CPF Mathematical Formalization Series - Paper 8: Unconscious Process Vulnerabilities: Mathematical Models for Depth Psychology in Cybersecurity

Giuseppe Canale, CISSP
Independent Researcher
g.canale@cpf3.org
ORCID: 0009-0007-3263-6897

September 24, 2025

Abstract

We present the complete mathematical formalization of Category 8 indicators from the Cybersecurity Psychology Framework (CPF): Unconscious Process Vulnerabilities. Each of the ten indicators (8.1-8.10) is rigorously defined through detection functions integrating Jungian analytical psychology, object relations theory, and computational linguistics. The formalization captures unconscious psychological mechanisms including shadow projection, transference phenomena, repetition compulsions, and archetypal activations that create systematic security blind spots. We provide explicit algorithms for detecting unconscious patterns through linguistic analysis, behavioral clustering, and symbolic interpretation. This work establishes the mathematical foundation for operationalizing depth psychological processes in cybersecurity contexts, addressing vulnerabilities that operate below conscious awareness and resist traditional security interventions.

1 Introduction and CPF Context

The Cybersecurity Psychology Framework (CPF) represents a paradigm shift from reactive security awareness to predictive vulnerability assessment through psychological state modeling [1]. Unlike traditional security frameworks that address conscious decision-making processes, CPF systematically identifies unconscious psychological vulnerabilities that create persistent security blind spots resistant to conventional interventions.

The CPF architecture comprises 100 indicators organized in a 10×10 matrix, each grounded in established psychological research. The framework employs a ternary assessment system (Green/Yellow/Red) while maintaining strict privacy protection through aggregated behavioral analysis rather than individual profiling.

This paper series provides complete mathematical formalization for each CPF category, enabling rigorous implementation and validation. Each indicator receives explicit detection functions, interdependency modeling, and algorithmic specifications. The mathematical approach serves dual purposes: ensuring reproducible implementations across organizations and establishing CPF as a scientifically rigorous methodology suitable for peer review and standardization.

Category 8 focuses on unconscious process vulnerabilities, drawing primarily from Jung's analytical psychology [2], Klein's object relations theory [3], and contemporary research on unconscious cognition [4]. These vulnerabilities exploit humans' unconscious psychological mechanisms—including shadow projection, transference, repetition compulsions, and archetypal activations—creating systematic security weaknesses that operate below conscious awareness and resist traditional security awareness training.

2 Theoretical Foundation: Unconscious Processes in Cybersecurity

Unconscious process vulnerabilities emerge from the intersection of depth psychology, computational linguistics, and behavioral pattern analysis. The unconscious mind contains not only repressed personal content but also collective patterns, archetypal structures, and automatic psychological mechanisms that profoundly influence security-relevant behavior [2].

Research demonstrates that unconscious processes account for approximately 95% of cognitive activity [4], with conscious awareness representing only the "tip of the iceberg" of psychological functioning. In cybersecurity contexts, these unconscious mechanisms create systematic vulnerabilities through several pathways: (1) shadow projection onto external threats, (2) transference of authority relationships, (3) repetition of historical trauma patterns, and (4) archetypal activation triggering predictable responses.

The mathematical models presented here capture these psychological mechanisms through three complementary approaches: (1) linguistic analysis for detecting unconscious content in communications, (2) behavioral pattern recognition for identifying repetitive cycles, and (3) symbolic analysis for archetypal activation detection.

3 Mathematical Formalization

3.1 Universal Detection Framework

Each unconscious process indicator employs the unified detection function:

$$D_i(t) = w_1 \cdot L_i(t) + w_2 \cdot B_i(t) + w_3 \cdot S_i(t) \tag{1}$$

where $D_i(t)$ represents the detection score for indicator i at time t, $L_i(t)$ denotes linguistic analysis (continuous [0,1]), $B_i(t)$ represents behavioral pattern score (continuous), and $S_i(t)$ represents symbolic analysis (normalized). Weights w_1, w_2, w_3 sum to unity and are calibrated through organizational baselines.

The temporal evolution follows exponential smoothing with unconscious-specific decay:

$$T_i(t) = \alpha \cdot D_i(t) + (1 - \alpha) \cdot T_i(t - 1) \tag{2}$$

where $\alpha = e^{-\Delta t/\tau}$ provides temporal decay with τ calibrated for unconscious process persistence (typically 72-168 hours).

3.2 Indicator 8.1: Shadow Projection onto Attackers

Definition: Unconscious projection of organizational disowned aspects onto external threat actors.

Mathematical Model:

The shadow projection index using complementary trait analysis:

$$SP_i(t) = \sum_{k=1}^{n} w_k \cdot \frac{|T^k_{internal}(t) - T^k_{external}(t)|}{T^k_{max}} \tag{3}$$

where $T^k_{internal}$ represents internal trait assessment, $T^k_{external}$ represents projected external trait, and w_k weights trait importance.

Linguistic Analysis: Shadow content detection through semantic opposition:

$$L_{8.1}(m) = \sum_i \cos(\mathbf{v}_{internal}, -\mathbf{v}_{threat}) \cdot frequency_i \tag{4}$$

where $\mathbf{v}$ represents word embeddings and negative cosine measures oppositional projection.

Behavioral Pattern Detection:

$$B_{8.1}(t) = \frac{\sum blame\_external(t)}{\sum total\_incidents(t)} \cdot complementarity\_index(t) \tag{5}$$

Detection Threshold:

$$R_{8.1}(t) = \begin{cases} 1 & \text{if } SP_i(t) > 0.7 \text{ and } blame\_ratio > 0.8 \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

3.3 Indicator 8.2: Unconscious Identification with Threats

Definition: Unconscious admiration or identification with threat actors' capabilities.

Mathematical Model:

The identification coefficient using sentiment and linguistic mimicry:

$$IC(t) = \alpha \cdot Sentiment_{admiration}(t) + \beta \cdot Mimicry_{linguistic}(t) + \gamma \cdot Fascination_{technical}(t) \tag{7}$$

where coefficients sum to unity and components measure different aspects of unconscious identification.

Mimicry Detection:

$$M_{linguistic}(t) = \frac{\sum_w freq_{org}(w) \cap freq_{threat}(w)}{\sum_w freq_{threat}(w)} \tag{8}$$

measuring linguistic convergence with threat actor vocabulary.

Technical Fascination Index:

$$TF_i(t) = \sum_j weight_j \cdot \frac{attention^j_{threat\_tech}}{attention^j_{defense\_tech}} \tag{9}$$

where j indexes different technical domains.

Detection Function:

$$D_{8.2}(t) = IC(t) \cdot \log(1 + engagement\_time(t)) \tag{10}$$

3.4 Indicator 8.3: Repetition Compulsion Patterns

Definition: Unconscious repetition of dysfunctional security patterns despite conscious intentions to change.

Mathematical Model:

The repetition compulsion index using cyclic pattern analysis:

$$RC_i(t) = \frac{1}{N} \sum_{c=1}^{N} \left(\frac{DFT_c(pattern)}{mean(DFT(noise))} \right)^2 \tag{11}$$

where DFT_c represents Discrete Fourier Transform for cycle c, identifying repetitive frequencies.

Pattern Persistence Measure:

$$PP(t) = \sum_{i=1}^{n} w_i \cdot e^{-\lambda \cdot time\_since\_i} \cdot similarity(pattern_i, current\_pattern) \tag{12}$$

Unconscious Resistance Function:

$$UR(t) = \frac{attempted\_changes(t)}{successful\_changes(t)} \cdot recurrence\_rate(t) \tag{13}$$

Detection Threshold:

$$R_{8.3}(t) = \begin{cases} 1 & \text{if } RC_i(t) > 3 \text{ and } UR(t) > 2 \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

3.5 Indicator 8.4: Transference to Authority Figures

Definition: Unconscious transfer of early authority relationships onto cybersecurity contexts.

Mathematical Model:

The transference coefficient measuring relationship projection:

$$TC_{ij}(t) = \sum_k w_k \cdot correlation(response_{ij}^k(t), archetype\_pattern_k) \tag{15}$$

where i represents individual, j represents authority figure, and k indexes archetypal patterns.

Authority Archetypal Patterns:

$$Parent\_Pattern : \{protection, control, judgment, disappointment\} \tag{16}$$

$$Teacher\_Pattern : \{guidance, evaluation, approval, criticism\} \tag{17}$$

$$Leader\_Pattern : \{vision, direction, loyalty, rebellion\} \tag{18}$$

Regression Analysis:

$$Regression\_Score(t) = \frac{adult\_responses(t) - expected\_professional(t)}{adult\_responses(t)} \tag{19}$$

Detection Function:

$$D_{8.4}(t) = TC(t) \cdot Regression\_Score(t) \cdot activation\_intensity(t) \tag{20}$$

3.6 Indicator 8.5: Countertransference Blind Spots

Definition: Security team unconscious reactions to organizational dynamics creating blind spots.

Mathematical Model:

The countertransference index using team dynamic analysis:

$$CTI(t) = \sum_{i,j} w_{ij} \cdot \frac{|reaction_i(stimulus_j) - baseline_i|}{std\_dev_i} \tag{21}$$

where i indexes team members, j indexes organizational stimuli.

Emotional Contagion Model:

$$EC_{team}(t) = \sum_k \lambda_k \cdot e^{-d_k/\sigma} \cdot affect_k(t) \tag{22}$$

where d_k represents emotional distance and σ controls contagion rate.

Blind Spot Formation:

$$BS(area, t) = 1 - \frac{detection\_rate_{area}(t)}{expected\_detection_{area}(t)} \tag{23}$$

Correlation with Team Dynamics:

$$D_{8.5}(t) = CTI(t) \cdot max(BS_{areas}(t)) \cdot team\_cohesion\_factor(t) \tag{24}$$

3.7 Indicator 8.6: Defense Mechanism Interference

Definition: Unconscious psychological defenses disrupting security processes.

Mathematical Model:

Defense mechanism detection through linguistic and behavioral analysis:

$$DM_i(t) = \sum_d w_d \cdot activation_d(t) \cdot interference_d(t) \tag{25}$$

where d indexes specific defense mechanisms.

Defense Mechanism Patterns:

$$Denial : negation\_frequency \cdot evidence\_rejection\_rate \tag{26}$$

$$Projection : attribution\_external \cdot responsibility\_deflection \tag{27}$$

$$Rationalization : explanation\_complexity \cdot justification\_frequency \tag{28}$$

$$Intellectualization : abstract\_language \cdot emotional\_distance \tag{29}$$

Interference Measurement:

$$I_d(process, t) = \frac{efficiency_{baseline} - efficiency_{during\_d}}{efficiency_{baseline}} \tag{30}$$

Aggregated Detection:

$$D_{8.6}(t) = \sum_{d,p} DM_d(t) \cdot I_d(process_p, t) \cdot criticality_p \tag{31}$$

3.8 Indicator 8.7: Symbolic Equation Confusion

Definition: Unconscious equation of symbols with reality creating security misperceptions.

Mathematical Model:

Symbolic equation index using semantic confusion analysis:

$$SE_i(symbol, t) = \frac{literal\_response\_rate(symbol, t)}{metaphorical\_recognition\_rate(symbol, t)} \tag{32}$$

Security Symbol Analysis: Common cybersecurity symbols and their literal interpretations:

$$firewall \rightarrow physical\_barrier\_assumption \tag{33}$$

$$virus \rightarrow biological\_disease\_model \tag{34}$$

$$attack \rightarrow military\_combat\_framework \tag{35}$$

$$defense \rightarrow castle\_siege\_mentality \tag{36}$$

Confusion Detection Function:

$$CF(t) = \sum_s freq(symbol_s, t) \cdot literalness\_score_s(t) \cdot impact\_weight_s \tag{37}$$

Reality Testing Impairment:

$$RTI(t) = 1 - \frac{accurate\_symbol\_interpretation(t)}{total\_symbol\_encounters(t)} \tag{38}$$

3.9 Indicator 8.8: Archetypal Activation Triggers

Definition: Unconscious archetypal patterns triggered by cybersecurity scenarios.

Mathematical Model:

Archetypal activation using Jungian pattern recognition:

$$AA_k(t) = \sum_i w_i \cdot match(trigger_i(t), archetype\_pattern_k) \tag{39}$$

where k indexes specific archetypes and i indexes trigger events.

Cybersecurity Archetypes:

$$Hero : savior\_complex \cdot individual\_responsibility \tag{40}$$
$$Shadow : external\_evil \cdot projection\_tendency \tag{41}$$
$$Wise\_Old\_Man : expert\_dependency \cdot authority\_seeking \tag{42}$$
$$Great\_Mother : protective\_instinct \cdot nurturing\_systems \tag{43}$$

Activation Strength:

$$AS_k(t) = \tanh(\beta \cdot \sum_i trigger\_intensity_i(t) \cdot archetype\_affinity_{k,i}) \tag{44}$$

Behavioral Prediction Model:

$$BP_k(action, t) = AA_k(t) \cdot P(action|archetype_k) \cdot context\_modifier(t) \tag{45}$$

3.10 Indicator 8.9: Collective Unconscious Patterns

Definition: Organization-wide unconscious patterns affecting security behavior.

Mathematical Model:

Collective pattern emergence using network analysis:

$$CP(t) = \frac{1}{N} \sum_{i=1}^{N} \sum_{j \neq i} w_{ij} \cdot sync(behavior_i(t), behavior_j(t)) \tag{46}$$

where $sync$ measures behavioral synchronization and w_{ij} represents connection strength.

Emergent Property Detection:

$$EP(property, t) = \frac{collective\_expression(property, t)}{\sum individual\_tendencies(property, t)} \tag{47}$$

where values ¿ 1 indicate emergent collective properties.

Cultural Complex Analysis:

$$CC_k(t) = \sum_i emotional\_charge_{k,i}(t) \cdot behavioral\_compulsion_{k,i}(t) \tag{48}$$

for complex k across organizational members i.

Detection Function:

$$D_{8.9}(t) = max(CP(t), EP(t), CC(t)) \cdot coherence\_index(t) \tag{49}$$

3.11 Indicator 8.10: Dream Logic in Digital Spaces

Definition: Primary process thinking in digital environments creating security vulnerabilities.

Mathematical Model:

Dream logic index using condensation and displacement analysis:

$$DL_i(t) = \alpha \cdot Condensation(t) + \beta \cdot Displacement(t) + \gamma \cdot Symbolization(t) \tag{50}$$

Primary Process Mechanisms:

$$Condensation(t) = \sum_{i,j} overlap(concept_i, concept_j, t) \tag{51}$$

$$Displacement(t) = \sum_{i} \frac{|importance_{perceived} - importance_{actual}|}{importance_{actual}} \tag{52}$$

$$Symbolization(t) = \sum_{s} \frac{symbolic\_meaning_s(t)}{literal\_meaning_s(t)} \tag{53}$$

Reality Testing Degradation:

$$RTD(t) = 1 - \frac{logical\_consistency(decisions_t)}{total\_decisions(t)} \tag{54}$$

Digital Omnipotence Index:

$$DOI(t) = \sum_{i} \frac{fantasy\_capability_i(t)}{actual\_capability_i(t)} \cdot weight_i \tag{55}$$

Detection Threshold:

$$R_{8.10}(t) = \begin{cases} 1 & \text{if } DL_i(t) > 2.5 \text{ and } RTD(t) > 0.3 \\ 0 & \text{otherwise} \end{cases} \tag{56}$$

4 Interdependency Matrix

The unconscious process indicators exhibit complex interdependencies captured through the correlation matrix $\mathbf{R}_8$:

$$\mathbf{R}_8 = \begin{pmatrix} 1.00 & 0.60 & 0.45 & 0.55 & 0.40 & 0.50 & 0.65 & 0.70 & 0.75 & 0.55 \\ 0.60 & 1.00 & 0.35 & 0.45 & 0.50 & 0.30 & 0.40 & 0.55 & 0.45 & 0.60 \\ 0.45 & 0.35 & 1.00 & 0.25 & 0.30 & 0.80 & 0.35 & 0.40 & 0.50 & 0.30 \\ 0.55 & 0.45 & 0.25 & 1.00 & 0.85 & 0.40 & 0.50 & 0.60 & 0.55 & 0.45 \\ 0.40 & 0.50 & 0.30 & 0.85 & 1.00 & 0.45 & 0.35 & 0.50 & 0.60 & 0.40 \\ 0.50 & 0.30 & 0.80 & 0.40 & 0.45 & 1.00 & 0.55 & 0.45 & 0.65 & 0.50 \\ 0.65 & 0.40 & 0.35 & 0.50 & 0.35 & 0.55 & 1.00 & 0.60 & 0.70 & 0.75 \\ 0.70 & 0.55 & 0.40 & 0.60 & 0.50 & 0.45 & 0.60 & 1.00 & 0.80 & 0.65 \\ 0.75 & 0.45 & 0.50 & 0.55 & 0.60 & 0.65 & 0.70 & 0.80 & 1.00 & 0.60 \\ 0.55 & 0.60 & 0.30 & 0.45 & 0.40 & 0.50 & 0.75 & 0.65 & 0.60 & 1.00 \end{pmatrix} \tag{57}$$

Key interdependencies include:

- Very strong correlation (0.85) between Transference (8.4) and Countertransference (8.5)
- Strong correlation (0.80) between Repetition Compulsion (8.3) and Defense Mechanisms (8.6)
- High correlation (0.80) between Archetypal Activation (8.8) and Collective Unconscious (8.9)
- Significant correlation (0.75) between Shadow Projection (8.1) and Collective Patterns (8.9)
- Notable correlation (0.75) between Symbolic Confusion (8.7) and Dream Logic (8.10)

5 Implementation Algorithms

Algorithm 1 Unconscious Process Vulnerability Assessment

```
Initialize linguistic models, archetypal patterns, baseline parameters
for each time step t do
    Collect communication data, behavioral logs, symbolic content
    for each indicator i ∈ {8.1, 8.2, ..., 8.10} do
        Perform linguistic analysis L_i(t) using NLP models
        Analyze behavioral patterns B_i(t) using clustering algorithms
        Conduct symbolic analysis S_i(t) using semantic networks
        Calculate D_i(t) = w_1 L_i(t) + w_2 B_i(t) + w_3 S_i(t)
        Update temporal state T_i(t) = α · D_i(t) + (1 − α) · T_i(t − 1)
    end for
    Compute interdependency corrections using R_8
    Identify archetypal activation patterns
    Detect collective unconscious emergence
    Generate depth psychological insights
    Update models with new pattern recognition
    Log results for validation and clinical correlation
end for
```

6 Validation Framework

Each indicator undergoes continuous validation through multiple metrics adapted for unconscious processes:

Depth Psychology Metrics:

$$Pattern\_Coherence = \frac{\sum consistent\_interpretations}{\sum total\_interpretations} \tag{58}$$

$$Unconscious\_Predictive\_Validity = \frac{TP_{future\_behavior}}{TP_{future\_behavior} + FP_{future\_behavior}} \tag{59}$$

$$Clinical\_Correlation = correlation(CPF\_scores, clinical\_assessments) \tag{60}$$

Linguistic Validation: Inter-rater reliability for unconscious content identification:

$$IRR = \frac{2 \cdot agreements}{total\_ratings} \tag{61}$$

Temporal Validation: Unconscious pattern persistence over time:

$$Persistence(pattern, \tau) = \frac{active\_duration(pattern)}{total\_observation\_period} \tag{62}$$

Cross-Cultural Validation: Archetypal universality testing:

$$Universality\_Index = \frac{\sum cultures\_expressing\_pattern}{\sum cultures\_observed} \tag{63}$$

Dream Work Correlation: For organizations conducting depth interventions:

$$Dream\_Correlation = correlation(collective\_dreams, security\_events) \tag{64}$$

7 Clinical Integration Guidelines

Given the psychological depth of these indicators, clinical integration follows established protocols:

Ethical Boundaries:

- No individual psychological profiling
- Aggregate analysis only
- Professional psychological consultation for interpretation
- Strict confidentiality protocols

Intervention Strategies:

- Group-level consciousness raising interventions
- Organizational shadow work facilitation
- Archetypal awareness training
- Symbolic literacy development

Professional Requirements:

- Jungian or depth psychology training for analysts
- Clinical supervision for unconscious process interpretation
- Ongoing education in organizational psychology
- Ethical oversight committee participation

8 Conclusion

This mathematical formalization of unconscious process vulnerabilities provides rigorous foundation for CPF Category 8 implementation. Each indicator receives explicit detection functions combining linguistic analysis, behavioral pattern recognition, and symbolic interpretation while maintaining psychological depth and clinical validity.

The interdependency matrix captures crucial correlations between unconscious mechanisms, enabling enhanced detection through multivariate analysis of depth psychological processes. Implementation algorithms provide clear guidance for system integration, while validation frameworks ensure both statistical rigor and clinical relevance.

The unconscious process category represents CPF's most psychologically sophisticated component, requiring integration of computational methods with depth psychological understanding. The mathematical rigor enables systematic detection of unconscious vulnerabilities while preserving the nuanced interpretive framework essential for meaningful psychological insight.

Future work will focus on clinical validation studies, cross-cultural archetypal pattern verification, and development of group-level interventions based on detected unconscious dynamics. The mathematical foundation enables both automated detection and human clinical interpretation, creating a hybrid approach suitable for organizational cybersecurity contexts.

By formalizing unconscious processes mathematically, we enable cybersecurity operations to address the deepest psychological layers affecting security behavior. This represents a fundamental advancement in human factors cybersecurity, moving beyond conscious awareness to engage with the unconscious foundations of organizational security culture.

References

[1] Canale, G. (2024). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences. *Preprint*.

[2] Jung, C. G. (1969). *The Archetypes and the Collective Unconscious*. Princeton University Press.

[3] Klein, M. (1946). Notes on some schizoid mechanisms. *International Journal of Psychoanalysis*, 27, 99-110.

[4] Bargh, J. A., & Chartrand, T. L. (1999). The unbearable automaticity of being. *American Psychologist*, 54(7), 462-479.

[5] Winnicott, D. W. (1971). *Playing and Reality*. Tavistock Publications.

[6] Bion, W. R. (1961). *Experiences in Groups*. Tavistock Publications.