

CPF Mathematical Formalization Series - Paper 6: Vulnerabilità delle Dinamiche di Gruppo: Modelli Matematici e Algoritmi di Rilevamento

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

November 18, 2025

Abstract

Presentiamo la formalizzazione matematica completa degli indicatori della Categoria 6 del Cybersecurity Psychology Framework (CPF): Vulnerabilità delle Dinamiche di Gruppo. Ciascuno dei dieci indicatori (6.1-6.10) è rigorosamente definito attraverso funzioni di rilevamento che combinano analisi di rete, misure di teoria dell'informazione e modelli di inferenza bayesiana. La formalizzazione cattura gli stati psicologici collettivi che emergono in contesti organizzativi, fondati sulla teoria delle assunzioni di base di Bion e sulla ricerca contemporanea sulle dinamiche di gruppo. Forniamo algoritmi espliciti per il rilevamento in tempo reale di punti ciechi di sicurezza collettivi, matrici di interdipendenza per l'analisi di correlazione e metriche di validazione per la calibrazione continua. Questo lavoro stabilisce le fondamenta matematiche per operationalizzare vulnerabilità psicologiche a livello di gruppo che creano debolezze di sicurezza sistematiche attraverso comportamenti collettivi emergenti.

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

1 Introduzione e Contesto CPF

Il Cybersecurity Psychology Framework (CPF) affronta il divario critico tra vulnerabilità psicologiche individuali e proprietà emergenti del comportamento collettivo nei contesti di sicurezza organizzativa [1]. Mentre le categorie precedenti si sono concentrate sulle vulnerabilità a livello individuale, la Categoria 6 cattura i fenomeni unici che sorgono quando gli individui si aggregano in gruppi, creando vulnerabilità che superano la somma delle debolezze individuali.

Le vulnerabilità delle dinamiche di gruppo rappresentano una classe distinta di minacce alla sicurezza che emergono da processi psicologici collettivi. Queste vulnerabilità non possono essere affrontate attraverso interventi focalizzati sull'individuo poiché sorgono dai pattern di interazione tra i membri del gruppo piuttosto che dalla psicologia di un singolo individuo. I modelli matematici presentati qui formalizzano questi stati collettivi emergenti, consentendo il rilevamento e la mitigazione sistematici di punti ciechi di sicurezza a livello di gruppo.

Questo paper continua la CPF Mathematical Formalization Series, fornendo definizioni matematiche rigorose per tutti i dieci indicatori di Vulnerabilità delle Dinamiche di Gruppo (6.1-6.10). Ogni indicatore riceve funzioni di rilevamento esplicite, modellazione di interdipendenza con categorie precedentemente formalizzate e specifiche algoritmiche che consentono l'implementazione immediata nei Security Operations Centers (SOC).

La Categoria 6 trae principalmente dal lavoro pionieristico di Bion sulle dinamiche di gruppo [2], dalla ricerca sul pensiero di gruppo di Janis [3] e dalle metodologie contemporanee di analisi delle reti

sociali. Queste fondamenta teoriche forniscono la base psicologica per modelli matematici che catturano come le assunzioni inconsce collettive creano vulnerabilità di sicurezza sistematiche nei contesti organizzativi.

2 Fondamento Teorico: Processi delle Dinamiche di Gruppo

Le vulnerabilità delle dinamiche di gruppo emergono dalla complessa interazione tra psicologia individuale e pattern di comportamento collettivo. La ricerca dimostra che i gruppi sviluppano proprietà emergenti che non possono essere previste dalle caratteristiche dei singoli membri [4]. Queste proprietà emergenti spesso includono meccanismi di difesa condivisi, punti ciechi collettivi e comportamenti di assunzione di rischio sincronizzati che creano vulnerabilità di sicurezza sistematiche.

La teoria delle assunzioni di base di Bion [2] identifica tre modalità primarie di funzionamento di gruppo che impattano direttamente la postura di sicurezza: dipendenza (ricerca di protezione onnipotente), lotta-fuga (percezione delle minacce come esterne) e accoppiamento (speranza per la salvezza futura attraverso nuove soluzioni). Ogni modalità crea pattern di vulnerabilità specifici che gli attaccanti possono sfruttare attraverso campagne mirate di ingegneria sociale.

L'analisi di rete moderna rivela che i pattern di flusso informativo nei gruppi organizzativi creano punti naturali di vulnerabilità [5]. Strutture di comunicazione centralizzate creano singoli punti di fallimento, mentre reti altamente connesse consentono la diffusione rapida sia di minacce che di meccanismi di difesa. I modelli matematici presentati qui catturano queste vulnerabilità strutturali attraverso misure di teoria dei grafi combinate con il rilevamento dello stato psicologico.

Le dinamiche temporali della formazione e dissoluzione dei gruppi creano anche finestre di vulnerabilità. Il modello forming-storming-norming-performing di Tuckman [6] identifica fasi specifiche dove la consapevolezza della sicurezza varia in modo prevedibile. I modelli matematici possono catturare queste transizioni di fase e predire periodi di vulnerabilità elevata.

3 Formalizzazione Matematica

3.1 Framework di Rilevamento Universale

Ogni indicatore delle dinamiche di gruppo impiega la funzione di rilevamento unificata estesa per l'analisi collettiva:

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

dove $D_i(t)$ rappresenta lo score di rilevamento per l'indicatore i al tempo t , $R_i(t)$ denota il rilevamento basato su regole, $A_i(t)$ rappresenta lo score di anomalia, $B_i(t)$ rappresenta la probabilità posteriori bayesiana e $N_i(t)$ rappresenta misure basate sulla rete uniche alle dinamiche di gruppo.

L'evoluzione temporale collettiva incorpora le dinamiche del consenso di gruppo:

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

dove $C_i(t)$ rappresenta il fattore di influenza del consenso calcolato attraverso modelli di dinamiche d'opinione.

3.2 Indicatore 6.1: Punti Ciechi di Sicurezza da Pensiero di Gruppo

Definizione: Soppressione collettiva di opinioni di sicurezza dissidenti che porta a punti ciechi sistematici.

Modello Matematico:

L'indice di diversità per il processo decisionale sulla sicurezza:

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

dove p_i rappresenta la frazione dei membri del gruppo che scelgono l'opzione di sicurezza i .

Metrica di Velocità del Consenso:

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

Rilevamento della Soppressione del Dissenso: L'entropia delle opinioni di sicurezza:

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

Rilevamento Basato su Regole:

$$R_{6.1}(t) = \begin{cases} 1 & \text{se } DI_{security} < 0.2 \text{ e } CS > \theta_{rapid} \\ 0 & \text{altrimenti} \end{cases} \quad (6)$$

Modello Bayesiano:

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

con evidenza che include basso tasso di dissenso, formazione rapida di consenso e assenza di validazione esterna.

3.3 Indicatore 6.2: Fenomeni di Spostamento Rischioso

Definizione: Gruppi che accettano rischi di sicurezza più elevati di quelli che gli individui accetterebbero da soli.

Modello Matematico:

Distribuzione della tolleranza al rischio individuale:

$$\mu_{individual} = \frac{1}{n} \sum_{i=1}^n RT_i \quad (8)$$

Tolleranza al rischio di gruppo:

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

Indice di Spostamento Rischioso:

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

Funzione di Rilevamento:

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

Misura di Polarizzazione: Usando vettori di cambiamento di atteggiamento:

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

dove $\mathbf{a}_i(t)$ rappresenta il vettore di atteggiamento dell'individuo i al tempo t .

3.4 Indicatore 6.3: Diffusione di Responsabilità

Definizione: Ridotta responsabilità individuale che porta a negligenza di sicurezza collettiva.

Modello Matematico:

Il coefficiente di diffusione della responsabilità:

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

dove n rappresenta la dimensione del gruppo, seguendo i risultati della psicologia sociale sull'effetto spettatore.

Distribuzione di Responsabilità:

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

Tasso di Completamento dei Compiti di Sicurezza:

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

Soglia di Rilevamento:

$$R_{6.3}(t) = \begin{cases} 1 & \text{se } STCR < 0.7 \text{ e } n > 3 \\ 0 & \text{altrimenti} \end{cases} \quad (16)$$

3.5 Indicatore 6.4: Pigrizia Sociale nei Compiti di Sicurezza

Definizione: Ridotto sforzo individuale nelle responsabilità di sicurezza collettiva.

Modello Matematico:

Sforzo individuale nel contesto di gruppo:

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

dove α rappresenta il coefficiente di pigrizia calibrato per organizzazione.

Funzione di Sforzo Collettivo:

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

Rilevamento di Pigrizia:

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

Metriche di Sforzo nei Compiti di Sicurezza: - Tempo di risposta agli alert di sicurezza - Qualità della documentazione di sicurezza - Partecipazione al training di sicurezza - Attività di ricerca proattiva delle minacce

3.6 Indicatore 6.5: Effetto Spettatore nella Risposta agli Incidenti

Definizione: Risposta ritardata agli incidenti per l'assunzione che altri agiranno.

Modello Matematico:

Probabilità di risposta individuale con n osservatori:

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

Modello di Tempo di Risposta:

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

Funzione di Risposta Collettiva:

$$P_{collective_response}(n) = 1 - \prod_{i=1}^n (1 - P_{response}(i, n)) \quad (22)$$

Algoritmo di Rilevamento:

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

3.7 Indicatore 6.6: Assunzioni di Gruppo di Dipendenza

Definizione: Eccessiva dipendenza da figure di autorità o tecnologia per la protezione della sicurezza.

Modello Matematico:

Misurazione dell'intensità della dipendenza:

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

Frequenza di Riferimento all'Autorità: Usando elaborazione del linguaggio naturale sulle comunicazioni:

$$ARF(m) = \frac{\text{count}(\text{authority_references}(m))}{|m|} \quad (25)$$

Indice di Dipendenza dalla Tecnologia:

$$TDI(t) = \frac{Automated_Decisions(t)}{Total_Security_Decisions(t)} \quad (26)$$

Score Composito di Dipendenza:

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

Funzione di Rilevamento:

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

3.8 Indicatore 6.7: Posture di Sicurezza Lotta-Fuga

Definizione: Posture difensive estreme che si alternano con comportamenti di evitamento.

Modello Matematico:

Intensità della risposta di lotta:

$$FRI(t) = \frac{Defensive_Actions(t)}{Threat_Detections(t)} \cdot Aggression_Level(t) \quad (29)$$

Intensità della risposta di fuga:

$$FLI(t) = \frac{Avoidance_Actions(t)}{Security_Requirements(t)} \cdot Withdrawal_Level(t) \quad (30)$$

Rilevamento di Oscillazione:

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

Risposta di Sicurezza Bipolare:

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

Analisi del Sentiment della Comunicazione: - Marcatori di linguaggio aggressivo: threat, attack, defend, fight - Marcatori di linguaggio di evitamento: defer, postpone, delegate, bypass

3.9 Indicatore 6.8: Fantasie di Speranza nell'Accoppiamento

Definizione: Aspettative irrealistiche per soluzioni di sicurezza future per risolvere problemi attuali.

Modello Matematico:

Tasso di riferimento a soluzioni future:

$$FSRR(t) = \frac{\text{count(future_solutions}(t))}{\text{count(current_actions}(t))} \quad (33)$$

Disparità negli Investimenti:

$$ID(t) = \frac{Budget_{future_solutions}(t)}{Budget_{current_fixes}(t)} \quad (34)$$

Indice di Fantasia di Speranza:

$$HFI(t) = FSRR(t) \cdot ID(t) \cdot \frac{1}{Implementation_Rate(t)} \quad (35)$$

Rilevamento di Pattern Linguistici: Linguaggio orientato al futuro: "will be," "going to," "soon," "next version" Evitamento del presente: "until then," "temporary," "waiting for"

Soglia di Rilevamento:

$$R_{6.8}(t) = \begin{cases} 1 & \text{se } HFI(t) > 2.0 \text{ e } Implementation_Rate < 0.3 \\ 0 & \text{altrimenti} \end{cases} \quad (36)$$

3.10 Indicatore 6.9: Scissione Organizzativa

Definizione: Divisione degli aspetti organizzativi in categorie idealizzate e demonizzate.

Modello Matematico:

Polarizzazione del sentiment nei riferimenti organizzativi:

$$SP(entity) = \frac{|Positive_Sentiment| - |Negative_Sentiment|}{|Positive_Sentiment| + |Negative_Sentiment|} \quad (37)$$

Indice di Scissione:

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

Classificazione degli Oggetti Buoni-Cattivi: Usando machine learning sulle comunicazioni organizzative:

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

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

Soglia di Scissione:

$$R_{6.9}(t) = \begin{cases} 1 & \text{se } SI(t) > 0.8 \text{ e } Ambiguity_Tolerance < 0.2 \\ 0 & \text{altrimenti} \end{cases} \quad (41)$$

3.11 Indicatore 6.10: Meccanismi di Difesa Collettivi

Definizione: Difese psicologiche a livello di gruppo che interferiscono con il test di realtà sulla sicurezza.

Modello Matematico:

Matrice di forza dei meccanismi di difesa:

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

Intensità della Difesa Collettiva:

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

Compromissione del Test di Realtà:

$$RTI(t) = \frac{Distorted_Perceptions(t)}{Total_Threat_Assessments(t)} \cdot CDI(t) \quad (44)$$

Rilevamento di Difese Specifiche:

Negazione Collettiva:

$$CD(t) = \frac{Ignored_Threats(t)}{Identified_Threats(t)} \quad (45)$$

Proiezione di Gruppo:

$$GP(t) = \frac{External_Attributions(t)}{Internal_Vulnerabilities(t)} \quad (46)$$

Razionalizzazione Organizzativa:

$$OR(t) = \frac{Justification_Attempts(t)}{Security_Failures(t)} \quad (47)$$

4 Matrice di Interdipendenza

Gli indicatori delle dinamiche di gruppo mostrano interdipendenze complesse catturate attraverso la matrice di correlazione \mathbf{R}_6 :

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

Interdipendenze chiave includono:

- Forte correlazione (0.90) tra Pigrizia Sociale (6.4) e Effetto Spettatore (6.5)
- Alta correlazione (0.85) tra Diffusione di Responsabilità (6.3) e Effetto Spettatore (6.5)
- Moderata correlazione (0.80) tra Scissione Organizzativa (6.9) e Meccanismi di Difesa Collettivi (6.10)
- Significativa correlazione (0.75) tra Pensiero di Gruppo (6.1) e Spostamento Rischioso (6.2)
- Notevole correlazione (0.75) tra Posture Lotta-Fuga (6.7) e Meccanismi di Difesa Collettivi (6.10)

Correlazioni cross-categoria con categorie precedentemente formalizzate:

- Categoria 1 (Autorità): Forte correlazione (0.70) tra Effetti del Gradiente di Autorità (1.6) e Assunzioni di Dipendenza (6.6)
- Categoria 2 (Temporale): Moderata correlazione (0.60) tra Pressione Temporale (2.2) e Pensiero di Gruppo (6.1)
- Categoria 4 (Affettiva): Alta correlazione (0.75) tra Decisioni Basate sulla Paura (4.1) e Posture Lotta-Fuga (6.7)
- Categoria 5 (Cognitiva): Forte correlazione (0.65) tra Fatica da Alert (5.1) e Pigrizia Sociale (6.4)

5 Algoritmi di Implementazione

6 Framework di Validazione

Gli indicatori delle dinamiche di gruppo richiedono approcci di validazione specializzati che tengano conto dell'emergenza del comportamento collettivo:

Metriche di Analisi di Rete:

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

$$Clustering_{coefficient} = \frac{\text{triangles}}{\text{connected triples}} \quad (50)$$

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

Algorithm 1 Valutazione delle Vulnerabilità delle Dinamiche di Gruppo

```
1: Inizializza grafo della struttura di gruppo  $G = (V, E)$ 
2: Inizializza parametri di baseline  $\mu_G, \Sigma_G, w_G$ 
3: for ogni passo temporale  $t$  do
4:   Aggiorna la topologia della rete di comunicazione
5:   Raccogli telemetria di interazione di gruppo  $\mathbf{x}_G(t)$ 
6:   for ogni indicatore  $i \in \{6.1, 6.2, \dots, 6.10\}$  do
7:     Calcola contributi individuali  $\mathbf{c}_i(t)$ 
8:     Calcola misure di rete  $N_i(t)$ 
9:     Calcola  $R_i(t)$  usando logica di gruppo basata su regole
10:    Calcola  $A_i(t)$  usando rilevamento di anomalia collettiva
11:    Calcola  $B_i(t)$  usando aggiornamento bayesiano di gruppo
12:    Calcola  $D_i(t) = w_1 R_i(t) + w_2 A_i(t) + w_3 B_i(t) + w_4 N_i(t)$ 
13:    Aggiorna dinamiche del consenso  $C_i(t)$ 
14:    Aggiorna stato temporale  $T_i(t) = \alpha \cdot D_i(t) + (1 - \alpha) \cdot T_i(t - 1) + \beta \cdot C_i(t)$ 
15:   end for
16:   Calcola interdipendenze cross-categoria
17:   Calcola stati di convergenza del gruppo
18:   Genera alert collettivi basati su soglie dinamiche
19:   Aggiorna baseline di gruppo con smoothing esponenziale
20:   Registra risultati per validazione e analisi di rete sociale
21: end for
```

Validazione del Comportamento Collettivo:

$$Emergence_{score} = \frac{Group_{behavior} - \sum Individual_{behavior}}{Group_{size}} \quad (52)$$

Misurazione delle Dinamiche del Consenso:

$$Consensus_{speed} = \frac{d}{dt} \left(\max_i opinion_i(t) \right) \quad (53)$$

Indice di Coesione di Gruppo:

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

Protocollo di Validazione Incrociata: Validazione incrociata temporale con stratificazione dell'appartenenza al gruppo:

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

Test di Significatività Statistica: Test U di Mann-Whitney per differenze di gruppo:

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

dove R_1 è la somma dei ranghi per il gruppo 1.

7 Conclusione

Questa formalizzazione matematica delle vulnerabilità delle dinamiche di gruppo fornisce le fondamenta analitiche per rilevare e mitigare vulnerabilità psicologiche collettive nei contesti di cybersecurity. I dieci

indicatori catturano l'intero spettro di fenomeni psicologici a livello di gruppo che creano punti ciechi di sicurezza sistematici oltre le vulnerabilità individuali.

La matrice di interdipendenza rivela correlazioni complesse tra fenomeni delle dinamiche di gruppo e stati psicologici individuali, consentendo il rilevamento migliorato attraverso analisi multivariata. I componenti basati sulla rete delle funzioni di rilevamento catturano le caratteristiche uniche del comportamento collettivo che non possono essere ridotte alla psicologia individuale.

Gli algoritmi di implementazione forniscono indicazioni chiare per integrare la valutazione delle dinamiche di gruppo nelle operazioni SOC esistenti, mentre i framework di validazione assicurano accuratezza sostenuta in ambienti organizzativi dinamici. L'approccio matematico consente il rilevamento in tempo reale di vulnerabilità collettive emergenti prima che possano essere sfruttate dagli attaccanti.

Direzioni di ricerca future includono approcci di machine learning per predire transizioni di stato di gruppo, adattamento culturale dei modelli di dinamiche di gruppo per organizzazioni internazionali e integrazione con metodologie di sviluppo organizzativo per la mitigazione sistematica delle vulnerabilità. Il rigore matematico stabilito qui fornisce le fondamenta per queste applicazioni avanzate assicurando implementazioni riproducibili attraverso contesti organizzativi diversi.

Le vulnerabilità delle dinamiche di gruppo rappresentano uno degli aspetti più sfidanti della sicurezza organizzativa, poiché emergono dalla complessa interazione tra psicologia individuale e comportamento collettivo. Fornendo modelli matematici per questi fenomeni, la Categoria 6 del CPF consente ai professionisti della sicurezza di affrontare vulnerabilità che sono state storicamente invisibili ai framework di sicurezza tradizionali.

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.