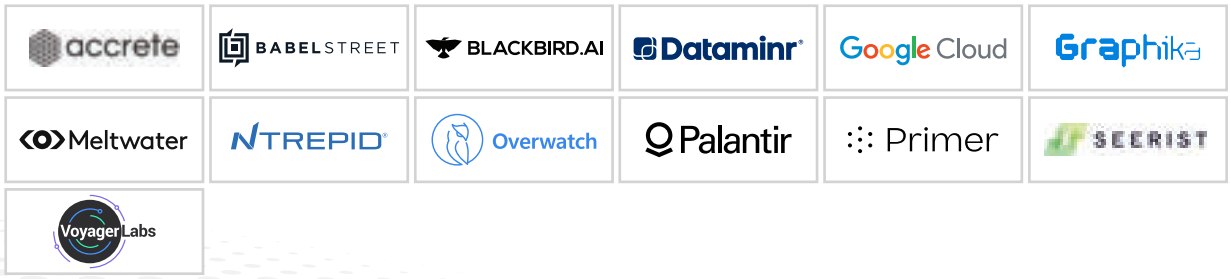
Open-Source Intelligence (OSINT) is an intelligence discipline that captures many different technologies. From analytic platforms that monitor financial transactions for hints of fraud to solutions that can identify terrorist networks on the dark web, OSINT technologies can enable any agency achieve their mission.

Audio & Visual

The audio and visual subcategory of Open-Source Intelligence (OSINT) involves gathering and analyzing visual data from publicly available sources such as satellite images, social media, and news footage. This subcategory employs techniques like geolocation, reverse image search, and metadata extraction to verify and contextualize information. These analyses provide critical insights into real-time events, geographical changes, and situational awareness. This capability supports intelligence operations and decision-making processes across various sectors.

Social Media

The social media subcategory of Open-Source Intelligence (OSINT) focuses on collecting and analyzing data from platforms like Twitter, Facebook, and Instagram. This subcategory uses techniques such as sentiment analysis, network mapping, and keyword monitoring to extract valuable insights from user-generated content. Social media OSINT helps organizations monitor trends, assess public sentiment, and detect emerging threats in real-time. This capability is essential for enhancing situational awareness, informing decision-making, and supporting intelligence operations across various sectors.



Dark Web

The dark web subcategory of Open Source Intelligence (OSINT) involves gathering and analyzing information from parts of the internet not indexed by traditional search engines, including encrypted and anonymous networks. This subcategory employs techniques such as web scraping, data mining, and natural language processing to uncover hidden forums, marketplaces, and communications. Deep and dark web OSINT helps organizations detect cyber threats, monitor illicit activities, and gather intelligence on criminal enterprises. This capability is crucial for enhancing cybersecurity, supporting law enforcement, and informing strategic decisions.

BABELSTREET | CLOUDBURST | DARKOWL | Dataminr | Palantir | SHADOWDRAGON | VoyagerLabs

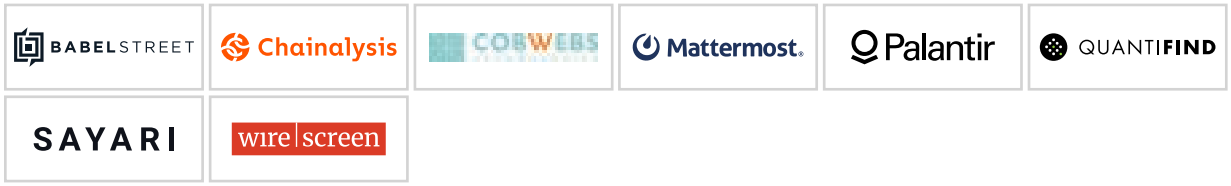
Cyber Threat Intelligence

The cyber subcategory of Open Source Intelligence (OSINT) focuses on collecting and analyzing data from publicly accessible digital sources to uncover cyber threats and vulnerabilities. Techniques such as network analysis, threat intelligence gathering, and vulnerability assessment are used to monitor and mitigate potential cyber risks. Cyber OSINT helps organizations stay ahead of emerging threats, understand the tactics of malicious actors, and enhance their overall cybersecurity posture. This capability is essential for protecting digital assets, ensuring data security, and supporting proactive defense strategies.

BigID | censys | CLOUDBURST | Dataminr | FLASHPOINT | interos | NVIDIA | Palantir | RAPID7 | Recorded Future | SpyCloud | STRIDER | ZEROFOX

Financial Monitoring

The financial monitoring subcategory of Open Source Intelligence (OSINT) focuses on collecting and analyzing publicly available financial data to identify trends, risks, and illicit activities. Techniques such as transaction analysis, market surveillance, and data aggregation are used to monitor financial markets, track suspicious transactions, and assess economic indicators. Financial monitoring OSINT helps organizations detect fraud, ensure regulatory compliance, and make informed financial decisions. This capability is essential for enhancing financial security, supporting regulatory enforcement, and guiding strategic investments.



Data Marketplace & CAI

A government data marketplace is a platform where government agencies can share, access, and purchase data sets to enhance their operations, decision-making processes, and public services. This marketplace facilitates the exchange of various types of data, including demographic information, economic statistics, environmental data, and more.

Managed Attribution

The managed attribution subcategory of Open Source Intelligence (OSINT) involves techniques to disguise the identity and location of analysts during online investigations. This includes using anonymization tools, secure browsers, and VPNs to protect the analyst's digital footprint. Managed attribution ensures that researchers can gather intelligence from public sources without revealing their presence or intentions. This capability is crucial for maintaining operational security, preventing detection by adversaries, and conducting covert online investigations.

Success Stories

Deep Media was tasked with providing a platform tool that prioritizes, translates, and surfaces highly relevant PAI information to the Air Force Cryptographic Office (AFCO) analysts to maximize their time utilization and analysis output.

DeepMedia

Rapid, Accurate & Scalable Deepfake Detection for AFCO

The Challenge:
Air Force Cryptographic Office (AFCO) faced scaling and training challenges to analyze accurately the vast volume of multilingual Publicly Available Information (PAI).

It takes years of linguistic training to process multilingual content competently. With the scale of images, videos, and audio samples being posted to the Internet, manual analysis of all the information is impossible.

The Solution:
Deep Media Designed and implemented a bespoke platform meeting AFCO's speed, accuracy, and media intelligence needs for analyzing PAI at scale. Incorporating significant improvements to the detection models, Deep Media's platform achieved high accuracies across image, face and audio modalities.

Key Takeaways:

- Challenge: Rapid, accurate, and scalable deepfake detection across multiple modalities
- Solution: A bespoke platform tailored to the needs and specifications of AFCO's analysts
- Impact: Exponentially increased ability to detect and analyze deep fake misinformation in multilingual PAI sources at scale

Sayari

OSINT Techniques: Tracking Down Fentanyl Networks

SAYARI

The Challenge:
Synthetic opioids still claim tens of thousands of American lives each year, and the illicit networks responsible are constantly adapting to counter-narcotic programs. Public data is vital to the ability to identify these risky networks quickly, effectively, and at scale, no matter what jurisdictional challenges investigators might face.

Following the 2023 Biden-Xi summit, China pledged to take steps to crack down on these sellers and take down these sites. However, there is evidence of Chinese firms continuing to market these precursors.

The Solution:
When tracking down fentanyl networks with publicly available information, investigators should use a number of different strategies. One effective method is to combine social media intelligence and OSINT techniques with public records to identify precursor producers.

The next step in this investigative process is to verify what you've found with OSINT and SOCMINT techniques in a risk intelligence platform like Sayari Graph. In platforms like Graph, you can view company profiles based on Chinese corporate data, including information such as shareholders, directors, and supervisors, combined with other types of data from different jurisdictions. In this case, you'll find that Hebei Huanhao Biotech is sanctioned by the United States, listed under an Illicit Drugs Executive Order on OFAC's Specially Designated Nationals (SDN) List.

Key Takeaways:
Using these methods, regulators, enforcers, and investigators can better understand fentanyl trafficking in order to dismantle these networks.To learn other methods for investigating illicit fentanyl networks and to see more example cases, watch the complete Carahsoft webcast, The Use of Publicly Available Information (PAI) in Disrupting Illicit Fentanyl Networks.

In May 2024, the Centers for Disease Control reported a decrease in drug overdose-related deaths for the first time since 2018. This change is thanks in part to concerted efforts by regulators, law enforcement, and private sector investigators to stem the flow of fentanyl and its chemical precursors into the United States.

Success story

RAPID, ACCURATE, & SCALABLE DEEPFAKE DETECTION FOR AFCO

Challenge

AFCO → **Air Force Cryptographic Office** faced scaling and training challenges to analyze accurately the vast volume of multilingual Publicly Available Information (PAI)

> *It takes years of linguistic training to process multilingual content competently. With the scale of images, videos, and audio samples being posted to the Internet, manual analysis of all the information is impossible.*

Deep Media was tasked with providing a platform tool that prioritizes, translates, and surfaces highly relevant PAI information to the AFCO analysts to maximize their time utilization and analysis output.

Solution

DEEP MEDIA → Designed and implemented a bespoke platform meeting AFCO's speed, accuracy, and media intelligence needs for analyzing PAI at scale. Incorporating significant improvements to the detection models, Deep Media's platform achieved high accuracies across image, face and audio modalities.

DeepMedia.AI
Deepfakes Detection and Media Intelligence

deepmedia.ai / deepidentify.ai
deepmedia-ai
@deepmediaai
@DeepMedia_AI

At A Glance

Customer: Air Force Cryptographic Office
Sector: Government
Country: United States

Challenge

Rapid, accurate, and scalable deepfake detection across multiple modalities

Solution

A bespoke platform tailored to the needs and specifications of AFCO's analysts

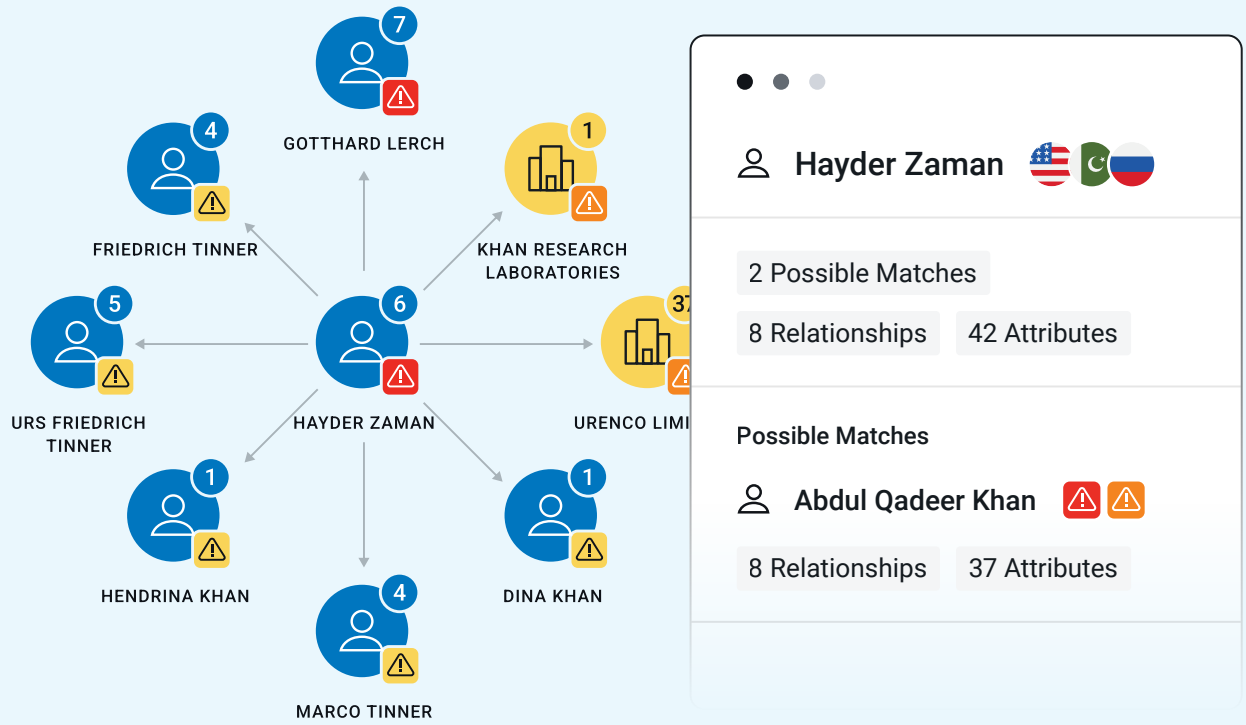
Impact

Exponentially increased ability to detect and analyze deep fake misinformation in multilingual PAI sources at scale

About The 16th Air Force Cryptologic Office

The 16th Air Force is headquartered at Joint Base San Antonio- Texas and focuses on information warfare in the modern age. Within the 16th Air Force, the Air Force Cryptologic Office (AFCO) leads cryptology within the U.S. Government, including both signals intelligence insights and cybersecurity products.

SAYARI



Delivering Information Advantage to National Security Missions

SAYARI SUPPORTS:

- Contested Logistics
- Counterintelligence and FOCI Risk
- Counterproliferation
- Counter Threat Finance
- Information Operations
- Strategic Competition
- Counternarcotics
- Export and Import Controls
- Law Enforcement and Criminal Investigations
- Regulation and Supervision
- Sanctions

Visit sayari.com to request a personalized demo

Flashpoint

US Fusion Center Improves Efficiency, Accuracy, and Collaboration with Open-Source Intelligence

State-owned and operated fusion centers serve as focal points in states and major urban areas as a resource to receive, analyze, gather, and share threat-related information between State, Local, Tribal, and Territorial (SLTT), federal, and private sector partners. They offer Homeland Security and Law Enforcement unique value by sharing information and providing partners with perspective on threats to their state or locality.

Fusion centers also serve as the primary contact between frontline personnel, state and local leadership, and the rest of the Homeland Security Enterprise.

The Challenge:
At a high level, this customer faced many challenges, including:

- A lean analyst team tackling myriad responsibilities
- Budget considerations and a need for vendor consolidation
- A need for real-time information about a wide range of critical events pertaining to specific locations

Before the team deployed Flashpoint, they relied heavily on searching surface web search engines like Google and conducting investigations directly within various social media networks.

Although these tactics can effectively collect general information, they have significant limitations. As well as being time and resource-intensive, basic search engines fail to deliver access, insights, and actionable intelligence.

The Solution:
Flashpoint provides the Fusion Center with access to a wide range of open-source data including social media, news articles, and chatter from illicit communities where threat actors are most active. This data is collected and delivered in real-time, allowing the Fusion Center to quickly identify, analyze, and respond to threats.

At a high level, this customer faced many challenges, including:

- Increased efficiency: Flashpoint has helped the Fusion Center to be more efficient in its investigations. Analysts can quickly find the information they need across myriad networks, saving time and resources. Example: While onboarding new analysts to Flashpoint solutions, customers have reported shortening the learning curve from approximately two weeks on the previous solution to two hours with Flashpoint.

- Improved accuracy: Flashpoint has helped the Fusion Center improve its intelligence accuracy. The Fusion Center can now identify threats more quickly and accurately, helping to mitigate infrastructure damage, prevent crimes, and protect citizens.

  Example: Flashpoint alerts helped prevent a potential shooting at an NYC synagogue. Read the full story here.

- Enhanced collaboration: Flashpoint has helped the Fusion Center enhance its collaboration with other law enforcement agencies. The Fusion Center can now share information more easily with other agencies, which has helped improve the state's overall security.

- Alleviated budget constraints due to higher analyst productivity: With the best data and the best intelligence from a single vendor, Flashpoint enables the team to do more with less, accelerating intelligence cycles and bolstering the team's ability to take decisive action.

Key Takeaways:
This customer finds Flashpoint to be a valuable force multiplier, facilitating efficiency, accuracy, and collaboration among its team. As a result, the Fusion Center is now better able to protect the state from the array of security threats they face and to be a better partner to their neighboring states and allied agencies.

As the industry leader in threat data and intelligence. Flashpoint enables mission-critical organizations worldwide to proactively and decisively confront security challenges with the most powerful data at the core. Book a demo to see how Flashpoint's combination of superior data, curated intelligence, and technology can force multiply your team to better protect people, places, and assets.

FLASHPOINT

The Best Data for The Best Intelligence

OSINT technology, data, and intelligence, tailored for mission-driven teams

flashpoint.io

BEST IN CLASS COLLECTIONS

- Defense
- Education
- Federal Civilian
- Law Enforcement
- Intelligence Community
- State, Local, and Tribal Government

PenLink

Using OSINT in Times of Social Unrest: Capitol Hill Riots

This case examines the events surrounding the January 6, 2021 Capitol Hill Riots, where demonstrators protested the certification of Joe Biden's electoral victory.

Among the protestors were groups like the Proud Boys, who are known for their endorsement of violence. The situation escalated into a riot, posing significant challenges for law enforcement tasked with maintaining order while respecting the constitutional right to protest.

The Challenge:
Law enforcement was faced with the daunting task of identifying and separating violent actors from peaceful protestors in real-time, amidst a rapidly escalating situation. The key challenge was to effectively monitor and analyze the vast amount of social media content, identify key agitators, and predict and prevent emerging threats of violence. The sheer volume of online activity, combined with the fast-paced nature of the unfolding events, made it nearly impossible to manually process and analyze the data in a timely manner.

The Solution:
PenLink's web intelligence platform, Tangles, was employed to address these challenges. The platform used Open-Source Intelligence (OSINT) to analyze social media and other online sources before, during, and after the riots. Utilizing artificial intelligence, machine learning, and Natural Language Processing to automatically collect, analyze, and visualize data from social media and other online sources, Tangles identified people of interest, suspicious activities, and provided real-time alerts. This technology enabled law enforcement to predict potential violence, manage situational awareness during the event, and gather evidence for post-event

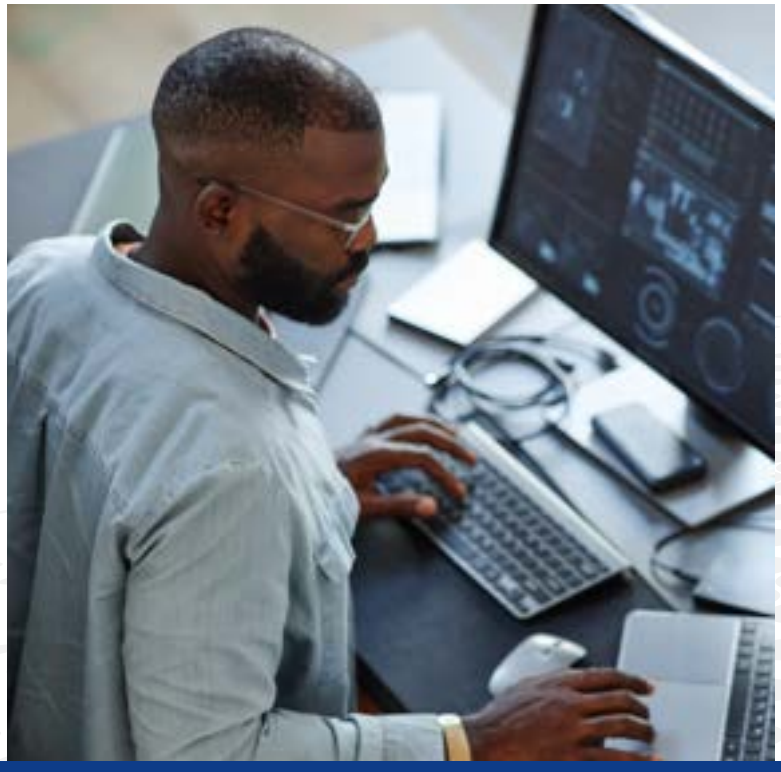
Key Takeaways:
PenLink's AI-powered OSINT solution allowed for the real-time collection and analysis of social media content, which was critical in identifying and mitigating threats. The technology's ability to provide actionable intelligence swiftly made it an indispensable tool for law enforcement during the riots and similar situations of social unrest.

Blackbird.ai

Why Government Leaders and Policymakers Need Narrative Risk Intelligence

Narrative intelligence systems empower government leaders and policymakers to proactively identify and mitigate narrative attacks caused by misinformation and disinformation, protect public trust, and make data-driven decisions.

Government leaders and policymakers are responsible for safeguarding public trust and ensuring the stability of their institutions. The rapid rise of generative AI coupled with social media, chat apps, the dark web, and alternative news sources has created new avenues for narrative attacks caused by misinformation, disinformation, and reputational threats stemming from negative stories and viral posts. To avoid these risks, government leaders must adopt a proactive, data-driven approach to narrative risk intelligence.



The Challenge:
Traditional government communication approaches often focus on crafting messages, engaging with media, and managing crises after they occur. While these strategies remain essential, they do not adequately address the growing threat of narrative-based attacks, which can undermine public trust in government institutions, erode citizen confidence, and create significant societal and economic risks.

Without a comprehensive narrative risk intelligence capability, government leaders and policymakers face growing challenges: Blind Spots in Media Monitoring, Cyber Risk, Erosion of Public Trust, Reactive Posture, Difficulty Prioritizing Risks.

The Solution:

- Early Warning of Threats: By continuously monitoring a wide range of sources, Constellation can identify emerging threats, such as disinformation campaigns or negative sentiment, before they escalate into full-blown crises. This early warning allows government agencies to get ahead of the narrative and proactively shape the conversation.

- Proactive Risk Mitigation: Armed with early warning and actionable insights, government leaders can take proactive steps to mitigate risks, such as engaging with influencers, correcting misinformation, or adjusting communication strategies. By taking a proactive approach, governments can minimize the impact of narrative threats and protect public trust.

- Data-Driven Decision Making: Constellation provides government leaders with a clear, data-driven understanding of the narrative landscape, enabling them to prioritize risks, allocate resources effectively, and make informed policy decisions. This data-driven approach ensures that government efforts are targeted, efficient, and effective.

- Enhanced Collaboration: Customizable alerts and dashboards ensure that key stakeholders across government agencies, from cybersecurity to leadership, stay informed and aligned in their response to narrative threats. This enhanced collaboration fosters a more resilient, adaptable government.

Key Takeaways:
The Impact of Narrative Intelligence on Government Organizations Narrative threats pose a significant risk to governments' societal stability and economic prosperity. The total cost of misinformation and disinformation to the global economy is estimated to be $78 billion per year, and for individual countries, the cost of a single crisis of public trust can reach billions of dollars in lost productivity, social unrest, and recovery efforts.

Some of Constellation's key benefits include: Enhanced Situational Awareness, Improved Decision Making, Increased Agility, Strengthened Public Engagement, and Enhanced Resilience.

BLACKBIRD.AI protects organizations from narrative attacks created by misinformation and disinformation that cause financial and reputational harm. Powered by our AI-driven proprietary technology, including the Constellation narrative intelligence platform, RAV3N Risk LMM, Narrative Feed, and our RAV3N Narrative Intelligence and Research Team, Blackbird.AI provides a disruptive shift in how organizations can protect themselves from what the World Economic Forum called the #1 global risk in 2024.

AI-Powered Open-Source Intelligence for Better Decision Making

PenLink equips civilian, defense, and intelligence communities with cutting-edge AI-powered digital intelligence. Leverage the entire web—open, deep, and dark—for unmatched analysis, turning information into actionable intelligence.

AI-Powered Web Intelligence

Advanced threat detection, intelligence gathering, and analysis.

- Visual Link Analysis
- Identity Resolution
- Real Time Alerts
- Digital Evidence
- Web Discovery
- Streamlined AI

Elevate Your Mission's Success

Discover more at penlink.com, or email info@penlink.com

penlink™

Comprehensive digital intelligence for a safer world.

BLACKBIRD.AI

NARRATIVE INTELLIGENCE GIVES YOU DECISION ADVANTAGE

$78B lost each year due to disinformation

53% of US respondents: "Organizational leaders should do whatever they can to stop the spread of misinformation."

88% of investors consider disinformation attacks on corporations a serious issue

25% of respondents thought security leaders were currently doing enough

PROTECT AGAINST NARRATIVE ATTACKS CREATED BY MISINFORMATION AND DISINFORMATION

- As they scale across social media, news, dark web
- The influcence behind them
- The anomalous bot behavior that scales them
- The cohorts that connect and amplify them

Contract Vehicles

Carahsoft & our Reseller Partners offers a number of contract options for purchasing OSINT solutions. Our contracts offer purchasing options for civilian, defense, state, and local government customers. Customers can purchase solutions off of six major contract vehicles:

Army OSINT Contract

Carahsoft provides OSINT solutions under the Army's Delivery Order GS00Q14OADU103-47QFCA19F0040. The contract allows the Army to purchase IT services, software, and data analytics capabilities from Carahsoft.

TX DIR

Department of Information Resources (DIR) contracts can be utilized by any State, Local, and Education agency in Texas to purchase OSINT solutions.

GSA Multiple Award Schedule (MAS)

Carahsoft holds a GSA Multiple Award Schedule (MAS) that allows customers to procure a wide variety of OSINT solutions. Carahsoft holds Contract #47QSWA18D008F and allows customers to purchase everything from social media analysis tools to commercially available data.

ITES-SW2

The purpose of the ITES-SW 2 acquisition is to support Army, Department of Defense (DoD) and all Federal Agency enterprise Information Technology (IT) infrastructure and info-structure goals by leveraging Commercially available-Off-The-Shelf (COTS) software products and maintenance in 14 product categories in addition to related incidental services and hardware.

NASA SEWP V

The NASA SEWP V GWAC (Government-Wide Acquisition Contract) provides the latest in Information Technology (IT) products and product-based services for all Federal Agencies. SEWP provides the best value and cost savings through innovative procurement tools and processes; premier customer service and outreach; and advocation of competition and cooperation within the industry.

NASPO ValuePoint Cooperative Purchasing Organization

The NASPO ValuePoint Cooperative Purchasing Organization (formerly WSCA-NASPO) provides the highest standard of excellence in public cooperative contracting. By leveraging the leadership and expertise of all states with the purchasing power of their public entities, NASPO ValuePoint delivers best value, reliable, competitively sourced contracts.

Since 1993 NASPO ValuePoint has been the cooperative purchasing arm of NASPO (the National Association of State Procurement Officials) encouraging, fostering and guiding the nation's most significant public contract cooperative. NASPO ValuePoint is a unified, nationally focused cooperative aggregating the demand of all 50 states, the District of Columbia and the organized US territories, their political subdivisions and other eligible entities spurring best value, innovation and competition in the marketplace.

Explore the benefits of how you can count on Carahsoft and our Reseller Partners:

- 24x7 availability call us at 888-662-2724
- Dedicated support specializing in serving enterprise ready solutions
- Ecosystem of value-added reseller partners
- Contract Expertise: We understand your procurement needs and the outcomes you're seeking
- Quick turnaround quote: Get the IT solutions you need with the fast, accurate service you deserve
- Substantial cost savings on OSINT products and service portfolio from certified technology brand partners
- Advanced technology solutions including Audio & Visual Analysis, Social Media Tools, Dark Web Monitoring, Financial Monitoring, Data Marketplaces, Managed Attribution, and more

OSINT Policies

The proliferation of social media and the internet across the world combined with cutting-edge technology has highlighted the importance of Open-Source Intelligence for the federal government. To better enable the adoption of this technology, agencies have released their own policies to guide how they will procure, use, and oversee the deployment of OSINT solutions.

2024 has seen four major OSINT policies released from different agencies—all building off prior policy decisions. Below are the highlights of those policies.

Intelligence Community OSINT Strategy

The Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA) released their Intelligence Community (IC) Open Source Intelligence (OSINT) Strategy in March 2024. The IC is leaning on industry to help make their OSINT mission a success.

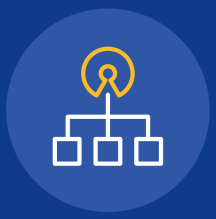
To advance the OSINT discipline, the IC will streamline data acquisition, develop innovative technologies to collect and derive insight from open source data, strengthen the coordination of open source collection activities across the community, update and standardize OSINT tradecraft, and develop a highly skilled OSINT workforce.

The strategy establishes the Director of the Central Intelligence Agency (D/CIA) serves as the OSINT Functional Manager (OSFM) for the IC. Day-to-day functions for the implementation of the strategy is vested in the Director of the Open Source Enterprise (D/OSE). D/OSE will work closely with the Defense Intelligence Enterprise Manager for OSINT at the Defense Intelligence Agency (DIA) and the IC OSINT Executive at the Office of the Director of National Intelligence (ODNI) to build out policy for this strategy.

The Four Strategic Focus Areas:

1. Coordinate Open Source Data Acquisition and Expand Sharing
The strategy seeks to expand the availability of Publicly Available Information (PAI) and Commercially Available Information (CAI) within the IC. To do this, OSINT leaders within the IC will coordinate with the IC Data Officers to acquire PAI and CAI for distribution across the IC based on mission needs.

CAI and PAI usage and metrics will be tracked in a "centralized, multi-domain data catalog." The IC also plans to build common OSINT platforms and "implement a pathway to deliver IC OSINT products to the broader U.S. Government."



2. Establish Integrated Open Source Collection Management
The IC will work to better "deconflict" its capabilities so that they are not wasting their "sensitive collection capabilities to obtain intelligence that can be derived from open source information." The IC will also begin constructing a "new and improved community-wide collection orchestration system."

3. Drive OSINT Innovation To Deliver New Capabilities
The IC will work to accelerate efforts around artificial intelligence, machine learning, and human language technologies to improve the value derived from OSINT. The IC is looking to test new capabilities on unclassified systems to acquire capabilities faster. They are also looking to industry and academia to "develop, test, and deploy OSINT tools and tradecraft."

4. Develop the Next-Generation OSINT Workforce and Tradecraft
The strategy calls for the "OSINT community [to] be at the forefront of the IC in testing the use of [Generative AI]." To do this, the workforce will need skills training to properly use the technology and develop frameworks for its use. Training on both Generative AI and OSINT in general must be conducted for "both OSINT professionals and all-source analysts who conduct OSINT activities."

EarlyBirds®

INNOVATION.
INTELLIGENCE.
COLLABORATION.

Empowering Asymmetric Excellence.

earlybirds.io

Intelligence Community Policy Framework for Commercially Available Information

The IC published a Framework for Commercially Available Information in May 2024. The framework lays out general principles for the access and collection of commercially available information (CAI) and how the IC deals with sensitive CAI.

The IC will be required to determine the original source of CAI datasets, determine if the data is biased, and ensure that data is not collected for the purpose of discrimination.

Sensitive CAI is classified as data that is either purchased from a commercial entity or given access for no cost through a commercial entity and contains substantial personally identifiable information (PII) of U.S. persons.

Access to CAI should be governed by the following requirements:

- Participation in the procurement process
- Consideration of mission need, legal authority, data sensitivity, privacy/civil liberties risk, privacy-enhancing techniques, data sourcing/integrity/quality, and security risks.
- IC agencies can use prior assessments of these products by other IC agencies
- Approval from element heads or delegated authority

Sensitive CAI is subject to requirements such as Authority to Operate (ATO), Privacy Overlays, and appropriate access restrictions on vendor systems.

IC agencies should have enhanced safeguards in place to protect sensitive CAI, procedures such as:

- Attribute-based access controls
- Procedures for auditing queries
- Written justification from senior executives for queries
- Approval from senior executives for any searches that constitute "data mining"
- Dissemination restriction
- Privacy-enhancing techniques
- Procedures for deleting U.S. person information

Upcoming Events

Potomac Officers Intel Summit

September 19, 2024 | McLean, VA

As the nature of intelligence evolves, the U.S. Intelligence Community is constantly adapting in order to stay ahead of new threats, technologies, global events and adversarial capabilities, especially in the peer competition era. Today's IC leaders are looking at ways to update the intelligence tradecraft, adopt cutting-edge technologies, become more agile, embrace reform and adapt to new classification trends. The Potomac Officers Club's 2024 Intel Summit celebrates a decade of bringing together the top IC officials, government decision makers and industry executives to discuss the challenges, opportunities, innovation initiatives and technologies shaping the future of American intelligence.

Scan the QR or visit: potomacofficersclub.com/events/poc-2024-10th-annual-intel-summit/

OsmosisCon

October 20 - 22, 2024 | Las Vegas, NV

Now in its 10th year, OSMOSISCon brings hundreds together to learn, share, and network at the Planet Hollywood Resort & Casino in Las Vegas, Nevada from October 20-22, 2024. The open-source skills-building conference's mission is to educate and train cyber intelligence investigators, researchers, reporters, and analysts on OSINT and SOCMINT techniques and best practices. Session's dive into all open-source techniques and skills related to exposing fraud, utilizing artificial intelligence, currents and future threats, and identifying unknown users.

Scan the QR or visit: osmosisinstitute.org/conference/

DoDIIS Worldwide 2024

October 27 - 30, 2024 | Omaha, NE

For 20 years, the DoDIIS Worldwide Conference has served as the premier IT conference showcasing cutting-edge technologies and forging partnerships to address the most pressing national security challenges. Experience an exciting lineup of distinguished speakers, collaborate with trusted partners, and learn about ground-breaking technical solutions to support the warfighter. The DoDIIS Conference is an immersive in-person event designed to launch partnerships and solutions for mission advantage.

Scan the QR or visit:
ncsi.com/event/dodiis/

SOFWeek 2025

May 5 - 9, 2025 | Tampa, FL

Held in Tampa, Florida, SOF Week is an annual conference for the international SOF community to learn, connect, and honor its members. The event is jointly sponsored by USSOCOM and the Global SOF Foundation. The 2024 edition attracted over 19,000 attendees.

Scan the QR or visit:
sofweek.org

Graphika

ATLAS

Open Source Intelligence and Data Feeds to Keep You Ahead of Emerging Online Threats.

ATLAS delivers intelligence and data feeds covering an expanding range of topics including:

China • **Russia** • **Middle East** • **Generative AI** • **and more.**

Our unparalleled open-source intelligence enables you to: **Identify threats** quickly, **take action, measure impact, and monitor changes** over time.

Learn More: Graphika.com

Book a Custom Demo

DARKOWL

Monitoring the Darknet for the Most Dangerous Threats to Organizations and Governments

DARKNET DATA, MONITORING, AND THREAT INTELLIGENCE FOR GOVERNMENTS AND GOVERNMENT AGENCIES

International and Domestic Terrorism

Detect potential threats and monitor persons of interest

Criminal Activity and Cybercrimes

Track illicit sales of drugs, human trafficking, and cyberweapons

National Security

Stay one step ahead of foreign Nation-State adversarial activity and attacks

www.darkowl.com

carahsoft

11493 Sunset Hills Road, Suite 100
Reston, Virginia 20190

(571) 590-6000
OSINT@Carahsoft.com

carahsoft.com/solve/OSINT