WHITEPAPER

The Unsolved Layer of OSINT Tradecraft

Dispersive® Stealth Networking

Why Network-Layer Attribution Is the Gap in the Intelligence Community's Managed Attribution Stack, and How Stealth Networking Closes It

Prepared for: OSINT practitioners, IC program managers, and mission partners

Aligned to: IC OSINT Strategy 2024–2026

Executive Summary

The Intelligence Community has correctly identified Open-Source Intelligence (OSINT) as the "INT of First Resort." The IC OSINT Strategy 2024–2026 calls for new tradecraft, deeper industry partnerships, and the ability to test capabilities on unclassified systems where speed matters more than accreditation cycles. Federal OSINT programs across CIA, DIA, INR, the Service intelligence components, and law enforcement have responded by investing heavily in managed attribution, the discipline of controlling what a target sees about a collector.

Yet the dominant managed attribution (MA) platforms in the IC, Authentic8 Silo, Ntrepid Nfusion, Flashpoint, and their peers, share a structural blind spot. They give analysts excellent control over the application-layer signature: browser fingerprint, language, time zone, user agent, OS. What they do not solve, because they cannot solve from the application layer, is the network-layer signature. Every one of these platforms still egresses through a single tunnel, from a single point of presence, with a single source IP at any given moment. That is precisely the signature modern adversaries fingerprint, correlate, and burn.

Dispersive® Stealth Networking closes that gap. It is not a replacement for browser-isolation MA platforms. It is the network-layer foundation that allows them to deliver on what they promise. By splitting sessions into multiple encrypted streams across continuously shifting independent paths, dissolving the tunnel signature itself, and concealing the endpoint behind a distributed deflect cloud, Dispersive removes the single observable network artifact that ties a collector to their mission.

This paper is written for IC OSINT program managers, tradecraft leads, and mission partners evaluating the next generation of attribution-managed collection. It assumes familiarity with the OSINT mission and current MA tooling. It argues a single thesis: in 2026, network attribution is the unsolved layer of the OSINT tradecraft stack, and stealth networking is what solves it.

Managed attribution controls the browser-layer identity.
Dispersive provides the invisible transport layer those platforms cannot.

1. OSINT Has Been Promoted. The Tradecraft Has Not Caught Up.

In March 2024, the Office of the Director of National Intelligence and the CIA jointly released the IC OSINT Strategy 2024–2026. The cover page bears a phrase that, two years on, has reshaped how the IC talks about its disciplines: OSINT is the "INT of First Resort." The strategy commits the IC to four goals: coordinating open-source data acquisition across agencies, integrating collection management, driving innovation in OSINT capabilities, and developing the next generation of OSINT workforce and tradecraft.

The Department of State's Bureau of Intelligence and Research published its complementary OSINT strategy in May 2024, organized around governance, capability investment, tradecraft, and external collaboration. The U.S. Marine Corps issued a request for information in 2021 explicitly listing "managed attribution" and "persistent managed attribution" among the capabilities required to support its enterprise OSINT analytics program. Across the IC, the line item is consistent: commercial internet service provider access, managed attribution, and tradecraft sufficient to operate on the open internet without burning the mission.

The reason this matters is not bureaucratic. It is operational. The open-source environment that OSINT analysts must work in is producing publicly available content at a scale that shifts the threat model for any collector who is not deliberately concealed. The targets of interest, adversary infrastructure, foreign-language media, hacker forums, ship-spotting blogs, dark web markets, sanctioned-entity websites, social media accounts in sensitive countries, are not passive document repositories. They are operated by entities that are watching who is watching them.

General Dynamics Information Technology, in describing the journey from open-source information to OSINT, frames it bluntly: "Adversaries are operating in the same spaces, and they can see what our intelligence teams are searching for through a variety of 'tells.'" Tradecraft, not just tools, is what separates a successful collection from a burned one.

Yet the tradecraft conversation inside the IC has matured asymmetrically. Workforce training, analytic standards, and platform consolidation have advanced rapidly. Network-layer tradecraft has not. The dominant operating assumption across federal MA deployments is still that a commercial managed-attribution platform, configured with rotating POPs and a controlled browser fingerprint, is sufficient. In 2017 that was a defensible assumption. In 2026, it is not.

2. What Adversaries Actually See

To understand why network-layer attribution is the unsolved problem, it helps to look at the OSINT collection event from the target's side of the wire. A foreign government website operator, a hostile forum administrator, or an adversary intelligence service watching a piece of infrastructure they care about does not see a query. They see a connection. That connection arrives with a set of observable attributes:

- A source IP address, which resolves to an autonomous system, a geographic region, and, with commercial enrichment, a likely organizational owner.
- A protocol fingerprint at the TLS, TCP, and IP layers, which an increasingly mature ecosystem of detection tools (JA3/JA4, TLS fingerprinting, ML-based VPN classifiers) can use to identify commercial VPN, proxy, and managed-attribution services even when the source IP itself is unremarkable.

- Timing, volume, and behavioral patterns, a request cadence, a session length, a working-hours signature, that can be correlated across visits to build a profile of the collector even without identifying them.
- Repeat-visit correlation, where the same POP, the same fingerprint, or the same behavioral pattern returning to multiple targets of intelligence interest is itself an intelligence signal.

Browser-isolation managed attribution platforms address some of these. They control the application-layer fingerprint extremely well. As Authentic8 describes its own platform, managed attribution lets analysts "control your digital fingerprint including language, time zone, keyboard settings, device, OS and more to blend in with normal traffic on sites of interest." That control is real and valuable.

What those platforms cannot do, by architectural definition, is dissolve the network-layer signature. They route the analyst's isolated browser session through a tunnel to a managed point of presence, and from there to the target. The tunnel is encrypted, the POP is geographically credible, but the tunnel exists, the POP is one of a finite vendor-managed set, and the source IP that touches the target is a single, observable, attributable address.

A 2025 academic paper in *Issues in Information Systems*, describing OSINT operations at Mercyhurst University's Center for Intelligence Research, Analysis and Training, identifies four explicit reasons for managed attribution: gaining access to data otherwise denied to U.S. IPs and points of presence, avoiding misinformation and obfuscation targeting networks, masking collectors' true interests and intentions, and protecting collector identity. Three of the four are network-layer problems. None are fully solved by browser-layer controls alone.

> *The uncomfortable truth for MA program managers: Your analysts have excellent application-layer cover and a single-path network footprint that any sophisticated target can fingerprint, block, or feed false information to. The browser is hidden - the wire is not.*

3. Why Single-Path Egress Is the Unsolved Layer

The reason every major commercial MA platform shares this limitation is not an oversight. It is an inheritance. Commercial managed attribution evolved out of remote-browser isolation, which evolved out of secure web gateways. The architectural lineage is application-layer security with network plumbing attached. The plumbing was good enough when the threat was casual fingerprinting and IP geolocation. It is not good enough when the threat is an adversary intelligence service running ML-based traffic classification across the inbound connections to its honeypots.

The single-path problem

All commercial managed attribution stacks today rely on a single tunnel from the analyst's isolated environment to a chosen point of presence, and a single source IP from that POP to the target. Vendors mitigate this by maintaining large pools of IPs across many regions. Flashpoint advertises points of presence in more than 40 regions and the option to "link additional gateways for extra layers of obfuscation," while Ntrepid maintains its Geosites network of "discreetly procured and managed IP addresses" that are "fully backstopped" to prevent attribution back to the vendor or the customer. But at any given moment, for any given session, the traffic leaves through one tunnel, from one IP, traversing one network path. That path is a single observable artifact.

What adversaries do with it

The defensive countermeasures are mature and inexpensive. Published academic research consistently demonstrates that machine-learning classifiers can identify VPN traffic with very high accuracy from encrypted handshake characteristics alone, with binary VPN detection studies reporting Random Forest F1-scores at 0.99, deep-learning classifiers exceeding 97% accuracy on standard datasets, and broader encrypted-traffic classification consistently above 95%. State-affiliated infrastructure operators, the entities running websites in the very countries OSINT analysts most need access to, have every incentive to maintain proprietary versions of these classifiers and to combine them with curated block lists of commercial MA egress ranges. Once an MA pool is identified, every analyst using that pool inherits the burn.

Why the industry response has plateaued

The standard mitigation, chaining additional gateways for extra obfuscation, moves the problem rather than solving it. Each additional hop adds latency, adds another tunnel signature to fingerprint, and ultimately still produces a single ingress point at the target. Tor-style multi-hop has the same limitation: traffic ultimately exits through a single observable node, and Tor exit nodes are themselves a fingerprint.

This is the architectural ceiling of the application-layer MA model. To go further, the network layer itself has to change.

4. Stealth Networking: A Different Architectural Premise

Dispersive® Stealth Networking starts from a different premise than the commercial MA category. Instead of choosing a better path, it dissolves the concept of a single path. The technology is rooted in patented Split-Session Multipath™ transport, originally developed for defense-grade secure communications and now productized for commercial and federal cloud environments.

How the architecture works

At the authenticated source, a single data session is dynamically split into multiple smaller, independent encrypted streams. Each stream is individually encrypted with a unique key and given its own forwarding instructions through a Dispersive header. The streams traverse the public internet through a distributed cloud of relay nodes, (Dispersive calls these deflects), with each stream taking a different path. Paths are selected dynamically and can be rolled mid-session in response to congestion or attack and never traverse the same combination of intermediate networks twice in a predictable pattern. At the authenticated destination, the streams are reassembled, the Dispersive headers are stripped, and the original packet is delivered to the receiving application.

The implications for managed attribution are direct:

- No single source IP touches the target. Each fragment of the session arrives from a different deflect, in a sequence determined by dynamic routing decisions the target cannot observe or predict.
- No tunnel signature exists to fingerprint. There is no monolithic VPN or proxy tunnel for ML classifiers to identify. The transport is tunnel-free at the session level.
- No single observer sees a complete flow. An adversary watching one path, even an adversary running a transit network, sees only fragments. Correlation across paths requires observing all of them simultaneously, which the architecture is specifically designed to make infeasible.

- Sessions survive disruption. If a path is degraded, jammed, or actively attacked, fragments reroute dynamically. The session does not drop, a property that matters as much for analyst productivity as for tradecraft.
- Routing is policy-driven and sovereign-aware. Path selection can actively avoid jurisdictions an analyst should not transit, a control that single-tunnel architectures cannot offer because they cannot inspect intermediate hops.

What it is not

Stealth networking is not a browser-isolation platform. It does not control the application-layer fingerprint, manage personas, or provide an analyst-facing virtual workspace. It is a transport-layer foundation that operates beneath, and complements, the existing MA platforms federal OSINT programs have already procured.

5. Where Stealth Networking Sits in the OSINT Stack

The most useful way to think about Dispersive in an existing OSINT environment is as the network-layer foundation underneath the managed attribution platform an analyst already uses. The two layers solve different problems and, in combination, address the full attribution surface.

Attribute Exposed to Target	Browser-Isolation managed attribution (Silo, Nfusion, etc.)	Dispersive Network Layer
Source IP / point of presence	Single egress IP per session, drawn from a finite vendor-managed pool	No single source IP. Packets fragmented across many independent paths and deflects
Tunnel signature	Recognizable VPN/proxy fingerprints. Machine Learning (ML)-based detectors flag commercial managed attribution (MA) pools	Tunnel-free transport. No exposed tunnel for Machine Learning (ML) detectors to fingerprint
Traffic correlation	Predictable flow on a single path enables timing and volume correlation	Split-session multipath defeats correlation. No single observer sees a complete flow
Browser fingerprint	Strong control: language, time zone, OS, fonts, headers	Out of scope. Complementary to existing managed attribution (MA) platforms
Resilience under attack or jamming	Single tunnel fails as one unit. Session is lost	Paths reroute dynamically mid-session. Sessions persist through path degradation
Sovereign / jurisdictional routing control	Choose POP region. Traffic still transits arbitrary intermediate networks	Path selection actively avoids high-risk jurisdictions. Routing is policy-driven

Read across each row: browser-isolation MA does excellent work in some categories, leaves observable artifacts in others. The categories where it leaves artifacts are precisely the ones an adversary intelligence service or sophisticated forum operator looks at first. Adding a stealth networking layer underneath the existing MA stack closes those rows without disturbing the workflows, vendor relationships, or training investments already in place.

6. Mission Scenarios

Three illustrative scenarios drawn from OSINT mission spaces show where the network-layer foundation matters most. These are composite descriptions of recurring tradecraft challenges, not specific operational events.

Scenario A: Persistent collection against a state-operated forum

An analytic team is tasked with persistent monitoring of a forum operated inside a denied area, where the operator is known to maintain block lists of commercial MA egress ranges and to feed deception content to identified collectors. The team's existing browser-isolation platform handles persona management and application-layer fingerprinting well. The mission risk is that the source IP, even rotated across the vendor's POP pool, falls within commercial MA ranges that the operator has already identified. With a stealth networking layer, no single source IP touches the forum. The collector's connection presents as fragmented traffic from multiple unrelated network paths, none of which is identifiable as a commercial MA egress.

Scenario B: In-region collection where a single-path tunnel is itself the signal

A practitioner needs to access content visible only to in-region users, regional news sites, public records portals, government press releases that geo-fence their content. The MA platform provides an in-region browser fingerprint and an in-region POP. The remaining risk is that the connection to that POP is itself a recognizable VPN tunnel pattern, identifiable by an in-country ISP or surveillance apparatus as a foreign collector tunneling into a domestic IP. Stealth networking dissolves the tunnel signature itself. There is no monolithic flow for an in-country observer to classify as VPN traffic, only fragments arriving along independent paths.

Scenario C: Tactical edge collection in a contested environment

A forward-deployed element conducting unclassified open-source collection from a contested or denied environment cannot rely on a single egress path. The path itself is targetable, jammable, or subject to host-nation surveillance. Stealth networking's dynamic multi-path routing, originally designed for exactly this class of problem, allows the collection session to traverse a mix of available transports (commercial internet, satellite, cellular) with paths reconfigured in motion as conditions change. The session survives degradation that would drop a conventional MA tunnel.

7. Alignment with the IC OSINT Strategy

The case for stealth networking maps directly onto three of the IC OSINT Strategy 2024–2026's explicit calls.

"Develop the next-generation OSINT workforce and tradecraft"

The strategy is unambiguous that tradecraft and training must be "flexible and updated regularly to keep pace with changes in the open source domain." Network-layer attribution is the most significant unaddressed change in that domain since the strategy was published. Equipping analysts with a network foundation that defeats the fingerprinting techniques adversaries deployed in the intervening period is squarely within the strategy's tradecraft modernization mandate.

"Drive OSINT innovation to deliver new capabilities"

The strategy specifically calls on the IC to "test new capabilities on unclassified systems that present fewer risks and barriers," and to "reimagine its relationships with industry and academia to leverage cutting-edge capabilities being developed and applied in the private sector." Stealth networking is exactly that class of private-sector capability, mature, fielded, defense-grade in origin, commercially scalable, ready for integration without the procurement and accreditation overhead of a classified program.

"External partnerships will be vital to success"

Dispersive's technology partnerships with hyperscale cloud providers and existing federal mission partners mean integration does not require greenfield infrastructure. Stealth networking can sit beneath existing managed attribution platforms, alongside existing analytic platforms, and inside existing cloud accreditation boundaries.

8. Conclusion: The Layer That Closes the Stack

OSINT is the INT of First Resort. The strategy is in place, the workforce is being built, the analytic platforms are being consolidated, and the managed attribution market has matured. What remains is the layer underneath: the network.

In 2026, every commercial managed attribution platform an IC OSINT program is likely to operate shares the same architectural blind spot, a single tunnel, a single egress, a single observable path. Adversaries have built their detection apparatus around exactly that blind spot. Closing it does not require ripping out existing investments. It requires adding a network-layer foundation that dissolves the single path itself.

That is what stealth networking does. It is the unsolved layer of OSINT tradecraft, finally addressable with a technology that was originally built for the harder problem and is now ready for the OSINT mission.

References

All sources cited in this paper are publicly available. URLs were accessed during preparation in April 2026.

1. Office of the Director of National Intelligence and Central Intelligence Agency, The IC OSINT Strategy 2024–2026, March 2024. https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf

2. Flashpoint, "Managed Attribution" product page, 2026. https://flashpoint.io/platform/managed-attribution/

3. B. Fuller, "Practical OSINT tips for better planning and tradecraft," Authentic8 Needlestack, February 23, 2023. https://www.authentic8.com/blog/OSINT-tips-planning-tradecraft

4. Dispersive Holdings, Inc., "Managed Attribution — Obfuscate & Protect Sensitive Operations," 2026. https://dispersive.io/use-case/managed-attribution

5. U.S. Department of State, Bureau of Intelligence and Research, Open Source Intelligence Strategy, May 2024. https://www.state.gov/wp-content/uploads/2024/05/INR-Open-Source-Intelligence-Strategy.pdf

6. Potomac Officers Club, "Marine Corps Posts RFI for Open-Source Intelligence Analysis Tool," February 2021. https://potomacofficersclub.com/news/marine-corps-posts-rfi-for-open-source-intelligence-analysis-tool/

7. ShadowDragon, "What is OSINT [Open-Source Intelligence]? 2026 Guide," February 2026. https://shadowdragon.io/blog/what-is-osint/

8. General Dynamics Information Technology, "The Journey from Open-Source Information to OSINT." https://www.gdit.com/perspectives/latest/the-journey-from-open-source-information-to-osint/

9. Representative published research on ML-based encrypted-traffic and VPN classification: (a) S. Seyyar et al., "Binary VPN Traffic Detection Using Wavelet Features and Machine Learning," arXiv:2502.13804, 2025; (b) Z. Zou et al., "A Deep Learning-Based Encrypted VPN Traffic Classification Method Using Packet Block Image," 2022; (c) E. Anderson and B. Anderson, "Robust Machine Learning for Encrypted Traffic Classification," arXiv:1603.04865; (d) ScienceDirect, "A comprehensive review on machine learning-based VPN detection: scenarios, methods, and open challenges," 2025.

10. Authentic8 / Fivecast, "Anonymity and obfuscation in OSINT," November 2023. https://www.fivecast.com/blog/anonymity-and-obfuscation-in-osint-fivecast-and-authentic8/

11. B. Fuller and J. Bayuk, "How Mercyhurst's CIRAT does OSINT — and why," Issues in Information Systems, Vol. 26, Issue 3, 2025, pp. 75–85. https://iacis.org/iis/2025/3_iis_2025_75-85.pdf

12. Defense Media Network, "Ntrepid Case Study: Managed Attribution for Open Source Intelligence (OSINT)," September 2019. https://www.defensemedianetwork.com/stories/ntrepid-case-study-managed-attribution-open-source-intelligence-osint-sponsored/

13. Amazon Web Services Partner Network Blog, "Unlocking Secure Data Access with Dispersive Stealth Networking and AWS," August 2025. https://aws.amazon.com/blogs/apn/unlocking-secure-data-access-with-dispersive-stealth-networking-and-aws/

Disclosure: This whitepaper is published by Dispersive Holdings, Inc. References to third-party managed attribution platforms (Authentic8 Silo, Ntrepid Nfusion, Flashpoint) are based on those vendors' own publicly available product descriptions and are intended to characterize the architectural category of browser-isolation managed attribution. They are not statements about the comparative merits of any specific deployment, configuration, or contract

About Dispersive Holdings, Inc.

Dispersive Holdings, Inc. (Dispersive) delivers stealth networking for ultra-secure, high-performance communications. Inspired by military-grade spread spectrum techniques, Dispersive's patented multipath software obfuscates and splits traffic across dynamically changing channels, ensuring networks remain virtually invisible and quantum-resilient by design. Trusted by defense, intelligence, critical infrastructure, and high-security enterprises, Dispersive is redefining how secure connectivity is done. Learn more at www.dispersive.io

Get Started with Dispersive

01	02	03
Mission & Attribution Assessment	**Technical Proof of Concept**	**Deploy & Scale**
A short, focused session to understand your collection environment, attribution requirements, and where network-layer exposure creates the highest operational risk.	A time-boxed validation in your environment to measure invisibility, resilience, and attribution protection under real operational conditions.	A targeted deployment across priority analysts, regions, or missions, expanding to full operational scale once value is confirmed.

This three-step path is designed to provide clarity on the mission need, proof in your own environment, and a controlled path to scale. Each phase builds on the last so you move from evaluation to operational coverage without disruption or re-architecture. To initiate the process, contact https://dispersive.io/company/contact-us

Others assume the network can be trusted.
Dispersive® Stealth Networking operates when it's not.

Dispersive Holdings, Inc.
300 Colonial Center Pkwy Suite 100 | Roswell, GA 30076 USA
dispersive.io | 1.844.403.5850

dispersive