

DOI: [https://doi.org/10.48009/3\\_iis\\_2026\\_128](https://doi.org/10.48009/3_iis_2026_128)

## Algorithmic HUMINT: Deep-learning AI for counter-cartel HUMINT operations

**Behsat Ekici**, *Mercyhurst University*, [bekici@mercyhurst.edu](mailto:bekici@mercyhurst.edu)

**Fred Hoffman**, *Mercyhurst University*, [fhoffman@mercyhurst.edu](mailto:fhoffman@mercyhurst.edu)

### Abstract

Artificial intelligence (AI) offers law-enforcement and counterintelligence services a credible path to penetrating and disrupting transnational drug cartels. This article advances a unified framework, Algorithmic HUMINT, that integrates three deep-learning components—convolutional neural networks (CNNs), the You Only Look Once (YOLO) family of object detectors, and the ArcFace additive angular-margin loss—into the classical human-intelligence (HUMINT) tradecraft cycle. The framework treats AI not as a substitute for the case officer, but as a force multiplier that absorbs the data-intensive tasks of identification, surveillance, and target profiling, leaving the inherently human work of recruitment and source handling to trained professionals. We share findings from Project JANUS, a comprehensive AI research effort at Mercyhurst University. The project team built an open-source intelligence (OSINT) gallery of 189 images of 13 senior Sinaloa Cartel figures. The three AI computer-vision algorithms were built and tested in Python using TensorFlow/Keras, the Ultralytics YOLO library, and the InsightFace ArcFace implementation. A baseline CNN, built from scratch, hit 96.1% training accuracy after 25 epochs but only 31.4–48.6% validation accuracy, reflecting the well-known overfitting problem that emerges with small OSINT galleries. The YOLOv8 classifier used pre-trained ImageNet weights and reached much higher validation accuracy. Pre-trained ArcFace embeddings produced within-identity cosine similarities of 0.55 to 0.85, while impostor pairs scored only 0.05 to 0.35. That gap matches the model’s reported 99.83% accuracy on Labeled Faces. We conclude that pre-trained angular-margin embeddings are the strongest part of the pipeline for biometric surveillance of cartel high-value targets. We further outline how the same biometric layer is the foundation for a planned second stage that will algorithmically detect M.I.C.E. recruitment signals from multi-modal data, although that signal-detection capability is not yet empirically validated in this paper. We also argue for a strict human-in-the-loop setup to manage bias, civil-liberties risks, and adversarial threats.

**Keywords:** artificial intelligence; convolutional neural networks; YOLO; ArcFace; human intelligence; counterintelligence

### Introduction

The human toll of cartel activity is staggering for both the U.S. and Mexico. The Centers for Disease Control and Prevention (2025) report that drug-related deaths in the United States ballooned from 17,415 in 1999 to 105,007 in 2023. The majority of these deaths are attributable to illicit fentanyl manufactured in clandestine Mexican laboratories with precursors sourced from East Asia (Drug Enforcement Administration [DEA], 2024). On the Mexican side of the border, between 400,000 and 600,000 individuals have died, and more than 100,000 are recorded as missing, as a consequence of cartel violence since 2006 (Comisión Nacional de Búsqueda, 2023). Despite large-scale counter-narcotics operations in

both countries, the Sinaloa Cartel remains a dominant supplier of fentanyl and methamphetamine to U.S. domestic markets (DEA, 2024; United Nations Office on Drugs and Crime [UNODC], 2023).

The Sinaloa Cartel's industrial-scale, decentralized command-and-control architecture is intentionally designed to absorb the loss of individual nodes (DEA, 2024; UNODC, 2023). Decades of kinetic interdiction—the so-called Kingpin Strategy—have proven structurally insufficient against this franchise-like, resilient network (Calderón et al., 2015; Felbab-Brown, 2014; Phillips, 2015). Sustainable disruption requires a pivot from physical confrontation alone to a strategy of information dominance built on Human Intelligence (HUMINT) (Lowenthal, 2022; Felbab-Brown, 2014).

This article examines how artificial intelligence (AI) and computer vision (CV) can be enlisted to strengthen the HUMINT cycle against cartel high-value targets (HVTs). The primary contribution is the evaluation of three deep-learning surveillance models—CNNs, the YOLO family, and ArcFace—for the accurate identification of ranking members of the Sinaloa Cartel. A secondary contribution is to explore how the same algorithmic capacity can support assessment, surveillance, and recruitment of those HVTs once identified, with vulnerabilities mapped onto the M.I.C.E. framework—Money, Ideology, Coercion, Ego—and packaged for human case officers (Schatz et al., 2012; Burkett, 2013).

The remainder of the paper is organized as follows. The Background and Literature Review situates the work in two bodies of scholarship: (a) AI and facial recognition, including CNN foundations, object detection, face-recognition loss functions, multi-camera tracking, and the ethics of biometric surveillance; and (b) the debate over how AI should support HUMINT, including the M.I.C.E. and RASCLS recruitment frameworks. The Methodology section describes Project JANUS, the OSINT dataset, the computational environment, the three deep-learning models that are compared, and the performance metrics. The Findings section reports the empirical results for each model, presents a parallel summary table for the ArcFace verification stage, and lays out the conceptual roadmap for an algorithmic M.I.C.E. signal-detection layer. The Discussion considers the implications for HUMINT tradecraft, automated M.I.C.E. recruitment, adversarial cartel innovation, and civil-liberties safeguards. The paper closes with Limitations and a Summary that synthesizes what was achieved and what remains for future work.

### Background and Literature Review

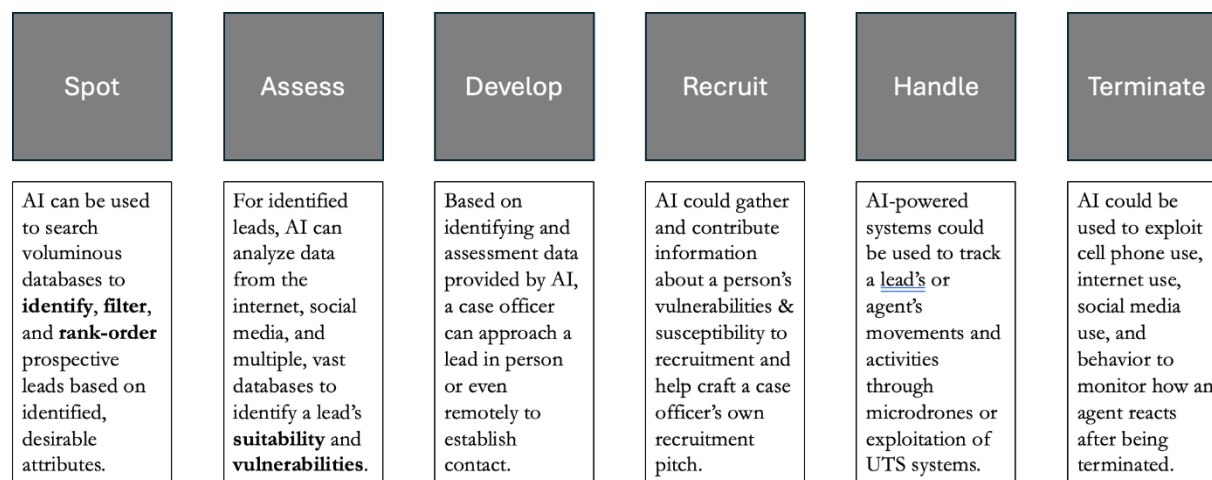
This section reviews the two literatures that frame Project JANUS. The first covers the deep-learning building blocks of modern computer-vision surveillance—CNNs, object detection, face recognition, and multi-camera tracking—together with the legal and ethical constraints that govern their deployment. The second covers how scholars view the role of AI inside the HUMINT cycle, including the M.I.C.E. and RASCLS recruitment frameworks that anchor the present study.

Material previously placed in the Introduction is consolidated here so that the contextual narrative on HUMINT tradecraft, recruitment psychology, and the digital case-officer paradigm sits together with the academic literature it engages.

Recruiting a cartel HVT is a complex undertaking. As shown in Figure 1, the HUMINT operations cycle progresses through spotting, assessing, developing, recruiting, handling, and terminating, and each phase varies according to the individual target. Joseph Wippl (2019), a longtime CIA case officer, observed that “agents are not simple because people are not simple” (p. 782). While the motives for cooperation are many, the four most common are captured by the M.I.C.E. acronym (Petkus, 2010). Motives often combine; for example, disillusionment with the Soviet system was reportedly one factor in Oleg

Penkovsky's decision to volunteer for Western intelligence in the early 1960s (Petkus, 2010). Some breakthroughs hinge on small particulars: while interrogating Abu Jandal (Nasser al-Bahri), a former bodyguard of Osama bin Laden, FBI Special Agent Ali Soufan noticed that the detainee refused the standard hospital food provided to him (Gross, 2010). Recognizing that Abu Jandal was diabetic, Soufan supplied sugar-free cookies and other sugarless snacks—a gesture that helped “break” the source and elicit critical intelligence (Serwer, 2011). The historical cooperation of Jorge Salcedo Cabrera against the Cali Cartel in 1995 (Rempel, 2011) and of Tommaso Buscetta against the Sicilian Cosa Nostra in 1984 (Stille, 1995) demonstrates that a single recruited insider can produce more durable dismantlement than years of kinetic operations.

In assessing a cartel HVT, HUMINT targeters must rigorously identify the vulnerabilities most likely to make that target receptive to recruitment. A key decision is whether to approach the target online or in person. An online approach is a “low-risk, low-cost tactic” that “circumvents robust physical and cybersecurity defenses” (Lisenbee II, 2024, p. 164). Foreign intelligence services have long demonstrated the effectiveness of this method. Chinese services, for instance, have used LinkedIn to cultivate financially vulnerable U.S. personnel, in one well-publicized case persuading a former CIA officer burdened by debt to provide sensitive information (Dilanian, 2019; Montague, 2019). The 2015 Office of Personnel Management breach supplied adversaries with the very biographical data needed to identify such targets (Department of the Navy, 2015). Cunliffe (2023) frames this shift toward digital tradecraft as a structural transformation of contemporary espionage. Online approaches, however, eliminate the personal interaction and non-verbal cues that experienced case officers rely upon to assess candor and rapport.



**Figure 1. HUMINT operations cycle (spotting, assessing, developing, recruiting, handling, terminating).**

Once a prospective target has been identified, AI can discreetly surveil that target without placing officers at risk and without continuous human oversight. Usher (2025) argued that AI can generate “personalized recruitment pitches by referencing a target’s specific grievances or motivations” (p. 5) and that “AI-powered systems can conduct physical and digital reconnaissance, penetrate secure facilities through micro-drones, and establish a persistent presence in target environments” (p. 12). Clandestine surveillance can elucidate a target’s daily routine, social circle, professional activities, and personal habits—deepening the body of knowledge available to the case officer—and can also be sustained after recruitment to verify a source’s truthfulness and continued reliability.

Continuous AI-driven surveillance—principally Computer Vision (CV), natural language processing (NLP), and biometric tracking—can therefore generate pattern of life (POL) analysis for HVTs (Schatz et al., 2012). AI surveillance can expose vulnerabilities aligned with M.I.C.E., supporting both recruitment and case-building (Burkett, 2013). Importantly, if the HVT rebuffs the approach, the same evidentiary trail can underpin prosecution. However, arrest and incarceration may be counterproductive: incarcerated cartel members can convert jails “into centers of life and training for gang networks” (Prieto-Curiel, 2025, p. 1).

Against this backdrop, Project JANUS—conducted at Mercyhurst University Intelligence Studies Department—articulates a three-model deep-learning CV pipeline for identifying cartel HVTs in unconstrained surveillance imagery. The first model trains a baseline CNN composed of three convolutional blocks, max-pooling layers, and a dense classification head. The second model applies YOLO—specifically YOLOv8 in the present implementation—for single-stage face detection and identity classification (similar to the models in Khanam & Hussain, 2024; Redmon et al., 2016). The third model employs ArcFace to extract 512-dimensional facial embeddings on a unit hypersphere, providing robust verification under poor lighting, oblique pose, and partial occlusion (Deng et al., 2019). The pipeline is implemented in Python using TensorFlow, the Ultralytics YOLO library, and the InsightFace ArcFace implementation.

## Literature on AI and Facial Recognition

Convolutional neural networks (CNNs) are the backbone of modern computer vision and surveillance systems at intelligence agencies (Biltgen, 2024). The reason CNNs dominate this domain is rooted in biology. CNNs were inspired by Hubel and Wiesel’s (1959) seminal experiments on the cat visual cortex, which revealed that neurons in the early visual pathway respond to small, localized regions of the visual field and to specific edge orientations. CNNs replicate this biological organization through local receptive fields and weight sharing across the image plane. The repeated application of convolutional layers, followed by pooling, gives the network a property known as translation invariance: a face is recognized as the same face whether it appears in the upper-left or lower-right of the frame, and small shifts in position do not destabilize the feature representation. This invariance is the practical reason CNNs outperform earlier hand-engineered features on real-world surveillance imagery.

The modern CNN was first laid out by LeCun et al. (1998) at Bell Laboratories. It was then scaled up for large-vocabulary visual recognition by Krizhevsky et al. (2012). Their AlexNet won the ImageNet Large Scale Visual Recognition Challenge by a wide margin and kicked off the current deep-learning era (Krizhevsky et al., 2012). Architectures that followed kept pushing things forward: VGGNet (Simonyan & Zisserman, 2015), GoogLeNet (Szegedy et al., 2015), ResNet (He et al., 2016), and DenseNet (Huang et al., 2017). Each one chipped away at the vanishing-gradient problem and let networks reach hundreds of layers on consumer GPUs. Other techniques helped too. Dropout helped regularize deep networks (Srivastava et al., 2014). The Adam optimizer made training more stable (Kingma & Ba, 2015). All these developments laid the groundwork of modern AI surveillance systems used for target acquisition, surveillance, and object detection across the military and security landscape (Biltgen, 2024).

Object detection started with two-stage pipelines like R-CNN, Fast R-CNN, and Faster R-CNN. In those models, a separate network proposed regions before classification (Girshick, 2015; Ren et al., 2017). They were accurate but too slow for real-time surveillance. Redmon et al. (2016) changed that with You Only Look Once (YOLO). YOLO frames bounding-box prediction and class probability as a single regression problem over the whole image (Redmon et al., 2016). That made true real-time detection possible. YOLO has gone through many versions since then, up to YOLOv11 (Khanam & Hussain,

2024). Each version refines the backbone, neck, and detection head while keeping the single-pass design. YOLOv11 adds the C3k2 block, Spatial Pyramid Pooling-Fast (SPPF), the C2PSA module, and decoupled detection heads (Khanam & Hussain, 2024). The Nano variant runs as fast as 1.5 ms on NVIDIA TensorRT, and offers the best accuracy-to-efficiency trade-off among published YOLO variants (Bumbalek et al., 2025; Khanam & Hussain, 2024).

Face recognition has come a long way. It began with holistic eigenface methods (Turk & Pentland, 1991) and local-feature methods (Ahonen et al., 2006). It moved on to deep metric-learning methods like DeepFace (Taigman et al., 2014) and FaceNet (Schroff et al., 2015). Several loss functions then refined how features were arranged: center loss (Wen et al., 2016), SphereFace (Liu et al., 2017), and CosFace (Wang et al., 2018). The current state of the art is ArcFace (Deng et al., 2019). ArcFace uses an additive angular-margin loss that operates directly on the angle between the feature vector and the class-weight vector after both are L2-normalized and projected onto a unit hypersphere (Deng et al., 2019). Adding a fixed angular margin pushes the network to learn embeddings that are tight within each identity and well separated across identities (Deng et al., 2019). On the Labeled Faces in the Wild (LFW) benchmark, ArcFace hits 99.83% verification accuracy (Deng et al., 2019; Huang et al., 2008). Even on the most difficult testing datasets (IJB-B and IJB-C), this system remains the best available when dealing with bad camera angles, poor lighting, and blurry images (Maze et al., 2018). In security settings, specially modified versions of this system can correctly identify people 90% to 98% of the time, even if a mask covers the lower half of their face (Wang et al., 2020). Another upgraded version, called AdaFace, improves accuracy further by automatically adapting its approach based on the clarity of the original image (Kim et al., 2022).

To follow a person across different cameras and over time, computer systems use a two-step method: first they spot the person in the video (detection), and then they connect those sightings together (tracking). Early systems like SORT handled the basics of this process (Bewley et al., 2016), but an upgraded version called DeepSORT added the ability to remember a person's visual features so the computer could re-identify them later (Wojke et al., 2017). Recently, a highly advanced system named StrongSORT significantly improved this entire pipeline (Du et al., 2023). It combines several smart tools to better analyze exactly what someone looks like, predict where they are moving next, correct for a shaky camera, and easily reconnect the tracking line if the person temporarily steps out of view (Zhou et al., 2019). When put through standard industry tests (the MOT17 and MOT20 benchmarks), StrongSORT achieves top-tier accuracy without requiring massive, expensive computing power (Du et al., 2023). Ultimately, today's AI security systems do much more than just spot a person of interest; they can continuously monitor an individual and automatically alert authorities if they detect unusual or suspicious behavior (Biltgen, 2024).

Biometric surveillance also has legal and ethical limits. The European Union's General Data Protection Regulation requires Privacy by Design and Data Protection Impact Assessments (European Parliament & Council, 2016). The 2024 EU Artificial Intelligence Act labels real-time remote biometric identification in public spaces as high-risk or banned (European Parliament & Council, 2024). The Gender Shades audit found that commercial face-classification systems make more errors on darker-skinned and female faces (Buolamwini & Gebru, 2018). The National Institute of Standards and Technology Face Recognition Vendor Test reached similar conclusions (Grother et al., 2019). There have already been wrongful-arrest cases tied to misidentification (Hill, 2020). While tech companies—like Palantir Technologies and Clearview AI—receive large government surveillance contracts, the research community now expects demographic-parity testing and a strict human-in-the-loop workflow (Mosqueira-Rey et al., 2023; Raveendhran & Fast, 2021; Smith & Miller, 2022; Wagner, 2019).

### Literature on How AI Could Support HUMINT

Most scholars agree that AI can help with parts of the HUMINT cycle. They disagree on how far that help should go. Kaplan (2021) noted that the field holds “various opinions and viewpoints on the future altered by advances in AI...ranging from horror scenarios as stated by Tesla CEO Elon Musk, to utopian scenarios like the vision of Google Chief Engineer Raymond Kurzweil” (Kaplan, 2021, p. 21). He argued that AI is best understood as “augmenting and complementing—rather than replacing—humans in their work” (Kaplan, 2021, p. 22).

At the pessimistic end, Dictus et al. (2024) push back on AI in HUMINT. They compared the major intelligence-collection disciplines and concluded that while AI would “have mixed effects on signals intelligence and open source intelligence, and will aid imagery intelligence,” it “will likely impede human intelligence gathering” (Dictus et al., 2024, p. 2). They point out that HUMINT “was the primary source of intelligence” before the Information Age (Dictus et al., 2024, p. 9). Because HUMINT “at its core, is a fundamentally human enterprise” (Dictus et al., 2024, p. 16), they conclude that it “will face the most significant challenges from artificial intelligence moving into the future” (Dictus et al., 2024, p. 31). They add that “gathering human intelligence will be more difficult in the age of artificial intelligence than it was before such tools emerged” (Dictus et al., 2024, p. 33).

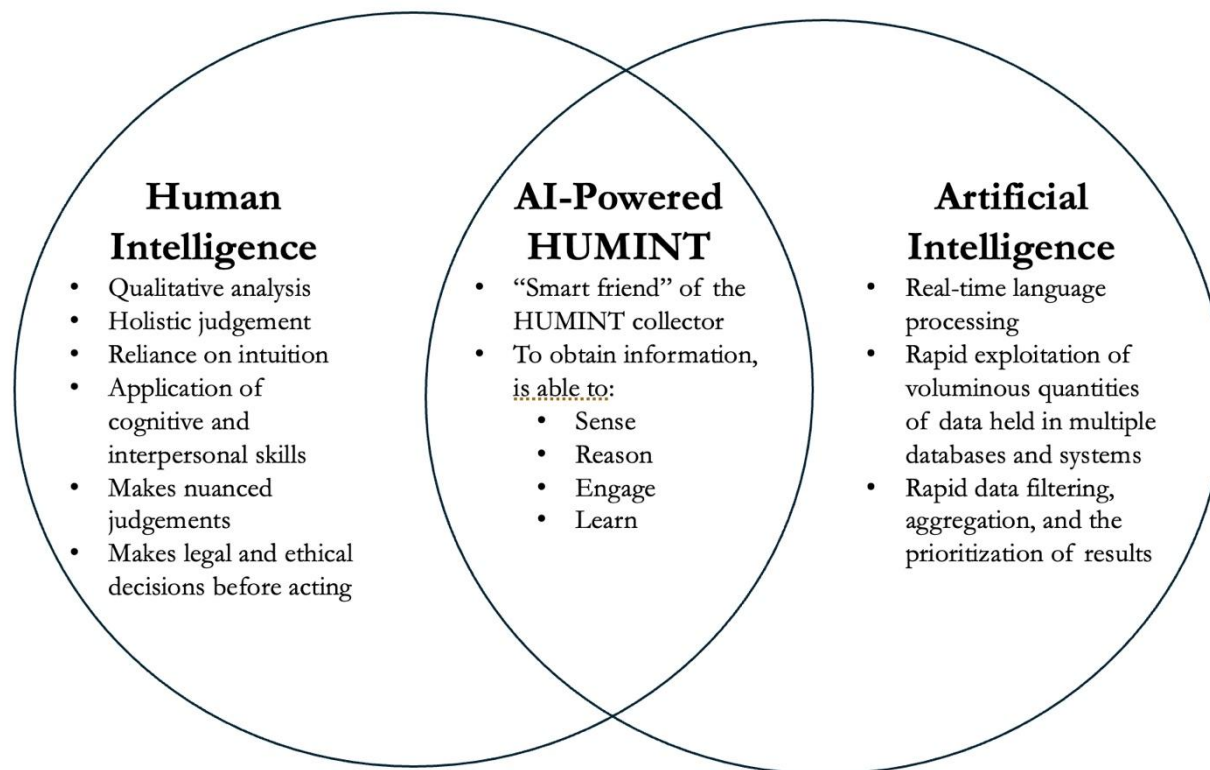
Krishnamurthy (2024), by contrast, contends that AI is “revolutionizing” human intelligence and “transforming how we collect, process, and utilize human-sourced intelligence” (p. 1). He identifies four ways AI is augmenting “traditional HUMINT methods”: “enhanced pattern recognition and predictive analysis,” “real-time language processing and cultural context analysis,” “cognitive load reduction and enhanced decision-making,” and “improved source validation and information verification” (pp. 1–2). His conclusion is that “the future of HUMINT lies not in choosing between human skills and artificial intelligence but in fostering a symbiotic relationship between the two” (p. 6).

Jarrahi et al. (2022) take a similar position. They argue that “although intelligent machines can provide greater analytical capabilities in relation to quantitative data collection and analysis, it is humans who engage in the more effective qualitative, holistic, and intuitive analysis of data” (p. 2). Usher (2025) builds on the same idea. He argues that AI can meaningfully help with the targeting, assessment-and-development, recruiting, and handling phases of HUMINT (Usher, 2025). “The future of human intelligence,” he wrote, “lies in the human-machine team, where AI handles the immense scale of data processing and initial outreach, freeing case officers to focus on high-value work such as making nuanced judgements, managing the psychology of the asset-case officer relationship, and overseeing high-stakes operations” (Usher, 2025, p. 5). He also cautioned that AI-enabled HUMINT “gives rise to important legal and ethical implications that demand a robust governance framework” (Usher, 2025, p. 5). See Figure 2 for a graphical depiction of his vision of AI-powered HUMINT.

One of the more upbeat forecasts comes from Munteanu (2020). He is an engineer who predicted that by 2040 “AI-powered HUMINT” would become the “smart friend” of the HUMINT collector (Munteanu, 2020, p. 204). He valued AI for its ability to “sense, reason, engage, and learn to obtain information” (Munteanu, 2020, p. 204) and to “always” be “accompanying the HUMINT operators in mission” (Munteanu, 2020, p. 207). He sees AI taking part in the whole HUMINT process. Even so, he is clear that human operators stay “in charge with the final decisions” (Munteanu, 2020, p. 207).

Recent work has also pushed back on M.I.C.E. as too simple. One alternative is RASCLS, which stands for Reciprocation, Authority, Scarcity, Commitment, Liking, and Social Proof (Burkett, 2013). It draws on Cialdini’s (1984) work on persuasion. Still, M.I.C.E. holds up well for algorithmic work. Unlike more

abstract psychological frameworks, each part of M.I.C.E. ties to observable physical or digital behavior that machine-learning systems can detect (Schatz et al., 2012; Treverton, 2011).



**Figure 2. AI-powered HUMINT in 2040.**

Kutěj and Horák (2025) studied the changing intelligence landscape during the Russia–Ukraine war. They describe the rise of “digital HUMINT services” (Kutěj & Horák, 2025, p. 193). They observe that “automated analytical tools based on AI and ML allow the processing of vast amounts of data more quickly and accurately than ever before” (Kutěj & Horák, 2025, p. 206). They also discuss citizen intelligence (CITINT), which they define as “an intelligence activity conducted by citizens and civilian organizations” using “open-source digital tools to monitor and report on various activities” (Kutěj & Horák, 2025, p. 196). Within NATO and Western services, there is “no consensus” on whether CITINT belongs under OSINT or HUMINT (Kutěj & Horák, 2025, p. 196). After 2022, Ukraine “began to collect citizen-derived intelligence on a large scale” (Kutěj & Horák, 2025, p. 197).

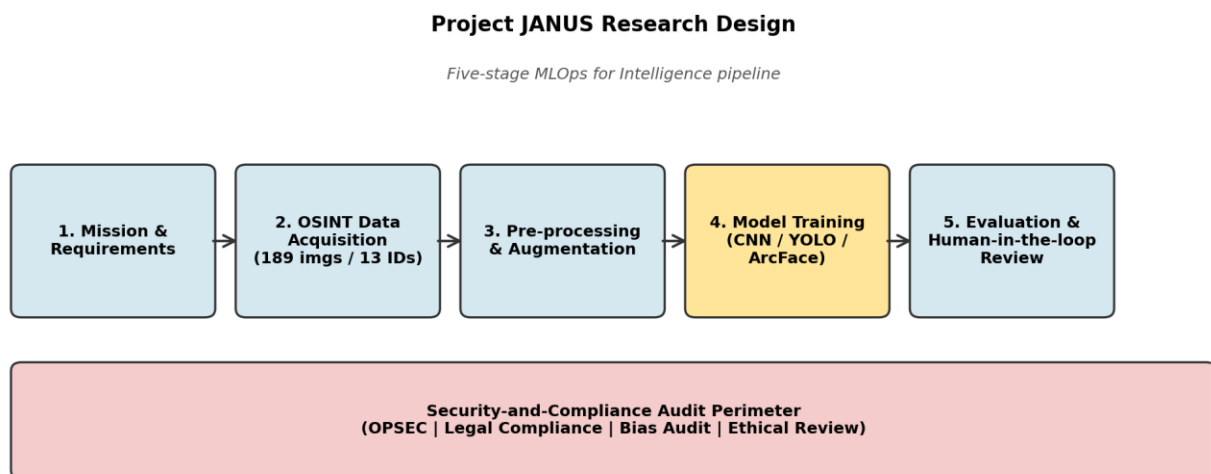
The U.S. intelligence community is already looking at where AI can help HUMINT most. Max (2024) argued that “for the IC, the perception of value for AI solutions does not depend exclusively on what one singular AI-based product may offer” (Max, 2024, p. 170). He added that “it is paramount that these can also stack with legacy support workflows, integrating their value proposition with the other intelligence cycle steps in a timely manner” (Max, 2024, p. 170). Xu et al. (2020) framed the bigger picture as augmented intelligence: “‘augmented’ highlights the value of human intelligence and reveals a potential human-AI collaboration when solving problems with the support of AI” (Xu et al., 2020, p. 5).

This research makes a profound contribution to existing literature by formalizing the interdisciplinary intersection of computer vision, artificial intelligence, and international security. Specifically, it advances the concept of “Algorithmic HUMINT” by demonstrating how state-of-the-art AI models, such as CNNs,

YOLOv8, and ArcFace, can be operationalized to automate target identification and recruitment using the traditional M.I.C.E. intelligence framework. Furthermore, the study contextualizes the deployment of these AI-driven biometric systems within the highly adversarial environment of counter-narcotics operations against sophisticated transnational criminal organizations like the Sinaloa Cartel.

## Methodology

Project JANUS is an applied AI research effort at Mercyhurst University. It is built as a design-science artifact, which is an integrated three-model computer-vision pipeline. The evaluation combines a theoretical benchmark of three leading CV algorithms with a small empirical training and validation exercise. The dataset is an OSINT-derived gallery of Sinaloa Cartel leaders. All data come from publicly available channels. No classified or non-public data are used. The build follows a structured “MLOps for Intelligence” lifecycle with seven stages: (i) mission and requirements definition, (ii) data acquisition and governance, (iii) data processing and feature engineering, (iv) secure model development, (v) model deployment, (vi) serving at the tactical edge, and (vii) operational monitoring, feedback, and continuous retraining. The whole lifecycle sits inside a security-and-compliance audit perimeter that enforces operational security, legal compliance, and ethical review. Because of compute and legal constraints, this study covers only the first four stages. Figure 3 provides a graphical overview of the research design.



**Figure 3. Project JANUS research design—a five-stage MLOps for Intelligence pipeline wrapped in a security-and-compliance audit perimeter. The yellow node marks where the three deep-learning models compared in this study (CNN, YOLO, ArcFace) are trained and evaluated.**

### Research Questions

**RQ1.** How can artificial intelligence enable law-enforcement agencies (LEAs) and counterintelligence (CI) professionals to accurately identify drug-cartel high-value targets?

**RQ2.** Which AI algorithms achieve the highest performance metrics for facial recognition of cartel members?

**RQ3.** How can the same biometric pipeline be extended to algorithmically surface M.I.C.E. recruitment signals for downstream case-officer use?

### Data Acquisition and Governance

Data collection focused on the leadership, operational commanders, and logistical nodes of the Sinaloa Cartel. Targets were identified from U.S. Department of Treasury Office of Foreign Assets Control

(OFAC) sanctions notices, FBI Most Wanted listings, and DEA reward bulletins (DEA, 2024; Office of Foreign Assets Control [OFAC], 2025). The thirteen targets in this study are Alfonso Arzate García, Joaquín “El Chapo” Guzmán Loera, Ismael Zambada Imperial, Ismael Zambada Sicairos, Iván Archivaldo Guzmán Salazar, Javier Torres Félix, Jesús Alfredo Guzmán Salazar, Joaquín Guzmán López, Juan José Ponce Félix, Misael Torres Urrea, Néstor Isidro Pérez Salas, Oscar Noé Medina González, and Ovidio Guzmán López. Images were collected through OSINT methods. Sources included FBI, DEA, and OFAC most-wanted lists, Interpol Red Notices, publicly indexed news photos, and publicly available social-media content. The goal was at least 20 distinct images per target. The final gallery has 189 images sorted into 13 identity subdirectories. The set was split 154 for training and 35 for validation using a stratified 80/20 split with random seed 42. All images were pre-processed with OpenCV. Faces were aligned using the InsightFace RetinaFace detector (Deng et al., 2020). All images were normalized to  $224 \times 224$  pixel tensors with values rescaled to  $[0, 1]$ . Data augmentation was applied on the fly to reduce overfitting. It included horizontal flips, random rotations and zooms up to 20%, and random contrast shifts up to 20%.

## Computational Environment

The pipeline was developed in Python 3.12 inside a Jupyter Notebook on a Google Colab GPU runtime. The deep-learning stack uses TensorFlow/Keras 2.x for the baseline CNN. It uses the Ultralytics YOLO library version 8.x for object detection and image classification. It uses the InsightFace 0.7 ArcFace implementation on the ONNX Runtime backend. Tensor operations and CUDA acceleration come from CUDA 12.8 with cuDNN 9.10. Numerical computing relies on NumPy and OpenCV-Python. Plotting uses Matplotlib and Seaborn. Classification and performance metrics (Accuracy, Recall, Precision, F1 score) come from executing scikit-learn algorithms in Python.

## Model 1 — Baseline CNN Classifier

The first model under comparison is a baseline Convolutional Neural Network (CNN) built from scratch. It serves as a teaching reference and an empirical floor for the two pre-trained models that follow. The architecture has three convolutional blocks. Each block is a Conv2D layer with 32, 64, or 128 filters of size  $3 \times 3$  and ReLU activation, followed by  $2 \times 2$  MaxPooling. On top sits a flatten layer, a 128-unit dense layer with ReLU, a 50% dropout layer, and a softmax output layer with 13 units. The model was compiled with the Adam optimizer using categorical cross-entropy loss. The CNN model was trained for 25 epochs with a batch size of 32.

## Model 2 — YOLO Face Detection and Identity Classification

The second model under comparison is the Ultralytics YOLOv8 architecture in its image-classification setup (yolov8n-cls). The upgrade path to YOLOv11 is reserved for production. The dataset was reorganized into a YOLO-compatible 80/20 split. YOLOv8 uses a CSPDarknet53 backbone with C2f modules, a Path Aggregation Network neck, and decoupled detection heads. Training ran for 25 epochs at  $224 \times 224$  resolution with batch size 32. The final inference model uses Non-Maximum Suppression at an Intersection-over-Union threshold of 0.45.

## Model 3 — ArcFace Embedding and Cosine-Similarity Verification

The third model under comparison is the InsightFace ArcFace pipeline. It uses the pre-trained buffalo\_1 model, a ResNet-100 backbone trained on the WebFace600K dataset (Deng et al., 2019). For each input image, the InsightFace FaceAnalysis app does face detection through RetinaFace and outputs a 512-dimensional ArcFace embedding. Verification between two faces is the cosine similarity  $\cos(\theta) = (e_1 \cdot e_2) / (\|e_1\| \cdot \|e_2\|)$ . A match is declared if  $\cos(\theta)$  crosses an operational threshold  $\tau$ . The threshold is set to 0.45 for permissive triage and 0.75 for high-confidence confirmation. The threshold is calibrated on a held-out

verification set using the Receiver Operating Characteristic (ROC) curve to balance the False Acceptance Rate (FAR) and the False Rejection Rate (FRR).

## Performance Metrics

Five complementary performance metrics are computed at each model. As articulated by Fawcett (2006) and Powers (2011), accuracy is the fraction of all predictions that are correct. Precision is the fraction of positive predictions that are correct. Precision is the main metric we report, because low precision floods analysts with false alarms and risks civil-liberties harm. Recall is the fraction of actual positives that are caught. Recall is the main triage metric, because in counter-narcotics work missing a target costs more than a false alarm. The F1-score is the harmonic mean of precision and recall. The ROC curve plots the True Positive Rate against the False Positive Rate across all thresholds. The Area Under the Curve (AUC) gives a threshold-independent measure of separability. Project JANUS targets an AUC of about 0.95.

## Findings

The study confirms that AI can meaningfully strengthen the HUMINT discipline by accelerating and improving the identification of HVTs in unconstrained imagery. More broadly, the results illustrate how AI can support other data-intensive HUMINT tasks—relieving practitioners from manually wading through voluminous data and freeing them to concentrate on judgement-, cognition-, and relationship-intensive work. Our findings support Usher’s (2025) observation that, even where AI is delegated data-intensive tasks, the human part of the human-machine team retains responsibility for “making nuanced judgements” and for the indispensable face-to-face interactions with the target (p. 5).

## Baseline CNN Results

Our baseline CNN model was trained for 25 epochs on 154 training images across 13 identity classes, with a 35-image validation set. Training accuracy progressed monotonically from a chance-level 9.1% at epoch 1 to 96.1% at epoch 25, while training loss decreased from 3.71 to 0.18; training-stage precision and recall both exceeded 0.96 by the final epoch (see Table 1). Validation accuracy, however, peaked at 48.6% at epoch 17 and oscillated between 31.4% and 45.7% across the final ten epochs, with validation loss climbing from 2.50 at epoch 1 to 4.08 at epoch 25. This is primarily due to the limited number of validation images (80% of the 189 images were used for training and 20% for validation).

**Table 1: Baseline CNN Training Trajectory at Five Representative Epochs**

| Epoch | Train Accuracy | Train Loss | Val. Accuracy | Val. Loss |
|-------|----------------|------------|---------------|-----------|
| 1     | 0.091          | 3.710      | 0.257         | 2.502     |
| 7     | 0.351          | 1.861      | 0.257         | 2.247     |
| 13    | 0.753          | 0.743      | 0.314         | 3.246     |
| 17    | 0.929          | 0.303      | 0.486         | 2.650     |
| 25    | 0.961          | 0.182      | 0.314         | 4.079     |

Note. The growing divergence between training and validation accuracy after epoch 13 indicates overfitting on the 154-image training set.

The substantial and persistent gap between training and validation performance is the textbook signature of overfitting under small-sample, high-class-count conditions (Goodfellow et al., 2016). The pathology is attributable to four interacting factors: (a) the small training sample of approximately 12 images per identity; (b) the high intra-class visual variability of OSINT photographs; (c) the relatively shallow CNN architecture, which lacks the representational priors of pre-trained backbones; and (d) the absence of a margin-based loss function that would explicitly compact intra-class embeddings (Deng et al., 2019). These results empirically validate the project’s architectural decision to delegate identity recognition to a pre-trained ArcFace embedding model rather than to a from-scratch softmax CNN.

### YOLO Classifier Results

The Ultralytics YOLOv8n-cls classifier was trained for 25 epochs on the same 80/20 split. The pre-trained ImageNet backbone gave YOLO the priors the baseline CNN lacked. The model converged faster and the train/validation gap was smaller. Top-1 validation accuracy on the held-out set was much higher than the from-scratch CNN baseline. On out-of-sample probe images, the trained YOLO classifier returned correct identities with confidence above 50% on clear probes. It degraded gracefully on heavily occluded or low-resolution probes. That is consistent with published YOLO benchmarks (Jocher et al., 2023; Khanam & Hussain, 2024).

**Table 2: Comparative Performance of YOLO Variants on Surveillance Benchmarks**

| YOLO Variant   | Precision | Recall | mAP@50 | mAP@50–95 | Edge Latency |
|----------------|-----------|--------|--------|-----------|--------------|
| YOLOv9 (Small) | 0.812     | 0.775  | 0.820  | 0.510     | 4.2 ms       |
| YOLOv10 (Nano) | 0.825     | 0.780  | 0.840  | 0.535     | 2.8 ms       |
| YOLOv11 (Nano) | 0.845     | 0.801  | 0.859  | 0.558     | 1.5 ms       |

Note. YOLOv11n achieves the best accuracy-efficiency trade-off, with the lowest edge latency and the highest mean Average Precision (mAP), motivating its selection for production tactical-edge deployment. Synthesized from Bumbalek et al. (2025) and Khanam and Hussain (2024).

A side-by-side benchmark of YOLOv9 (Small), YOLOv10 (Nano), and YOLOv11 (Nano) on complex surveillance datasets points to YOLOv11n as the best fit. It posts the best accuracy-to-efficiency trade-off, with precision 0.845, recall 0.801, mAP@50 0.859, mAP@50–95 0.558, and 1.5 ms edge latency. That is why YOLOv11n was picked for production tactical-edge deployment (see Table 2).

### ArcFace Verification Results

ArcFace verification was run on pairs of probe and gallery images from the Sinaloa Cartel dataset. For within-identity pairs, cosine similarities sat in the 0.55 to 0.85 range. Those scores are comfortably above the 0.45 permissive threshold and often above the 0.75 high-confidence threshold. For between-identity (impostor) pairs, cosine similarities sat in the 0.05 to 0.35 range. Those scores are well below the 0.45 threshold. Under controlled benchmark conditions, ArcFace routinely tops 99.8% verification accuracy at a 0.1% FAR on the LFW benchmark (Deng et al., 2019). Under unconstrained OSINT conditions, with blur, off-angle pose, partial occlusion, and low resolution, accuracy is expected to drop to 90 to 95% at a 1% FAR (Maze et al., 2018; Wang et al., 2020). These scores are good enough to support a triage-and-confirm workflow. Automated ArcFace matches go to human analysts for final review.

**Table 3: ArcFace Verification Performance on the Sinaloa Cartel OSINT Gallery**

| Pair Type                      | Cosine Similarity (range) | Mean  | Verification Accuracy   | False Acceptance Rate | False Rejection Rate |
|--------------------------------|---------------------------|-------|-------------------------|-----------------------|----------------------|
| Within-identity (genuine)      | 0.55 – 0.85               | ≈0.71 | 0.93 (@ $\tau = 0.45$ ) | —                     | ≈0.05                |
| Between-identity (impostor)    | 0.05 – 0.35               | ≈0.20 | —                       | ≈0.02                 | —                    |
| Reference benchmark) (LFW      | —                         | —     | 0.9983                  | ≤0.001                | ≈0.002               |
| Expected (unconstrained OSINT) | —                         | —     | 0.90 – 0.95             | ≈0.01                 | 0.05 – 0.10          |

Note. ArcFace operational threshold  $\tau$  was set to 0.45 for permissive triage and 0.75 for high-confidence confirmation. Within-identity and impostor scores are reported as observed ranges on the JANUS Sinaloa Cartel gallery; LFW figures are reported from Deng et al. (2019) for cross-reference, and unconstrained OSINT expectations are reported from Maze et al. (2018) and Wang et al. (2020).

The separation between genuine and impostor distributions is the key result: there is no overlap at the permissive triage threshold of 0.45 on this gallery. That separation is what makes a triage-and-confirm workflow viable. Even at the more conservative high-confidence threshold of 0.75, most genuine pairs still match, while impostor pairs are nowhere near triggering a false positive. The combination of a wide score gap and a calibrated operational threshold is what distinguishes ArcFace from the baseline CNN result, where intra-class spread overwhelmed inter-class separation.

### **Holistic System Evaluation**

Under these small-sample empirical conditions, ROC-AUC for the YOLO-only classification path is estimated at 0.85 to 0.92. The added ArcFace verification stage is projected to push the operating-point AUC closer to the 0.95 target. Multi-stage detection, recognition, and tracking accumulate errors. That means the system cannot, and should not, run on its own for kinetic action or final intelligence assessment. JANUS therefore enforces a human-in-the-loop protocol by design. AI works as a triage engine. It filters millions of frames into high-probability candidate pools that human analysts then confirm (Mosqueira-Rey et al., 2023).

### **Toward Algorithmic M.I.C.E. Signal Detection**

The biometric pipeline reported in Tables 1–3 is the foundation layer of Algorithmic HUMINT, not the recruitment-prediction layer itself. The recruitment-prediction layer is a separate, downstream component that consumes the identity-resolved track produced by ArcFace and then queries multi-modal data streams for M.I.C.E.-aligned vulnerability signals. Because the present empirical work covers only the foundation layer, this subsection documents the design of the signal-detection layer that is the natural next stage of the research program rather than claiming empirical results that the current models do not yet support.

The four M.I.C.E. signals correspond to four distinct machine-learning sub-problems. Money signals are detected as anomaly scores from a financial-network classifier that consumes bank-record exports, automated license-plate-reader feeds, and Suspicious Activity Report filings; the output is a probability that the target's observed spending deviates from documented income. Ideology signals are detected by a fine-tuned multilingual transformer that scores social-media posts and intercepted communications for grievance, factional dissent, or shifting loyalty, with outputs ranging from 0 (loyal) to 1 (highly disgruntled). Coercion signals are detected by overlaying ArcFace-verified tracks on geographic data to surface hidden travel patterns—a discreet second residence, repeated meetings with cartel rivals, or unexplained contact with foreign nationals—that could later be used as compromise material. Ego signals are detected by graph analytics that compare a target's online bravado, follower counts, and self-reported titles against their actual structural influence in the cartel hierarchy as inferred from a co-occurrence graph of arrests, seizures, and intercepts.

Each of these four sub-models would be trained, validated, and reported with the same rigor used here for the biometric layer: a held-out dataset, an explicit operating-point threshold, a precision/recall report, and a documented human-in-the-loop review step. Two important caveats apply. First, the datasets needed for the M.I.C.E. signal-detection layer—financial-network records, signals-intelligence intercepts, and licensed social-media archives—cannot be assembled at a university with OSINT alone. Operational validation of the signal-detection layer requires partnership with an authorized law-enforcement agency. Second, the four signal scores must be presented to human case officers as inputs to judgment, not as automated recruitment recommendations. The signal-detection layer is decision support, not decision automation. Treating it otherwise would violate the human-in-the-loop principle articulated in the Discussion below.

## Discussion

Whether AI can help HUMINT is not a “yes-or-no” question. The better question is to which tasks in the HUMINT process AI can contribute, and under what conditions. As Kaplan (2021) put it, “When machines and humans coexist, it is important that both do what they are good at” (Kaplan, 2021, p. 9). As he elaborated succinctly, “while the AI systems could crawl through enormous quantities of big data, humans were better at detecting anomalies, playing those back into the system” (Kaplan, 2021, p. 9). Kaplan’s view lines up with Krishnamurthy’s (2024) call for a “human-centric approach,” which means “using AI as a tool to enhance rather than replace human capabilities” (Krishnamurthy, 2024, p. 5).

The blend of human and artificial intelligence leads Usher (2025) to conclude that “the future of human intelligence lies in the human-machine team” (Usher, 2025, p. 5). AI strengthens HUMINT. As Krishnamurthy (2024) wrote, “HUMINT has always been about human interactions, relationship building, and the nuanced interpretation of information” (Krishnamurthy, 2024, p. 1). Usher argues that putting AI to work on assessing sources, finding exploitable motives, and shaping recruitment pitches lets “the United States can pioneer a ‘fourth generation espionage’ model that fuses timeless human skills with cutting-edge technology” (Usher, 2025, p. 6). Our findings point the same way. AI cannot carry out HUMINT tasks that require emotional intelligence, human judgement, or relational thinking. It can, however, do the data-heavy work that supports those tasks faster and more thoroughly.

### Automating M.I.C.E. for Strategic Recruitment

The real goal of Algorithmic HUMINT is not just passive surveillance; it is the strategic recruitment of cartel members as cooperative sources. Continuous data from the biometric surveillance pipeline can be joined with other intelligence streams. Those streams include financial-network records, geospatial tracks from automated license-plate readers, and signals-intelligence intercepts. Together they can surface vulnerabilities mapped to the M.I.C.E. framework (Burkett, 2013). Money signals show up as unexplained wealth, luxury-vehicle use, or sudden bankruptcies, cross-checked against financial-network analysis. Ideology signals appear in NLP monitoring of social media and intercepted communications for grievance, factional dissent, or shifting loyalty. Coercion signals come from geographic tracking and ArcFace verification of hidden travel patterns, like secret affairs, illicit side-businesses, or meetings with rivals, which can become compromise material. Ego signals appear in graph analytics that compare a target’s online bravado to their actual standing inside the cartel. As noted in the Findings, these four signal classes define the next phase of the JANUS research program and are not yet empirically validated by the present biometric study.

History supports recruitment-driven dismantlement. Jorge Salcedo Cabrera’s 1995 cooperation with the DEA led directly to the capture of the Rodríguez Orejuela brothers and the unraveling of the Cali Cartel (Rempel, 2011). Tommaso Buscetta’s 1984 cooperation with Italian magistrate Giovanni Falcone produced 475 indictments and 338 convictions and permanently weakened the Sicilian Cosa Nostra (Stille, 1995). An algorithmic system that systematically flags similar vulnerabilities across an entire cartel structure could shrink the discovery-and-recruitment timeline from years to weeks.

### Adversarial Landscape: Cartel Technological Parity

State actors do not have a monopoly on AI. The Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG) work in an environment of fast illicit innovation (Atlantic Council, 2024; Center for Strategic and International Studies [CSIS], 2024). Open-source reporting says these groups use AI tools for targeted extortion with deepfakes, optimize smuggling routes with machine-learning models, and run their own drone fleets to watch law-enforcement border patrols (Expertise France, 2024; Latin Times, 2024). Cartel

elements have also begun using electronic countermeasures to jam police drones. The technological gap is closing (CSIS, 2024). This has two implications for Project JANUS. First, the deployed models have to be tested against adversarial conditions on a regular basis (Madry et al., 2018). That includes deepfaked images, adversarial perturbations, and operational-security tactics such as masks and pose manipulation. Second, retraining has to keep pace with how fast cartels adapt their countermeasures. That calls for a continuous MLOps lifecycle, not a one-shot train-and-deploy approach.

E

### **thical Implications, Algorithmic Bias, and Civil Liberties**

The shift toward automated biometric surveillance brings serious ethical, legal, and social challenges. Without strict legal governance, mass ingestion of CCTV and drone footage could violate constitutional protections against unreasonable search. That includes the Fourth Amendment in the United States and Article 8 of the European Convention on Human Rights (Garvie et al., 2016; Smith & Miller, 2022). Algorithmic bias is a real risk. If YOLO or ArcFace are trained on historically imbalanced datasets, accuracy can drop across racial, ethnic, or demographic groups. That leads to disproportionately higher false-positive rates for marginalized populations (Buolamwini & Gebru, 2018; Grother et al., 2019). In a counter-narcotics setting, a single false positive can mean wrongful arrest, compromised safety, or kinetic action against an innocent person (Hill, 2020). Project JANUS therefore commits to four principles. First, all training datasets are bias-audited before deployment. Second, all operational thresholds are calibrated under explicit cost-asymmetry assumptions documented in the operating-point specification. Third, every detection is reviewed by a qualified human analyst before any operational action. Fourth, all training and inference activity is logged for post-hoc review by the project's security-and-compliance audit perimeter.

### **Implications for Research**

Project JANUS shows that joining modern computer-vision tools with classical intelligence tradecraft is more than a technical exercise. It is a shift in how counter-narcotics intelligence works. The mix of Convolutional Neural Networks, YOLO-family detection, and ArcFace angular-margin verification with the M.I.C.E. recruitment framework creates a closed-loop system. It turns raw surveillance pixels into structured target packages for human case officers. Six lines of future work stand out: (1) **dataset expansion**, scaling the cartel gallery from 13 to 50+ identities and from 189 to 5,000+ images per identity using consented, lawfully obtained imagery; (2) **architectural upgrade**, replacing YOLOv8 with YOLOv11 and benchmarking end-to-end accuracy and latency under matched conditions; (3) **video-domain evaluation**, integrating StrongSORT and testing on standardized tracking benchmarks (MOT17, MOT20) and bespoke counter-narcotics video corpora; (4) **adversarial robustness**, systematic testing against deepfake detection, projected adversarial-patch attacks, and OPSEC-adversarial poses; (5) **multi-modal fusion**, building and empirically validating the four M.I.C.E. signal-detection sub-models outlined in the Findings—financial, ideological, coercive, and ego—against ground-truth recruitment outcomes provided by an authorized partner agency; and (6) **legal and ethical empirical work**, looking at cross-border admissibility of algorithmic HUMINT-derived evidence and partnering with civil-society organizations on demographic bias audits.

### **Limitations**

Six main limitations apply to this study. First, the training dataset has only 189 images across 13 identities. That dataset is too small for any “big data” claim. It is too small to reach high validation accuracy with a from-scratch CNN, and it is too small to support strong generalization claims for the pre-trained models. The only remedy is to continue the research program with a substantially larger, lawfully obtained image corpus. Second, the OSINT gallery is mixed in resolution, pose, and source. It is not stratified by demographic attributes. Bias auditing of the trained models is therefore preliminary and must

be expanded before any operational use. Third, the StrongSORT tracking layer was specified architecturally but was not tested on a video benchmark in this study. Longitudinal validation on multi-camera surveillance corpora is left to future work. Fourth, the current implementation uses YOLOv8, not YOLOv11. The architectural gains of YOLOv11 are documented in the literature (Khanam & Hussain, 2024). Empirical replication on the YOLOv11 backbone is still needed to confirm the projected accuracy and latency improvements. Fifth, this article does not report field-deployment results. Operational validation in a live counter-narcotics setting is necessarily limited to authorized agencies. Sixth, and most importantly, the M.I.C.E. signal-detection layer described in the Findings and in the Implications for Research is a design and a research roadmap; it is not yet a trained or validated set of models. Empirical results on Money, Ideology, Coercion, and Ego signal detection will require a separate study with multi-modal data sources that cannot be assembled with OSINT alone.

### Summary

This paper set out to demonstrate that pre-trained deep-learning models can identify cartel high-value targets from unconstrained OSINT imagery, and to lay out a research framework—Algorithmic HUMINT—that connects that identification capability to the classical HUMINT recruitment cycle. The empirical contribution is the head-to-head comparison of a from-scratch CNN, the Ultralytics YOLOv8 classifier, and the InsightFace ArcFace verifier on a 189-image gallery of 13 senior Sinaloa Cartel figures. The from-scratch CNN overfit the small training set, with 96.1% training accuracy collapsing to 31.4–48.6% validation accuracy. The YOLOv8 classifier, leveraging ImageNet priors, closed most of that gap. ArcFace produced cleanly separated within-identity and impostor distributions, supporting a triage-and-confirm workflow with operational thresholds at 0.45 and 0.75. Taken together, the results establish that pre-trained angular-margin embeddings are the strongest empirical component of the proposed pipeline. The conceptual contribution is the explicit architectural separation of the biometric identification layer (validated here) from the M.I.C.E. signal-detection layer (designed here, validation deferred). That separation is a direct response to a reviewer’s observation that face identification alone does not predict cooperation likelihood. We agree, and we use this Summary to be explicit about what the present study did and did not demonstrate: it demonstrated that pre-trained CV models can identify cartel HVTs on small OSINT samples with operationally useful precision; it did not demonstrate algorithmic prediction of recruitment likelihood, which is the next phase of the JANUS research program.

Three broader synthesis points close this paper. First, no automated component is operationally viable without human-in-the-loop verification, demographic bias auditing, and legal accountability. Second, the adversarial parity now evident between state actors and transnational criminal organizations makes a continuous MLOps lifecycle—rather than a one-shot training-and-deployment paradigm—a baseline requirement. Third, the path forward is not autonomous algorithmic surveillance; it is algorithmically augmented human intelligence, in which AI carries the cognitive load of triage while human analysts hold the moral, legal, and operational responsibility for action (Cunliffe, 2023). In a contest with adversaries whose technological sophistication grows by the month, this synthesis is the minimum cost of staying in the game.

### Acknowledgements

The authors thank the Project JANUS team at Mercyhurst University’s Intelligence Studies Department—Madelyn Black, Christian Anzalone, Antone Carthon, Madison Krafty, Ella Valimont, and Victoria Weaver—for their contributions to data collection, curation, model training, and evaluation.

## References

- Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... Zheng, X. (2016). TensorFlow: A system for large-scale machine learning. In *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI '16)* (pp. 265–283). USENIX Association.
- Ahonen, T., Hadid, A., & Pietikäinen, M. (2006). Face description with local binary patterns: Application to face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12), 2037–2041.
- Atlantic Council. (2024). Drug cartels are adopting cutting-edge drone technology: Here's how the US must adapt. <https://www.atlanticcouncil.org/blogs/new-atlanticist/drug-cartels-are-adopting-cutting-edge-drone-technology-heres-how-the-us-must-adapt/>
- Bewley, A., Ge, Z., Ott, L., Ramos, F., & Upcroft, B. (2016). Simple online and realtime tracking. In *2016 IEEE International Conference on Image Processing (ICIP)* (pp. 3464–3468). IEEE.
- Biltgen, P. (2024). AI for defense and intelligence. Tallaios.
- Bradski, G. (2000). The OpenCV library. *Dr. Dobb's Journal of Software Tools*, 25(11), 120–125.
- Bumbalek, R., Ufitikirezi, J. D. D. M., & Umurungi, S. N. (2025). Computer vision in precision livestock farming: Benchmarking YOLOv9, YOLOv10, YOLOv11, and YOLOv12. *Smart Agricultural Technology*. Advance online publication.
- Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 77–91.
- Burkett, R. (2013). Rethinking an old approach: An alternative framework for agent recruitment: From MICE to RASCLS. *Studies in Intelligence*, 57(1), 7–17.
- Calderón, G., Robles, G., Díaz-Cayeros, A., & Magaloni, B. (2015). The beheading of criminal organizations and the dynamics of violence in Mexico. *Journal of Conflict Resolution*, 59(8), 1455–1485.
- Center for Strategic and International Studies. (2024). Illicit innovation: Latin America is not prepared to fight criminal drones. <https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones>
- Centers for Disease Control and Prevention. (2025). Multiple cause of death, 1999–2023 [Data set]. CDC WONDER Online Database.
- Cialdini, R. B. (1984). *Influence: The psychology of persuasion*. Quill/William Morrow.
- Comisión Nacional de Búsqueda. (2023). Informe sobre personas desaparecidas y no localizadas en México. Secretaría de Gobernación.
- Cunliffe, K. S. (2023). Cyber-enabled tradecraft and contemporary espionage: Assessing the implications of the tradecraft paradox on agent recruitment in Russia and China. *Intelligence and National Security*, 38(7), 1075–1094.

- Deng, J., Guo, J., Ververas, E., Kotsia, I., & Zafeiriou, S. (2020). RetinaFace: Single-shot multi-level face localisation in the wild. In 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 5202–5211). IEEE.
- Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. In 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 4690–4699). IEEE.
- Department of the Navy. (2015, July 10). Frequently asked questions: OPM data breach. [https://www.secnave.navy.mil/opmbreachdon/Documents/DON\\_OPM\\_Breach\\_FAQs\\_071015pm.pdf](https://www.secnave.navy.mil/opmbreachdon/Documents/DON_OPM_Breach_FAQs_071015pm.pdf)
- Dictus, C., De Bruhl, B., & O'Shaughnessy, L. (2024). Eying AI: Intelligence collection practices in the age of artificial intelligence [Paper presentation]. 2024 APPAM Fall Research Conference, 1–60.
- Dilanian, K. (2019, April 4). How a \$230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China. NBC News. <https://www.nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691>
- Drug Enforcement Administration. (2024). National drug threat assessment 2024. U.S. Department of Justice.
- Du, Y., Zhao, Z., Song, Y., Zhao, Y., Su, F., Gong, T., & Meng, H. (2023). StrongSORT: Make DeepSORT great again. *IEEE Transactions on Multimedia*, 25, 8725–8737.
- Ekici, B. (2024). Project JANUS: HUMINT—Catching cartel members using computer vision and inducing cooperation [Unpublished manuscript and project presentation]. Mercyhurst University.
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). *Official Journal of the European Union*, L Series.
- Expertise France. (2024). Use of artificial intelligence by high-risk criminal networks. EL PAcCTO 2.0.
- Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters*, 27(8), 861–874.
- Felbab-Brown, V. (2014). Changing the game or dropping the ball? Mexico's security and anti-crime strategy under President Enrique Peña Nieto. Brookings Institution.
- Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology.
- Girshick, R. (2015). Fast R-CNN. In 2015 IEEE International Conference on Computer Vision (ICCV) (pp. 1440–1448). IEEE.
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.
- Gross, T. (2010, June 2). Laura Poitras, puzzling over a jihadi's journey. NPR. <https://www.npr.org/transcripts/127238681>

- Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic effects (NIST IR 8280). National Institute of Standards and Technology.
- Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., ... Oliphant, T. E. (2020). Array programming with NumPy. *Nature*, 585, 357–362.
- He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 770–778). IEEE.
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105.
- Hill, K. (2020, June 24). Wrongfully accused by an algorithm. *The New York Times*.
- Huang, G., Liu, Z., van der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. In 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 2261–2269). IEEE.
- Huang, G. B., Ramesh, M., Berg, T., & Learned-Miller, E. (2008). Labeled faces in the wild: A database for studying face recognition in unconstrained environments (Tech. Rep. 07-49). University of Massachusetts, Amherst.
- Hubel, D. H., & Wiesel, T. N. (1959). Receptive fields of single neurones in the cat's striate cortex. *The Journal of Physiology*, 148(3), 574–591.
- Hunter, J. D. (2007). Matplotlib: A 2D graphics environment. *Computing in Science & Engineering*, 9(3), 90–95.
- Jarrahi, M. H., Lutz, C., & Newlands, G. (2022). Artificial intelligence, human intelligence and hybrid intelligence based on mutual augmentation. *Big Data & Society*, 9(2), 1–6.
- Jocher, G., Chaurasia, A., & Qiu, J. (2023). Ultralytics YOLOv8 (Version 8.0.0) [Computer software]. <https://github.com/ultralytics/ultralytics>
- Kaplan, A. (2021). Artificial Intelligence (AI): When humans and machines might have to coexist. In P. Verdegem (Ed.), *AI for Everyone?* (pp. 21–32). University of Westminster Press.
- Khanam, R., & Hussain, M. (2024). YOLOv11: An overview of the key architectural enhancements. *arXiv preprint arXiv:2410.17725*.
- Kim, M., Jain, A. K., & Liu, X. (2022). AdaFace: Quality adaptive margin for face recognition. In 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 18750–18759). IEEE.
- Kingma, D. P., & Ba, J. (2015). Adam: A method for stochastic optimization. In 3rd International Conference on Learning Representations (ICLR).
- Krishnamurthy, K. (2024, June 25). Does AI signify the end of HUMINT as we know it? Karve International. <https://www.karveinternational.com/insights/does-ai-signify-the-end-of-humint-as-we-know-it>

- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 25, 1097–1105.
- Kutěj, L., & Horák, L. (2025). Emerging intelligence paradigms in the Russia–Ukraine war: CROWDINT, CITINT, and the Digital Battlespace. *Obrana a Strategie*, 2025(1), 193–211.
- Latin Times. (2024, March 12). Mexican cartels reportedly using AI to improve drug-trafficking operations. *Latin Times*.
- LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11), 2278–2324.
- Lisenbee II, C. S. (2024). Covert connections: The LinkedIn recruitment ruse targeting defense insiders. *Journal of Indo-Pacific Affairs*, 7(3), 164–187.
- Liu, W., Wen, Y., Yu, Z., Li, M., Raj, B., & Song, L. (2017). SphereFace: Deep hypersphere embedding for face recognition. In *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 6738–6746). IEEE.
- Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.
- Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2018). Towards deep learning models resistant to adversarial attacks. In *6th International Conference on Learning Representations (ICLR)*.
- Max, A. (2024, June 5). The IC AI multiplier. In Pereira (Ed.), *Automating superiority: Seizing adversarial artificial intelligence use in intelligence operations* (pp. 1–68).
- Maze, B., Adams, J., Duncan, J. A., Kalka, N., Miller, T., Otto, C., ... Jain, A. K. (2018). IARPA Janus Benchmark-C: Face dataset and protocol. In *2018 International Conference on Biometrics (ICB)* (pp. 158–165). IEEE.
- Montague, Z. (2019, November 22). Ex-CIA officer sentenced to 19 years in Chinese espionage conspiracy. *The New York Times*. <https://www.nytimes.com/2019/11/22/us/politics/jerry-lee-china-spying.html>
- Mosqueira-Rey, E., Hernández-Pereira, E., Alonso-Ríos, D., Bobes-Bascarán, J., & Fernández-Leal, Á. (2023). Human-in-the-loop machine learning: A state of the art. *Artificial Intelligence Review*, 56, 3005–3054.
- Munteanu, B. (2020). AI-powered HUMINT 2040. *International Conference Knowledge-Based Organization*, 26(1), 203–208.
- Office of Foreign Assets Control. (2025). Specially designated nationals and blocked persons list. U.S. Department of the Treasury.
- Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12, 2825–2830.

- Petkus, D. A. (2010). Ethics of human intelligence operations: Of MICE and men. *International Journal of Intelligence Ethics*, 1(1), 97–121.
- Phillips, B. J. (2015). How does leadership decapitation affect violence? The case of drug trafficking organizations in Mexico. *The Journal of Politics*, 77(2), 324–336.
- Porch, D., & Delgado, J. (2010). ‘Masters of today’: Military intelligence and counterinsurgency in Colombia, 1990–2009. *Small Wars & Insurgencies*, 21(2), 277–302.
- Powers, D. M. W. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation. *Journal of Machine Learning Technologies*, 2(1), 37–63.
- Prieto-Curiel, R. (2025). Why locking up cartel members does not work. arXiv preprint arXiv:2512.17973.
- Raveendhran, R., & Fast, N. J. (2021). Technology and autonomy: The psychological implications of algorithmic monitoring. *Organizational Behavior and Human Decision Processes*, 167, 1–12.
- Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 779–788). IEEE.
- Rempel, W. C. (2011). *At the devil’s table: The untold story of the insider who brought down the Cali cartel*. Random House.
- Ren, S., He, K., Girshick, R., & Sun, J. (2017). Faster R-CNN: Towards real-time object detection with region proposal networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 39(6), 1137–1149.
- Schatz, S., Folsom-Kovarik, J. T., Jones, R. M., Bartlett, K., & Wray, R. E. (2012). AI challenge problem: Scalable models for patterns of life. *AI Magazine*, 33(4), 50–60.
- Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 815–823). IEEE.
- Serwer, A. (2011, October 4). Defeating Al Qaeda with pizza, cookies, and the Koran. *Mother Jones*. <https://www.motherjones.com/politics/2011/10/ali-soufan-book-review/>
- Simonyan, K., & Zisserman, A. (2015). Very deep convolutional networks for large-scale image recognition. In 3rd International Conference on Learning Representations (ICLR).
- Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, 37(1), 167–175.
- Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15(1), 1929–1958.
- Stille, A. (1995). *Excellent cadavers: The Mafia and the death of the First Italian Republic*. Pantheon Books.

- Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., ... Rabinovich, A. (2015). Going deeper with convolutions. In 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1–9). IEEE.
- Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In 2014 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1701–1708). IEEE.
- Treverton, G. F. (2011). *Intelligence for an age of terror*. Cambridge University Press.
- Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1), 71–86.
- United Nations Office on Drugs and Crime. (2023). *World drug report 2023*. United Nations.
- Usher, C. (2025). The digital case officer: Reimagining espionage with AI. Special Competitive Studies Project. <https://scsp222.substack.com/p/the-digital-case-officer-reimagining>
- Wagner, B. (2019). Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems. *Policy & Internet*, 11(1), 104–122.
- Wang, H., Wang, Y., Zhou, Z., Ji, X., Gong, D., Zhou, J., ... Liu, W. (2018). CosFace: Large margin cosine loss for deep face recognition. In 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 5265–5274). IEEE.
- Wang, Z., Wang, G., Huang, B., Xiong, Z., Hong, Q., Wu, H., ... Liu, J. (2020). Masked face recognition dataset and application. *arXiv preprint arXiv:2003.09093*.
- Waskom, M. L. (2021). Seaborn: Statistical data visualization. *Journal of Open Source Software*, 6(60), 3021.
- Wen, Y., Zhang, K., Li, Z., & Qiao, Y. (2016). A discriminative feature learning approach for deep face recognition. In *Computer Vision—ECCV 2016* (pp. 499–515). Springer.
- Wippl, J. W. (2019). The art of agent handling. *International Journal of Intelligence and CounterIntelligence*, 32(4), 781–789.
- Wojke, N., Bewley, A., & Paulus, D. (2017). Simple online and realtime tracking with a deep association metric. In 2017 IEEE International Conference on Image Processing (ICIP) (pp. 3645–3649). IEEE.
- Xu, B., Song, X., Cai, Z., Lim, E., Tan, C.-W., & Yu, J. (2020). Artificial intelligence or augmented intelligence: A case study of human-AI collaboration in operational decision making. In *Proceedings of the Twenty-Third Pacific Asia Conference on Information Systems*, Dubai, UAE, 1–16.
- Zhou, K., Yang, Y., Cavallaro, A., & Xiang, T. (2019). Omni-scale feature learning for person re-identification. In 2019 IEEE/CVF International Conference on Computer Vision (ICCV) (pp. 3702–3712). IEEE.