CPF Mathematical Formalization Series - Paper 6: Group Dynamic Vulnerabilities: Mathematical Models and Detection Algorithms

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 6 indicators from the Cybersecurity Psychology Framework (CPF): Group Dynamic Vulnerabilities. Each of the ten indicators (6.1-6.10) is rigorously defined through detection functions combining network analysis, information-theoretic measures, and Bayesian inference models. The formalization captures the collective psychological states that emerge in organizational settings, grounded in Bion's basic assumptions theory and contemporary group dynamics research. We provide explicit algorithms for real-time detection of collective security blind spots, interdependency matrices for correlation analysis, and validation metrics for continuous calibration. This work establishes the mathematical foundation for operationalizing group-level psychological vulnerabilities that create systematic security weaknesses through emergent collective behaviors.

1 Introduction and CPF Context

The Cybersecurity Psychology Framework (CPF) addresses the critical gap between individual psychological vulnerabilities and the emergent properties of collective behavior in organizational security contexts [1]. While previous categories have focused on individual-level vulnerabilities, Category 6 captures the unique phenomena that arise when individuals aggregate into groups, creating vulnerabilities that exceed the sum of individual weaknesses.

Group dynamic vulnerabilities represent a distinct class of security threats that emerge from collective psychological processes. These vulnerabilities cannot be addressed through individual-focused interventions as they arise from the interaction patterns between group members rather than from any single individual's psychology. The mathematical models presented here formalize these emergent collective states, enabling systematic detection and mitigation of group-level security blind spots.

This paper continues the CPF Mathematical Formalization Series, providing rigorous mathematical definitions for all ten Group Dynamic Vulnerability indicators (6.1-6.10). Each indicator receives explicit detection functions, interdependency modeling with previously formalized categories, and algorithmic specifications enabling immediate implementation in Security Operations Centers (SOCs).

Category 6 draws primarily from Bion's groundbreaking work on group dynamics [2], Janis's groupthink research [3], and contemporary social network analysis methodologies. These theoretical foundations provide the psychological grounding for mathematical models that capture how collective unconscious assumptions create systematic security vulnerabilities in organizational contexts.

2 Theoretical Foundation: Group Dynamic Processes

Group dynamic vulnerabilities emerge from the complex interplay between individual psychology and collective behavior patterns. Research demonstrates that groups develop emergent properties that cannot be predicted from individual member characteristics [4]. These emergent properties often include shared defense mechanisms, collective blind spots, and synchronized risk-taking behaviors that create systematic security vulnerabilities.

Bion's [2] basic assumption theory identifies three primary modes of group functioning that directly impact security posture: dependency (seeking omnipotent protection), fight-flight (perceiving threats as external), and pairing (hoping for future salvation through new solutions). Each mode creates specific vulnerability patterns that attackers can exploit through targeted social engineering campaigns.

Modern network analysis reveals that information flow patterns in organizational groups create natural points of vulnerability [5]. Centralized communication structures create single points of failure, while highly connected networks enable rapid spread of both threats and defense mechanisms. The mathematical models presented here capture these structural vulnerabilities through graph-theoretic measures combined with psychological state detection.

The temporal dynamics of group formation and dissolution also create vulnerability windows. Tuckman's [6] forming-storming-norming-performing model identifies specific phases where security awareness varies predictably. Mathematical models can capture these phase transitions and predict periods of heightened vulnerability.

3 Mathematical Formalization

3.1 Universal Detection Framework

Each group dynamic indicator employs the unified detection function extended for collective analysis:

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

where $D_i(t)$ represents the detection score for indicator i at time t, $R_i(t)$ denotes rule-based detection, $A_i(t)$ represents anomaly score, $B_i(t)$ represents Bayesian posterior probability, and $N_i(t)$ represents network-based measures unique to group dynamics.

The collective temporal evolution incorporates group consensus dynamics:

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

where $C_i(t)$ represents the consensus influence factor calculated through opinion dynamics models.

3.2 Indicator 6.1: Groupthink Security Blind Spots

Definition: Collective suppression of dissenting security opinions leading to systematic blind spots.

Mathematical Model:

The diversity index for security decision-making:

$$DI_{security}(t) = 1 - \sum_{i=1}^{n} p_i^2 \tag{3}$$

where p_i represents the fraction of group members choosing security option i.

Consensus Speed Metric:

$$CS(t) = \frac{d}{dt}\left(\max_i p_i(t)\right) \tag{4}$$

Dissent Suppression Detection: The entropy of security opinions:

$$H_{opinions}(t) = -\sum_{i=1}^{n} p_i(t) \log_2 p_i(t) \tag{5}$$

Rule-based Detection:

$$R_{6.1}(t) = \begin{cases} 1 & \text{if } DI_{security} < 0.2 \text{ and } CS > \theta_{rapid} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

Bayesian Model:

$$P(groupthink|evidence) = \frac{P(evidence|groupthink) \cdot P(groupthink)}{P(evidence)} \tag{7}$$

with evidence including low dissent rate, rapid consensus formation, and external validation absence.

3.3 Indicator 6.2: Risky Shift Phenomena

Definition: Groups accepting higher security risks than individuals would accept alone.

Mathematical Model:

Individual risk tolerance distribution:

$$\mu_{individual} = \frac{1}{n} \sum_{i=1}^{n} RT_i \tag{8}$$

Group risk tolerance:

$$RT_{group}(t) = f(\text{discussion}(t), \text{consensus}(t), \text{polarization}(t)) \tag{9}$$

Risky Shift Index:

$$RSI(t) = \frac{RT_{group}(t) - \mu_{individual}}{\sigma_{individual}} \tag{10}$$

Detection Function:

$$D_{6.2}(t) = \max(0, RSI(t) - \theta_{shift}) \tag{11}$$

Polarization Measure: Using attitude change vectors:

$$P_{polar}(t) = \frac{1}{n} \sum_{i=1}^{n} \|\mathbf{a}_i(t) - \mathbf{a}_i(0)\|_2 \tag{12}$$

where $\mathbf{a}_i(t)$ represents individual i's attitude vector at time t.

3.4 Indicator 6.3: Diffusion of Responsibility

Definition: Reduced individual accountability leading to collective security negligence.

Mathematical Model:

The responsibility diffusion coefficient:

$$RDC(n) = 1 - \frac{1}{\sqrt{n}} \tag{13}$$

where n represents group size, following social psychology findings on bystander effect.

Accountability Distribution:

$$A_{total} = \sum_{i=1}^{n} A_i \cdot (1 - RDC(n)) \tag{14}$$

Security Task Completion Rate:

$$STCR(n,t) = \frac{C_{completed}(t)}{C_{assigned}(t)} \cdot e^{-\lambda \cdot RDC(n)} \tag{15}$$

Detection Threshold:

$$R_{6.3}(t) = \begin{cases} 1 & \text{if } STCR < 0.7 \text{ and } n > 3 \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

3.5 Indicator 6.4: Social Loafing in Security Tasks

Definition: Reduced individual effort on collective security responsibilities.

Mathematical Model:

Individual effort in group context:

$$E_i(n) = E_{individual} \cdot \left(1 - \frac{\alpha \log(n)}{n}\right) \tag{17}$$

where α represents the loafing coefficient calibrated per organization.

Collective Effort Function:

$$E_{collective}(n) = \sum_{i=1}^{n} E_i(n) = n \cdot E_{individual} \cdot \left(1 - \frac{\alpha \log(n)}{n}\right) \tag{18}$$

Loafing Detection:

$$LD(t) = \frac{E_{expected}(t) - E_{observed}(t)}{E_{expected}(t)} \tag{19}$$

Security Task Effort Metrics: - Response time to security alerts - Quality of security documentation - Participation in security training - Proactive threat hunting activities

3.6 Indicator 6.5: Bystander Effect in Incident Response

Definition: Delayed incident response due to assumption others will act.

Mathematical Model:

Probability of individual response with n observers:

$$P_{response}(i,n) = P_{base} \cdot \frac{1}{\sqrt{n}} \cdot Responsibility_i \tag{20}$$

Response Time Model:

$$RT_{expected}(n) = RT_{base} \cdot \sqrt{n} \cdot \left(1 + \frac{Ambiguity}{Clarity}\right) \tag{21}$$

Collective Response Function:

$$P_{collective\_response}(n) = 1 - \prod_{i=1}^{n}(1 - P_{response}(i,n)) \tag{22}$$

Detection Algorithm:

$$D_{6.5}(t) = \frac{RT_{observed}(t) - RT_{expected}(n)}{RT_{expected}(n)} \tag{23}$$

3.7 Indicator 6.6: Dependency Group Assumptions

Definition: Over-reliance on authority figures or technology for security protection.

Mathematical Model:

Dependency intensity measurement:

$$DI(t) = \frac{\sum_i Requests_{authority}(i,t)}{\sum_i Decisions_{independent}(i,t)} \tag{24}$$

Authority Reference Frequency: Using natural language processing on communications:

$$ARF(m) = \frac{\text{count(authority\_references}(m))}{|m|} \tag{25}$$

Technology Dependency Index:

$$TDI(t) = \frac{Automated\_Decisions(t)}{Total\_Security\_Decisions(t)} \tag{26}$$

Composite Dependency Score:

$$DS(t) = w_1 \cdot DI(t) + w_2 \cdot ARF(t) + w_3 \cdot TDI(t) \tag{27}$$

Detection Function:

$$R_{6.6}(t) = \begin{cases} 1 & \text{if } DS(t) > \mu_{baseline} + 2\sigma_{baseline} \\ 0 & \text{otherwise} \end{cases} \tag{28}$$

3.8 Indicator 6.7: Fight-Flight Security Postures

Definition: Extreme defensive postures alternating with avoidance behaviors.

Mathematical Model:

Fight response intensity:

$$FRI(t) = \frac{Defensive\_Actions(t)}{Threat\_Detections(t)} \cdot Aggression\_Level(t) \tag{29}$$

Flight response intensity:

$$FLI(t) = \frac{Avoidance\_Actions(t)}{Security\_Requirements(t)} \cdot Withdrawal\_Level(t) \tag{30}$$

Oscillation Detection:

$$OSC(t,w) = \text{variance}\left(\frac{FRI(t) - FLI(t)}{FRI(t) + FLI(t)}\right)_{t-w:t} \tag{31}$$

Bipolar Security Response:

$$BSR(t) = |FRI(t) - FLI(t)| \cdot OSC(t,w) \tag{32}$$

Communication Sentiment Analysis: - Aggressive language markers: threat, attack, defend, fight - Avoidance language markers: defer, postpone, delegate, bypass

3.9 Indicator 6.8: Pairing Hope Fantasies

Definition: Unrealistic expectations for future security solutions to solve current problems.

Mathematical Model:

Future solution reference rate:

$$FSRR(t) = \frac{\text{count(future\_solutions}(t))}{\text{count(current\_actions}(t))} \tag{33}$$

Investment Disparity:

$$ID(t) = \frac{Budget_{future\_solutions}(t)}{Budget_{current\_fixes}(t)} \tag{34}$$

Hope Fantasy Index:

$$HFI(t) = FSRR(t) \cdot ID(t) \cdot \frac{1}{Implementation\_Rate(t)} \tag{35}$$

Linguistic Pattern Detection: Future-focused language: "will be," "going to," "soon," "next version" Present avoidance: "until then," "temporary," "waiting for"

Detection Threshold:

$$R_{6.8}(t) = \begin{cases} 1 & \text{if } HFI(t) > 2.0 \text{ and } Implementation\_Rate < 0.3 \\ 0 & \text{otherwise} \end{cases} \tag{36}$$

3.10 Indicator 6.9: Organizational Splitting

Definition: Division of organizational aspects into idealized and demonized categories.

Mathematical Model:

Sentiment polarization in organizational references:

$$SP(entity) = \frac{|Positive\_Sentiment| - |Negative\_Sentiment|}{|Positive\_Sentiment| + |Negative\_Sentiment|} \tag{37}$$

Splitting Index:

$$SI(t) = \frac{1}{n} \sum_{i=1}^{n} |SP(entity_i)| \tag{38}$$

Good-Bad Object Classification: Using machine learning on organizational communications:

$$P(good|entity) = \sigma(\mathbf{w}_{good}^T \mathbf{f}_{entity}) \tag{39}$$

$$P(bad|entity) = \sigma(\mathbf{w}_{bad}^T \mathbf{f}_{entity}) \tag{40}$$

Splitting Threshold:

$$R_{6.9}(t) = \begin{cases} 1 & \text{if } SI(t) > 0.8 \text{ and } Ambiguity\_Tolerance < 0.2 \\ 0 & \text{otherwise} \end{cases} \tag{41}$$

3.11 Indicator 6.10: Collective Defense Mechanisms

Definition: Group-level psychological defenses interfering with security reality testing.

Mathematical Model:

Defense mechanism strength matrix:

$$\mathbf{D} = \begin{pmatrix} Denial & Projection & Rationalization \\ Intellectualization & Displacement & Sublimation \end{pmatrix} \tag{42}$$

Collective Defense Intensity:

$$CDI(t) = \sum_{i,j} D_{ij}(t) \cdot Activation_{ij}(t) \tag{43}$$

Reality Testing Impairment:

$$RTI(t) = \frac{Distorted\_Perceptions(t)}{Total\_Threat\_Assessments(t)} \cdot CDI(t) \tag{44}$$

Specific Defense Detection:
Collective Denial:

$$CD(t) = \frac{Ignored\_Threats(t)}{Identified\_Threats(t)} \tag{45}$$

Group Projection:

$$GP(t) = \frac{External\_Attributions(t)}{Internal\_Vulnerabilities(t)} \tag{46}$$

Organizational Rationalization:

$$OR(t) = \frac{Justification\_Attempts(t)}{Security\_Failures(t)} \tag{47}$$

4 Interdependency Matrix

The group dynamic indicators exhibit complex interdependencies captured through the correlation matrix $\mathbf{R}_6$:

$$\mathbf{R}_6 = \begin{pmatrix} 1.00 & 0.75 & 0.50 & 0.45 & 0.60 & 0.35 & 0.40 & 0.30 & 0.65 & 0.70 \\ 0.75 & 1.00 & 0.40 & 0.35 & 0.30 & 0.25 & 0.45 & 0.20 & 0.55 & 0.60 \\ 0.50 & 0.40 & 1.00 & 0.80 & 0.85 & 0.30 & 0.25 & 0.20 & 0.35 & 0.45 \\ 0.45 & 0.35 & 0.80 & 1.00 & 0.90 & 0.25 & 0.20 & 0.15 & 0.30 & 0.40 \\ 0.60 & 0.30 & 0.85 & 0.90 & 1.00 & 0.20 & 0.25 & 0.15 & 0.35 & 0.50 \\ 0.35 & 0.25 & 0.30 & 0.25 & 0.20 & 1.00 & 0.60 & 0.70 & 0.45 & 0.55 \\ 0.40 & 0.45 & 0.25 & 0.20 & 0.25 & 0.60 & 1.00 & 0.50 & 0.65 & 0.75 \\ 0.30 & 0.20 & 0.20 & 0.15 & 0.15 & 0.70 & 0.50 & 1.00 & 0.40 & 0.45 \\ 0.65 & 0.55 & 0.35 & 0.30 & 0.35 & 0.45 & 0.65 & 0.40 & 1.00 & 0.80 \\ 0.70 & 0.60 & 0.45 & 0.40 & 0.50 & 0.55 & 0.75 & 0.45 & 0.80 & 1.00 \end{pmatrix} \tag{48}$$

Key interdependencies include:

- Strong correlation (0.90) between Social Loafing (6.4) and Bystander Effect (6.5)
- High correlation (0.85) between Diffusion of Responsibility (6.3) and Bystander Effect (6.5)
- Moderate correlation (0.80) between Organizational Splitting (6.9) and Collective Defense Mechanisms (6.10)
- Significant correlation (0.75) between Groupthink (6.1) and Risky Shift (6.2)
- Notable correlation (0.75) between Fight-Flight Postures (6.7) and Collective Defense Mechanisms (6.10)

Cross-category correlations with previously formalized categories:

- Category 1 (Authority): Strong correlation (0.70) between Authority Gradient Effects (1.6) and Dependency Assumptions (6.6)

- Category 2 (Temporal): Moderate correlation (0.60) between Time Pressure (2.2) and Groupthink (6.1)
- Category 4 (Affective): High correlation (0.75) between Fear-Based Decisions (4.1) and Fight-Flight Postures (6.7)
- Category 5 (Cognitive): Strong correlation (0.65) between Alert Fatigue (5.1) and Social Loafing (6.4)

5 Implementation Algorithms

Algorithm 1 Group Dynamic Vulnerability Assessment

```
Initialize group structure graph G = (V, E)
Initialize baseline parameters μ_G, Σ_G, w_G
for each time step t do
    Update communication network topology
    Collect group interaction telemetry x_G(t)
    for each indicator i ∈ {6.1, 6.2, ..., 6.10} do
        Compute individual contributions c_i(t)
        Calculate network measures N_i(t)
        Compute R_i(t) using rule-based group logic
        Compute A_i(t) using collective anomaly detection
        Compute B_i(t) using group Bayesian update
        Calculate D_i(t) = w_1 R_i(t) + w_2 A_i(t) + w_3 B_i(t) + w_4 N_i(t)
        Update consensus dynamics C_i(t)
        Update temporal state T_i(t) = α · D_i(t) + (1 − α) · T_i(t − 1) + β · C_i(t)
    end for
    Compute cross-category interdependencies
    Calculate group convergence states
    Generate collective alerts based on dynamic thresholds
    Update group baselines with exponential smoothing
    Log results for validation and social network analysis
end for
```

6 Validation Framework

Group dynamic indicators require specialized validation approaches that account for collective behavior emergence:

Network Analysis Metrics:

$$Centrality_{betweenness}(i) = \sum_{s \neq i \neq t} \frac{\sigma_{st}(i)}{\sigma_{st}} \tag{49}$$

$$Clustering_{coefficient} = \frac{\text{triangles}}{\text{connected triples}} \tag{50}$$

$$Information_{flow} = \sum_{(i,j)} w_{ij} \cdot d(i,j)^{-1} \tag{51}$$

Collective Behavior Validation:

$$Emergence_{score} = \frac{Group_{behavior} - \sum Individual_{behavior}}{Group_{size}} \tag{52}$$

Consensus Dynamics Measurement:

$$Consensus_{speed} = \frac{d}{dt}\left(\max_i \text{opinion}_i(t)\right) \tag{53}$$

Group Cohesion Index:

$$GCI = \frac{\sum_{i,j} similarity(i,j)}{n(n-1)/2} \tag{54}$$

Cross-Validation Protocol: Temporal cross-validation with group membership stratification:

$$CV_{group} = \frac{1}{k}\sum_{i=1}^{k} Performance(Model_i, Group_{test,i}) \tag{55}$$

Statistical Significance Testing: Mann-Whitney U tests for group differences:

$$U = n_1 n_2 + \frac{n_1(n_1+1)}{2} - R_1 \tag{56}$$

where R_1 is the sum of ranks for group 1.

7 Conclusion

This mathematical formalization of group dynamic vulnerabilities provides the analytical foundation for detecting and mitigating collective psychological vulnerabilities in cybersecurity contexts. The ten indicators capture the full spectrum of group-level psychological phenomena that create systematic security blind spots beyond individual vulnerabilities.

The interdependency matrix reveals complex correlations between group dynamic phenomena and individual psychological states, enabling enhanced detection through multivariate analysis. The network-based components of the detection functions capture the unique characteristics of collective behavior that cannot be reduced to individual psychology.

Implementation algorithms provide clear guidance for integrating group dynamic assessment into existing SOC operations, while validation frameworks ensure sustained accuracy in dynamic organizational environments. The mathematical approach enables real-time detection of emergent collective vulnerabilities before they can be exploited by attackers.

Future research directions include machine learning approaches for predicting group state transitions, cultural adaptation of group dynamic models for international organizations, and integration with organizational development methodologies for systematic vulnerability mitigation. The mathematical rigor established here provides the foundation for these advanced applications while ensuring reproducible implementations across diverse organizational contexts.

Group dynamic vulnerabilities represent one of the most challenging aspects of organizational security, as they emerge from the complex interaction between individual psychology and collective behavior. By providing mathematical models for these phenomena, CPF Category 6 enables security professionals to address vulnerabilities that have historically been invisible to traditional security frameworks.

References

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

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

[3] Janis, I. L. (1971). Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes. *Houghton, Mifflin*.

[4] Arrow, H., McGrath, J. E., & Berdahl, J. L. (2000). *Small groups as complex systems: Formation, coordination, development, and adaptation*. Sage Publications.

[5] Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of small-world networks. *Nature*, 393(6684), 440-442.

[6] Tuckman, B. W. (1965). Developmental sequence in small groups. *Psychological Bulletin*, 63(6), 384-399.