Public Information

Is Reshaping Open Source Intelligence in the Age of AI

Article by **Sal Artiaga**

March, 7 2026

Introduction

For most of modern history, intelligence was synonymous with secrets. It was synonymous with clandestine meetings, intercepts, clandestine sources, and satellite imagery that only a handful of people would ever have access to. The mystique of intelligence was one of scarcity. It was assumed that if one side possessed secrets, they possessed a strategic advantage. But between 2024 and 2026, that assumption was challenged in a way that will forever change how we think about strategy and how we think about intelligence.

The new strategic advantage is not derived from what is hidden, but from what is publicly available. Publicly Available Information (PAI) is now the largest and fastest-growing source of exploitable information in all of human history. Open Source Intelligence (OSINT) is now the discipline that converts that information into knowledge. The relationship between the two is critical. One is the raw material, and the other is the process by which that material becomes meaningful. But this relationship is not static. The growth of PAI and the simultaneous acceleration of artificial intelligence are causing OSINT to grow and evolve in ways that are unlike anything seen before. **Intelligence is no longer defined solely by secrecy. It is defined by synthesis.**

Defining PAI and OSINT or Fuel and Engine

PAI refers to any information that is legally and ethically accessible to the public. It includes news media, academic publications, corporate filings, social media posts, satellite imagery, commercial data feeds, government reports, Internet of Things (IoT) telemetry, and information accessible through sub scription services. PAI exists independently of intelligence work. It is the byproduct of digital society. It is the exhaust of modern life.

OSINT, by contrast, is not the information itself. It is the intelligence product derived from PAI through structured collection, validation, contextualization, and analysis. PAI becomes OSINT only when it is directed toward answering specific intelligence requirements. **Without analysis, PAI is noise. With disciplined processing, it becomes a decision advantage.** The distinction matters. Confusing PAI with OSINT risks drowning in data. Treating OSINT as a professionalized analytic discipline elevates it from research to intelligence.

The PAI Explosion

The scale of PAI generation between 2024 and 2026 is unprecedented. Daily global data generation now approaches 463 exabytes. Every transaction, sensor, shipment, photograph, and digital interaction leaves a trace. IoT deployments continue to expand across manufacturing, healthcare, agriculture, and urban infrastructure. Commercial satellite constellations now number in the tens of thousands of low Earth-orbit platforms, providing high-frequency geospatial

observations once reserved for classified systems.

This is not merely a quantitative change. It is architectural. The surface web, deep web, and dark web now represent layered ecosystems of insight. Commercial satellite imagery provides near-real-time monitoring of industrial output and military mobilization. Social media reveals intent and sentiment before official policy statements emerge. Blockchain analysis exposes financial flows in public ledgers.

The world has become radically transparent. Not completely visible, but sufficiently observable that secrets often hide in plain sight. For OSINT professionals, this is both an opportunity and a burden. The opportunity lies in access. The burden lies in volume.

AI as the Processing Engine

The traditional image of an OSINT analyst manually combing through articles and forums is obsolete. The volume and velocity of PAI exceed human cognitive capacity.

Artificial intelligence has become the

M6
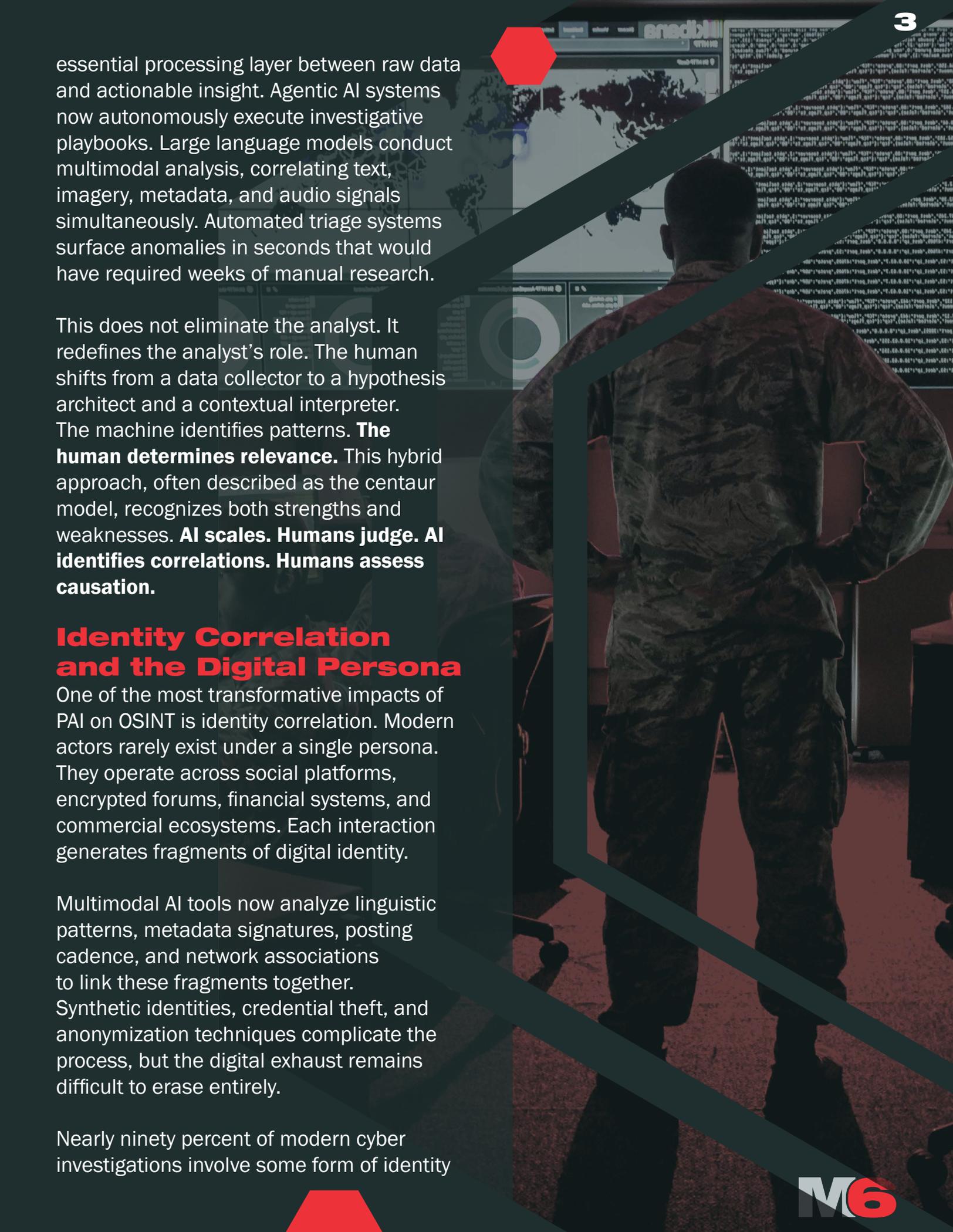
essential processing layer between raw data and actionable insight. Agentic AI systems now autonomously execute investigative playbooks. Large language models conduct multimodal analysis, correlating text, imagery, metadata, and audio signals simultaneously. Automated triage systems surface anomalies in seconds that would have required weeks of manual research.

This does not eliminate the analyst. It redefines the analyst's role. The human shifts from a data collector to a hypothesis architect and a contextual interpreter. The machine identifies patterns. **The human determines relevance.** This hybrid approach, often described as the centaur model, recognizes both strengths and weaknesses. **AI scales. Humans judge. AI identifies correlations. Humans assess causation.**

Identity Correlation and the Digital Persona

One of the most transformative impacts of PAI on OSINT is identity correlation. Modern actors rarely exist under a single persona. They operate across social platforms, encrypted forums, financial systems, and commercial ecosystems. Each interaction generates fragments of digital identity.

Multimodal AI tools now analyze linguistic patterns, metadata signatures, posting cadence, and network associations to link these fragments together. Synthetic identities, credential theft, and anonymization techniques complicate the process, but the digital exhaust remains difficult to erase entirely.

Nearly ninety percent of modern cyber investigations involve some form of identity

weakness. OSINT professionals increasingly operate as digital anthropologists, mapping behavior across ecosystems. PAI provides raw traces. AI provides connective tissue. Human analysts determine the narrative coherence.

When Data Lies

The same openness that empowers OSINT also creates vulnerability. Between 2024 and 2026, the field has confronted a veracity crisis. AI-generated content, synthetic media, and deliberate data-poisoning campaigns now contaminate the information environment. Training data poisoning attacks alter the AI model's logic during its development phase. Backdoor triggers embedded in public code repositories can influence downstream systems months later. Coordinated influence networks flood the web with articles designed not for humans, but for machine ingestion. Deepfakes complicate visual authentication. Synthetic audio undermines confidence in recorded statements. The boundary between authentic and fabricated PAI blurs.

For OSINT, this introduces a paradox.

The discipline depends on openness. Yet openness is increasingly exploited. Verification becomes the core task. Source provenance, cross-domain validation, and adversarial skepticism are no longer optional. They are foundational tradecraft.

Professionalization of the OSINT Workforce

The modern OSINT practitioner is not simply a researcher; the modern OSINT practitioners are the technological generalist. Scripting languages, network infrastructure, forensic validation, and operational security are now the norm.

The Intelligence Community's OSINT strategy for 2024-2026 highlights the professionalization of the field. Standard operating procedures, training foundries, and cross-agency frameworks are the means by which the Intelligence Community is attempting to take OSINT from ad hoc to institutional backbone. Without methodology, the practitioner drowns in irrelevant information; with methodology, they navigate the complexities.

M6

From Data Deluge to Decision Advantage

The relationship between PAI and OSINT defines the intelligence paradigm of 2026. PAI is the environment. OSINT is the science of transforming this environment into insight. The explosion of data available to everyone has moved the center of gravity away from secret collection and more towards synthesis.

Artificial intelligence is a tool that has made this shift possible, but it is also a tool that, rather than replacing human judgment, has increased its potential for opportunity and risk to a greater degree than ever before. The best organizations are those that are able to harness machine scale, human doubt, human discipline, and human understanding of context.

The future of intelligence is no longer about uncovering a treasure trove of secrets, but about understanding truth in a world of radical transparency. The future of OSINT is not about who is able to gather the most data, but who is able to use that data responsibly. **In a world where information is abundant, advantage belongs to those who can transform noise into knowledge.**