Il CPF Educational Framework: Un Curriculum Universale per la Literacy in Cybersecurity Psicologica

Companion Educativo al Cybersecurity Psychology Framework

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

December 17, 2025

Abstract

Il Cybersecurity Psychology Framework (CPF) fornisce una rigorosa fondazione teorica e operativa per comprendere le vulnerabilità umane nei contesti di security. Tuttavia, la teoria senza pedagogia rimane inaccessibile; i framework senza percorsi educativi diventano artefatti piuttosto che strumenti di cambiamento. Questo paper presenta il CPF Educational Framework, un curriculum strutturato progettato per introdurre, sviluppare e specializzare i discenti attraverso l'intero spettro della literacy in cybersecurity psicologica. A differenza dei tradizionali programmi di security awareness che assumono attori razionali modificabili attraverso il trasferimento di informazioni, questo approccio educativo riconosce che le decisioni di security avvengono sostanzialmente al di sotto della consapevolezza cosciente e che un'educazione efficace deve coinvolgere i processi pre-cognitivi, le dinamiche di gruppo e la complessa interazione tra intelligenza umana e artificiale. Il framework comprende quattro moduli universali—"Non Decidi Tu," "Come Ti Fregano," "Il Gruppo Pensa Per Te," e "Tu e le Macchine"—che formano uno scheletro concettuale invariante. Questo scheletro viene poi modulato attraverso quattro livelli di sviluppo (Base, Intermedio, Avanzato, Specialistico), ciascuno calibrato sulla complessità appropriata, sugli esempi contestuali e sull'integrazione con la documentazione tecnica del CPF. Il curriculum posiziona i paper fondamentali del CPF come waypoint progressivi: la Taxonomy come mappa di riferimento, il Dense Implementation Companion come specifica operativa, l'Intervention Framework come metodologia di remediation, e il Depth paper come mentore teorico che accompagna i discenti durante tutto il loro viaggio. Questa architettura educativa abilita sia iniziative di literacy su larga scala sia sviluppo professionale specializzato, mantenendo la coerenza con il framework scientifico sottostante.

Keywords: educazione alla cybersecurity, literacy psicologica, curriculum design, fattori umani, processi pre-cognitivi, security awareness, lifelong learning

Contents

1 Introduzione: L'Imperativo Pedagogico

1.1 Il Fallimento dell'Educazione Tradizionale alla Security

L'investimento globale in training di cybersecurity awareness supera i $5 miliardi annui, eppure le metriche fondamentali degli incidenti di security legati al fattore umano non mostrano alcun miglioramento corrispondente [20, 17]. Questo fallimento persistente richiede una spiegazione. Il Cybersecurity Psychology Framework ne offre una: l'educazione tradizionale alla security opera su un modello fondamentalmente errato della cognizione e del comportamento umano.

Il paradigma educativo prevalente assume che gli esseri umani siano attori razionali che, quando informati sui rischi e le conseguenze, modificheranno il loro comportamento di conseguenza. Questa assunzione contraddice decenni di ricerca in neuroscienze, economia comportamentale e teoria psicoanalitica. Gli esperimenti fondamentali di Benjamin Libet hanno dimostrato che le decisioni motorie avvengono 300-500 millisecondi prima della consapevolezza cosciente [13]. La teoria del dual-process di Daniel Kahneman rivela che il System 1 (veloce, automatico, emotivo) domina il System 2 (lento, deliberato, razionale) precisamente negli ambienti pressati dal tempo e cognitivamente sovraccarichi dove avvengono le decisioni di security [9]. La ricerca sulle dinamiche di gruppo di Wilfred Bion mostra che il comportamento collettivo emerge da basic assumption inconsce che operano interamente al di sotto della consapevolezza cosciente [1].

Se le decisioni di security vengono prese prima della consapevolezza cosciente, se i processi automatici dominano quelli deliberati, se le dinamiche di gruppo plasmano il comportamento individuale attraverso canali inconsci—allora l'educazione che mira solo ai processi coscienti, razionali e individuali fallirà necessariamente. La domanda non è se l'educazione tradizionale alla security sia implementata male, ma se le sue assunzioni fondamentali siano sbagliate.

1.2 Una Filosofia Educativa Differente

Il CPF Educational Framework procede da assunzioni differenti. Assumiamo che:

- **I processi pre-cognitivi determinano sostanzialmente il comportamento di security.** L'educazione deve quindi coinvolgere questi processi, non semplicemente informare la consapevolezza cosciente.
- **L'apprendimento non è trasferimento di informazioni ma sviluppo del riconoscimento di pattern.** L'obiettivo non è riempire i discenti di fatti ma sviluppare la loro capacità di riconoscere pattern di vulnerabilità in se stessi, negli altri e nelle organizzazioni.
- **L'educazione è ignizione, non completamento.** In un dominio caratterizzato da costante evoluzione e variazione individuale, l'educazione formale fornisce la scintilla iniziale; lo sviluppo successivo avviene attraverso l'esplorazione auto-diretta con gli strumenti disponibili (inclusi AI tutor, risorse della community e ritorno alle strutture formali quando necessario).
- **Lo stesso scheletro concettuale serve tutti i discenti.** Ciò che varia non sono gli insight fondamentali ma la loro applicazione contestuale, la complessità degli esempi e la profondità del grounding teorico.
- **La vulnerabilità psicologica è permanente e pervasiva.** A differenza delle vulnerabilità tecniche che possono essere patchate, le vulnerabilità psicologiche sono

intrinseche alla cognizione umana. L'educazione mira non all'eliminazione ma alla consapevolezza, al riconoscimento e all'accomodamento strategico.

Queste assunzioni producono un framework educativo fondamentalmente diverso dalla tradizionale security awareness. Non insegniamo regole da seguire ma pattern da riconoscere. Non assumiamo che i discenti cambieranno la loro natura ma che possano comprenderla. Non posizioniamo l'educazione come una credenziale completata ma come un viaggio iniziato.

1.3 Il Viaggio dell'Eroe: Una Metafora Organizzativa

Il monomito di Joseph Campbell—il viaggio dell'eroe—fornisce un'utile metafora organizzativa per l'esperienza educativa del CPF [2]. Il discente inizia nel mondo ordinario della fiducia ingenua nella propria razionalità e autonomia. La chiamata all'avventura arriva attraverso il riconoscimento che "non decidi tu"—che i processi pre-cognitivi plasmano sostanzialmente il comportamento. L'attraversamento della soglia avviene quando questo riconoscimento diventa personale, quando il discente vede questi pattern operare nella propria esperienza.

Il viaggio attraverso il mondo speciale coinvolge un engagement progressivamente più profondo con i meccanismi della vulnerabilità: influenza sociale, dinamiche di gruppo, risposte allo stress, processi inconsci. Ogni stadio rivela nuovi aspetti di come la psicologia umana crea pattern sfruttabili. Il discente incontra alleati (compagni di viaggio, risorse educative, AI tutor) e nemici (bias cognitivi, resistenza difensiva, l'attrazione delle illusioni confortevoli).

In questa metafora, la documentazione tecnica del CPF serve funzioni narrative specifiche:

- **La Taxonomy** è la mappa del mondo speciale—l'enumerazione sistematica dei territori da esplorare, dei pericoli da riconoscere, dei pattern da comprendere.
- **Il Dense Implementation Companion** serve come manuale tecnico—le specifiche operative che traducono la comprensione concettuale in detection e response azionabili.
- **L'Intervention Framework** rappresenta il dono del ritorno—la metodologia che trasforma la comprensione personale in capacità di cambiamento organizzativo.
- **Il Depth paper** funziona come la figura del mentore che appare durante tutto il viaggio, fornendo grounding teorico quando necessario, spiegando perché la mappa è disegnata così com'è, offrendo saggezza che si approfondisce ad ogni nuovo incontro.

Il viaggio dell'eroe non finisce. Il ritorno al mondo ordinario trova il discente trasformato, che vede pattern precedentemente invisibili, che riconosce vulnerabilità in sé e nell'ambiente, equipaggiato con framework per lo sviluppo continuo. Ma il viaggio continua perché la vulnerabilità psicologica continua, perché il threat landscape evolve, perché la comprensione si approfondisce con l'esperienza.

1.4 Struttura del Documento

Questo paper procede come segue. La Sezione 2 presenta il Framework Universale: i quattro moduli che costituiscono lo scheletro concettuale invariante applicabile a tutti i livelli di sviluppo. La Sezione 3 dettaglia la Modulazione Contestuale: come ogni modulo si adatta ai livelli Base, Intermedio, Avanzato e Specialistico mantenendo l'integrità concettuale. La

Sezione 4 affronta l'Architettura di Integrazione: come il framework educativo si connette e incorpora progressivamente la documentazione tecnica del CPF. La Sezione 5 fornisce una Guida all'Implementazione: considerazioni pratiche per il deployment di questo curriculum attraverso i contesti educativi. La Sezione 6 discute Assessment e Progressione: come viene valutato lo sviluppo del discente e come vengono gestite le transizioni tra livelli. La Sezione 7 conclude con riflessioni sul futuro dell'educazione alla cybersecurity psicologica.

2 Il Framework Universale: Quattro Moduli

Lo scheletro concettuale dell'educazione CPF comprende quattro moduli, ciascuno che affronta un dominio fondamentale di vulnerabilità psicologica. Questi moduli sono universali nel senso che i loro insight core si applicano a tutte le età, contesti e livelli di sviluppo. Ciò che varia non è l'insight ma la sua elaborazione, esemplificazione e profondità teorica.

I quattro moduli sono:

1. **Non Decidi Tu** — Le neuroscienze e la psicologia del decision-making pre-conscio
2. **Come Ti Fregano** — I meccanismi dell'influenza sociale e della manipolazione
3. **Il Gruppo Pensa Per Te** — Le dinamiche collettive e le loro implicazioni per la security
4. **Tu e le Macchine** — Le vulnerabilità dell'interazione umano-AI

Ogni modulo è progettato per funzionare sia indipendentemente sia come parte della sequenza integrata. La sequenza conta: il Modulo 1 stabilisce il riconoscimento fondamentale che il controllo cosciente è più limitato di quanto l'intuizione suggerisca; il Modulo 2 applica questo riconoscimento all'influenza interpersonale; il Modulo 3 si estende ai fenomeni collettivi; il Modulo 4 introduce le complicazioni nuove dei sistemi artificiali. Tuttavia, qualsiasi modulo può servire come punto d'ingresso per discenti con interessi o bisogni specifici.

2.1 Modulo 1: Non Decidi Tu

2.1.1 Insight Core

L'insight core del Modulo 1 è che le decisioni umane avvengono attraverso processi sostanzialmente al di fuori della consapevolezza cosciente, e che questi processi pre-consci sono sia sfruttabili sia largamente non modificabili attraverso il solo sforzo cosciente.

Questo insight contraddice intuizioni profonde sull'autonomia e l'autocontrollo. La maggior parte delle persone sperimenta le proprie decisioni come prodotti della deliberazione cosciente—"ci pensano" e poi "decidono." L'evidenza neuroscientifica e psicologica suggerisce che questa esperienza è parzialmente illusoria: la decisione è spesso già stata presa da processi pre-consci, e la deliberazione cosciente è una narrativa post-hoc che accompagna piuttosto che causare la decisione [13, 19].

2.1.2 Fondamenti Teorici

Il Modulo 1 attinge a tre tradizioni teoriche primarie:

Neuroscienze del Decision-Making.

- Gli esperimenti di Libet hanno dimostrato che il potenziale di prontezza del cervello—attività elettrica che indica preparazione motoria—precede la consapevolezza cosciente dell'intenzione di muoversi di circa 350 millisecondi [13]
- Soon et al. hanno esteso questo risultato, mostrando che i pattern di attività cerebrale potevano predire le decisioni fino a 10 secondi prima della consapevolezza cosciente [19]
- Questi risultati suggeriscono che la consapevolezza cosciente della decisione è effetto piuttosto che causa

Teoria del Dual-Process.

- Il framework System 1/System 2 di Kahneman fornisce un modello accessibile per comprendere la relazione tra elaborazione automatica e deliberata [9]
- Il System 1 opera automaticamente, velocemente, con poco senso di controllo volontario
- Il System 2 alloca attenzione alle attività mentali effortful, inclusi i calcoli complessi
- Crucialmente, il System 2 spesso serve come razionalizzatore post-hoc delle conclusioni del System 1 piuttosto che come valutatore indipendente

Ipotesi del Marcatore Somatico.

- La ricerca di Damasio dimostra che le emozioni e gli stati corporei influenzano sostanzialmente il decision-making attraverso meccanismi che bypassano la deliberazione cosciente [4]
- Il "gut feeling" non è metaforico ma riflette stati somatici reali che guidano la scelta attraverso canali pre-consci

2.1.3 Implicazioni per la Security

Le implicazioni per la security del controllo cosciente limitato sono profonde:

- Le decisioni di security prese sotto pressione temporale, carico cognitivo o attivazione emotiva sono dominate da processi pre-consci che potrebbero non allinearsi con gli interessi di security.
- Il training che mira solo alla conoscenza cosciente ("ricordati di controllare l'indirizzo del mittente") potrebbe fallire nell'influenzare il comportamento reale quando i processi pre-consci puntano diversamente.
- Gli attaccanti che possono triggerare stati emotivi specifici o carichi cognitivi possono prevedibilmente spostare il decision-making verso pattern sfruttabili.
- L'auto-assessment della vulnerabilità è inaffidabile perché i processi che creano vulnerabilità operano al di sotto della soglia dell'accesso cosciente.

2.1.4 Obiettivi di Apprendimento del Modulo

Completando il Modulo 1, i discenti saranno in grado di:

1. Spiegare l'evidenza del decision-making pre-conscio e le sue implicazioni per il comportamento di security.
2. Identificare situazioni in cui le proprie decisioni sono probabilmente dominate dall'elaborazione del System 1.
3. Riconoscere le condizioni (pressione temporale, carico cognitivo, attivazione emotiva) che spostano il decision-making lontano dal controllo deliberato.
4. Articolare perché il training tradizionale di security awareness ha efficacia limitata.
5. Descrivere la relazione tra questo modulo e le Categorie CPF 5 (Cognitive Overload), 7 (Stress Response) e 8 (Unconscious Processes).

2.1.5 Connessione alla Documentazione CPF

Il Modulo 1 introduce concetti che sono sistematicamente sviluppati nella Taxonomy CPF e teoricamente fondati nel Depth paper. Specificamente:

- La Categoria 5 della Taxonomy (Cognitive Overload Vulnerabilities) operazionalizza le dinamiche System 1/System 2 in indicatori misurabili.
- La Categoria 7 della Taxonomy (Stress Response Vulnerabilities) mappa la risposta neurobiologica allo stress sui comportamenti security-relevant.
- La Categoria 8 della Taxonomy (Unconscious Process Vulnerabilities) estende la fondazione neuroscientifica nel territorio psicoanalitico.
- La sezione del Depth paper su "The Integration Problem" spiega come queste disparate tradizioni teoriche sono riconciliate all'interno del framework CPF.

I discenti al livello Base ricevono queste connessioni come riferimenti in avanti—inviti all'esplorazione futura. I discenti ai livelli Avanzato e Specialistico si impegnano direttamente con il materiale referenziato.

2.2 Modulo 2: Come Ti Fregano

2.2.1 Insight Core

L'insight core del Modulo 2 è che la cognizione sociale umana si è evoluta per la cooperazione in piccoli gruppi ed è sistematicamente sfruttabile attraverso meccanismi di influenza prevedibili che operano largamente al di sotto della consapevolezza cosciente.

Gli esseri umani sono animali sociali la cui sopravvivenza dipendeva storicamente dalla cooperazione all'interno di piccoli gruppi di individui conosciuti. Le scorciatoie cognitive che hanno facilitato questa cooperazione—reciprocità, consistenza, social proof, deferenza all'autorità, liking, risposta alla scarsità—rimangono attive in ambienti moderni per i quali sono scarsamente adattate. La comunicazione digitale rimuove gli indizi che storicamente segnalavano affidabilità o inganno. Le reti globalizzate connettono gli individui con altri sconosciuti che possono sfruttare la programmazione sociale progettata per l'interazione su scala di villaggio.

2.2.2 Fondamenti Teorici

Il Modulo 2 attinge primariamente all'analisi sistematica dei principi di influenza di Robert Cialdini [3], integrata dalla psicologia evoluzionistica e dalle neuroscienze sociali.

I Sei Principi di Influenza. Cialdini ha identificato sei principi fondamentali attraverso i quali le persone sono influenzate:

1. **Reciprocità**: Sentiamo l'obbligo di restituire i favori, anche quelli non richiesti, anche quando il ritorno eccede il dono originale.
2. **Commitment e Consistenza**: Una volta presa una posizione, sperimentiamo pressione a comportarci coerentemente con quell'impegno.
3. **Social Proof**: Determiniamo il comportamento corretto osservando cosa fanno gli altri, specialmente in situazioni ambigue.
4. **Autorità**: Ci sottomettiamo alle figure di autorità percepite, spesso senza valutazione cosciente della loro reale competenza o legittimità.
5. **Liking**: Compliamo più prontamente con persone che ci piacciono, e il liking è influenzato da similarità, complimenti e mera familiarità.
6. **Scarsità**: Valutiamo le cose di più quando sono rare o stanno diventando rare, e questa valutazione distorce il decision-making.

Contesto di Psicologia Evoluzionistica. Questi meccanismi di influenza non sono arbitrari ma riflettono pressioni evolutive. La reciprocità ha abilitato la cooperazione oltre la parentela. La consistenza segnalava affidabilità ai potenziali cooperatori. Il social proof forniva informazioni sui pericoli e le opportunità ambientali. La deferenza all'autorità facilitava il coordinamento. Il liking promuoveva la coesione in-group. La risposta alla scarsità assicurava attenzione alle risorse rare.

Ricerca sull'Autorità di Milgram. Gli esperimenti sull'obbedienza di Stanley Milgram hanno dimostrato che persone ordinarie avrebbero somministrato scosse elettriche apparentemente pericolose a vittime innocenti quando istruite da una figura di autorità [15]. Questa ricerca ha rivelato la profondità della deferenza all'autorità—un override pre-conscio dell'etica e del giudizio personali.

2.2.3 Implicazioni per la Security

I meccanismi di influenza sociale si mappano direttamente sui vettori di attacco:

- **Reciprocità** abilita attacchi quid pro quo: "Ti ho aiutato con quel problema tecnico, ora potresti solo..."
- **Escalation del commitment** abilita escalation graduale delle richieste: piccola compliance iniziale porta a maggiore compliance successiva.
- **Social proof** abilita claim di azione collettiva: "I tuoi colleghi hanno già fornito le loro credenziali per l'audit."
- **Autorità** abilita attacchi di impersonation: CEO fraud, fake IT support, false affermazioni regolatorie.

- **Liking** abilita manipolazione basata sul rapport: stabilire connessione personale prima dello sfruttamento.
- **Scarsità** abilita attacchi di urgenza: "Questa offerta scade in 10 minuti" o "Solo 3 posti rimanenti."

2.2.4 Obiettivi di Apprendimento del Modulo

Completando il Modulo 2, i discenti saranno in grado di:

1. Identificare ciascuno dei sei principi di influenza di Cialdini in esempi del mondo reale.
2. Riconoscere quando i principi di influenza vengono impiegati contro di loro nelle comunicazioni digitali.
3. Spiegare le origini evolutive della suscettibilità a questi meccanismi di influenza.
4. Descrivere tipi di attacco specifici (phishing, pretexting, social engineering) in termini dei principi di influenza che sfruttano.
5. Articolare strategie difensive che tengano conto della natura pre-conscia della suscettibilità all'influenza.
6. Connettere questo modulo alle Categorie CPF 1 (Authority-Based), 2 (Temporal) e 3 (Social Influence) vulnerabilities.

2.2.5 Connessione alla Documentazione CPF

Il Modulo 2 introduce le categorie di vulnerabilità che formano le prime tre colonne della Taxonomy CPF:

- La Categoria 1 (Authority-Based Vulnerabilities) mappa sistematicamente i pattern di deferenza all'autorità inclusi compliance senza questionamento, effetti del gradiente di autorità e normalizzazione delle eccezioni executive.
- La Categoria 2 (Temporal Vulnerabilities) operazionalizza i meccanismi di scarsità e urgenza inclusi deadline-driven risk acceptance e hyperbolic discounting delle minacce future.
- La Categoria 3 (Social Influence Vulnerabilities) fornisce l'enumerazione completa degli indicatori derivati da Cialdini inclusi reciprocity exploitation, commitment escalation e social proof manipulation.

Il Dense Implementation Companion specifica come queste vulnerabilità si manifestano in comportamenti osservabili e come la detection logic può identificare i tentativi di sfruttamento. I discenti avanzati si impegnano direttamente con queste specifiche.

2.3 Modulo 3: Il Gruppo Pensa Per Te

2.3.1 Insight Core

L'insight core del Modulo 3 è che il comportamento collettivo emerge da dinamiche a livello di gruppo che non sono riducibili alla somma delle psicologie individuali, e che queste dinamiche creano vulnerabilità di security sistematiche invisibili all'analisi focalizzata sull'individuo.

Quando gli esseri umani si radunano in gruppi, accade qualcosa che trascende la cognizione individuale. I gruppi sviluppano le proprie assunzioni, difese e pattern di comportamento. Gli individui all'interno dei gruppi si comportano diversamente da come farebbero da soli, spesso senza consapevolezza di questa influenza. Il gruppo diventa un'entità psicologica con le proprie dinamiche, e queste dinamiche possono creare blind spot di security, amplificare il risk-taking, diffondere la responsabilità e sovrascrivere il giudizio individuale.

2.3.2 Fondamenti Teorici

Il Modulo 3 attinge primariamente alla teoria delle dinamiche di gruppo di Wilfred Bion [1], integrata dalla ricerca su groupthink, social loafing e comportamento collettivo.

Le Basic Assumption di Bion. Bion ha identificato tre basic assumption che i gruppi adottano inconsciamente quando affrontano l'ansia:

1. **Dependency (baD)**: Il gruppo si comporta come se si fosse riunito per essere protetto da un leader onnisciente, onnipotente. Nei contesti di security, questo si manifesta come over-reliance sui vendor di security, sull'autorità del CISO, o sui "silver bullet" tecnologici.
2. **Fight-Flight (baF)**: Il gruppo si comporta come se si fosse riunito per combattere o fuggire da un nemico. Nei contesti di security, questo si manifesta come difesa perimetrale aggressiva combinata con negazione delle minacce insider, o come evitamento e minimizzazione dei rischi riconosciuti.
3. **Pairing (baP)**: Il gruppo si comporta come se si fosse riunito per assistere alla nascita di un nuovo leader o idea che li salverà. Nei contesti di security, questo si manifesta come acquisizione continua di tool e speranza in soluzioni future mentre le vulnerabilità fondamentali rimangono non affrontate.

Queste basic assumption operano inconsciamente. I membri del gruppo non decidono di adottarle; vi vengono attirati da forze a livello di gruppo. La basic assumption fornisce sicurezza psicologica gestendo l'ansia, ma lo fa a costo di un engagement realistico con le minacce reali.

Groupthink. L'analisi di Irving Janis sui disastri di politica estera ha identificato il groupthink—una modalità di ragionamento collettivo in cui il desiderio di armonia sovrasta la valutazione realistica [8]. I sintomi del groupthink includono illusione di invulnerabilità, razionalizzazione collettiva, credenza nella moralità intrinseca, stereotipizzazione degli outgroup, pressione sui dissidenti, auto-censura, illusione di unanimità e mindguard auto-nominati.

Sistemi di Difesa Sociale. La ricerca di Isabel Menzies Lyth sui servizi infermieristici ha rivelato che le organizzazioni sviluppano "sistemi di difesa sociale"—strutture e pratiche che servono funzioni difensive inconsce contro l'ansia [14]. Questi sistemi appaiono irrazionali da una prospettiva di task ma sono altamente razionali da una prospettiva difensiva. Intervenire nei sistemi di difesa sociale senza affrontare l'ansia sottostante produce crisi psicologica piuttosto che miglioramento.

2.3.3 Implicazioni per la Security

Le dinamiche di gruppo creano vulnerabilità di security distintive:

- **Groupthink** produce blind spot di security dove la valutazione critica è soppressa per mantenere la coesione di gruppo.
- **Risky shift** (polarizzazione di gruppo) porta i team ad accettare rischi che nessun membro individuale accetterebbe da solo.
- **Diffusione della responsabilità** significa che i task di security posseduti da "tutti" sono effettivamente posseduti da nessuno.
- **Social loafing** riduce lo sforzo individuale sulle responsabilità di security collettive.
- **Bystander effect** paralizza l'incident response quando multiple persone assistono a un evento di security.
- **Basic assumption** distorcono la percezione e la risposta organizzativa alle minacce in modi prevedibili.

2.3.4 Obiettivi di Apprendimento del Modulo

Completando il Modulo 3, i discenti saranno in grado di:

1. Descrivere le tre basic assumption di Bion e identificare le loro manifestazioni nelle posture di security organizzativa.
2. Riconoscere i sintomi del groupthink nei processi decisionali di team.
3. Spiegare come diffusione della responsabilità, social loafing e bystander effect compromettono le funzioni di security.
4. Articolare perché gli interventi focalizzati sull'individuo sono insufficienti per le vulnerabilità a livello di gruppo.
5. Identificare indicatori di dinamiche di gruppo non salutari nei propri team e organizzazioni.
6. Connettere questo modulo alla Categoria CPF 6 (Group Dynamic Vulnerabilities) e agli indicatori correlati attraverso altre categorie.

2.3.5 Connessione alla Documentazione CPF

Il Modulo 3 fornisce la fondazione concettuale per la Categoria 6 della Taxonomy CPF, che include:

- Gli Indicatori 6.1-6.5 affrontano i fenomeni di gruppo classici (groupthink, risky shift, diffusione della responsabilità, social loafing, bystander effect)
- Gli Indicatori 6.6-6.8 operazionalizzano le basic assumption di Bion (dependency, fight-flight, pairing)

- Gli Indicatori 6.9-6.10 affrontano i fenomeni a livello organizzativo (organizational splitting, meccanismi di difesa collettivi)

La sezione del Depth paper su "The Integration Problem" spiega come la teoria psicoanalitica di gruppo di Bion è integrata con la psicologia cognitiva e tradotta in indicatori organizzativi misurabili. L'Intervention Framework fornisce guida specifica per affrontare le vulnerabilità a livello di gruppo, attingendo alla teoria del cambiamento organizzativo e alla metodologia di consultazione psicoanalitica.

2.4 Modulo 4: Tu e le Macchine

2.4.1 Insight Core

L'insight core del Modulo 4 è che l'interazione umano-AI introduce vulnerabilità psicologiche nuove che combinano e trasformano le vulnerabilità affrontate nei moduli precedenti, creando una categoria emergente di rischio di security che i framework esistenti non affrontano adeguatamente.

Man mano che i sistemi di intelligenza artificiale diventano integrali alle operazioni di security e alla vita quotidiana, gli esseri umani interagiscono con entità che non sono né umane né tool tradizionali. Queste interazioni attivano meccanismi psicologici progettati per contesti sociali umani, producendo distorsioni caratteristiche: antropomorfizzazione che attribuisce intenzioni umane a processi algoritmici, automation bias che over-trust le raccomandazioni delle macchine, algorithm aversion che paradossalmente rifiuta la guida dell'AI anche quando superiore al giudizio umano.

Queste vulnerabilità non sono semplicemente item aggiuntivi in una lista. Interagiscono con e trasformano le vulnerabilità dei moduli precedenti. La deferenza all'autorità si estende ai sistemi AI percepiti come autorevoli. Le dinamiche di gruppo ora includono team umano-AI con comportamenti collettivi nuovi. Il decision-making pre-conscio è influenzato da raccomandazioni AI che bypassano la valutazione deliberata.

2.4.2 Fondamenti Teorici

Il Modulo 4 rappresenta un'integrazione teorica nuova, poiché il CPF è tra i primi framework ad affrontare sistematicamente le vulnerabilità psicologiche AI-specific nei contesti di security. La base teorica attinge a:

Ricerca sull'Antropomorfizzazione. Gli esseri umani attribuiscono prontamente stati mentali, intenzioni ed emozioni a entità non-umane, inclusi i sistemi AI [6]. Questa antropomorfizzazione non è meramente metaforica ma influenza il comportamento reale: le persone che percepiscono l'AI come human-like sono più propense a fidarsi delle sue raccomandazioni, sentire connessione emotiva e essere manipolabili attraverso l'interfaccia AI.

Ricerca sull'Automation Bias. L'automation bias si riferisce alla tendenza a over-rely sui sistemi automatizzati, anche quando l'evidenza suggerisce che il sistema sta errando [16]. Questo bias produce errori caratteristici: errori di omissione (fallimento nel rilevare problemi perché il sistema non ha allertato) ed errori di commissione (seguire raccomandazioni automatizzate incorrette).

Ricerca sull'Algorithm Aversion. Paradossalmente, gli esseri umani a volte rifiutano le raccomandazioni algoritmiche anche quando gli algoritmi dimostratamente superano il giudizio

umano [5]. Questa algorithm aversion è particolarmente triggerata quando gli esseri umani osservano l'algoritmo fare errori, anche se i tassi di errore umano sono più alti.

Ricerca sul Human-AI Teaming. La ricerca emergente sulla collaborazione umano-AI rivela che i team misti esibiscono dinamiche nuove che non possono essere predette dalle sole dinamiche di gruppo umano. La calibrazione della fiducia, l'allocazione dei ruoli e l'attribuzione della responsabilità funzionano diversamente quando i membri del team includono sistemi AI.

2.4.3 Implicazioni per la Security

Le vulnerabilità AI-specific creano rischi di security distintivi:

- **Antropomorfizzazione** abilita la manipolazione attraverso interfacce AI: un attaccante che compromette un AI assistant guadagna la relazione di fiducia che l'umano ha sviluppato con quell'assistant.
- **Automation bias** produce over-reliance sui tool di security AI, vigilanza umana ridotta e atrofia delle skill nei team di security.
- **Algorithm aversion** produce sotto-utilizzo delle capacità di security AI, particolarmente dopo che si osservano errori dell'AI.
- **AI hallucination acceptance** porta gli esseri umani a fidarsi di output AI confidenti che sono fattualmente incorretti.
- **Human-AI team dysfunction** produce modalità di failure nuove nelle operazioni di security che includono componenti AI.
- **Adversarial AI exploitation** usa i bias AI-related degli esseri umani come vettori di attacco.

2.4.4 Obiettivi di Apprendimento del Modulo

Completando il Modulo 4, i discenti saranno in grado di:

1. Spiegare antropomorfizzazione, automation bias e algorithm aversion, con esempi da contesti di security.
2. Riconoscere le proprie tendenze verso bias AI-related nelle interazioni con sistemi AI.
3. Descrivere come le vulnerabilità AI-specific interagiscono con e trasformano le vulnerabilità dei moduli precedenti.
4. Articolare strategie di calibrazione della fiducia appropriate per i tool di security AI.
5. Identificare indicatori di dinamiche di team umano-AI non salutari.
6. Connettere questo modulo alla Categoria CPF 9 (AI-Specific Bias Vulnerabilities) e comprendere la sua interazione con altre categorie.

2.4.5 Connessione alla Documentazione CPF

Il Modulo 4 fornisce la fondazione concettuale per la Categoria 9 della Taxonomy CPF, che include:

- Gli Indicatori 9.1-9.3 affrontano i bias AI core (antropomorfizzazione, automation bias, algorithm aversion)
- Gli Indicatori 9.4-9.6 affrontano le dinamiche di autorità e fiducia AI (AI authority transfer, effetti uncanny valley, ML opacity trust)
- Gli Indicatori 9.7-9.10 affrontano le modalità di failure AI-specific (hallucination acceptance, human-AI team dysfunction, AI emotional manipulation, algorithmic fairness blindness)

Il Dense Implementation Companion fornisce specifiche operative per rilevare le vulnerabilità AI-specific, inclusa la quantificazione dell'antropomorfizzazione attraverso l'analisi dell'uso dei pronomi e del linguaggio emotivo, e la misurazione dell'automation bias attraverso il tracking dell'override rate.

3 Modulazione Contestuale: Quattro Livelli di Sviluppo

I quattro moduli descritti sopra costituiscono lo scheletro concettuale invariante dell'educazione CPF. Questo scheletro viene modulato attraverso quattro livelli di sviluppo, ciascuno calibrato su:

- **Complessità**: Profondità teorica e sofisticazione tecnica
- **Contesto**: Esempi, scenari e applicazioni rilevanti per la situazione del discente
- **Integrazione**: Connessione alla documentazione tecnica CPF
- **Outcome**: Capacità attese al completamento

I quattro livelli sono:

1. **Livello Base** (età 14-16, popolazione generale)
2. **Livello Intermedio** (età 16-19, pre-professionale)
3. **Livello Avanzato** (università, inizio carriera)
4. **Livello Specialistico** (professionisti della security)

Questi livelli non sono rigide fasce di età ma stadi di sviluppo che i discenti attraversano al proprio ritmo. Un quattordicenne con particolare attitudine potrebbe progredire rapidamente al livello Intermedio; un professionista che incontra il CPF per la prima volta inizia dal livello Base indipendentemente dall'età. I livelli descrivono gradienti di complessità, non categorie demografiche.

3.1 Livello Base: Ignizione

3.1.1 Target Audience

Il Livello Base è progettato per discenti senza esposizione precedente ai concetti di cybersecurity psicologica. Il target primario sono gli adolescenti (età 14-16) nell'istruzione secondaria, ma il livello è ugualmente appropriato per adulti che cercano un orientamento iniziale.

3.1.2 Filosofia Educativa

Al Livello Base, la filosofia educativa enfatizza l'*ignizione rispetto al completamento*. L'obiettivo non è una copertura comprensiva ma un engagement sufficiente a innescare l'esplorazione continua. Il Livello Base dovrebbe lasciare i discenti con:

- Riconoscimento che le loro decisioni sono meno autonome di quanto assumessero
- Consapevolezza di tecniche di manipolazione specifiche che potrebbero incontrare
- Vocabolario per discutere le vulnerabilità psicologiche
- Curiosità verso una comprensione più profonda
- Conoscenza che esistono risorse più approfondite (la documentazione CPF)

3.1.3 Esempi Contestuali

Gli esempi del Livello Base attingono da contesti familiari al target:

- **Manipolazione sui social media**: Come le piattaforme sfruttano i bias cognitivi per massimizzare l'engagement
- **Psicologia del gaming**: Loot box, meccaniche FOMO, pressione sociale negli ambienti multiplayer
- **Truffe online**: Phishing, romance scam, fake giveaway che targetizzano i giovani
- **Influenza dei pari**: Come social proof e conformità operano nei contesti sociali adolescenziali
- **AI assistant**: Antropomorfizzazione di Siri, Alexa, ChatGPT; calibrazione appropriata della fiducia

3.1.4 Adattamenti dei Moduli

Modulo 1 (Non Decidi Tu) al Livello Base:

Le neuroscienze sono semplificate in dimostrazioni accessibili. I discenti sperimentano piuttosto che studiare l'elaborazione pre-conscia attraverso:

- Dimostrazioni dell'effetto Stroop che mostrano l'elaborazione automatica
- Illusioni ottiche che dimostrano gap percezione-cognizione

- Semplici esperimenti di tempo di reazione che rivelano ritardi di elaborazione
- Discussione dei "gut feeling" e dell'intuizione nel decision-making

Il framework System 1/System 2 viene introdotto attraverso esempi quotidiani (giudizi istantanei sulle persone, matematica intuitiva versus calcolata) prima dell'applicazione ai contesti di security.

Modulo 2 (Come Ti Fregano) al Livello Base:

I principi di influenza vengono insegnati attraverso esercizi di riconoscimento usando esempi reali:

- Analisi di email di phishing per identificare urgenza (scarsità), claim di autorità e social proof
- Esame di pubblicità sui social media per sfruttamento di reciprocità e liking
- Review dell'influencer marketing per meccanismi di autorità e social proof
- Discussione di esperienze personali di tentativi di manipolazione

L'obiettivo è il riconoscimento dei pattern, non la teoria comprensiva. I discenti dovrebbero essere in grado di dire "questo è un gioco di scarsità" o "stanno usando l'autorità" quando incontrano manipolazione.

Modulo 3 (Il Gruppo Pensa Per Te) al Livello Base:

Le dinamiche di gruppo vengono introdotte attraverso scenari relazionabili:

- Perché le persone condividono informazioni non verificate quando "tutti" le condividono
- Come le chat di gruppo creano pressione a conformarsi
- Perché i bystander non intervengono nell'harassment online
- Come i clan di gaming e le community online sviluppano il proprio "groupthink"

Le basic assumption di Bion sono semplificate in concetti accessibili: "cercare un salvatore" (dependency), "noi contro loro" (fight-flight), "aspettare la prossima grande cosa" (pairing).

Modulo 4 (Tu e le Macchine) al Livello Base:

Le vulnerabilità AI vengono introdotte attraverso esperienza diretta:

- Esercizi con AI chatbot per dimostrare tendenze all'antropomorfizzazione
- Discussione di quando le raccomandazioni AI dovrebbero e non dovrebbero essere fidate
- Esame di contenuto AI-generated (immagini, testo) e rischi di hallucination
- Considerazione delle implicazioni privacy delle interazioni con AI assistant

3.1.5 Integrazione con la Documentazione CPF

Al Livello Base, la documentazione CPF viene referenziata ma non assegnata. La Taxonomy viene menzionata come "una mappa comprensiva di 100 modi diversi in cui queste vulnerabilità si manifestano nelle organizzazioni." Ai discenti viene detto che un'esplorazione più profonda è disponibile quando saranno pronti, ma non si assume che la perseguiranno.

La funzione del riferimento alla documentazione a questo livello è di:

- Segnalare che c'è altro da imparare (stimolazione della curiosità)
- Fornire un landmark per l'esplorazione auto-diretta futura
- Stabilire il CPF come un corpo di conoscenza coerente, non lezioni isolate

3.1.6 Assessment

L'assessment del Livello Base enfatizza il riconoscimento rispetto al recall:

- Dati scenari, identificare quali vulnerabilità psicologiche vengono sfruttate
- Dati esempi, classificare le tecniche di manipolazione per principio di influenza
- Esercizi di riflessione sulle esperienze personali con i fenomeni discussi
- Nessun requisito di produrre contenuto tecnico o impegnarsi con documentazione formale

3.1.7 Durata e Formato

Il Livello Base comprende quattro sessioni di 90-120 minuti ciascuna, per un totale di circa 8 ore di istruzione. Il formato può essere istruzione in classe, workshop o apprendimento online self-paced. Ogni sessione corrisponde a un modulo ma include componenti interattive e esperienziali sostanziali.

3.2 Livello Intermedio: Fondazione

3.2.1 Target Audience

Il Livello Intermedio serve discenti che hanno completato il Livello Base (o esposizione equivalente) e cercano una comprensione più profonda. Il target primario sono adolescenti più grandi (età 16-19) che si preparano alla vita professionale, ma il livello è appropriato per qualsiasi discente pronto a impegnarsi con materiale più complesso.

3.2.2 Filosofia Educativa

Al Livello Intermedio, la filosofia educativa si sposta dall'ignizione alla *costruzione delle fondazioni*. I discenti sviluppano:

- Comprensione sistematica delle categorie di vulnerabilità

- Capacità di analizzare incidenti del mondo reale attraverso la lente CPF
- Familiarità con la Taxonomy come risorsa di riferimento
- Competenza iniziale nell'applicare framework a situazioni nuove
- Consapevolezza dei percorsi professionali nella cybersecurity psicologica

3.2.3 Esempi Contestuali

Gli esempi del Livello Intermedio si espandono per includere contesti organizzativi e professionali:

- **Scenari workplace**: Situazioni del primo lavoro, contesti di stage, sfide professionali entry-level
- **Case study**: Incidenti di security documentati analizzati attraverso lente psicologica
- **Dinamiche organizzative**: Come le gerarchie workplace creano vulnerabilità all'autorità
- **Comunicazione professionale**: Vettori di manipolazione email, messaging e video call
- **Implicazioni di carriera**: Come la conoscenza di cybersecurity psicologica si applica a varie professioni

3.2.4 Adattamenti dei Moduli

Modulo 1 (Non Decidi Tu) al Livello Intermedio:

La fondazione teorica viene approfondita:

- Gli esperimenti di Libet vengono spiegati in dettaglio, incluse considerazioni metodologiche
- System 1/System 2 viene connesso a bias cognitivi specifici (availability, anchoring, affect heuristic)
- Viene introdotta l'ipotesi del marcatore somatico
- Le implicazioni per il decision-making di security vengono sistematicamente esplorate

I discenti si impegnano con fonti primarie (estratti da *Thinking, Fast and Slow* di Kahneman) e analisi secondaria.

Modulo 2 (Come Ti Fregano) al Livello Intermedio:

Il framework di influenza diventa strumento analitico:

- Ciascuno dei principi di Cialdini viene studiato in profondità con evidenza sperimentale

- Gli esperimenti sull'autorità di Milgram vengono esaminati, incluse considerazioni etiche
- Incidenti di security reali (Business Email Compromise, campagne di phishing major) vengono analizzati
- Strategie difensive vengono sviluppate e criticate

I discenti praticano l'analisi degli incidenti usando le Categorie 1-3 della Taxonomy come riferimento.

Modulo 3 (Il Gruppo Pensa Per Te) al Livello Intermedio:

La teoria delle dinamiche di gruppo viene introdotta propriamente:

- Le basic assumption di Bion vengono insegnate con esempi clinici e organizzativi
- Il modello di groupthink di Janis viene applicato ai failure di security
- Viene introdotto il concetto di sistemi di difesa sociale di Menzies Lyth
- Case study organizzativi dimostrano vulnerabilità a livello di gruppo

I discenti analizzano le dinamiche di team in contesti familiari (progetti scolastici, team sportivi, guild di gaming) usando framework di dinamiche di gruppo.

Modulo 4 (Tu e le Macchine) al Livello Intermedio:

La psicologia AI viene connessa alla letteratura di ricerca:

- Viene reviewata la ricerca sull'antropomorfizzazione
- Vengono esaminati gli studi sull'automation bias, incluse conseguenze del mondo reale
- Vengono discusse le sfide del human-AI teaming
- Vengono considerate le capacità AI emergenti e le loro implicazioni psicologiche

I discenti valutano criticamente i sistemi AI che usano, applicando framework di calibrazione della fiducia.

3.2.5 Integrazione con la Documentazione CPF

Al Livello Intermedio, la Taxonomy diventa un riferimento di lavoro:

- I discenti vengono introdotti alla matrice completa 10×10
- Indicatori specifici vengono referenziati nel contenuto del modulo
- Gli esercizi richiedono di localizzare e applicare indicatori della Taxonomy
- La struttura della Taxonomy (categorie, indicatori, attack vector mapping) viene spiegata

Il Depth paper viene menzionato come la fondazione teorica sottostante la struttura della Taxonomy. I discenti comprendono che un grounding teorico più profondo è disponibile ma non sono tenuti a impegnarsi con esso.

3.2.6 Assessment

L'assessment del Livello Intermedio include componenti analitici:

- Analisi di incidenti: Data una descrizione di incidente di security, identificare le vulnerabilità psicologiche sfruttate usando la terminologia della Taxonomy
- Costruzione di scenari: Creare scenari di attacco realistici che sfruttano categorie di vulnerabilità specificate
- Paper di riflessione: Analizzare esperienze personali o osservate usando framework CPF
- Navigazione della Taxonomy: Dimostrare capacità di localizzare indicatori rilevanti per situazioni date

3.2.7 Durata e Formato

Il Livello Intermedio comprende otto sessioni di 90-120 minuti ciascuna, per un totale di circa 16 ore di istruzione. È atteso tempo aggiuntivo di studio autonomo (circa 8 ore) per review della documentazione e completamento degli assignment. Il formato può includere istruzione in classe, discussione seminariale o apprendimento online strutturato con interazione tra pari.

3.3 Livello Avanzato: Elaborazione

3.3.1 Target Audience

Il Livello Avanzato serve discenti che perseguono carriere professionali o accademiche che coinvolgeranno la cybersecurity psicologica. Il target primario sono studenti universitari in campi rilevanti (cybersecurity, psicologia, organizational behavior, human-computer interaction) e professionisti a inizio carriera. Il completamento del Livello Intermedio (o competenza equivalente dimostrata) è prerequisito.

3.3.2 Filosofia Educativa

Al Livello Avanzato, la filosofia educativa enfatizza *elaborazione e applicazione*. I discenti sviluppano:

- Comprensione profonda dei fondamenti teorici attraverso tutte le categorie CPF
- Competenza nell'applicare framework a situazioni organizzative complesse
- Familiarità con le metodologie di implementazione (Dense paper)
- Introduzione agli approcci di intervento (Intervention Framework)
- Capacità di contribuire all'assessment della security organizzativa

3.3.3 Esempi Contestuali

Gli esempi del Livello Avanzato si impegnano con complessità di scala professionale:

- **Advanced Persistent Threat**: Attacchi multi-stage che sfruttano vulnerabilità psicologiche nel tempo
- **Operazioni nation-state**: Cyber warfare con componenti psicologiche
- **Insider threat**: Dinamiche motivazionali e organizzative complesse
- **Trasformazione organizzativa**: Iniziative di cambiamento della security culture
- **Regulatory compliance**: Fattori psicologici nei programmi di compliance
- **Incident response**: Dimensioni psicologiche della gestione delle crisi

3.3.4 Adattamenti dei Moduli

Al Livello Avanzato, i moduli si espandono oltre lo scheletro dei quattro moduli per comprendere tutte e dieci le categorie CPF. I quattro moduli originali diventano unità estese che incorporano categorie correlate:

Unità 1: Vulnerabilità Cognitive Individuali

- Il contenuto del Modulo 1 si espande al trattamento completo delle Categorie 5 (Cognitive Overload) e 7 (Stress Response)
- La Categoria 8 (Unconscious Processes) viene introdotta con fondamenti psicoanalitici dal Depth paper
- La ricerca neuroscientifica viene reviewata in profondità
- Vengono discussi i principi di design degli strumenti di assessment

Unità 2: Meccanismi di Influenza Sociale

- Il contenuto del Modulo 2 si espande al trattamento sistematico delle Categorie 1 (Authority), 2 (Temporal) e 3 (Social Influence)
- Il set completo di indicatori viene reviewato con definizioni operative
- L'attack vector mapping viene esaminato in dettaglio
- Vengono introdotte le specifiche del Dense paper per la detection logic

Unità 3: Dinamiche Collettive

- Il contenuto del Modulo 3 si espande al trattamento completo della Categoria 6 (Group Dynamics)
- Viene aggiunta la Categoria 4 (Affective Vulnerabilities), incluse le relazioni oggettuali kleiniane
- Viene studiata la psicodinamica organizzativa (Menzies Lyth, Hirschhorn)

- Vengono introdotti i principi dell'Intervention Framework per l'intervento a livello di gruppo

Unità 4: Vulnerabilità Emergenti

- Il contenuto del Modulo 4 si espande al trattamento completo della Categoria 9 (AI-Specific Biases)
- La Categoria 10 (Critical Convergent States) viene introdotta con fondazione di systems theory
- Viene spiegato l'interdependency modeling (reti bayesiane)
- Vengono discusse le sfide di integrazione attraverso le categorie

3.3.5 Integrazione con la Documentazione CPF

Al Livello Avanzato, è atteso un engagement completo con la documentazione CPF:

La Taxonomy è il riferimento primario, con tutti i 100 indicatori studiati.

Il Dense Implementation Companion viene introdotto per la specifica operativa:

- Lo schema OFTLISRV viene spiegato e applicato
- La matematica della detection logic (distanza di Mahalanobis, modellazione temporale) viene reviewata
- Vengono discussi i pathway di integrazione SOC
- Viene esaminata la metodologia di validazione

L'Intervention Framework viene introdotto per la metodologia di remediation:

- Vengono studiati i principi di intervention design
- Vengono spiegate le dinamiche di resistenza
- Viene reviewata l'integrazione della change theory (Lewin, Schein, Kotter)
- Vengono discusse le considerazioni di scaling

Il Depth paper serve come riferimento teorico durante tutto il corso:

- L'analisi del problema di integrazione fornisce contesto per la struttura del framework
- La sezione sull'architettura di assessment informa la comprensione delle sfide di misurazione
- La sezione sull'interdependency modeling fonda l'approccio delle reti bayesiane
- La sezione sull'imperativo di validazione incornicia le opportunità di ricerca

3.3.6 Assessment

L'assessment del Livello Avanzato richiede competenza dimostrata con la documentazione completa:

- **Analisi comprensiva di incidenti**: Analisi CPF completa di incidenti di security complessi usando tutte le categorie e la documentazione rilevanti
- **Design di assessment**: Sviluppare strumenti di assessment per categorie di vulnerabilità specificate seguendo lo schema OFTLISRV
- **Proposta di intervento**: Progettare un approccio di intervento per vulnerabilità organizzativa usando la metodologia dell'Intervention Framework
- **Proposta di ricerca**: Identificare opportunità di validazione e progettare approccio di studio
- **Presentazione**: Comunicare concetti e analisi CPF a un pubblico non specialistico

3.3.7 Durata e Formato

Il Livello Avanzato comprende un corso semestrale completo (circa 45 ore di istruzione) più studio indipendente sostanziale (circa 90 ore) per review della documentazione, completamento degli assignment e lavoro di progetto. Il formato tipicamente combina lezioni, seminari, discussioni di case study e apprendimento basato su progetto.

3.4 Livello Specialistico: Mastery

3.4.1 Target Audience

Il Livello Specialistico serve professionisti della security che applicheranno il CPF in contesti operativi. Il target include analisti SOC, consultant di security, psicologi organizzativi che lavorano in contesti di security e ricercatori che contribuiscono allo sviluppo del framework. Il completamento del Livello Avanzato (o competenza equivalente dimostrata) è prerequisito.

3.4.2 Filosofia Educativa

Al Livello Specialistico, la filosofia educativa enfatizza *mastery e contributo*. I discenti sviluppano:

- Competenza operativa nell'assessment e intervento CPF
- Capacità di implementare detection logic in ambienti SOC
- Expertise nella metodologia di assessment organizzativo
- Capacità di condurre programmi di intervento
- Potenziale di contribuire all'estensione e validazione del framework

3.4.3 Esempi Contestuali

Il Livello Specialistico lavora con realtà operative:

- **Integrazione SOC live**: Implementazione degli indicatori CPF in operazioni di security reali
- **Assessment organizzativo**: Conduzione di assessment CPF completi nelle organizzazioni
- **Implementazione di interventi**: Gestione di programmi di cambiamento che affrontano vulnerabilità psicologiche
- **Esecuzione di ricerca**: Progettazione e conduzione di studi di validazione
- **Estensione del framework**: Sviluppo di nuovi indicatori o raffinamento di quelli esistenti

3.4.4 Struttura del Curriculum

Il Livello Specialistico va oltre la struttura a moduli verso lo sviluppo basato su competenze in tre track:

Track A: Detection e Monitoring

- Mastery completa del Dense Implementation Companion
- Implementazione di detection logic in sistemi operativi
- Modellazione di reti bayesiane per analisi delle interdipendenze
- Esecuzione della metodologia di validazione
- Integrazione del workflow SOC

Track B: Assessment e Consultazione

- Mastery completa dell'architettura di assessment
- Metodologia di assessment organizzativo
- Implementazione della protezione della privacy
- Interpretazione e comunicazione dei risultati
- Sviluppo delle skill di consultazione

Track C: Intervento e Cambiamento

- Mastery completa dell'Intervention Framework
- Implementazione del change management
- Skill di navigazione della resistenza
- Metodologia di scaling
- Valutazione degli outcome

Gli specialisti possono focalizzarsi su un track o sviluppare competenza attraverso track multipli.

3.4.5 Integrazione con la Documentazione CPF

Al Livello Specialistico, tutta la documentazione è riferimento operativo:

- **Taxonomy**: Memorizzazione completa degli indicatori; capacità di applicare senza riferimento
- **Dense paper**: Implementazione operativa di tutte le specifiche
- **Intervention Framework**: Applicazione pratica di tutti i principi di intervento
- **Depth paper**: Risorsa teorica per situazioni complesse e estensione del framework

3.4.6 Assessment

L'assessment del Livello Specialistico è basato su competenze e pratico:

- **Track A**: Implementare detection logic funzionale per indicatori specificati; dimostrare integrazione SOC operativa
- **Track B**: Condurre assessment organizzativo; consegnare report e presentazione di qualità professionale
- **Track C**: Progettare e iniziare programma di intervento; documentare metodologia e risultati iniziali
- **Tutti i track**: Contribuire allo sviluppo del framework attraverso ricerca di validazione, raffinamento degli indicatori o estensione della documentazione

3.4.7 Durata e Formato

Il Livello Specialistico è sviluppo professionale continuo piuttosto che corso delimitato. La specializzazione iniziale richiede circa 100-200 ore di sviluppo focalizzato più esperienza pratica supervisionata. Lo sviluppo continuo avviene attraverso pratica, engagement con la community e contributo all'evoluzione del framework.

4 Architettura di Integrazione

Il CPF Educational Framework è progettato per integrarsi con la documentazione tecnica CPF attraverso esposizione progressiva e engagement che si approfondisce. Questa sezione dettaglia come i quattro paper—Taxonomy, Dense Implementation Companion, Intervention Framework e Depth—funzionano all'interno della struttura educativa.

4.1 Funzioni dei Documenti nel Viaggio di Apprendimento

Ogni paper CPF serve una funzione pedagogica distinta:

4.1.1 La Taxonomy: La Mappa

La Taxonomy fornisce l'enumerazione comprensiva delle vulnerabilità psicologiche—100 indicatori attraverso 10 categorie. Nel viaggio educativo, funziona come:

- **Al Livello Base**: Un landmark distante—i discenti sanno che esiste e rappresenta il territorio completo
- **Al Livello Intermedio**: Un riferimento di lavoro—i discenti navigano sezioni specifiche e localizzano indicatori rilevanti
- **Al Livello Avanzato**: Un framework comprensivo—i discenti padroneggiano la struttura completa e comprendono le relazioni tra categorie
- **Al Livello Specialistico**: Uno strumento operativo—i practitioner applicano automaticamente gli indicatori e contribuiscono al raffinamento

4.1.2 Il Dense Implementation Companion: Il Manuale Tecnico

Il Dense paper traduce gli indicatori concettuali in specifiche operative—detection logic, telemetry source, response protocol. Funziona come:

- **Ai Livelli Base e Intermedio**: Non direttamente impegnato; menzionato come esistente per applicazione avanzata
- **Al Livello Avanzato**: Introdotto e studiato; i discenti comprendono lo schema OFTLISRV e i fondamenti matematici
- **Al Livello Specialistico**: Riferimento operativo; i practitioner implementano le specifiche in ambienti reali

4.1.3 L'Intervention Framework: Il Dono del Ritorno

L'Intervention Framework fornisce metodologia per affrontare le vulnerabilità identificate—intervention design, navigazione della resistenza, scaling. Funziona come:

- **Ai Livelli Base e Intermedio**: Non direttamente impegnato; menzionato come esistente per la remediation
- **Al Livello Avanzato**: Introdotto e studiato; i discenti comprendono i principi di intervento e l'integrazione della change theory
- **Al Livello Specialistico**: Guida pratica; i practitioner progettano e implementano programmi di intervento

4.1.4 Il Depth Paper: Il Mentore

Il Depth paper fornisce fondamenti teorici—sfide di integrazione, architettura di assessment, interdependency modeling. Nella metafora del viaggio dell'eroe, funziona come il mentore che:

- Appare quando è necessaria una comprensione più profonda

- Spiega perché la mappa è disegnata così com'è
- Fornisce saggezza che si approfondisce ad ogni incontro
- Rimane disponibile durante tutto il viaggio per guida

Educativamente:

- **Al Livello Base**: Non direttamente impegnato; rappresenta la "profondità sotto" che attende esplorazione
- **Al Livello Intermedio**: Estratto; sezioni specifiche illuminano punti teorici
- **Al Livello Avanzato**: Studiato; i discenti si impegnano con le sfide di integrazione e gli impegni teorici
- **Al Livello Specialistico**: Risorsa di riferimento; i practitioner vi ritornano quando affrontano situazioni complesse

4.2 Engagement Progressivo con la Documentazione

La seguente tabella riassume l'engagement con la documentazione attraverso i livelli:

Table 1: Engagement con la Documentazione per Livello

Documento	Base	Intermedio	Avanzato	Specialistico
Taxonomy	Riferimento	Uso di lavoro	Mastery completa	Operativo
Dense	Menzione	Menzione	Studio	Implementazione
Intervention	Menzione	Menzione	Studio	Applicazione
Depth	Accenno	Estratto	Studio	Riferimento

4.3 Architettura dei Cross-Reference

All'interno di ogni modulo a ogni livello, cross-reference espliciti alla documentazione creano percorsi per esplorazione più profonda:

Esempio: Modulo 2 (Come Ti Fregano)

- **Livello Base**: "La lista completa delle vulnerabilità all'autorità è nella Taxonomy CPF, Categoria 1. Quando sarai pronto ad andare più in profondità, è lì che troverai indicatori come 'Authority gradient inhibiting security reporting' e 'Executive exception normalization.' "
- **Livello Intermedio**: "Rivedi gli indicatori 1.1 fino a 1.10 della Taxonomy. Per ogni indicatore, identifica un esempio del mondo reale dalla tua esperienza o ricerca. Presta particolare attenzione a come questi indicatori potrebbero apparire nel tuo futuro workplace."
- **Livello Avanzato**: "Il Dense Implementation Companion specifica detection logic per le vulnerabilità authority-based usando funzioni di compliance rate e Bayesian legitimacy assessment. Rivedi la sezione 3.1 e progetta un approccio di detection per l'indicatore 1.1 adattato a un contesto organizzativo specifico."

- **Livello Specialistico**: "Implementa la specifica OFTLISRV per gli indicatori 1.1-1.3 nel tuo ambiente SOC. Documenta telemetry source, processo di calibrazione delle threshold e metodologia di validazione."

4.4 Il Pattern di Riferimento alla Triade

Durante tutto il framework educativo, un pattern consistente referenzia i tre documenti operativi come triade:

> "Il CPF fornisce tre risorse integrate: la *Taxonomy* ti dice **cosa** cercare, il *Dense Implementation Companion* ti dice **come** rilevarlo, e l'*Intervention Framework* ti dice **cosa fare al riguardo**. Questi tre documenti formano un loop chiuso dall'identificazione attraverso la detection alla remediation."

Questo riferimento alla triade appare a ogni livello, con specificità crescente:

- **Livello Base**: La triade viene menzionata come il sistema completo che attende esplorazione
- **Livello Intermedio**: La struttura della triade viene spiegata e la Taxonomy viene attivamente usata
- **Livello Avanzato**: Tutti e tre i documenti vengono studiati; l'integrazione viene compresa
- **Livello Specialistico**: Tutti e tre i documenti vengono applicati; l'integrazione viene praticata

Il Depth paper sta a parte dalla triade come fondazione teorica sottostante tutti e tre. È il "perché" dietro il "cosa," "come" e "cosa fare."

5 Guida all'Implementazione

Questa sezione fornisce guida pratica per implementare il CPF Educational Framework attraverso vari contesti educativi.

5.1 Implementazione nell'Istruzione Secondaria

5.1.1 Integrazione Curricolare

Il contenuto del Livello Base può essere integrato nei curricula dell'istruzione secondaria esistenti attraverso:

- **Computer Science / Digital Literacy**: Casa naturale per i Moduli 2 e 4
- **Psicologia / Social Studies**: Casa naturale per i Moduli 1 e 3
- **Educazione alla Salute**: Connessione a stress, manipolazione e benessere
- **Unità Standalone**: Intensivo di quattro settimane all'interno di qualsiasi corso rilevante

5.1.2 Preparazione degli Insegnanti

Gli insegnanti che implementano il Livello Base dovrebbero:

- Completare almeno il Livello Intermedio essi stessi
- Comprendere il contesto CPF più ampio anche se non lo insegnano
- Avere accesso alla documentazione per domande degli studenti che eccedono il Livello Base
- Connettersi con la community CPF per supporto e aggiornamenti

5.1.3 Requisiti di Risorse

L'implementazione del Livello Base richiede:

- Accesso a Internet per dimostrazioni e esempi
- Capacità di proiezione per contenuto visivo
- Nessun software specializzato o attrezzatura di laboratorio
- Raccomandato: Accesso a AI assistant per dimostrazioni del Modulo 4

5.2 Implementazione nell'Istruzione Superiore

5.2.1 Posizionamento del Corso

Il contenuto del Livello Avanzato può essere implementato come:

- **Corso Dedicato**: "Psychological Cybersecurity" o "Human Factors in Security"
- **Componente di Corso**: Modulo all'interno di corsi più ampi di cybersecurity, psicologia organizzativa o HCI
- **Seminario Graduate**: Engagement focalizzato sulla ricerca con validazione e estensione del framework
- **Certificato Professionale**: Continuing education per professionisti della security

5.2.2 Considerazioni sui Prerequisiti

Il Livello Avanzato assume:

- Familiarità di base con concetti psicologici (o iscrizione concorrente a corsi di psicologia)
- Comprensione fondamentale dell'information security (o iscrizione concorrente)
- Literacy statistica sufficiente per comprendere la matematica della detection logic
- Literacy di ricerca sufficiente per impegnarsi con letteratura accademica

Il Livello Intermedio può essere offerto come corso ponte per studenti privi di prerequisiti.

5.2.3 Allineamento dell'Assessment

L'implementazione nell'istruzione superiore dovrebbe allinearsi con i requisiti di assessment istituzionali:

- Esami scritti possono assessare conoscenza teorica
- Analisi di case study può assessare competenza di applicazione
- Lavoro di progetto può assessare integrazione e sintesi
- Proposte di ricerca possono assessare potenziale di contributo

5.3 Implementazione nel Training Professionale

5.3.1 Deployment Organizzativo

Le organizzazioni che implementano l'educazione CPF dovrebbero considerare:

- **Ampiezza vs. Profondità**: Livello Base per tutti i dipendenti; Avanzato/Specialistico per i team di security
- **Integrazione con Training Esistente**: I moduli CPF possono supplementare o sostituire i programmi di awareness convenzionali
- **Integrazione dell'Assessment**: L'educazione CPF può connettersi ai programmi di assessment CPF organizzativi
- **Considerazioni Culturali**: I concetti CPF dovrebbero allinearsi con i valori organizzativi e lo stile di comunicazione

5.3.2 Sviluppo degli Specialisti

Le organizzazioni che sviluppano specialisti CPF interni dovrebbero:

- Identificare candidati con background appropriato (security + interesse per la psicologia)
- Fornire sviluppo strutturato attraverso tutti e quattro i livelli
- Supportare l'applicazione pratica con progetti di assessment organizzativo
- Connettere gli specialisti con la community CPF più ampia

5.4 Apprendimento Auto-Diretto

5.4.1 Percorso del Discente Individuale

I discenti auto-diretti possono progredire attraverso il framework usando:

- Questo paper come guida al curriculum

- La documentazione CPF come risorse primarie
- AI tutor (come Claude o simili) per apprendimento interattivo
- Community online per interazione tra pari
- Applicazione pratica nei contesti disponibili (security personale, osservazione sul workplace)

5.4.2 Apprendimento Assistito da AI

I large language model possono servire come risorse educative:

- Spiegando concetti a livelli di complessità appropriati
- Generando scenari di pratica per l'analisi
- Fornendo feedback sui tentativi di analisi del discente
- Rispondendo a domande sul contenuto della documentazione
- Adattando ritmo e focus ai bisogni individuali del discente

Questo modello di apprendimento assistito da AI si allinea con la filosofia educativa che l'educazione formale fornisce ignizione mentre lo sviluppo successivo avviene attraverso esplorazione auto-diretta con gli strumenti disponibili.

6 Assessment e Progressione

6.1 Framework delle Competenze

La progressione del discente viene assessata contro competenze organizzate per modulo e livello:

6.1.1 Competenze del Modulo 1

- **Base**: Può spiegare che le decisioni avvengono parzialmente al di fuori della consapevolezza cosciente; può identificare contesti decisionali ad alto rischio
- **Intermedio**: Può descrivere la teoria del dual-process e applicarla a scenari di security; può identificare bias cognitivi in esempi
- **Avanzato**: Può analizzare vulnerabilità del decision-making usando il framework completo delle Categorie 5/7/8; può progettare approcci di assessment
- **Specialistico**: Può implementare detection logic per vulnerabilità cognitive; può condurre assessment organizzativo

6.1.2 Competenze del Modulo 2

- **Base**: Può riconoscere tecniche di influenza di base in esempi; può identificare manipolazione nelle comunicazioni personali
- **Intermedio**: Può analizzare incidenti usando il framework di influenza completo; può progettare approcci difensivi
- **Avanzato**: Può applicare sistematicamente gli indicatori delle Categorie 1/2/3; può progettare metodologie di detection
- **Specialistico**: Può implementare detection dell'influenza sociale in sistemi operativi; può condurre assessment della vulnerabilità organizzativa

6.1.3 Competenze del Modulo 3

- **Base**: Può riconoscere dinamiche di gruppo di base in contesti familiari; può identificare pressione alla conformità
- **Intermedio**: Può analizzare dinamiche di team usando framework di Bion e groupthink; può identificare pattern organizzativi
- **Avanzato**: Può applicare il framework completo della Categoria 6; può progettare interventi a livello di gruppo
- **Specialistico**: Può assessare dinamiche di gruppo organizzative; può implementare programmi di intervento

6.1.4 Competenze del Modulo 4

- **Base**: Può riconoscere l'antropomorfizzazione in sé e negli altri; può calibrare appropriatamente la fiducia nell'AI
- **Intermedio**: Può analizzare pattern di interazione umano-AI; può identificare rischi di automation bias
- **Avanzato**: Può applicare il framework completo della Categoria 9; può progettare protocolli di interazione AI
- **Specialistico**: Può assessare dinamiche di team umano-AI; può implementare operazioni di security AI-aware

6.2 Criteri di Progressione

6.2.1 Da Base a Intermedio

La progressione richiede dimostrazione di:

- Competenza di riconoscimento attraverso tutti e quattro i moduli
- Curiosità di engagement (desiderio di imparare di più)
- Padronanza del vocabolario di base
- Nessun assessment formale richiesto; auto-progressione accettabile

6.2.2 Da Intermedio ad Avanzato

La progressione richiede dimostrazione di:

- Competenza analitica attraverso tutti e quattro i moduli
- Familiarità con la Taxonomy (può navigare e applicare)
- Capacità di analisi degli incidenti
- Raccomandato: Assessment formale o portfolio review

6.2.3 Da Avanzato a Specialistico

La progressione richiede dimostrazione di:

- Mastery comprensiva del framework
- Fluenza nella documentazione (può lavorare con tutti e quattro i paper)
- Esperienza di applicazione pratica
- Richiesto: Assessment pratico supervisionato o credenziale professionale

6.3 Sviluppo Continuo

Il CPF Educational Framework non termina al Livello Specialistico. Lo sviluppo continuo include:

- **Raffinamento della pratica**: Migliorare l'applicazione attraverso l'esperienza
- **Contributo al framework**: Estendere la validazione, raffinare gli indicatori, sviluppare applicazioni
- **Engagement con la community**: Condividere conoscenza, fare mentoring a practitioner in sviluppo
- **Adattamento all'evoluzione**: Aggiornare la conoscenza man mano che threat landscape e framework evolvono

7 Conclusione: L'Educazione come Viaggio Continuo

7.1 Sintesi del Framework

Il CPF Educational Framework fornisce un approccio strutturato allo sviluppo della literacy in cybersecurity psicologica attraverso l'intero spettro dalla consapevolezza iniziale alla mastery professionale. Le sue caratteristiche chiave includono:

- **Scheletro universale**: Quattro moduli che affrontano domini fondamentali di vulnerabilità, applicabili a tutti i livelli

- **Modulazione contestuale**: Adattamento di complessità, esempi e engagement con la documentazione allo sviluppo del discente
- **Integrazione progressiva**: Incorporazione sistematica della documentazione tecnica CPF man mano che i discenti avanzano
- **Filosofia dell'ignizione**: Educazione come scintilla per lo sviluppo auto-diretto continuo piuttosto che credenziale completata

7.2 Il Viaggio Continuo

La metafora del viaggio dell'eroe rimane adatta per descrivere la relazione del discente con l'educazione CPF. Non c'è destinazione finale. Il viaggio continua perché:

- **La vulnerabilità psicologica è permanente**: A differenza delle vulnerabilità tecniche che possono essere patchate, l'architettura cognitiva umana rimane sfruttabile
- **Il threat landscape evolve**: Gli attaccanti sviluppano tecniche nuove che sfruttano vulnerabilità durature in modi nuovi
- **La comprensione si approfondisce**: Ogni ritorno ai concetti fondamentali rivela nuove implicazioni e applicazioni
- **Il framework si sviluppa**: Il CPF stesso evolve attraverso validazione, raffinamento e estensione

Il practitioner educato non è uno che ha "completato" il training CPF ma uno che ha interiorizzato i suoi pattern di pensiero, che vede vulnerabilità psicologiche dove altri vedono solo sistemi tecnici, che riconosce in se stesso gli stessi meccanismi che identifica nelle organizzazioni.

7.3 La Visione Più Ampia

Il CPF Educational Framework serve una visione più ampia dello sviluppo professionale individuale. Se la literacy in cybersecurity psicologica diventa diffusa—se i pattern insegnati in questi moduli diventano conoscenza comune—il landscape della security cambia fondamentalmente.

Considerate un mondo dove ogni dipendente riconosce la manipolazione dell'autorità quando la incontra, dove ogni team comprende come le dinamiche di gruppo creano blind spot, dove ogni organizzazione progetta sistemi tenendo conto delle limitazioni cognitive, dove ogni interazione AI avviene con appropriata calibrazione della fiducia. Questo non è un mondo senza incidenti di security. La vulnerabilità umana è permanente. Ma è un mondo dove lo sfruttamento è più difficile, dove le difese sono informate da modelli accurati della psicologia umana, dove il fallimento persistente della security awareness a livello conscio è stato sostituito da un'educazione che coinvolge i meccanismi reali del decision-making umano.

Il CPF Educational Framework è un contributo verso quel mondo. Il viaggio inizia con il riconoscimento che "non decidi tu"—che il sé che legge queste parole è meno autonomo di quanto l'intuizione suggerisca. Continua attraverso la comprensione di come questa autonomia limitata viene sfruttata, come i gruppi amplificano le vulnerabilità individuali, come i sistemi artificiali introducono complicazioni nuove. Non finisce mai, perché il territorio che mappa è il paesaggio permanente della cognizione umana.

La profondità sotto attende esplorazione. Il viaggio continua.

Nota sulla Composizione Assistita da AI

Questo manoscritto presenta il framework educativo originale e i contributi intellettuali dell'autore. Nel processo di composizione, l'autore ha utilizzato un large language model come strumento ausiliario per il raffinamento stilistico e la consistenza formattativa. Le idee core, l'architettura educativa, la metodologia di integrazione e l'analisi pedagogica sono esclusivamente prodotto dell'expertise dell'autore. L'autore è interamente responsabile per l'accuratezza e l'integrità del contenuto pubblicato.

Ringraziamenti

L'autore riconosce il lavoro fondamentale nell'educazione alla cybersecurity, nella ricerca psicologica e nello sviluppo organizzativo su cui questo framework educativo si costruisce. Un riconoscimento speciale va ai ricercatori i cui contributi teorici—Kahneman, Cialdini, Bion, Klein, Milgram e molti altri—rendono possibile questa integrazione.

References

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

[2] Campbell, J. (1949). *The hero with a thousand faces*. New York: Pantheon Books.

[3] Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York: Collins.

[4] Damasio, A. (1994). *Descartes' error: Emotion, reason, and the human brain*. New York: Putnam.

[5] Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General*, 144(1), 114-126.

[6] Epley, N., Waytz, A., & Cacioppo, J. T. (2007). On seeing human: A three-factor theory of anthropomorphism. *Psychological Review*, 114(4), 864-886.

[7] Hirschhorn, L. (1988). *The workplace within: Psychodynamics of organizational life*. Cambridge, MA: MIT Press.

[8] Janis, I. L. (1982). *Groupthink: Psychological studies of policy decisions and fiascoes*. Boston: Houghton Mifflin.

[9] Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

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

[11] Kotter, J. P. (1996). *Leading change*. Boston: Harvard Business School Press.

[12] Lewin, K. (1947). Frontiers in group dynamics: Concept, method and reality in social science. *Human Relations*, 1(1), 5-41.

[13] Libet, B., Gleason, C. A., Wright, E. W., & Pearl, D. K. (1983). Time of conscious intention to act in relation to onset of cerebral activity. *Brain*, 106(3), 623-642.

[14] Menzies Lyth, I. (1960). A case-study in the functioning of social systems as a defence against anxiety. *Human Relations*, 13, 95-121.

[15] Milgram, S. (1974). *Obedience to authority.* New York: Harper & Row.

[16] Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), 230-253.

[17] SANS Institute. (2023). *Security Awareness Report 2023.* SANS Security Awareness.

[18] Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). San Francisco: Jossey-Bass.

[19] Soon, C. S., Brass, M., Heinze, H. J., & Haynes, J. D. (2008). Unconscious determinants of free decisions in the human brain. *Nature Neuroscience*, 11(5), 543-545.

[20] Verizon. (2023). *2023 Data Breach Investigations Report.* Verizon Enterprise.

[21] Winnicott, D. W. (1971). *Playing and reality.* London: Tavistock Publications.