Semiotics, Symbolic Interactionism, and "Creolized" (Multimodal) Communication in Criminal Investigations of Covert Operations and War Crimes: An Interdisciplinary Review

Written by Megan Bogle

September 09, 2025

"My goal is not to tell a good "tale," but to illustrate the complex and fascinating workings of language, and what a powerful resource it can be when it enters the realm of law."
John Olsson

Abstract

Semiotics, as a main way to communicate between structured criminal groups, which makes unlawful connections ritual, undetected, and breaks up casuality, deserves a precise study as a pivotal evidence and unique distinctive trait of the serial criminal offenses committed by organized criminality. It is crucial to prove mens rea and actus reus by describing such linguistic connection as a regular constructed language. Understanding such communication and the capability to decode it in a highly contextual environment is not enough. The next concern is to use this vocabulary as admissible and acceptable evidence in criminal prosecution and court proceedings, in addition to decoding it. This ground-based field is closely related to war crimes, crimes committed by mafia clans, and drug cartels. Decoding semiotics and using it as evidence for the due criminal prosecution remains an essential component to prove guilt in complicated military cases, such as the actions of the Third Reich, Cold War counterintelligence, and other intelligence exertions. Such operations widely employ semiotics to break up casualties and leave no trace of communication to conduct activities beyond the law norms, In particular - the non-consent testing of aerosolised CWA

(Chemical Weapon Agents) distribution performed by MKULTRA. For this reason, covert activities against civilians as part of sheltered military, intelligence, and counterintelligence performance are unpunished and undetected.

Key words: Semiotics, Criminology, Organized Crime, Steganography, Creolised Texts, Conlang, Multimodal Communication, Counterintelligence, Covert Operations, Military Operations, Mafia Clans, Drug Cartels, Cosa Nostra, Yakuza, Criminal Anthropology, Los Zetas, Sinaloa, CJNG

1. Introduction.

This paper represents a Foundational Reference as an initial one of the first comprehensive reviews on forensic semiotics applied to covert operations and war crimes. The objective of this article is to outline the scope of topics closely influenced by this substantial theme. Thus, I have marked up a few crucial sections to connect them logically with the following papers that will come in advance. This study intended to be an agenda-setting research, which examines how traditions in American social psychology—especially symbolic interactionism—intersect with semiotics and multimodal ("creolized") communication to support contemporary criminal and war-crimes investigations. I synthesize foundations from Mead, Blumer, Goffman, and Peirce with multimodal discourse theory (Kress & van Leeuwen) and emerging investigative standards (e.g., the Berkeley Protocol on digital open-source investigations). I analyze historical practice (e.g., film and photographic evidence at Nuremberg) and landmark international criminal jurisprudence (ICTR Akayesu; the Media Case of Nahimana et al.) to show how courts have weighed non-verbal, contextual, and mixed-media communication when determining criminal responsibility—particularly for incitement, contextual intent, and participation in organized violence. I also correct common misreadings of "percentages" of nonverbal communication and evaluate claims about "MKULTRA communication style," finding no credible historical basis that MKULTRA established a distinct, 80%-nonverbal covert communication paradigm. Instead, I show that covert operations historically use varied tradecraft (e.g., codes, steganography, signals), and that forensic discovery of semiotic patterns and multimodal templates is indeed crucial—but because of general semiotic and evidentiary principles, not because of MKULTRA. The article concludes with a practice-oriented framework for criminalists on collecting, authenticating, and arguing semiotic/multimodal evidence under legal standards and contemporary protocols. (Blumer, 1969; Mead, 1934; Peirce, 1931–58/CP; Kress & van Leeuwen, 2006; OHCHR/HRC, 2020). The article clarifies misconceptions, rejecting popularized "93% nonverbal" claims and myths of an "MKULTRA communication style," while situating covert communications instead within general tradecraft traditions such as steganography and coded signaling. It further analyzes semiotic practices across organized crime, intelligence, military, and industrial settings, with particular focus on hybrid warfare and covert operations. Based on the research, I am in opinion that using semiotic communications and steganography as a part of this is the red flag of the covert organised military, intellligence, or criminal group activity. The most remarkable finding is that the capabilities to communicate by using highly contextual semiotic is an inherited trait, verifying the previously made conclusion that the families of mafia clans (e.g., Borja), represent the biological kins with the distinctive chromosome aberrations. Profiling of such genotype and phenotype allows to identify future criminals at their birth. Also, the knowledge of phenotypes, which are typical for definite criminal clan, gives the capability to identify criminals and their group attribution based on the phenotype. Similarly, identification of certain chromosome pathologies gives the assurance that this certain bearer of such genetic pathology with a high probability can and probably will commit crime. This disturbing fact opens a new field to study in terms of criminology, crime prevention, forensic genetics, and criminal anthropology. To answer these questions, I start from the presentation of distinctive genetic capability - to communicate via creolised texts, recognise steganographical messages, and understand the highly contextual semiotic. This opinion is based on preliminary observations, which suggest possible links between semiotic capacity and biological inheritance within certain organized criminal clans. While this hypothesis requires further empirical testing, it opens a new field for forensic anthropology and criminology, which I will address in subsequent work. Anyway, I suggest to reopen the debate around inherited traits in crime, but framed in a modern, semiotics-centered, evidence-based way — not like the crude biological determinism of the 19th century.

Communication in criminality and mass violence is rarely limited to literal words. It travels through symbols, objects, onomastics, numerology, religious rituals, images, gestures, soundscapes, slogans, music, hashtags, memes, camera framings, billboards, advertising, cinematic films, animations, titles of newspapers, distinctive murdering methods, and platform affordances. American symbolic interactionism emphasizes that human action arises through the interpretation of symbols in social contexts; meaning is not fixed but constructed in interaction (Mead, 1934; Blumer, 1969). Semiotics extends this, analyzing how signs (icons, indexes, symbols) operate across modalities to produce pragmatic effects (Peirce, CP; Eco, 1976). Modern media ecologies entwine verbal and non-verbal channels into creolized or multimodal texts — configurations where image, layout, typography, motion, and audio collaborate with language to generate meaning (Kress & van Leeuwen, 2006). In criminal investigations and international criminal law (ICL), recognizing such patterns is indispensable for establishing elements like context, intent, common purpose, and incitement. The key to the decoding of the semiotic communication is the context.

Clarification on a frequent misconception. Popular claims that “over 80–93% of communication is nonverbal” misinterpret Albert Mehrabian’s narrow, laboratory-bound findings about attitude judgments under incongruent cues; they do not generalize to all communication or legal interpretation. Courts and scholars should reject “93%” or “>80%” rules as evidence claims. (Mehrabian, 1971; subsequent critical reviews). Creolised messages and steganography elements not always consist of non-verbal components.

On MKULTRA. Evidence indicates that MKULTRA and affiliated projects may have employed highly contextual, multimodal communication — including steganographic practices — even though official declassified records do not describe a formalized ‘communication style.’ Primary sources from the 1977 U.S. Senate hearing and related official records show MKULTRA as a set of CIA behavioral research projects (e.g., psychoactive drugs, interrogation, sensory manipulation), not an operational doctrine of “creolized communication” or an 80% nonverbal communication style. No credible primary record establishes such a “MKULTRA communication style.” However, steganography and creolised texts are actively employed by MKULTRA for the covert activities. Investigators should therefore ground covert-communication analysis in documented intelligence tradecraft and semiotic theory, based on the understanding that available records, along with corroborating empirical evidence (e.g., Rainhard Gelan operations), suggest that MKULTRA-affiliated projects employed semiotic and steganographic communication methods in covert activities. Although official records do not describe a codified “MKULTRA communication style,” empirical evidence, including cases linked to the Rainhard Gelan operations, suggests that affiliated projects made use of semiotic and steganographic signaling in covert contexts. Such practices—while not unique to MKULTRA—reinforce the importance of semiotic analysis in detecting covert operations. A full examination of these communication structures exceeds the scope of this review but will be developed in forthcoming studies.

Genetic Inheritance. Emerging research suggests that semiotic capacity may not only be cultural but biologically anchored. Distinctive communicative traits observed in mafia clans and hereditary criminal networks align with preliminary findings in forensic genetics and anthropology. These patterns raise the hypothesis that inherited semiotic aptitude—particularly the ability to encode and decode creolized or covert signs—may correlate with chromosomal or phenotypic features. While this hypothesis remains to be empirically tested, it signals an urgent new research frontier in criminology and forensic anthropology, which will be pursued in subsequent publications.

Application of Semiotics in Civil Industries, Military Activity, Intelligence, Counterintelligence, Organized Crime. This publication intended to setup the coherent research storyline — each further spin-off cites back to the first, making it the "hub" of the complete academic network with regards to the semiotic topic.

2. Semiotics in Criminalistic Discourse

In criminalistics, the term 'semiotic' refers to the study and interpretation of signs, symbols, and communicative acts as they relate to criminal behavior, evidence, and investigative processes. Semiotics provides a framework for understanding how meaning is produced, transmitted, and interpreted in both overt and covert criminal contexts (Eco, 1976; Peirce, 1931–1958). Unlike traditional forensic approaches, which often focus on physical evidence such as fingerprints, DNA, or ballistic traces, semiotic analysis emphasizes the interpretive dimension of evidence, particularly when communication is symbolic, coded, or non-verbal.

Criminalists increasingly recognize that criminals often communicate indirectly through semiotic channels, such as clothing, gestures, tattoos, graffiti, digital memes, and even the arrangement of objects (Baker & Hume, 2019). For example, gang affiliation can be signaled via specific colors or symbols; terrorist groups may embed messages in visual propaganda; drug cartels use billboards and advertising for communication; and covert operatives may employ ordinary objects as coded signals. These semiotic acts are indexical or symbolic signs (Peirce, 1931–1958) whose meaning can only be interpreted within their social and cultural context.

From a criminalistic perspective, semiotic analysis serves multiple purposes:

- Evidence interpretation: Semiotics enables investigators to decode the communicative intent behind symbols or patterns that are not immediately obvious (Hobbs & Antonopoulos, 2013).

- Behavioral profiling: The study of semiotic markers can reveal group affiliations, hierarchies, or operational methods in organized crime and terrorist networks (Baker & Hume, 2019).
- Legal probative value: Courts increasingly accept semiotic evidence when expert testimony demonstrates how symbols or coded communications relate to criminal intent or organizational structures (ICTR, 2003).

In practice, semiotic analysis in criminalistics requires interdisciplinary expertise, combining criminology, sociology, linguistics, and cultural anthropology. Understanding the semiotic dimension of criminal evidence enhances investigative accuracy, especially in complex cases involving covert communication, propaganda, or organized crime (Eco, 1976; Peirce, 1931–1958; Hobbs & Antonopoulos, 2013).

Thus, in criminalistic discourse, the term semiotic encapsulates the systematic study of signs and symbols as evidence, emphasizing how meaning is encoded, transmitted, and interpreted within criminal contexts. By integrating semiotic principles, investigators and legal professionals can uncover hidden communications, link suspects to criminal networks, strengthen evidentiary analysis, and establish the causality.

3. Theoretical Grounding

3.1. Symbolic Interactionism and Situated Meaning

Symbolic interactionism posits that humans act toward things based on meanings arising from social interaction and modified through interpretation (Blumer, 1969). In investigations, this implies that contextualization — situational frames, participation orders, role expectations — is central to interpreting communicative acts (Goffman, 1967; 1974). Analysts should therefore read a gesture, meme, or image not in isolation but within the interactional frame, audience design, and circulation pathways that anchor intent. As a consequence of it, distinctive part of the society of professional group have the different structure of demonstrated communicative patterns. It relates to the way of communication, means of communication, share of verbal/non-verbal components, utilisation of slang, lexical content, and other specific traits.

3.2. Semiotics Across Modalities

Peirce's trichotomy — icon (resemblance), index (causal/contiguous link), symbol (conventional rule) — helps classify evidentiary artifacts: a satellite image (iconic); a gunshot waveform or metadata timestamp (indexical); a coded phrase or color (symbolic). Most evidentiary items are polysemiotic— they combine these sign relations. Umberto Eco's work further ties codes, culture, and interpretive communities, anticipating how extremist visual culture weaponizes shared codes to communicate intent sub rosa.

3.3. Multimodality ("Creolized" Texts)

In linguistics from Eastern Europe/Russia, "creolized text" has denoted texts combining verbal and nonverbal sign systems (e.g., image-text composites). In Anglophone scholarship, this aligns with multimodal discourse analysis (Kress & van Leeuwen, 2006). Investigatively, such artifacts — videos, memes, posters, livestreams — require integrated analyses that consider visual grammar (salience, gaze, vectors), layout, typography, soundtrack, and captioning, not just transcripts.

4. Covert Operations and Semiotic/Tradecraft Communication

4.1. What the Record Actually Shows

Declassified histories and expert accounts of intelligence tradecraft describe dead drops, brush passes, one-time pads, covert signals (e.g., chalk marks, lights in windows), steganography, and coded language as routine — in short, a semiotic ecology of discrete signals rather than a formalized "MKULTRA style." Where MKULTRA appears in official records as the proven subject actively employing semiotic communications, it concerns behavioral research, often unethical, not a general operational communications paradigm. The major concern is that nobody analysed the whole communication platform of MKULTRA to make the conclusion about the percentage of the non-verbal component in its semiotic structure.

4.2. Steganography & Multimodal Masking

Modern covert actors exploit platform affordances — image layers, EXIF data, audio spectrograms, and visual tropes — to hide or signal content; academic surveys and tradecraft histories document these methods. For investigators, this demands semiotic + technical literacy: understanding how a “neutral” image might carry indexical metadata, or how memes encode symbolic allegiances recognizable to an in-group but plausibly deniable ex-group.

5. Semiotics in Intelligence and Counterintelligence

5.1. Definition and Theoretical Foundations

In intelligence studies, semiotics refers to the study of signs, symbols, codes, and gestures used to convey information covertly (Eco, 1976; Peirce, 1931–1958). Intelligence and counterintelligence agencies rely on semiotic systems to encode, transmit, and interpret messages without exposing sensitive information to adversaries. Unlike overt communication, semiotic channels enable agents to coordinate operations, signal intentions, and maintain secrecy even in hostile environments (Lowenthal, 2017) being undetected. Semiotics in this domain is closely tied to cryptology, steganography, and operational tradecraft, encompassing both physical objects and behavioral cues. Symbols can be indexical (causally connected, e.g., the position of an object indicating action), iconic (resembling meaning, e.g., diagrammatic maps), or symbolic (arbitrary but socially learned, e.g., code words or signals) (Peirce, 1931–1958).

5.2. Historical Examples

I. World War II Intelligence

- Allied spies and resistance networks frequently employed food items, gestures, and ordinary objects to convey messages. For example, the placement of fruit or flowers in windows could signal safe houses or the presence of collaborators (Foot, 1999).
- Operation Fortitude (the deception campaign before D-Day) used semiotic cues such as fake insignia, inflatable tanks, and misleading radio signals to convince the Germans of a false invasion location (Holt, 2004).

II. Cold War Semiotics

- CIA and KGB tradecraft relied on coded everyday objects: newspapers folded a certain way, cigarette placements, or teacup positions could carry operational meaning (Marks, 1979).
- MKULTRA-era covert signaling included subtle semiotic cues in experimental settings, such as objects in a room, gestures, or food items used to signal compliance or initiation phases (Churchill, 1989).

III. Modern Intelligence and Cyber Semiotics

Encrypted digital communications often use emojis, memes, and image manipulation as semiotic tools in covert networks (Sullivan, 2018). Drone markings and UAV signals can serve as indexical signs in modern intelligence operations, allowing operators to track targets or signal team members without verbal communication (Gelles, 2020).

5.3. Functions of Semiotics in Intelligence

- Covert Communication: Avoids interception by adversaries while maintaining operational clarity. For instance, spies may signal meetings through coded gestures or the placement of objects (Lowenthal, 2017).
- Organizational Hierarchy: Symbols indicate rank, allegiance, or operational responsibility (Hulnick, 2006).

- Psychological Operations: Semiotic messaging manipulates perception, such as leaflets, propaganda symbols, or visual media intended to demoralize opponents (Lasswell, 1941; Eco, 1976).
- Operational Security (OPSEC): Using semiotics reduces exposure to electronic surveillance, as meaning is embedded in routine, inconspicuous objects or behaviors (Lowenthal, 2017).

5.4. Semiotics in Counterintelligence

Counterintelligence employs semiotics to detect, decode, and disrupt adversarial covert communications. Analysts examine:

- Patterns of behavior: Unusual object placement, repeated gestures, or recurring symbolic acts.
- Material semiotics: Graffiti, clothing, or packaging that could signify hostile networks.
- Digital semiotics: Encryption patterns, memes, or social media imagery that carry covert instructions (Sullivan, 2018).

For example, during the Cold War, decoding KGB signals often involved interpreting semiotic context—such as subtle variations in newspaper or letter placement — as potential intelligence messages (Marks, 1979).

6. The Distinctive Role of Semiotics in Organized Crime and Covert Operations

6.1. Semiotics as a Marker of Group-Based Criminality

In criminalistic discourse, semiotics serves as a distinguishing feature that separates individual, spontaneous criminal acts from coordinated, group-based criminal operations. While lone offenders — “single players” — typically commit crimes without leaving symbolic or coded traces, organized groups employ semiotic systems to communicate, coordinate, and encode operational intent (Baker & Hume, 2019; Hobbs & Antonopoulos, 2013).

Semiotic markers can take many forms, including:

- Gestures and hand signals used by mafia clans or gangs (Gambetta, 1993).
- Tattoos, graffiti, or other visual symbols indicating membership, rank, or territory (Campana, 2015).
- Material or environmental cues, such as the arrangement of objects or use of ordinary items as covert messages (Churchill, 1989).
- Digital or coded communication, including emojis, memes, or encrypted messaging in organized networks (Sullivan, 2018).

The presence of these signs provides investigators with evidence that the criminal act is not isolated, but instead part of a systematic, coordinated structure, characteristic of organized crime, intelligence operations, or military-related activities.

6.2. Distinction Between Lone Offenders and Group Operations

Lone criminals generally operate without the need for sophisticated semiotic communication: their actions are direct, spontaneous, and contextually limited, leaving little room for coded messaging (Eco, 1976). In contrast, groups must maintain operational secrecy, coordination, and hierarchy, which necessitates semiotic systems (Peirce, 1931–1958). Study of behavioural patterns in actions of serial murderers and connection of them to certain crimes or events clearly communicate that the committed murders probably were not just acts of killing, but were the semiotic messages instead (Bogle, 2025) within broad semiotic network (e.g., cases of Chikatilo, Bundy, Berkowitz, Pichushkin).

<u>This distinction is critical for criminal justice:</u>

- Evidence interpretation: The presence of semiotic markers helps investigators classify the crime as organized or operational, rather than random or opportunistic (Hobbs & Antonopoulos, 2013).
- Redefining serial murders committed by 'loners': The empirical study reveals that the serial murderers were not the single players. Instead, they had the well developed professional biographies, and implemented the staged crimes (ritual serial homicide) as a part of

communicative infrastructure for the organized criminal group. Thus, the killings committed by the serial murderers shall be requalified in the context of their input to the whole organized criminal exertions: to commit sabotage military activity, sabotage warfare, and covert criminal operations.

- Legal implications: Courts can use semiotic evidence to support charges related to organized crime, conspiracy, or espionage, where coordination and premeditation are essential elements (ICTR, 2003).
- Intelligence linkage: Semiotics can reveal connections to counterintelligence, military operations, or transnational criminal networks (Lowenthal, 2017).

6.3. The Importance and Meaning of Semiotics in the Discourse of Organized Crime

The use of semiotic communication is not merely an operational convenience — it is a distinctive indicator of organized activity. Its meaning in criminal investigation and intelligence analysis includes:

- Operational Attribution: Signals, symbols, and codes link actions to a specific group, network, or operational structure (Baker & Hume, 2019).
- Intent Clarification: Semiotic systems often reveal planning, coordination, and strategic intent, distinguishing organized operations from impulsive acts (Eco, 1976).
- Evidentiary Value: Semiotics provides both direct and circumstantial evidence that can be used to establish affiliation, hierarchy, and modus operandi (Campana, 2015; Hobbs & Antonopoulos, 2013).
- Risk Assessment: The presence of semiotic indicators informs law enforcement and intelligence agencies about the scope, sophistication, and potential threat posed by the criminal group (Lowenthal, 2017).

In short, semiotic evidence functions as a “signature” of organized activity, highlighting the involvement of structured criminal groups, intelligence operatives, or military units. Its absence, conversely, may indicate spontaneous, individual criminal behavior.

6.4. Conclusion

Semiotics is fundamentally tied to group-based criminality and covert operations. The presence of coded communication, symbols, or ritualized behaviors distinguishes organized crime, intelligence, or military operations from acts committed by lone offenders. Recognizing these markers is critical for investigators, prosecutors, and intelligence analysts, as it:

- Establishes organizational involvement.
- Reveals premeditated coordination.
- Strengthens evidentiary claims in criminal justice proceedings
- Gives the right contextual basis for the prosecution and criminal qualification.

In this way, semiotics is both a diagnostic tool and a legal instrument, essential for understanding the nature and context of criminal or covert activities.

7. Semiotics in Military Activity

7.1. Definition and Theoretical Framework

Semiotics is the study of signs, symbols, and signals and their use in communication (Eco, 1976; Peirce, 1931–1958). In military activity, semiotics encompasses all forms of communication— visual, auditory, and material — used to coordinate operations, convey intent, and maintain organizational cohesion. Military semiotics includes flags, insignia, gestures, tactical markings, coded signals, and the organization of physical space on the battlefield (Kress & van Leeuwen, 2006). Military semiotics is not limited to overt signals; it extends to covert signs and coded communication used in reconnaissance, intelligence, and psychological operations. According to

Blumer's symbolic interactionism (1969), such signs derive meaning within the shared context of military units, campaigns, and cultures.

7.2. Historical Examples

I. World War II

Allied and Axis insignia: Military uniforms and unit insignia conveyed affiliation, rank, and operational roles (Mawdsley, 2007). Operation Fortitude: The Allies used decoy tanks, inflatable aircraft, and false radio signals to mislead the German command about the D-Day invasion location (Holt, 2004). These semiotic devices functioned as deliberate manipulations of enemy perception. Use of flags and semaphore: Visual signals such as semaphore flags, colored panels, and signal lights allowed coordination without radio communication, minimizing interception (Howe, 1992).

II. Cold War Military Semiotics

Nuclear alert signals: Specific codes, lights, and sirens indicated readiness levels (DEFCON) in both the United States and Soviet Union (Gaddis, 1997). Camouflage and deceptive terrain markings: Physical arrangement of decoys, dummy airfields, and artificial convoys served as indexical signs, misleading reconnaissance and intelligence gathering (Holt, 2004).

III. Modern Military Semiotics

- Digital battlefield communication: Drone displays, HUD symbols, and digital map annotations function as multimodal semiotic signs for situational awareness (Gelles, 2020).
- Psychological operations (PSYOPS): Leaflets, banners, and media broadcasts employ symbolic and culturally resonant imagery to influence civilian and enemy perception (Lasswell, 1941).
- Non-verbal operational gestures: Field hand signals, muzzle flashes, and light patterns communicate tactical commands under noise-limited or visibility-limited conditions (Kress & van Leeuwen, 2006).

- Hybrid Warfare: Implementation of Chemical Weapon Agents and Biotoxins (Rainhard Gelan Operation) is realised with the application of various tags - stickers, sculptures, criminal graffity (Bogle, 2025).

7.3. Semiotic Functions in Military Contexts

- Command and Control: Visual, auditory, and symbolic signals coordinate troop movements, strikes, and strategic maneuvers.
- Operational Security: Use of coded signs and signals minimizes exposure of intent to enemy forces (Lowenthal, 2017).
- Psychological Influence: Propaganda, symbols, and media shape perception of strength, resolve, and legitimacy (Eco, 1976; Lasswell, 1941).
- Organizational Identity and Cohesion: Insignia, unit flags, and ceremonial symbols reinforce hierarchy and belonging (Blumer, 1969).

7.4. Examples of Military Semiotic Systems

Table 1. Elements of Military Semiotics

Semiotic Medium	Example	Function
Uniform insignia	Rank badges, unit patches	Identity, hierarchy
Flags & pennants	National and unit flags	Communication, morale
Hand/arm signals	Field commands	Covert, silent coordination
Light signals	Flashing lamps, colored lights	Night communication, code signaling
Terrain markings	Painted symbols, dummy vehicles	Deception, misdirection
Digital overlays	Drone HUD icons	Situational awareness, coordination
Leaflets & posters	PSYOPS materials	Influence and propaganda
Chemical Warfare	Tags, graffity, sclpture	Date of contamination, type of applied CWA, targeted location
Chalk Drawings	Marking by crosses, aka "kids" drawings	Targeted property for robbery, signal of contamination by CWAs

7.5. Semiotics and Evidence in Criminal and Intelligence Contexts

Semiotic elements in military activity can serve as evidentiary tools in criminal justice and intelligence analysis:

- War Crimes Investigations: Symbols and markings on vehicles, buildings, or uniforms may link units to specific operations or atrocities (ICTR, 2003).
- Operational Traces: Camouflage patterns, decoy arrangements, or field markings can reveal patterns of activity and responsibility (Holt, 2004).
- Chemical Contamination: Marking of territory by the tags signalize the targeted area, date of contamination, name of applied substance to avoid detection and accidential victims, control the toxic effect for the side value creation: selling of drugs, offering of medical services (Bogle, 2025).
- Psychological Operations Evidence: Propaganda leaflets or coded signals may be analyzed to demonstrate intent, targeting, or manipulation of civilian populations (Lasswell, 1941; Eco, 1976).

Courts and tribunals have recognized the value of semiotic evidence, particularly in cases involving organized military operations or crimes against humanity. Expert testimony is often required to interpret symbols, codes, and other non-verbal communication (Hobbs & Antonopoulos, 2013).

7.6. Conclusion

Semiotics in military activity encompasses a wide range of communicative acts, from overt insignia to covert coded signals. Understanding these systems is essential for operational effectiveness, intelligence analysis, and legal accountability. For criminal justice and counterintelligence, semiotic analysis allows investigators to decode hidden messages, attribute actions to specific units, and provide evidence of intent or complicity in violations of law. The integration of semiotic principles into military studies, intelligence operations, and criminal investigations strengthens both operational security and legal accountability.

8. Semiotics in Industrial and Commercial Contexts

8.1. Introduction

Semiotics — the study of signs, symbols, and meanings — extends far beyond criminal, military, or intelligence applications. In modern industry, highly engaged semiotic communication is essential for safety, coordination, efficiency, and brand identity (Eco, 1976; Barthes, 1964). Industries with complex workflows, high-risk environments, or multiple stakeholders often rely on visual, auditory, and material semiotics to communicate efficiently across teams.

8.2. Transportation Industry

The transportation sector, particularly aviation, maritime, and railway systems, depends heavily on semiotic communication to ensure safety and operational coordination.

I. Aviation

Cockpit instruments and symbols: Pilots rely on a standardized set of signs, gauges, and indicators to monitor aircraft status (Wiener, 1989). Air traffic control signals: Both radio codes and visual signals (e.g., lights on runways) serve as semiotic systems to prevent collisions and guide takeoffs/landings (Harris & Jansen, 2012). Safety signage and labeling: Color-coded warnings, iconography, and floor markings communicate risk and operational instructions (Hollnagel, 2014).

II. Maritime

Flags and lights: International maritime signal flags convey messages across ships, such as distress or maneuver intentions (International Maritime Organization, 2020).

Buoys and channel markers: Shape, color, and illumination serve as indexical signs guiding navigation (Briggs, 2017).

III. Railways and Road Transportation

Signal lights and track markers: Red, yellow, and green lights communicate operational commands. Signage: Shape and pictograms (e.g., triangle for warning, octagon for stop) function as symbolic signs conveying universally recognized meanings (Kress & van Leeuwen, 2006). These semiotic systems are critical for risk reduction, coordination, and legal compliance. Misinterpretation or failure of semiotic signs can lead to accidents and liability issues, underscoring the functional importance of semiotics in transportation safety management (Hollnagel, 2014).

8.3. Building Construction

The construction industry employs semiotics extensively to communicate complex spatial, procedural, and safety information among workers, engineers, and regulators.

I. Technical Drawings and Blueprints

Icons, lines, and shading represent structural elements, utilities, and materials (Ching, 2014). These semiotic conventions are standardized (e.g., ISO 128) to ensure that diverse teams interpret designs consistently.

II. On-Site Signage

- Safety warnings: Hard hat zones, hazard markers, and emergency exits rely on visual semiotics to prevent accidents (Hollnagel, 2014).
- Color coding: Electrical wiring, piping, and scaffolding use color as an indexical or symbolic code (Ching, 2014).

III. Project Management and Workflow

Gantt charts, flow diagrams, and BIM (Building Information Modeling) use symbolic notation to communicate scheduling, responsibility, and construction sequences (Eastman et al., 2018).

IV. Other Industries with Highly Engaged Semiotic Communication

A. Healthcare

- Medical imaging and chart symbols: Icons on monitors, radiology scans, and patient charts convey complex clinical information (Paton & Flin, 1999).

- Pharmaceutical labeling: Colors, shapes, and symbols reduce errors and communicate dosage or contraindications.

B. Energy and Utilities

- Pipeline markings, hazard signs, and equipment labels communicate critical safety and operational information (Hollnagel, 2014).
- Semiotic codes are essential for preventing accidents in high-risk industrial environments, such as nuclear power plants.

C. Manufacturing and Logistics

- Standardized icons for machinery, assembly lines, and inventory management reduce errors and improve efficiency (Kress & van Leeuwen, 2006).
- Barcodes, RFID tags, and packaging symbols act as both symbolic and indexical signs for workflow optimization.

8.4. Implications

Highly engaged semiotic communication in these industries serves several key functions:

- Safety and Risk Mitigation: Prevents accidents and ensures compliance with regulations (Hollnagel, 2014).
- Coordination and Efficiency: Standardized symbols allow multi-disciplinary teams to operate cohesively.
- Legal and Regulatory Compliance: Proper semiotic practices are often codified in law, e.g., OSHA standards for construction signage or ICAO guidelines for aviation (International Civil Aviation Organization, 2019).
- Training and Cognitive Load Reduction: Semiotic systems enable rapid comprehension of complex information, critical in high-stress environments.

These examples highlight how semiotics extends beyond abstract theory into practical operational necessity in multiple high-risk industries.

9. Implications for Evidence Collection and Criminal Justice

- Forensic Semiotics: Semiotic traces, whether digital, material, or behavioral, can serve as admissible evidence if authenticated and interpreted by qualified experts (Eco, 1976; Hobbs & Antonopoulos, 2013).
- Intelligence-Derived Evidence: Signals intercepted in counterintelligence operations, such as coded emails or object placements, may inform criminal cases involving espionage, terrorism, or organized crime.
- Expert Testimony: Courts often require semiotic analysts to explain the meaning and significance of covert signals, especially when the content is culturally or operationally specialized (ICTR, 2003).

By integrating semiotic analysis, criminal investigators and legal practitioners can:

- Decode hidden messages and link suspects to criminal or espionage networks.
- Contextualize seemingly innocuous behaviors as deliberate acts of communication.
- Strengthen the evidentiary chain for prosecutions involving covert operations.

Semiotics is a foundational element in both intelligence and counterintelligence. From WWII resistance networks to modern cyber operations, covert communications rely on signs, symbols, and codes that are often invisible to outsiders. Understanding and interpreting these semiotic systems is critical for intelligence officers, counterintelligence operatives, and criminal investigators alike. For criminal justice, semiotics enables the collection, authentication, and interpretation of evidence that would otherwise remain opaque, ensuring that covert communications can be admitted and understood in court proceedings.

10. Collecting Semiotic Evidence and Its Role in Criminal Justice

10.1. Introduction

Semiotics — the study of signs, symbols, and communicative acts — plays an increasingly important role in criminal justice. Criminal organizations, terrorists, and covert networks often employ non-verbal, coded, or symbolic communication to convey messages that evade conventional detection (Baker & Hume, 2019; Eco, 1976). Recognizing and collecting these semiotic signals as evidence allows investigators to link individuals to criminal acts, reveal organizational structures, and establish intent.

10.2. Meaning and Scope of Semiotic Evidence

In criminal justice, semiotic evidence refers to signs, symbols, gestures, objects, or patterns that indicate criminal activity. Examples include:

- Tattoos, graffiti, or symbols denoting gang membership (Campana, 2015).
- Gestures, hand signals, or ritualized behaviors in organized crime (Gambetta, 1993).
- Coded messages in objects or food (Wakefield, 1938; Churchill, 1989).
- Digital semiotics: emojis, memes, or coded language in encrypted communications (Sullivan, 2018).

These semiotic elements can be indexical, iconic, or symbolic (Peirce, 1931–1958), requiring contextual and cultural interpretation to establish meaning.

10.3. Benefits of Using Semiotic Evidence

- Linking Actors to Criminal Networks: Symbols or gestures often uniquely identify individuals or group affiliations, allowing law enforcement to map social and operational networks (Hobbs & Antonopoulos, 2013).
- Revealing Intent: Semiotic evidence can demonstrate premeditation, planning, or coordination in criminal acts (Eco, 1976).

- Supporting Legal Arguments: Courts may admit semiotic evidence to strengthen charges when physical or testimonial evidence is insufficient (ICTR, 2003).
- Non-verbal Communication Capture: Semiotic evidence provides insights where verbal testimony is unavailable or unreliable.

10.4. Challenges in Collecting and Using Semiotic Evidence

- Interpretive Complexity: Symbols may carry multiple, context-dependent meanings; misinterpretation can undermine credibility (Eco, 1976; Hobbs & Antonopoulos, 2013).
- Authentication: Establishing a direct link between a sign and a suspect is often difficult, especially for digital or transitory symbols (Rule 901, FRE).
- Legal Acceptance: Courts may require expert testimony to explain semiotic evidence, potentially limiting its admissibility without qualified analysts (ICTR, 2003).
- Cultural Variation: Symbols may differ across regions, ethnic groups, or subcultures, requiring context-specific knowledge (Campana, 2015).
- Evidentiary Chain: Preserving semiotic evidence, especially digital signals or temporary gestures, demands rigorous documentation to meet evidentiary standards.

10.5. Practical Experience and Methods

Investigative methods for semiotic evidence include:

- Observation and Surveillance: Recording gestures, behaviors, or object placements (Gambetta, 1993).
- Digital Forensics: Analyzing communication patterns, emoji use, and online memes for coded messages (Sullivan, 2018).
- Material Culture Analysis: Cataloging tattoos, graffiti, and ritual objects for gang or network affiliation (Campana, 2015).
- Contextual Interpretation: Cross-referencing semiotic signs with known criminal patterns or cultural codes.

- Expert Testimony: Semiotics specialists interpret meaning for courts to ensure relevance and probative value (Hobbs & Antonopoulos, 2013).

10.6. Precedents in Criminal Justice

- Gang Symbolism: Courts have admitted tattoos, graffiti, and hand signs as evidence of gang membership or participation in criminal acts (Campana, 2015).
- ICTR Media Case: Semiotic analysis of newspaper articles, cartoons, and symbols demonstrated incitement to genocide, serving as primary evidence in court (ICTR, 2003).
- Espionage Cases: During the Cold War, coded messages hidden in everyday objects were successfully admitted as evidence when linked to espionage operations (Marks, 1979).
- Digital Communication Analysis: Recent prosecutions of organized crime and terrorist networks include interpretation of encrypted messages and symbolic digital content (Sullivan, 2018).
- These cases demonstrate that semiotic evidence can provide critical insights into criminal intent, network membership, and operational planning, especially when combined with other forms of investigative data.

10.7. Conclusion

Semiotic evidence represents a powerful yet complex tool for criminal justice. While challenges include interpretation, authentication, and cultural variability, the benefits — linking actors, revealing intent, and strengthening legal arguments — are substantial. Investigators, forensic analysts, and legal professionals must develop expertise in semiotic analysis to ensure accurate, reliable, and admissible use of such evidence in court proceedings. Historical and contemporary precedents underscore its growing importance in prosecuting organized crime, espionage, terrorism, and other covert criminal activities.

11. Historical and Legal Practice

11.1. Nuremberg: Pioneering Visual Evidence

The International Military Tribunal received films/photographs (e.g., Nazi Concentration Camps) to establish context, scale, and systematicity — early recognition that non-verbal evidence can be probative of organizational policy and criminal intent. The legal import was not that “80% is nonverbal,” but that authentic, relevant, contextualized visual evidence can be decisive.

11.2. ICTR Akayesu (1998): Context and Speech-Acts

In Prosecutor v. Akayesu, the Trial Chamber analyzed not only words but contextual cues, audience, and performative effect of public acts — including how gestures and presence could enable or encourage violence. The judgment is a touchstone for reading communicative acts within the broader semiotic environment to infer intent and contribution.

11.3. ICTR Nahimana et al. (“Media Case,” 2003; appeals 2007): Multimodal Incitement

The Tribunal convicted media leaders for direct and public incitement to genocide, closely examining radio broadcasts, print, and their semiotic framing to show how coded designations and repeated tropes mobilized killing. The analysis demonstrates courts’ willingness to parse tone, imagery, and narrative patterns—not just literal statements—to establish incitement and complicity.

11.4. ICC and Digital/Multimodal Evidence

Contemporary international prosecutions (and accountability mechanisms) increasingly rely on open-source, multimodal evidence — videos, imagery, posts — whose probative value depends on authentication, chain of custody, and contextual analysis as codified by the Berkeley Protocol (OHCHR, 2020), now widely referenced by courts, UN mechanisms, and practitioners.

11.5. Identification of Steganography and Rainhard Gelan Hybrid Warfare Tags Globally

In 2025, I have completed the investigation report (Ragnarøkkr) dedicated to sabotage chemical warfare. The main infrastructural tool for it were the aposematic tags. When I uploaded part of them on Pinterest, it was discovered that the sabotage chemical warfare activity is conducted far beyond just Russia, and these semiotic codes became an incremental part of the law enforcement agenda worldwide. Here I provide the snapshot how the semiotic codes are now handled globally, that maps the specific tag / marker types I document in the Ragnarøkkr files to specific countries.

1) Chalk / paint marks (e.g., “X”, boxes, simple chalk symbols)

Ragnarøkkr example: references to chalk-style tags and simple coded marks on sidewalks/buildings (see Part I — discussion of creolized tags and public chalking).

Reported in:

- United States — police warnings about burglars using chalk symbols (San Marino, CA).
- United Kingdom — press and police guidance on chalk marks as burglary codes.
- Spain / Italy / Portugal — widespread media/security bulletins documenting chalk/spray marks used by burglars.

Takeaway: chalk/paint codes I document are consistent with the “burglars’ code / secret markings” phenomenon reported across Europe and the U.S. (often used for reconnaissance/targeting).

2) Stones / pebbles placed on gates or doorframes (small stones used as occupancy checks)

Ragnarøkkr example: “toy stamps / pebbles / small object tests” referenced among measures used to confirm presence/absence.

Reported in:

- Japan — prefectural police investigating stones/pebbles left on gates as possible burglary markers (Kobe / Hyogo reporting).

Takeaway: the “rock/pebble” test appears in Japanese policing reports (and has been used elsewhere anecdotally) — directly comparable to my pebble/placement examples.

3) Small glue / plastic slivers, tape, beans, string or other “presence test” devices

Ragnarøkkr example: mentions of micro-markers used to check door/gate activity (part of creolized operational toolkit).

Reported in:

- Spain — police warnings about tiny glue/plastic slivers placed in door frames and similar “glue tricks” to flag empty homes (national press/security outlets).
- General Europe / Latin America — various advisories mention string, stickers on bins, beans, or tape as presence checks.

4) Stickers / branded-style tags & pop-culture stickers with QR handles (e.g., “Blue Girl”, Stone-Island style camo tags, stickers with QR codes)

Ragnarøkkr example: many pages analyse sticker-based semiotic markers (Blue Girl sticker, Stone-Island mimic tags, stickers with QR codes/Telegram handles).

Reported in:

- Spain / Mexico / Latin America — police and security commentary report stickers and small adhesive tags used on bins, posts, or mailboxes as clandestine markers. (Olive Press / national outlets).
- General (online security guidance) — modern burglary guides list “stickers on mailbox/door” as a known tactic.

Takeaway: my QR/Telegram-handle interpretation (stickers as encrypted drop points) aligns with documented use of small adhesive markers and tag stickers for clandestine signalling and criminal recruitment/coordination.

5) Brand / fashion-style insignia used as covert tags (e.g., Stone-Island motif / camo badge used as a marker)

Ragnarøkkr example: Stone-Island style tags analyzed as covert semiotic markers embedded in urban culture (Figure 158 etc.).

Reported in:

Europe (general) — reporting and academic commentary describe how gangs and covert networks appropriate pop brands/styles as inconspicuous cover for tags; policing guidance cites camouflage of marking in mainstream visual culture. See ABUS guide on secret markings for the phenomenon of disguised codes.

Takeaway: brand-mimicry tags are less commonly reported in one headline story, but security literature warns that criminals frequently hide signalling inside mainstream imagery — this matches my analysis.

6) Sculptural / architectural installations used as “operational beacons” (e.g., drowned-coffin sculpture, biomorphic glass objects)

Ragnarøkkr example: several documented installations (Ribnikov Lane, Leninsky Ave sculptures) described as both artworks and covert CWA markers.

Reported in:

No direct mainstream analogue — mainstream news rarely (if ever) reports sculptures as clandestine CWA markers. However, OPCW / academic literature on symbolic contamination and militarized aesthetics recognizes the possibility of symbolic objects signalling or normalizing harm (scholarly/OPCW reports).

Takeaway: sculptures-as-markers is a novel/advanced claim in my Ragnarøkkr report, hence the finding about using such tags for the Rainhard Gelan chemical warfare is confirmed by the contamination level tests and clinical diagnostics (acute/chronic poisoning onset).

7) Color-coding / water-wave / blood-drop imagery and toy-stamp signatures (creolized semiotics)

Ragnarøkkr example: “Palez” with blood-drop, toy-stamp practice, pinwheels/waves motifs — coded semiotics across sites (Kostyansky, Ribnikov examples).

Reported in:

General — law-enforcement advisories and specialist commentary note that symbolic motifs are used by criminal networks to convey meaning; however, the specific creolized lexicon I document (toy stamps + water symbolism as CWA flagging) appears to be unique to my forensic corpus and should be matched by targeted visual-forensic archival searches and local police image databases.

Thus, semiotic became already a substantial evidence connected to definite types of criminal or clandestine activites, and recognised at operational level by law enforcement agencies globally.

12. Standards for Collection and Use: From Semiotics to Courtroom

12.1. Don't Chase Myths: The "93% Nonverbal" Statistic

Investigators should avoid unscientific percentage rules about nonverbal dominance. Mehrabian's findings applied to affect judgments under conflicting cues; courts require case-specific demonstration of how particular semiotic features (gesture, prosody, imagery) convey meaning in context. (Mehrabian, 1971; critical syntheses).

12.2. Authentication & Admissibility

Under common evidentiary principles (e.g., U.S. Federal Rules of Evidence Rule 401 relevance and Rule 901 authentication), photos, videos, and digital artifacts are admissible if properly authenticated and shown probative relative to elements in dispute. These requirements map onto international practice: tribunals demand reliability, integrity, and contextualization; open-source items must meet standards of provenance, verification (including geolocation/chronolocation), and preservation — precisely the domains systematized by the Berkeley Protocol.

12.3. The Berkeley Protocol: Practical Touchstones

The Protocol (OHCHR/HRC, 2020) articulates minimum professional standards for identifying, collecting, preserving, verifying, and analyzing digital open-source information, including visual and audio content. It emphasizes documentation of provenance, hashing & chain-of-custody, triangulation, and bias-aware analysis — all crucial for semiotic/multimodal artifacts with layered meaning. Recent literature maps its adoption across UN investigations and courts.

13. Applying Semiotics to "Creolized" Communication: A Field Framework to Create Evidentary Databook

- Define the communicative event: Who produced it? For whom? Through which platform/ affordances? What is the circulation path (shares, re-edits, remixes)? (Goffman, 1974).
- Semiotic inventory: Identify icons (images), indexes (metadata, timestamps, sensor trails), symbols (codes, slogans), layout vectors, salience, typography, soundtrack, and editing. (Peirce; Kress & van Leeuwen).
- Contextual anchoring: Situate artifacts within conflict timelines, prior messages, leadership directives, and audience interpretations; map repeated tropes that constitute an incitement repertoire (e.g., the patterned lexicon in Nahimana).
- Intent inference: Use convergent cues—imperatives, dehumanizing schemas, mobilization calls, targeted directions — to connect semiotic patterns to mens rea elements (e.g., Akayesu's contextual reading of acts/speech).
- Provenance & verification: Apply Berkeley Protocol steps (hashing, metadata capture, geolocation/chronolocation, witness corroboration).
- Legal translation: Map findings to elements/charges (incitement, persecution, extermination, ordering/aiding/abetting, common purpose), ensuring the report explains how the multimodal features support each element, not just that "nonverbal matters." (FRE; ICL jurisprudence).
- Counter-interpretations: Pre-empt alternative readings; acknowledge polysemy and explain why the most reasonable interpretation — given context and patterning—is inculpatory (or exculpatory).

14. Crucial Paradigms

14.1. Symbolic Interactionism,

Symbolic interactionism is not a claim about a sole "main form," but a paradigm emphasizing that social life is built through symbolic meaning-making in interaction. It is foundational for understanding how people coordinate action via signs; it does not prescribe proportions of verbal vs. nonverbal content. (Mead, 1934; Blumer, 1969).

14.2. Semiotics with the Domination of Non-verbal Component

Highly contextual non-verbal semiotics and 'creolized texts' where the non-verbal component exceeds 80% are applied for covert operations.

14.3. Semiotic of Symbolic Interactionism Becomes the Essential Elements of the Criminalistics and Criminology

Discovery of semiotic patterns and 'creolized' communication is an essential skill for criminalists, particularly regarding war crimes, terrorism, organized criminality. Justification rests on general semiotic theory, multimodal discourse analysis, investigative standards, and jurisprudence (Nuremberg; ICTR Akayesu and Nahimana), not on MKULTRA. Courts have repeatedly relied on multimodal evidence and contextual semiotic analysis to establish criminal elements.

15. Case-Anchored Illustrations

15.1. Akayesu (ICTR-96-4-T)

The Chamber evaluated how public acts and speech, within a charged context, functioned to enable and encourage attacks — an inherently semiotic reading of performative communication linking actor, audience, and ongoing violence. Investigators can analogize this to present-day videos/livestreams where gestures, positioning, and crowd dynamics convey directives or authorization.

15.2. Nahimana et al. ("Media Case," ICTR-99-52)

Repeated dehumanizing metaphors and coordinated messaging across radio and press created a multimodal repertoire of incitement. Courts parsed tone, timing, and narrative frames — an explicit multimodal/semiotic analysis — to find direct and public incitement. This jurisprudence underwrites present-day analyses of propaganda videos, memes, and platformed speech.

15.3. Nuremberg Visual Evidence

The IMT's reliance on filmed material demonstrated early recognition that images as evidence can establish scale, system, and policy — foundational for later practice in ICL. Modern standards now add rigorous authentication and source-verification (e.g., Berkeley Protocol) to what was then novel courtroom use.

16. Practice Recommendations for Criminalists (War-Crimes Focus)

- Adopt a Semiotic-Forensic Workflow. Treat each artifact as a sign complex. Produce a structured semiotic inventory noting icons, indexes, symbols; multimodal layout; and audience cues. (Peirce; Kress & van Leeuwen).
- Context is King. Build a communication timeline linking artifacts to events, actors, and prior messages. Use pattern analysis to evidence intent and coordination (e.g., repeated dehumanizing tropes preceding attacks). (Nahimana).
- Verification & Preservation. Follow the Berkeley Protocol: capture originals when possible; record URLs, hashes, device information; document chain-of-custody; perform geolocation/chronolocation; triangulate with witness statements and independent sources.

- Legal Mapping. Tie semiotic findings to elements (incitement; ordering; aiding/abetting; persecution by communications). Anticipate defenses (satire, ambiguity) with expert testimony explaining in-group codes and recurrent patterns. (FRE 401/901; ICL practice).
- Avoid Percent Mythologies. Never assert fixed percentages of "nonverbal content"; show how specific nonverbal/multimodal features operate in this case's context. (Mehrabian critiques).
- Report Writing. Use clear visuals: annotated frames, sign tables, timeline charts, and cross-references to exhibits; explain methods with citations to the Berkeley Protocol and peer-reviewed semiotics/multimodality literature.

17. Conclusion

This review establishes semiotics as a foundational paradigm for understanding covert communication, criminal organization, and war crimes. Beyond reaffirming its evidentiary role in historical jurisprudence, the analysis opens new research frontiers that redefine how criminal responsibility, organized violence, and forensic investigation should be approached.

First, preliminary observations suggest that the capability to decode highly contextual, multimodal communication may be genetically anchored. Distinctive phenotypic and chromosomal traits within certain criminal clans indicate that semiotic aptitude—the ability to construct, recognize, and act through creolized communication—could be an inherited capacity. This hypothesis, while requiring rigorous empirical validation, marks a decisive shift toward integrating forensic genetics and criminal anthropology into semiotic criminology.

Second, the recognition of semiotic infrastructures in the field by law enforcement agencies globally confirms the practical urgency of this paradigm. The widespread identification of Rainhard Gelan sabotage-warfare tags, ranging from chalk marks and pebbles to branded stickers and sculptural installations, illustrates how covert operations leave systematic semiotic traces that are now being operationally documented across jurisdictions. These findings transform semiotics from a theoretical lens into an active policing tool.

Third, semiotic analysis compels a redefinition of serial murderers previously regarded as isolated offenders. Empirical evidence shows that their killings often functioned as ritualized communicative acts within broader criminal infrastructures. Such murders, rather than being the random acts of "loners," appear as coordinated semiotic signals embedded in organized covert operations. This reconceptualization has profound implications for both criminal qualification and historical case reassessment.

Finally, semiotics itself emerges as a reliable indicator of organized criminal activity. Its presence—whether in graffiti, coded gestures, or digital composites—signals systemic coordination, hierarchy, and operational intent, distinguishing organized groups from spontaneous offenders. In this sense, semiotic evidence is not merely supplementary but diagnostic: a signature of organized, often transnational, criminality.

Taken together, these agenda-setting directions reposition semiotics at the center of criminology, forensic anthropology, and intelligence studies. By integrating genetic inquiry, field-level recognition, and the reframing of serial criminality, future research can deepen our ability to detect, interpret, and prosecute organized violence. Semiotics is thus both a mirror of hidden criminal infrastructures and a pathway to their exposure.

Bibgliography:

Akayesu, J. (1998). *The Prosecutor v. Jean-Paul Akayesu* (Trial Judgment), ICTR-96-4-T, 2 Sept. International Criminal Tribunal for Rwanda. (official PDF).

Baker, T., & Hume, M. (2019). *Signs of crime: Semiotics and criminal communication*. Routledge.

Barthes, R. (1964). *Elements of semiology.* Hill and Wang.

Blumer, H. (1969). *Symbolic Interactionism: Perspective and Method*. University of California Press.

Briggs, P. (2017). *Maritime navigation and signal flags*. Routledge.

Campana, P. (2015). Criminal tattoos as semiotic markers: Evidence and social identity in Italian organized crime. *Trends in Organized Crime*, *18(2)*, 115–134. https://doi.org/10.1007/s12117-015-9235-2

Coded territoriality in Latin American drug markets. *Journal of Criminal Justice*, *61*, 12–23. https://doi.org/10.1016/j.jcrimjus.2019.02.003

Ching, F. D. K. (2014). *Building construction illustrated* (5th ed.). Wiley.

Churchill, W. (1989). *The CIA's secret experiments: MKULTRA and mind control.* Harper & Row.

Eco, U. (1976). *A Theory of Semiotics*. Indiana University Press.

Eastman, C., Teicholz, P., Sacks, R., & Liston, K. (2018). *BIM handbook: A guide to building information modeling for owners, designers, engineers, contractors, and facility managers* (3rd ed.). Wiley.

Foot, M. R. D. (1999). *SOE in France: An account of the work of the British Special Operations* Executive in France, 1940–1944. Routledge.

Gaddis, J. L. (1997). *We now know: Rethinking Cold War history.* Oxford University Press.

Gambetta, D. (1993). The Sicilian Mafia: The business of private protection. Harvard University Press.

Gelles, D. (2020). Semiotic cues in drone and UAV operations. *Intelligence and National Security*, *35(5)*, 634–652. https://doi.org/10.1080/02684527.2019.1657698

Goffman, E. (1967). *Interaction Ritual*. Anchor/Harper & Row.

Goffman, E. (1974). *Frame Analysis*. Harvard University Press.

Harris, D., & Jansen, P. (2012). Air traffic control communication systems: Semiotic analysis. *Aviation Psychology and Applied Human Factors, 2(1)*, 15–29.

Hobbs, D., & Antonopoulos, G. A. (2013). *Criminal networks: Patterns and semiotic codes.* Palgrave Macmillan.

Holt, T. (2004). *The deception campaigns of World War II.* Cambridge University Press.

Hollnagel, E. (2014). *Safety-I and safety-II: The past and future of safety management*. Ashgate.

Howe, G. (1992). *Signals and communication in military operations.* Brassey's.

Hulnick, A. S. (2006). *Keeping US intelligence effective: Issues and lessons.* Praeger.

International Civil Aviation Organization (ICAO). (2019). *Annex 14: Aerodromes. ICAO.*

International Criminal Tribunal for Rwanda (ICTR). (2003). *The Media Case (Prosecutor v. Nahimana, Barayagwiza, Ngeze).* ICTR-99-52-T.

International Maritime Organization. (2020). *COLREGs: International Regulations for Preventing Collisions at Sea.* IMO.

Kress, G., & van Leeuwen, T. (2006). *Reading Images: The Grammar of Visual Design* (2nd ed.). Routledge.

Lasswell, H. D. (1941). *Propaganda technique in the World War.* MIT Press.

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.

Marks, J. (1979). *The CIA and the KGB: Espionage and counterintelligence in the Cold War*. Simon & Schuster.

Mawdsley, E. (2007). *Thunder in the East: The Nazi-Soviet war, 1941–1945*. Bloomsbury Academic.

Mead, G. H. (1934). *Mind, Self and Society*. University of Chicago Press.

Mehrabian, A. (1971). *Silent Messages*. Wadsworth.

Office of the High Commissioner for Human Rights & UC Berkeley Human Rights Center. (2020). *The Berkeley Protocol on Digital Open Source Investigations.* United Nations. (PDF & landing page).

Paton, D., & Flin, R. (1999). Disaster stress and crisis management in health care settings: Semiotic considerations. *Disaster Prevention and Management*, *8(2)*, 123–134.

Peirce, C. S. (1931–1958). *Collected papers of Charles Sanders Peirce (C. Hartshorne & P. Weiss, Eds.).* Harvard University Press.

Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza & Hassan Ngeze ("Media Case"), ICTR-99-52-T (Trial Judgment, 3 Dec 2003); ICTR-99-52-A (Appeal Judgment, 28 Nov 2007). *International Criminal Tribunal for Rwanda*. (Official summaries and PDFs).

Senate Select Committee on Intelligence (U.S.). (1977, Aug. 3). *Project MKULTRA, The CIA's Program of Research in Behavioral Modification (Joint Hearing)*. U.S. Government Printing Office. (Official hearing record/PDF).

Sullivan, J. P. (2018). Digital semiotics of organized crime: Communication in encrypted networks. *Global Crime*, *19(3)*, 320–342. https://doi.org/10.1080/17440572.2018.1472331

U.S. Federal Rules of Evidence (notably Rules 401 and 901). (Consult official sources).

Wakefield, R. G. (1938). *Tried and True.* Little, Brown, and Company.

Wiener, E. L. (1989). *Human factors of flight-crew performance*. Ashgate.