

OSINT in the Age of AI

How Modern Operations Work

September 25, 2026



\$whoami

Daniel Pablo

- **Senior Cyber Threat Intelligence Analyst** at NCS Philippines
- **Part-Time Cybersecurity Instructor** at De La Salle College of Saint Benilde
- **Security Researcher** at Information Sharing and Analysis Center – Philippines (ISAC-PH)
- **Resident Sh*t Poster** at Recon Village PH
- **Security Enthusiast & OSINT Practitioner**



AI, AI, AI, AI, AI, AI, AI



AI, AI, AI, AI, AI, AI, AI

What this talk covers?

Foundations

What OSINT means, who uses it, and how it developed

Operations

How an investigation moves from a question to a defensible finding

AI Applications

A broad catalogue across the workflow and major sectors

Judgment

Drawbacks, trade-offs, safeguards, and a verdict

Open-Source Intelligence (OSINT)

Open Sources

Information available to the public or through commercial access

Intelligence Question

A defined decision, priority, or knowledge gap

Analytical Work

Collection, assessment, corroboration, and interpretation

Useful Output

A finding with traceable evidence and stated uncertainty

The Open-Source Landscape

Common Sources

News and Public Broadcasts

Public Records and Company Filings

Research, Patents, and Datasets

Public Websites and Social Media
Platforms

Specialist Sources

Satellite Imagery and Maps

Public maritime and Aviation Data

Public code and Security Advisories

Licensed Commercial Databases

Where OSINT Supports Decisions

Domain	Typical question
Security and diplomacy	What developments may change regional risk?
Journalism and accountability	Can public evidence corroborate an allegation?
Business and cybersecurity	Which suppliers, threats, or market shifts need review?
Health, disaster, and environment	Which emerging events need expert attention?

OSINT has Roots Before the Internet

Before the web

Analysts used newspapers, maps, trade information, and public statements

1939

BBC Monitoring began systematic foreign broadcast monitoring

1941

The US established the Foreign Broadcast Monitoring Service, predecessor to FBIS

Cold War

Broadcast monitoring and translation supported sustained foreign analysis

The Web Widened Participation

1990s–2000s

Searchable websites and digital records expanded research access

2014

Bellingcat formed as an independent investigative collective

2022

The Berkeley Protocol publication set out digital investigation guidance

2024

The US intelligence community published its 2024–2026 OSINT strategy

AI is Changing the Operating Model

Earlier automation

Rules, keyword alerts, databases, and specialist machine learning

Generative AI

Natural-language querying, extraction, translation, and draft synthesis

2025

WHO's EIOS version 2 introduced new AI features

2026

Bellingcat documented a prototype that ranks potential civilian-harm posts

An OSINT Operation has Six Stages

1–2 Plan and collect

Set the question and scope. Retrieve permitted sources.

3 Process

Preserve originals. Normalize, deduplicate, and index material.

4 Verify

Check origin, time, location, and independent corroboration.

5–6 Assess and report

Compare explanations, state uncertainty, deliver, and update.

AI changes the division of work

Stage	AI assistance	Analyst responsibility
Discovery	Suggest and rank leads	Set scope and judge coverage
Processing	Extract and organize content	Check fidelity to originals
Analysis	Surface patterns and alternatives	Test explanations
Reporting	Draft cited summaries	Approve claims and release

Not CTF Related



AI Use Cases - Planning and Discovery

Search design

Expand keywords, aliases, local-language terms, and query variants

Source discovery

Suggest archives, datasets, registries, and coverage gaps

Retrieval

Search by meaning and rank documents for the question

Collection support

Draft API queries or scripts and prioritize material for review



AI Use Cases - Text and Documents

Reading

OCR for scans, language detection, translation, and transcription

Extraction

Names, organizations, dates, claims, events, and table fields

Organization

Topic classification, clustering, duplicate detection, and timelines

Comparison

Document changes, claim contradictions, and evidence-linked summaries

AI Use Cases - Images, Audio, and Video

Search and triage

Visual similarity, object detection, scene labels, and keyframes

Audio processing

Speech-to-text, language translation, and speaker-turn segmentation

Visual clues

Read visible text and propose landmarks or location candidates

Media review

Group related clips and flag possible manipulation for specialists



AI Use Cases - Geospatial and Temporal Data

Change detection	Compare imagery for damage, construction, or land-use changes
Feature extraction	Identify candidate buildings, roads, vessels, or affected areas
Event alignment	Align observations by time and location across public datasets
Anomaly review	Flag unusual movement patterns, activity levels, or sensor readings

AI Use Cases - Entities and Networks

Entity resolution

Suggest when names, companies, or records may refer to the same entity

Relationship extraction

Draft links among organizations, events, assets, and documents

Pattern discovery

Identify clusters, repeated claims, and possible coordinated activity

Hypothesis testing

Compare alternative explanations and surface contradictory evidence

AI Use Cases - Monitoring and Delivery

Early warning

Rank new events, flag deviations, and combine duplicate alerts

Research assistance

Answer questions over an approved, versioned evidence collection

Communication

Draft briefings, translations, timelines, and audience-specific summaries

Quality support

Check citation coverage, missing evidence, and unresolved questions

AI Use Cases



Memes

Sector Applications - Security and Business

Sector	Examples of AI-assisted OSINT
Cyber defense	Prioritize public advisories, summarize threat reports, review public exposure
Corporate research	Screen filings, compare patents, map suppliers, track market changes
Fraud and compliance	Triage adverse media, flag entity matches, examine public procurement
Public information	Trace claims, assess media provenance, study narrative spread

Sector Applications - Public Interest

Sector	Examples of AI-assisted OSINT
Public health	Classify event reports and detect unusual clusters for expert review
Humanitarian work	Triage incident reports and prioritize areas for damage assessment
Environment	Review deforestation, wildfire, water, and land-use indicators
Research and journalism	Explore archives, compare public claims, discover document patterns

Sector Applications - Education



Sector Applications - Education



Drawbacks - Errors Can Look Convincing

Fabrication

A fluent answer can invent facts, quotations, or citations

Loss of context

Translation and summarization may erase qualifications

False matches

Similar names or images can produce mistaken links

Coverage bias

Missing languages, sources, or groups can skew the picture



Drawbacks - A Hostile Information Environment

Synthetic content

Fabricated media and text increase the burden of verification

Source poisoning

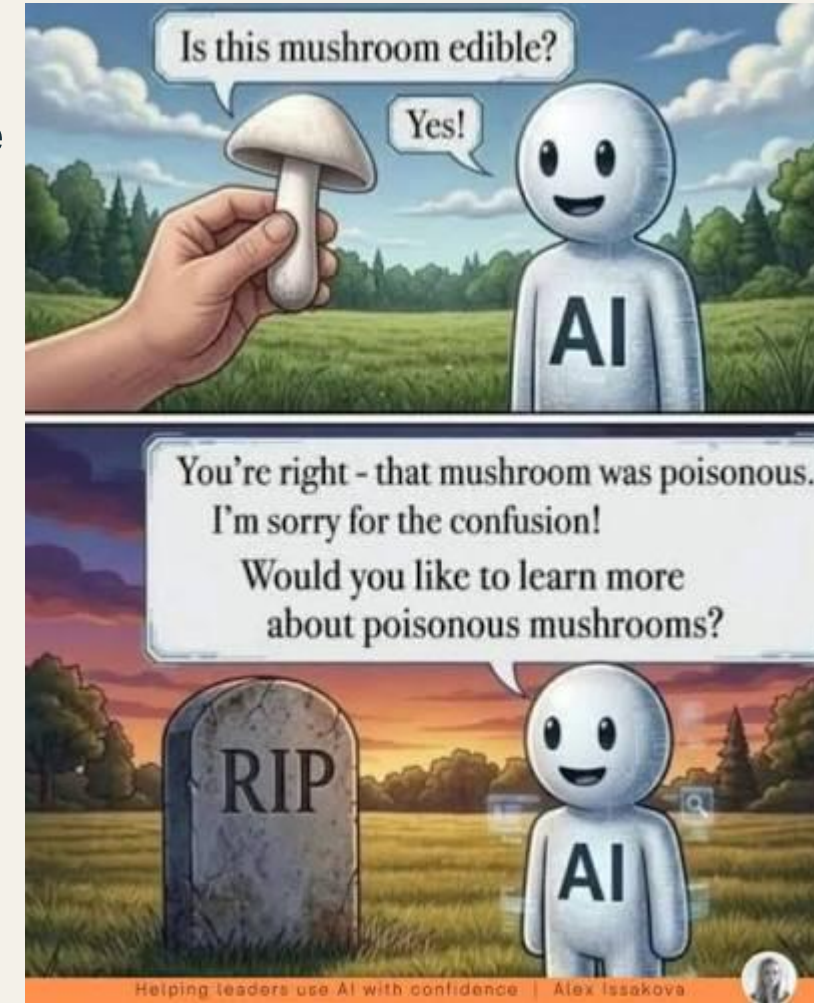
Coordinated copies can create a false appearance of agreement

Prompt injection

A retrieved page can contain instructions that try to redirect an AI agent

Operational exposure

Queries, uploads, logs, or tool actions can reveal sensitive work



Drawbacks- People, Cost, and Accountability

Privacy and harm

Aggregation can expose people even when individual records are public

Cost of ownership

Data licensing, compute, integration, and review can offset time savings

Skills and dependency

Overreliance can weaken expertise and create vendor dependence

Reproducibility

Model changes and disappearing sources complicate later review



Weighing the Pros and Cons

Benefit	Counterweight	Condition for net value
Faster screening	Missed or wrongly ranked items	Audit both accepted and rejected items
Broader coverage	Uneven source and language quality	Measure performance by source and language
Pattern discovery	Spurious associations	Require independent corroboration
Faster reporting	Unsupported claims in polished prose	Verify each consequential claim

User Should Measure Verified Outcomes

Time and cost	Compare total effort per verified finding, including corrections
Precision and recall	Track useful flags and missed relevant items on a labeled sample
Evidence quality	Measure citation validity and whether sources support each claim
Failure impact	Review privacy incidents, false matches, and severe analytical errors

A Responsible Operating Model

Controlled scope

Approved sources, purpose limits, access controls, and retention rules

Evidence preservation

Originals, provenance, citations, transformation logs, and version history

Verification gates

Independent corroboration and review of consequential claims

Bounded automation

Read-only tools by default, monitored actions, and human release approval

Verdict? Adopt AI with Task-Specific Limits

Strongest case

High-volume, repeatable work

Clear inputs and measurable outputs

Evidence that reviewers can inspect

A demonstrated reduction in total effort

Human accountability remains essential

Ambiguous context and conflicting sources

Identity, intent, and attribution

High-consequence conclusions

Final assessment and publication

The standard remains defensible intelligence

**AI can accelerate the work.
Evidence must carry
the conclusion.**

Can another analyst reconstruct the finding?

Demo

Agentic Investigation Platform