CPF Mathematical Formalization Series - Paper 4: Affective Vulnerabilities: Emotional State Models and Security Decision Impairment

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

September 26, 2025

Abstract

We present the complete mathematical formalization of Category 4 indicators from the Cybersecurity Psychology Framework (CPF): Affective Vulnerabilities. Each of the ten indicators (4.1-4.10) is mathematically defined through emotion-cognition interaction models, affective state dynamics, and decision impairment functions. The formalization integrates Klein's object relations theory, Bowlby's attachment framework, and contemporary affective neuroscience to quantify how emotional states systematically compromise security decision-making. We provide explicit algorithms for real-time emotional state monitoring, decision quality assessment, and affective bias detection. This work establishes the mathematical foundation for understanding how emotions create predictable security vulnerabilities that persist despite technical controls and conscious awareness.

Keywords: Applied Mathematics, Interdisciplinary Psychology, Computational Statistics, Mathematical Modeling, Cybersecurity Research

1 Introduction and CPF Context

The Cybersecurity Psychology Framework (CPF) recognizes that security decisions occur within emotional contexts that fundamentally alter risk assessment and behavioral choices [1]. While Categories 1-3 examined authority, temporal, and social vulnerabilities, Category 4 addresses how affective states create systematic biases that adversaries can predict and exploit.

Traditional security models assume emotionally neutral decision-makers who evaluate risks rationally. However, neuroscience research demonstrates that emotions are not obstacles to rational thinking but integral components of all decision processes [2]. The ventromedial prefrontal cortex, critical for security-relevant decisions, receives direct input from emotional processing centers, making purely rational security assessment neurologically impossible.

Affective vulnerabilities differ from other psychological vulnerabilities in their temporal dynamics and physiological basis. Unlike cognitive biases that respond to logical intervention, emotional states involve neurochemical changes that persist independently of conscious awareness. This creates vulnerabilities that remain active even when individuals recognize their emotional state and attempt rational correction.

The mathematical models presented integrate three complementary theoretical frameworks: (1) psychoanalytic object relations theory for understanding emotional transference to systems and threats, (2) attachment theory for modeling trust relationships with security infrastructure, and (3) affective neuroscience for quantifying emotion-cognition interactions. This multi-theoretical approach ensures comprehensive coverage of affective vulnerability mechanisms.

2 Theoretical Foundation: Affective Psychology and Security

Affective vulnerabilities emerge from the fundamental architecture of human emotion-cognition interaction [3]. The limbic system processes threat information 200-300ms before conscious awareness, creating emotional responses that influence subsequent rational analysis. This temporal precedence makes emotional vulnerabilities particularly dangerous in security contexts where rapid decisions are required.

Klein's object relations theory [4] provides crucial insights into how individuals develop emotional relationships with abstract security concepts. Security systems, policies, and threats become internalized objects that evoke complex emotional responses including idealization, persecution anxiety, and reparative fantasies. These unconscious emotional relationships create predictable patterns of security behavior that persist across conscious policy changes.

Bowlby's attachment theory [5] explains how early relational patterns influence trust in security infrastructure. Secure attachment promotes balanced risk assessment, while insecure attachment styles create systematic distortions: anxious attachment leads to over-reliance on security systems, avoidant attachment promotes security independence at the cost of collaboration, and disorganized attachment creates inconsistent security behaviors.

Contemporary affective neuroscience reveals that emotions serve as somatic markers that guide decision-making through rapid pattern recognition [2]. In security contexts, these emotional shortcuts often reflect outdated threat models or inappropriate generalizations from personal experience to organizational risk.

The mathematical formalization captures these mechanisms through emotional state dynamics, attachment-mediated trust functions, and decision impairment models that account for both conscious and unconscious emotional influences on security behavior.

3 Mathematical Formalization

3.1 Universal Affective Detection Framework

Each affective vulnerability indicator employs the unified detection function with emotional state weighting:

$$D_i(t) = w_1 \cdot R_i(t) + w_2 \cdot A_i(t) + w_3 \cdot E_i(t) + w_4 \cdot T_i(t) \tag{1}$$

where $D_i(t)$ represents detection score, $R_i(t)$ denotes rule-based detection, $A_i(t)$ represents anomaly score, $E_i(t)$ represents emotional state factor, and $T_i(t)$ represents temporal emotional dynamics.

The emotional state evolution incorporates both immediate responses and emotional momentum:

$$E_i(t) = \alpha \cdot Emotion_i(t) + \beta \cdot E_i(t-1) + \gamma \cdot \sum_j Emotional\_Contagion_{j,i}(t) \tag{2}$$

where γ captures emotional contagion effects from other individuals in the network.

3.2 Indicator 4.1: Fear-Based Decision Paralysis

Definition: Security decision impairment through overwhelming fear response leading to inaction or delayed action.

Mathematical Model:

Fear intensity function incorporating threat perception and vulnerability assessment:

$$F_i(t) = P_{threat}(t) \cdot V_{vulnerability}(t) \cdot \frac{1}{C_{control}(t) + \epsilon} \tag{3}$$

where P_{threat} represents perceived threat probability, $V_{vulnerability}$ measures perceived personal vulnerability, and $C_{control}$ represents perceived control over outcomes.

Decision Paralysis Model:

$$DP(F,T,O) = \frac{F^\alpha}{F^\alpha + \beta^\alpha} \cdot \left(1 - \frac{1}{1 + e^{-\gamma(T-T_0)}}\right) \cdot \frac{1}{1+O} \tag{4}$$

where F is fear intensity, T is time pressure, T_0 is paralysis threshold, and O is number of options.

Action Delay Function:

$$AD(t) = \tau_0 \cdot e^{\delta \cdot F(t)} \cdot (1 + \zeta \cdot Uncertainty(t)) \tag{5}$$

where τ_0 is baseline decision time and δ, ζ are scaling parameters.

Detection Function:

$$D_{4.1}(t) = \begin{cases} 1 & \text{if } DP > 0.7 \text{ and } AD > 2 \cdot AD_{baseline} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

3.3 Indicator 4.2: Anger-Induced Risk Taking

Definition: Increased risk tolerance and impulsive security decisions driven by anger or frustration.

Mathematical Model:

Anger-modulated risk assessment:

$$R_{perceived}(A) = R_{objective} \cdot (1 - \alpha \cdot A) + \beta \cdot A \cdot R_{reward\_focus} \tag{7}$$

where A represents anger intensity, α controls risk minimization, and β controls reward amplification.

Impulsivity Enhancement Model:

$$I(A,T) = I_0 \cdot (1 + \gamma \cdot A) \cdot e^{-\delta \cdot T} \tag{8}$$

where I_0 is baseline impulsivity, T is reflection time, and γ, δ are scaling factors.

Regulatory Depletion Function:

$$RD(t) = RD_0 \cdot e^{-\lambda \cdot \int_0^t Anger(\tau) d\tau} \tag{9}$$

representing decreasing self-regulatory capacity under sustained anger.

Risk Taking Probability:

$$P_{risk}(A, RD) = \frac{A^\mu \cdot (1 - RD)^\nu}{1 + A^\mu \cdot (1 - RD)^\nu} \tag{10}$$

Detection Algorithm:

$$D_{4.2}(t) = \begin{cases} 1 & \text{if } P_{risk} > 0.6 \text{ and } I > I_{threshold} \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

3.4 Indicator 4.3: Trust Transference to Systems

Definition: Inappropriate emotional trust relationships with security systems based on human relationship patterns.

Mathematical Model:

Attachment-based trust function:

$$T_{system}(A,R,S) = w_1 \cdot A_{security} + w_2 \cdot R_{reliability} + w_3 \cdot S_{similarity} + w_4 \cdot A \cdot S \tag{12}$$

where $A_{security}$ is attachment security, $R_{reliability}$ is system reliability, $S_{similarity}$ is human-likeness, and w_4 captures interaction effects.

Trust Calibration Error:

$$TCE = |T_{system} - T_{appropriate}| \tag{13}$$

Anthropomorphization Index:

$$AI = \sum_{attributes} w_{attr} \cdot \frac{Human\_Attribution_{attr}}{System\_Capability_{attr} + \epsilon} \tag{14}$$

Transference Detection Model:

$$TD(H, S) = \frac{\sum_{patterns} Similarity(H_{pattern}, S_{interaction})}{\sum_{patterns} 1} \tag{15}$$

where patterns include dependency, idealization, and control dynamics.

Detection Framework:

$$R_{4.3}(t) = \begin{cases} 1 & \text{if } TCE > 0.5 \text{ and } AI > 0.7 \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

3.5 Indicator 4.4: Attachment to Legacy Systems

Definition: Emotional resistance to security updates based on attachment relationships with familiar systems.

Mathematical Model:

Legacy attachment strength:

$$LA(F, T, S) = \alpha \cdot F_{familiarity}^{\beta} + \gamma \cdot T_{time\_invested} + \delta \cdot S_{success\_history} \tag{17}$$

where familiarity, time investment, and success history create emotional bonds.

Change Resistance Function:

$$CR(LA, U) = \frac{LA^{\eta}}{LA^{\eta} + (U \cdot Necessity)^{\eta}} \tag{18}$$

where U represents understanding of change benefits and η controls resistance curve steepness.

Loss Aversion in System Change:

$$LAV = \lambda \cdot (Functionality_{lost} + Familiarity_{lost}) - Improvements_{gained} \tag{19}$$

with loss aversion coefficient $\lambda > 1$.

Modernization Delay Model:

$$MD(t) = \int_0^t CR(\tau) \cdot Security\_Gap\_Increase(\tau) d\tau \tag{20}$$

Detection Function:

$$D_{4.4}(t) = \begin{cases} 1 & \text{if } CR > 0.8 \text{ and } MD > MD_{critical} \\ 0 & \text{otherwise} \end{cases} \tag{21}$$

3.6 Indicator 4.5: Shame-Based Security Hiding

Definition: Concealment of security incidents or vulnerabilities due to shame, leading to delayed response and increased damage.

Mathematical Model:

Shame intensity function:

$$S_i(E, R, V) = \alpha \cdot E_{exposure} \cdot R_{responsibility} + \beta \cdot V_{vulnerability\_feeling} + \gamma \cdot C_{competence\_threat} \tag{22}$$

where exposure, responsibility, and competence threat contribute to shame intensity.

Disclosure Inhibition Model:

$$DI(S, T) = \frac{S^{\delta}}{S^{\delta} + (Support_{available} \cdot T_{trust})^{\delta}} \tag{23}$$

where available support and interpersonal trust moderate shame effects.

Incident Concealment Probability:

$$P_{conceal}(S, C, T) = \sigma\left(\epsilon \cdot S - \zeta \cdot C_{consequences\_known} - \eta \cdot T_{time\_pressure}\right) \tag{24}$$

Damage Amplification Factor:

$$DAF(t) = 1 + \theta \cdot \int_0^t P_{conceal}(\tau) \cdot Threat\_Active(\tau) d\tau \tag{25}$$

Detection Algorithm:

$$D_{4.5}(t) = \begin{cases} 1 & \text{if } DI > 0.6 \text{ and } DAF > 1.5 \\ 0 & \text{otherwise} \end{cases} \tag{26}$$

3.7 Indicator 4.6: Guilt-Driven Overcompliance

Definition: Excessive security behaviors driven by guilt, leading to inefficient resource allocation and potential security theater.

Mathematical Model:

Guilt-mediated compliance function:

$$GC(G, P) = Baseline_{compliance} + \alpha \cdot G^{\beta} \cdot P_{past\_failures} \tag{27}$$

where guilt intensity and past failure experiences drive overcompliance.

Resource Misallocation Index:

$$RMI = \frac{\sum_{measures} Effort_{measure} \cdot (1 - Effectiveness_{measure})}{\sum_{measures} Effort_{measure}} \tag{28}$$

Security Theater Detection:

$$ST = \frac{Visible\_Security\_Measures}{Effective\_Security\_Measures} \tag{29}$$

Guilt Perpetuation Model:

$$\frac{dG}{dt} = -\kappa \cdot G + \lambda \cdot Trigger_{events} + \mu \cdot Overcompliance\_Failure \tag{30}$$

Detection Framework:

$$R_{4.6}(t) = \begin{cases} 1 & \text{if } RMI > 0.4 \text{ and } ST > 1.8 \\ 0 & \text{otherwise} \end{cases} \tag{31}$$

3.8 Indicator 4.7: Anxiety-Triggered Mistakes

Definition: Increased error rates in security procedures due to anxiety-induced cognitive impairment.

Mathematical Model:

Anxiety-performance relationship (inverted-U curve):

$$Performance(A) = P_{max} \cdot e^{-\frac{(A-A_{optimal})^2}{2\sigma^2}} \tag{32}$$

where $A_{optimal}$ represents optimal anxiety level and σ controls curve width.

Error Rate Enhancement:

$$ER(A) = ER_{baseline} \cdot (1 + \alpha \cdot max(0, A - A_{threshold})) \tag{33}$$

Attention Narrowing Effect:

$$AN(A) = Attention_{baseline} \cdot e^{-\beta \cdot A} \tag{34}$$

Working Memory Impairment:

$$WMI(A) = WM_{capacity} \cdot \frac{1}{1 + \gamma \cdot A} \tag{35}$$

Mistake Probability Function:

$$P_{mistake}(A, C) = \frac{ER(A) \cdot (1 - AN(A)) \cdot (1 - WMI(A))}{C_{complexity} + \epsilon} \tag{36}$$

Detection Algorithm:

$$D_{4.7}(t) = \begin{cases} 1 & \text{if } P_{mistake} > 0.3 \text{ and } A > A_{threshold} \\ 0 & \text{otherwise} \end{cases} \tag{37}$$

3.9 Indicator 4.8: Depression-Related Negligence

Definition: Reduced security vigilance and maintenance behaviors due to depression-induced apathy and cognitive impairment.

Mathematical Model:

Depression impact on security motivation:

$$SM(D) = SM_{baseline} \cdot e^{-\alpha \cdot D} \cdot (1 - \beta \cdot Anhedonia) \tag{38}$$

where D represents depression severity and anhedonia measures reduced reward sensitivity.

Maintenance Behavior Decline:

$$MB(D, T) = MB_0 \cdot e^{-\gamma \cdot D \cdot T} \cdot \frac{1}{1 + \delta \cdot Fatigue} \tag{39}$$

Vigilance Degradation Model:

$$VD(t) = \int_0^t Depression(\tau) \cdot Cognitive\_Load(\tau) \cdot e^{-\lambda(t-\tau)} d\tau \tag{40}$$

Risk Perception Blunting:

$$RPB(D) = \frac{Risk_{perception}}{1 + \epsilon \cdot D \cdot Emotional\_Numbing} \tag{41}$$

Detection Function:

$$D_{4.8}(t) = \begin{cases} 1 & \text{if } MB < 0.5 \cdot MB_0 \text{ and } RPB < 0.7 \\ 0 & \text{otherwise} \end{cases} \tag{42}$$

3.10 Indicator 4.9: Euphoria-Induced Carelessness

Definition: Reduced risk perception and security conscientiousness during positive emotional states.

Mathematical Model:

Euphoria-modulated risk perception:

$$RP(E) = RP_{baseline} \cdot \frac{1}{1 + \alpha \cdot E^{\beta}} + \gamma \cdot Optimism\_Bias \tag{43}$$

where E represents euphoria intensity and optimism bias reduces threat salience.

Approach Motivation Enhancement:

$$AM(E) = AM_{baseline} + \delta \cdot E \cdot (1 - Inhibitory\_Control) \tag{44}$$

Security Procedure Shortcuts:

$$SPS(E, T) = \frac{E^{\epsilon}}{E^{\epsilon} + T^{\epsilon}_{time\_pressure}} \cdot Convenience_{factor} \tag{45}$$

Overconfidence Function:

$$OC(E, S) = Confidence_{baseline} + \zeta \cdot E - \eta \cdot S_{skill\_level} \tag{46}$$

Detection Algorithm:

$$D_{4.9}(t) = \begin{cases} 1 & \text{if } SPS > 0.5 \text{ and } OC > OC_{threshold} \\ 0 & \text{otherwise} \end{cases} \tag{47}$$

3.11 Indicator 4.10: Emotional Contagion Effects

Definition: Spread of emotional states through organizational networks, amplifying individual emotional vulnerabilities.

Mathematical Model:

Emotional contagion propagation:

$$\frac{dE_i}{dt} = -\alpha_i \cdot E_i + \sum_{j \in N(i)} \beta_{ij} \cdot f(E_j - E_i) + \xi_i(t) \tag{48}$$

where $f(x) = tanh(\gamma \cdot x)$ represents contagion function and $\xi_i(t)$ is individual emotional noise.

Network Emotional State:

$$NES(t) = \sum_i w_i \cdot E_i(t) \tag{49}$$

with weights w_i based on network centrality and influence.

Contagion Amplification Factor:

$$CAF = \frac{Variance(E_{group}) - Variance(E_{individual})}{Variance(E_{individual})} \tag{50}$$

Emotional Cascade Probability:

$$ECP(t) = \Phi\left(\frac{NES(t) - \mu_{threshold}}{\sigma_{noise}}\right) \tag{51}$$

where Φ is the cumulative normal distribution.

Detection Framework:

$$D_{4.10}(t) = \begin{cases} 1 & \text{if } CAF > 2.0 \text{ and } ECP > 0.8 \\ 0 & \text{otherwise} \end{cases} \tag{52}$$

4 Interdependency Matrix

The affective vulnerability indicators exhibit complex interdependencies captured through correlation matrix $\mathbf{R}_4$:

$$\mathbf{R}_4 = \begin{pmatrix} 1.00 & -0.45 & 0.35 & 0.30 & 0.60 & 0.25 & 0.75 & 0.40 & -0.55 & 0.50 \\ -0.45 & 1.00 & -0.20 & -0.25 & -0.40 & -0.30 & -0.35 & -0.50 & 0.40 & 0.30 \\ 0.35 & -0.20 & 1.00 & 0.70 & 0.45 & 0.40 & 0.30 & 0.25 & -0.30 & 0.35 \\ 0.30 & -0.25 & 0.70 & 1.00 & 0.55 & 0.35 & 0.25 & 0.45 & -0.35 & 0.40 \\ 0.60 & -0.40 & 0.45 & 0.55 & 1.00 & 0.50 & 0.65 & 0.35 & -0.45 & 0.55 \\ 0.25 & -0.30 & 0.40 & 0.35 & 0.50 & 1.00 & 0.30 & 0.25 & -0.25 & 0.35 \\ 0.75 & -0.35 & 0.30 & 0.25 & 0.65 & 0.30 & 1.00 & 0.45 & -0.40 & 0.60 \\ 0.40 & -0.50 & 0.25 & 0.45 & 0.35 & 0.25 & 0.45 & 1.00 & -0.65 & 0.30 \\ -0.55 & 0.40 & -0.30 & -0.35 & -0.45 & -0.25 & -0.40 & -0.65 & 1.00 & -0.35 \\ 0.50 & 0.30 & 0.35 & 0.40 & 0.55 & 0.35 & 0.60 & 0.30 & -0.35 & 1.00 \end{pmatrix} \tag{53}$$

Key interdependencies include:

- Strong correlation (0.75) between Fear Paralysis (4.1) and Anxiety Mistakes (4.7)
- High correlation (0.70) between Trust Transference (4.3) and Legacy Attachment (4.4)
- Strong negative correlation (-0.65) between Depression Negligence (4.8) and Euphoria Carelessness (4.9)
- Significant correlation (0.65) between Shame Hiding (4.5) and Anxiety Mistakes (4.7)

Cross-Category Dependencies: Critical relationships with Authority (Category 1), Temporal (Category 2), and Social (Category 3) vulnerabilities:

- $R_{1.5,4.1} = 0.80$: Fear-based compliance strongly correlates with fear paralysis
- $R_{2.3,4.9} = 0.70$: Deadline pressure correlates with euphoria-induced carelessness
- $R_{3.9,4.5} = 0.75$: Social identity threats strongly correlate with shame-based hiding
- $R_{1.1,4.3} = 0.65$: Authority compliance correlates with system trust transference

5 Implementation Algorithms

6 Validation Framework

Affective vulnerability validation requires specialized metrics accounting for emotional dynamics and individual differences:

Emotion-State Classification Metrics:

$$Precision_{emotional} = \frac{\sum_{states} |TP_{state}| \cdot w_{state}}{\sum_{states} |TP_{state} + FP_{state}| \cdot w_{state}} \tag{54}$$

$$Recall_{emotional} = \frac{\sum_{states} |TP_{state}| \cdot w_{state}}{\sum_{states} |TP_{state} + FN_{state}| \cdot w_{state}} \tag{55}$$

where w_{state} provides importance weighting for different emotional states.

Algorithm 1 Affective Vulnerability Assessment

```
Initialize emotional parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$
Load baseline emotional profiles and attachment patterns
for each time step $t$ do
    Extract emotional context: physiological_markers(t), behavioral_patterns(t)
    Calculate emotional state dynamics for each individual
    for each indicator $i \in \{4.1, 4.2, \ldots, 4.10\}$ do
        Compute emotional intensity metrics $E_i(t)$
        Calculate rule-based detection $R_i(t)$
        Compute emotion-weighted anomaly score $A_i(t)$
        Evaluate temporal emotional dynamics $T_i(t)$
        Calculate detection score $D_i(t)$
        Apply emotional contagion propagation model
        Update attachment relationship states
    end for
    Compute interdependency corrections using $\mathbf{R}_4$
    Apply cross-category correlations with Categories 1-3
    Generate emotion-aware alerts with contagion predictions
    Update emotional baseline models
    Log results for affective pattern refinement
end for
```

Algorithm 2 Emotional Contagion Network Analysis

```
Input: Communication network $G(V, E)$, emotional states $\mathbf{E}(t)$
Initialize contagion parameters $\beta_{ij}$, decay rates $\alpha_i$
for each time step $t$ do
    for each individual $i \in V$ do
        Calculate emotional influence from neighbors
        Compute individual emotional susceptibility
        Apply contagion differential equation
        Update emotional state $E_i(t+1)$
    end for
    Calculate network emotional moments (mean, variance)
    Detect emotional cascade initiation
    Identify emotional superspreaders
    Predict contagion trajectory
    Generate early warning for emotional crises
    Update network contagion parameters
end for
Return emotional vulnerability map with propagation predictions
```

Temporal Emotional Dynamics Validation: Mean Absolute Error for emotional state prediction:

$$MAE_{emotion} = \frac{1}{T}\sum_{t=1}^{T} |Emotion_{predicted}(t) - Emotion_{actual}(t)| \tag{56}$$

Contagion Propagation Accuracy: Network-level emotional spread prediction:

$$CPA = 1 - \frac{|Predicted\_Affected \triangle Actual\_Affected|}{|Actual\_Affected|} \tag{57}$$

Decision Impairment Correlation: Pearson correlation between emotional state and decision quality:

$$r_{emotion,decision} = \frac{\sum_i (E_i - \bar{E})(D_i - \bar{D})}{\sqrt{\sum_i (E_i - \bar{E})^2 \sum_i (D_i - \bar{D})^2}} \tag{58}$$

Attachment Pattern Validation: Classification accuracy for attachment-based trust behaviors:

$$APA = \frac{Correct_{attachment\_classifications}}{Total_{attachment\_assessments}} \tag{59}$$

Emotional Cascade Early Warning: Prediction accuracy for emotional contagion events:

$$ECEW = \frac{TP_{cascade\_predictions}}{TP_{cascade\_predictions} + FN_{cascade\_predictions}} \tag{60}$$

Target validation metrics: Precision ¿ 0.85, Recall ¿ 0.80, MAE ¡ 0.15, CPA ¿ 0.75, ECEW ¿ 0.70.

7 Conclusion

This mathematical formalization of affective vulnerabilities provides a comprehensive framework for understanding how emotional states systematically compromise security decision-making. The integration of psychoanalytic object relations theory, attachment theory, and affective neuroscience creates a robust foundation for predicting and mitigating emotion-based security weaknesses.

The interdependency matrix reveals critical patterns: negative emotions (fear, anxiety, shame, depression) cluster together and amplify each other, while positive emotions (euphoria) create distinct vulnerability patterns. The strong correlations between affective vulnerabilities and other CPF categories demonstrate that emotions act as both direct vulnerability sources and amplifiers for authority, temporal, and social influence effects.

The mathematical models capture the nonlinear dynamics of emotion-cognition interaction, including emotional momentum, contagion effects, and attachment-mediated trust relationships. This enables prediction of emotional vulnerability states before they manifest in observable security incidents, supporting proactive rather than reactive security strategies.

The implementation algorithms provide real-time emotional state monitoring with network-aware contagion modeling. Organizations can anticipate emotional vulnerability cascades based on communication patterns, stress indicators, and attachment relationship dynamics, enabling targeted interventions before widespread security degradation occurs.

Validation frameworks account for the unique challenges of measuring emotional states and their security implications, including individual differences, temporal dynamics, and network propagation effects. The proposed metrics ensure both statistical rigor and practical applicability for organizational security contexts.

Future work will extend this affective modeling approach to cognitive overload (Category 5) and group dynamics (Category 6), with particular attention to emotion-cognition interaction effects and collective emotional states. The mathematical foundation established here enables evidence-based emotional security strategies that work with human psychological realities rather than against them.

The affective vulnerability category demonstrates that security is fundamentally an emotional as well as cognitive phenomenon. Emotions are not obstacles to rational security behavior but integral components that must be understood and accounted for in security system design. By formalizing these emotional dynamics mathematically, we enable security approaches that harness rather than fight human emotional responses, creating more resilient and sustainable security outcomes.

References

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

[2] Damasio, A. R. (1994). *Descartes' Error: Emotion, Reason, and the Human Brain*. New York: Putnam.

[3] LeDoux, J. (2000). Emotion circuits in the brain. *Annual Review of Neuroscience*, 23, 155-184.

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

[5] Bowlby, J. (1969). *Attachment and Loss: Vol. 1. Attachment*. New York: Basic Books.