Scientific Research Publishing

Journal of Information Security, 2026, 17(3), 243-275
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cognitive Perimeter Targeting: Behavioral Intelligence and SOCMINT in Multinational Cybersecurity Operations

Troy C. Troublefield[1,2,3]

[1]Department of Cyberpsychology, Capitol Technology University, Laurel, MD, USA
[2]Department of Information Technology, Capella University, Minneapolis, MN, USA
[3]Department of International Business, International School of Management, Paris, France
Email: drtroytroublefield@yahoo.com

How to cite this paper: Troublefield, T.C. (2026) Cognitive Perimeter Targeting: Behavioral Intelligence and SOCMINT in Multinational Cybersecurity Operations. *Journal of Information Security*, **17**, 243-275.
https://doi.org/10.4236/jis.2026.173013

Received: April 9, 2026
Accepted: June 26, 2026
Published: June 29, 2026

Abstract

Multinational organizations operating in shared cybersecurity environments face a compounding intelligence challenge: the behavioral dynamics that determine human susceptibility to social engineering, insider threat development, and coordinated disinformation campaigns are not captured by conventional technical security monitoring, yet available evidence consistently positions them as the dominant attack surface in contemporary advanced persistent threat (APT) and hybrid cyber-influence operations, with Verizon's 2024 Data Breach Investigations Report attributing 68% of breaches to a non-technical human element, and establishing social engineering as structurally prior to technical exploitation in APT attack chains. This article develops and applies the Behavioral Intelligence in the Cognitive Domain (BICD) framework to multinational cybersecurity contexts, reconceptualizing Social Media Intelligence (SOCMINT) as an epistemologically distinct discipline from Open-Source Intelligence (OSINT) grounded in behavioral rather than documentary epistemology, and arguing that this distinction has direct and under-explored consequences for multinational security operations centers (MSOCs), joint cyber defense coordination cells, and cross-border incident response teams. The BICD framework integrates five cyberpsychology mechanisms, online disinhibition, platform-conditioned identity performance, algorithmic belief environment formation, social proof manipulation, and digital cognitive bias amplification, into a structured analytical procedure for producing explanatory and predictive threat intelligence from human behavioral data in digital environments. The framework then specifies how BICD-derived intelligence products inform narrative-based countermeasure design, organizational resilience architecture, and cross-jurisdictional threat communication, creating a struc-

tured intelligence-to-defense pipeline applicable to the multinational cybersecurity operating environment. The article engages emerging scholarship in cognitive cybersecurity (2021-2025), AI-driven social engineering threats (2022-2025), and multinational cyber coordination frameworks to situate the BICD framework within current organizational and operational debates. Implications for multinational security governance, cross-border intelligence sharing, and practitioner training are addressed throughout.

Keywords

Cyberpsychology, SOCMINT Epistemology, Cognitive Cybersecurity, Behavioral Intelligence, Multinational Cybersecurity, Social Engineering, Insider Threat, Cognitive Domain, AI-Enhanced Influence, Cross-Border Cyber Defense

1. Introduction

Multinational organizations, whether international financial institutions, cross-border critical infrastructure operators, multilateral defense alliances, or global technology firms, share a structural vulnerability that technical cybersecurity frameworks have not fully resolved: the human cognitive layer that mediates all organizational behavior is simultaneously the most targeted and the least systematically analyzed element of the cybersecurity posture. Advanced persistent threat (APT) actors, state-sponsored influence operations, and sophisticated criminal networks have converged on the recognition that the most efficient attack vector against hardened technical defenses is not exploitation of software vulnerabilities but exploitation of the behavioral and psychological vulnerabilities of the individuals who operate, manage, and make decisions within target organizations [1] [2]. Social engineering, spear-phishing, business email compromise, insider threat cultivation, and coordinated cognitive influence operations are unified by their targeting of human behavioral dynamics rather than technical system weaknesses.

The cybersecurity intelligence challenge this creates for multinational organizations is specific and under-addressed. Existing Security Operations Center (SOC) monitoring is optimized for technical threat indicators, network anomalies, endpoint behavioral deviations, malware signatures, and authentication pattern irregularities. Human behavioral threat indicators, the social media activity patterns, community engagement dynamics, and digital identity performances that precede and enable social engineering, insider threat development, and organizational influence operations, are either not collected, collected but not analyzed through frameworks calibrated to their behavioral character, or analyzed through OSINT frameworks designed for documentary evidence rather than behavioral evidence [3] [4]. The result is a persistent intelligence gap in the human layer of multinational cybersecurity that technical monitoring architecture cannot close, regardless of its sophistication.

This article addresses the gap by developing and applying the BICD framework to the multinational cybersecurity operating environment. The BICD framework, originally developed for military intelligence and influence operations contexts, reconceptualizes SOCMINT as an epistemologically distinct analytical discipline and integrates five cyberpsychology mechanisms into a structured intelligence-to-defense pipeline applicable to cross-border cyber threat environments [5]. The framework's application to multinational cybersecurity generates three original contributions. First, it provides the epistemological foundation for integrating behavioral threat intelligence into multinational SOC operations in ways that are methodologically defensible, quality-controlled, and appropriately confidence-calibrated. Second, it operationalizes five cyberpsychology mechanisms as behavioral threat indicators with specific implications for insider threat programs, social engineering countermeasures, and organizational resilience architecture. Third, it develops a four-stage intelligence-to-defense pipeline connecting behavioral threat analysis to countermeasure design, cross-jurisdictional threat communication, and adaptive organizational learning applicable to the governance and operational structures characteristic of multinational organizations.

Four constructs appear throughout this article and require precise operational definition at the outset to reduce interpretive ambiguity across later sections. Documentary epistemology, as used here, refers to the foundational knowledge assumption of conventional OSINT: that the primary evidential unit is a document, artifact, or statement whose security-relevant content is assessed through evaluation of its factual accuracy, attribution, and verifiability against external reference points. Behavioral epistemology, by contrast, refers to the alternative foundational assumption underlying SOCMINT as reconceptualized in this article: that the primary evidential unit is a pattern of human behavior, expressed across digital interactions, platform communications, and identity performances, whose security-relevant content is assessed through interpretation of what those patterns reveal about psychological states, vulnerabilities, and probable future behavioral trajectories, independent of the literal truth or falsity of any individual statement. A behavioral threat indicator (BTI) is an observable, mechanism-anchored digital behavioral pattern that, when interpreted through an appropriate cyberpsychology framework, constitutes evidence of elevated susceptibility to a specific threat vector, active engagement in a threat-relevant behavioral trajectory, or organizational influence susceptibility exploitable by an adversary. Authenticity confidence is the analyst-assigned probability estimate that a detected behavioral pattern reflects the genuine psychological characteristics of the individual or account exhibiting it, rather than an artifact of platform mechanics, strategic self-presentation, or adversary-controlled synthetic behavior; it is expressed as a confidence tier (high, moderate, low, or indeterminate) rather than a precise numerical probability, and it gates the intelligence tier to which a BICD analysis product can be assigned.

The article proceeds as follows. The Methodology section describes the theoret-

ical synthesis methodology. The Theoretical Foundation section develops the SOCMINT epistemological distinction and situates it within cognitive cybersecurity literature. The BICD Mechanisms section presents five cyberpsychology mechanisms as behavioral threat indicators with multinational cybersecurity applications. The Intelligence-to-Defense Pipeline section specifies four operational stages connecting behavioral threat analysis to organizational security response. The Discussion section addresses implementation requirements, cross-jurisdictional governance challenges, and ethical boundaries. The Conclusion presents doctrine and oversight implications for multinational cybersecurity organizations.

2. Methodology

2.1. Framework Development

The BICD framework is developed through theoretical synthesis methodology, an approach that produces new analytical constructs by identifying mechanistic connections between bodies of knowledge and deriving their joint operational implications [6]. Theoretical synthesis is appropriate when the primary intellectual problem is one of integration and operationalization rather than empirical discovery: when the knowledge required to address a practical problem exists in fragmented form across multiple disciplines but has not been assembled into actionable frameworks with sufficient analytical specificity to guide practice.

Stage one conducted domain mapping across five disciplinary areas relevant to multinational cybersecurity: cyberpsychology and human-computer interaction research; intelligence studies with specific focus on SOCMINT and OSINT epistemology; cognitive cybersecurity and organizational security research; multinational governance and cross-jurisdictional coordination literature; and narrative persuasion and social engineering research. Literature selection combined systematic database searching, PsycINFO, ACM Digital Library, IEEE Xplore, ProQuest, and Google Scholar, with citation network analysis to identify both foundational theoretical sources and the most recent empirical literature. Priority was given to peer-reviewed scholarship published from 2019 onward for empirical claims about digital behavioral dynamics, AI-enhanced social engineering threats, and multinational cybersecurity coordination.

Stage two extracted operationalizable mechanisms from the cyberpsychology literature, applying three selection criteria: empirical demonstration in peer-reviewed research; systematic alteration of behavioral expression in digital compared to offline contexts; and generation of observable, analyst-identifiable indicators in social media and organizational communication data relevant to cybersecurity threat analysis. Each mechanism that met the selection criteria was analyzed for its epistemological implications, specifically, the conditions under which it generates reliable threat intelligence indicators versus analytical artifacts, and the analytical procedures required to distinguish reliably between the two in multinational organizational contexts.

Stage three developed the intelligence-to-defense pipeline by specifying the structural connection between BICD analytical outputs and multinational cybersecurity countermeasure design parameters. This stage drew on social engineering countermeasure research, insider threat program literature, cross-jurisdictional intelligence sharing frameworks, and organizational resilience scholarship to identify the specific inputs that behavioral threat intelligence products should provide to security decision-makers, and the procedures through which those inputs translate into organizational security design decisions.

2.2. Search Protocol and Source Retention

To support auditability of the theoretical synthesis process, this subsection documents the search protocol, screening criteria, and retention decisions applied during Stage One domain mapping. Database searching was conducted across five databases: PsycINFO, ACM Digital Library, IEEE Xplore, ProQuest Dissertations & Theses, and Google Scholar. Searches were executed in two phases. Phase One used domain-specific seed queries to identify literature within each of the five mapped disciplines. Search strings included, but were not limited to: cyberpsychology AND ("social media" OR "digital behavior" OR "online identity"); SOCMINT AND (intelligence OR "open source" OR epistemology); ("cognitive cybersecurity" OR "human factors") AND ("cybersecurity" OR "insider threat"); ("multinational" OR "cross-border") AND ("cybersecurity governance" OR "cyber coordination"); and ("social engineering" OR "influence operation") AND ("narrative" OR "persuasion" OR "disinformation").

Phase Two applied forward and backward citation tracking from the highest-relevance sources identified in Phase One to ensure foundational theoretical works predating the 2019 priority window were not excluded. All searches were conducted with an emphasis on literature published from 2019 to early 2025 for empirical behavioral and threat-specific claims. Foundational theoretical works, including Suler (2004) on online disinhibition, Cialdini (2018) on social proof, Kahneman (2011) on cognitive bias, and Heuer (1999) on analytic tradecraft, were retained regardless of publication date where they remain the primary theoretical anchor for a mechanism claim. Screening applied three inclusion criteria: 1) the source addresses one or more of the five mapped domains at a depth permitting mechanism extraction; 2) for empirical claims, the source reports peer-reviewed primary or secondary research; 3) the source generates at least one operationalizable mechanism or analytical procedure relevant to behavioral threat intelligence in digital environments.

Sources were excluded if they addressed general cybersecurity without behavioral or psychological specificity, if they were practitioner or trade literature without peer review for empirical claims, or if their primary application domain was unrelated to organizational, intelligence, or security contexts. Across both phases, an initial corpus of approximately 210 sources was identified. After title and abstract screening against the inclusion criteria, 108 sources advanced to full-text

review. Of these, 40 were retained as primary sources contributing directly to mechanism selection, epistemological architecture, or pipeline design; an additional 18 were retained as contextual or corroborating sources cited in the manuscript. The remaining 50 full-text-reviewed sources were excluded as insufficiently specific to the behavioral-intelligence-in-digital-environments focus of the synthesis. The reference list in this article reflects the 40 primary and 18 contextual sources retained after full-text review.

3. Theoretical Foundation

Epistemological Distinctions and the Human Layer

Contemporary cybersecurity scholarship has reached a convergent conclusion that the human cognitive layer constitutes the primary attack surface in advanced cyber threat environments [7] [8]. While technical defenses, firewalls, intrusion detection systems, endpoint protection platforms, cryptographic controls, have matured significantly, threat actors have correspondingly shifted investment toward the exploitation of human behavioral vulnerabilities that technical defenses cannot directly address. [9] annual Data Breach Investigations Report estimated that the human element remains a contributing factor in over 68% of data breaches, a proportion that has remained stable across multiple reporting periods despite sustained investment in technical security controls. For multinational organizations operating across multiple jurisdictions, languages, regulatory environments, and organizational cultures, this human-layer attack surface is amplified by the cognitive and communicative complexity that cross-border operations introduce.

The cognitive domain framework, developed initially in military intelligence scholarship and catalyzed by NATO's 2021 cognitive warfare study, provides the conceptual architecture for understanding why the human layer is both systematically targeted and so analytically underserved in conventional cybersecurity practice [10] [11]. Cognitive domain theory holds that beliefs, perceptions, reasoning processes, and decision-making structures constitute a structured terrain with observable properties that can be analyzed, targeted, and defended. Applied to multinational cybersecurity, this framework reframes the threat analysis objective from exclusively technical to dual-layer: organizations must monitor technical threat indicators and behavioral threat indicators that together constitute a comprehensive picture of organizational vulnerability. The failure to integrate behavioral threat intelligence into security operations produces a systematic blind spot whose exploitation has become a defining characteristic of sophisticated threat actors targeting multinational organizations.

[12] identified the insider threat as among the most consequential and analytically elusive cybersecurity challenges, a characterization that has been repeatedly confirmed in subsequent decades of research and operational experience. The behavioral dynamics that precede and enable insider threat activity, identity performance changes, community disengagement, radicalization or grievance escalation in digital environments, are precisely the dynamics that BICD mechanism analysis

is designed to detect. For multinational organizations, insider threat complexity is further compounded by cross-cultural differences in behavioral norms, platform usage patterns, and the contextual factors that mediate online disinhibition, making cross-cultural behavioral calibration a prerequisite for effective multinational behavioral threat intelligence.

To clarify the original contribution of this article relative to the author's prior published work, a brief demarcation is warranted. The BICD framework's foundational architecture, its epistemological claim that SOCMINT requires a behavioral rather than documentary analytical approach, its identification of five cyberpsychology mechanisms (online disinhibition, platform-conditioned identity performance, algorithmic belief environment formation, social proof manipulation, and digital cognitive bias amplification) as the primary analytical units, and its procedure for deriving confidence-calibrated intelligence products from behavioral indicator analysis, was developed and published in the context of military intelligence and influence operations, specifically for information support operations and cognitive domain threat analysis in that prior work [5]. The present article does not originate those elements; it extends and adapts them.

The original contributions of this article are threefold: first, the reconceptualization of the BICD epistemological framework as applicable to the distinctive operating conditions of multinational civilian and hybrid security organizations, conditions characterized by cross-jurisdictional legal complexity, organizational heterogeneity, and the absence of military authority structures; second, the operationalization of the five mechanisms as behavioral threat indicators specifically calibrated to the insider threat, social engineering, and organizational influence operation vectors that constitute the primary threat surface for multinational security operations centers rather than the military PSYOP and counterterrorism applications of the prior work; and third, the development of the four-stage intelligence-to-defense pipeline as an operational architecture connecting BICD analytical products to countermeasure design, cross-jurisdictional threat communication, and adaptive organizational security learning in the multinational civilian context. Readers are directed to [5] for the foundational framework development; the present article's contribution is the application architecture, operational specifications, and governance analysis developed therein for the multinational cybersecurity context.

4. SOCMINT vs. OSINT: Epistemological Distinctions

4.1. Behavioral versus Documentary Analysis for Multinational Cybersecurity

The epistemological distinction between SOCMINT and OSINT has direct operational significance for multinational cybersecurity organizations that collect and analyze social media data as part of insider threat programs, supply chain security monitoring, and threat actor tracking. The dominant institutional approach treats SOCMINT as a collection modality within OSINT, distinguished by source type,

social media platforms, but governed by the same analytical principles as other open-source collection [13]. This approach has organizational convenience: it avoids creating new disciplinary categories, leverages existing OSINT infrastructure, and simplifies training requirements. Its operational weakness is that it produces systematic analytical errors with direct security consequences.

[4] established that SOCMINT occupies a fundamentally different position in the intelligence cycle because its primary data is not reported information but enacted behavior mediated by platform architecture, social context, and psychological state. Under this analysis, the conventional OSINT analyst's task, interpreting the content of deliberately published information and assessing its credibility against known source characteristics, is epistemologically inappropriate for SOCMINT because social media posts are not deliberate publications to a public audience in the relevant sense. They are behavioral acts whose informational content is inseparable from the psychological and social conditions that produced them. Applied to cybersecurity contexts, this epistemological distinction determines whether behavioral threat indicators, expressions of grievance, identity shifts indicating radicalization, community engagement patterns suggesting social engineering targeting, are interpreted accurately or misread through documentary analytical assumptions that introduce systematic errors into threat assessments.

[3] formalized this distinction by proposing a difference between OSINT's documentary epistemology, in which information is treated as evidence of facts about the world, and SOCMINT's required behavioral epistemology, in which data is treated as evidence of psychological states, social dynamics, and environmental influences that mediated its production. The practical implication for multinational cybersecurity is substantial: the same text that a documentary epistemology reads as a statement of intent requires a behavioral epistemology to read as a behavioral act whose relationship to underlying intent is mediated by platform anonymity level, audience composition, social pressure dynamics, and individual psychological state. Misapplying documentary epistemology to behavioral data produces overconfident threat assessments from disinhibited expression, misattribution of intent from performative posting designed for a specific audience, and failure to distinguish organic threat indicators from coordinated inauthentic signals manufactured by adversaries to divert security resources.

4.2. AI-Generated Synthetic Behavioral Data as Multinational Cybersecurity Threat

The operational deployment of AI systems capable of generating synthetic behavioral data at scale represents a qualitative escalation in the threat environment facing multinational organizations' behavioral threat intelligence programs [14]. Large language models, deployed through coordinated bot networks and influence operation infrastructure, produce social media content, posts, comments, engagement patterns, apparent employee communications, that is behaviorally indistinguishable from organic human expression at the level of individual in-

stance analysis. [14] provide evidence that generative language models reduce the cost and increase the scale of targeted influence operations in experimental settings, while [15] demonstrates in controlled conditions that LLM-generated spear-phishing messages achieve click rates comparable to human-crafted messages; both findings are from experimental rather than operational field studies and should be interpreted as establishing feasibility and elevated risk potential rather than confirmed operational baseline effectiveness. For multinational cybersecurity organizations, this creates three intersecting threats. First, adversaries can manufacture apparent evidence of insider activity, grievance escalation, or social engineering targeting security resources toward false threats while concealing genuine ones. Second, synthetic behavioral signals can be used to corrupt the training data of machine learning-based behavioral anomaly detection systems, degrading their discriminative validity over time. Third, AI-generated spear-phishing content, now capable of incorporating contextually accurate behavioral and relational details sourced from social media analysis, has substantially increased the success rate of targeted social engineering against employees of multinational organizations [15].

[16] identify AI-enhanced influence operations as among the primary emerging threats to the validity of SOCMINT-based intelligence products, noting that current statistical anomaly detection methods for distinguishing synthetic from organic behavioral data can be defeated by sufficiently sophisticated generative systems. The adversarial implication for multinational organizations is direct: state actors and well-resourced criminal organizations can now engineer the behavioral data environment that security analysts observe, manufacturing apparent threat signals, false indicators of employee compromise, and artificial social engineering targeting patterns that will mislead analysts applying conventional SOCMINT methods. The BICD framework addresses this threat by incorporating AI-generated content detection as a mandatory analytical step preceding any mechanism-based interpretation, and by specifying the conditions under which behavioral threat intelligence products derived from potentially contaminated data environments should be treated as low-confidence indicators requiring cross-validation against alternative collection sources.

5. The BICD Framework: Five Cyberpsychology Mechanisms

5.1. Key Behavioral Dynamics for Multinational Threat Detection

The BICD framework identifies five cyberpsychology mechanisms that meet the three-criterion selection standard: empirical demonstration in peer-reviewed research, systematic alteration of digital behavioral expression relative to offline behavior, and generation of analyst-identifiable observational indicators in data relevant to multinational cybersecurity threat analysis. Each mechanism is specified with its theoretical basis, the behavioral signals it produces in organizational and social media data, the analytical procedure for interpreting those signals in cybersecurity contexts, the epistemological limitations bounding valid inference, and the measurable implications for multinational security operations that apply the

mechanism correctly versus those that ignore it.

5.2. Mechanism One: Online Disinhibition and Insider Threat Detection

Online disinhibition, the tendency for individuals to engage in behaviors in digital environments that social norms, self-monitoring, and anticipated consequences would suppress in face-to-face contexts, was first systematically described by [17] and remains one of the most empirically robust and operationally significant findings in cyberpsychology for organizational security applications. [17] identified six psychological mechanisms producing disinhibition: dissociative anonymity (the perception that online identity is separable from offline identity and consequences); invisibility (absence of physical cues that create social accountability); asynchronicity (temporal flexibility reducing the pressure of immediate social response); solipsistic introjection (the blurring of internal mental communication and external expression); dissociative imagination (perceiving the online environment as consequence-free or game-like); and minimization of authority (reduced deference to status hierarchies where conventional status markers are absent).

For multinational cybersecurity organizations, disinhibition creates what the BICD framework designates the behavioral authenticity problem: observed behavioral signals in organizational communication and social media data may reflect either genuine psychological states with security implications, genuine grievance, radicalization, planning for harmful action, or artifact expressions produced by the disinhibiting environment itself rather than by any stable underlying disposition [18]. The analytical failure mode, which institutional OSINT approaches to social media monitoring systematically produce, is treating disinhibition-driven artifact expression as high-confidence intelligence about genuine intent, producing false positive threat assessments that erode the credibility of behavioral threat intelligence programs and consume security resources disproportionate to actual risk.

The security implications of disinhibition are particularly acute for insider threat programs in multinational organizations. Employees expressing workplace grievances on anonymous forums, pseudonymous social media accounts, or encrypted messaging platforms may be engaging in disinhibition-driven emotional release with no behavioral correlate in organizational action, or may be exhibiting genuine precursor indicators of insider threat development. Distinguishing between these two categories requires behavioral epistemology, not documentary content analysis, and the analytical procedures the BICD framework specifies.

The BICD procedure for addressing the behavioral authenticity problem in cybersecurity contexts specifies three analytical steps. Platform anonymity calibration assigns a disinhibition coefficient to each monitored communication channel based on its identity verification requirements, social accountability mechanisms, moderation practices, and documented behavioral norms. Longitudinal consistency analysis applies this coefficient to evaluate whether observed expressions persist across multiple timeframes, platform types, and social contexts: expres-

sions that recur consistently across high and low disinhibition environments receive higher authenticity confidence ratings. Behavioral-organizational congruence assessment, where observable behavioral evidence is available in organizational systems, access pattern changes, policy compliance deviation, communication volume shifts, compares expressed content against observable organizational behavior to derive empirical congruence rates that calibrate the reliability of verbal expression as an indicator of underlying disposition.

5.3. Mechanism Two: Platform-Conditioned Identity Performance and Threat Actor Attribution

Research in cyberpsychology and social computing establishes that individuals construct and perform multiple context-dependent identities adapted to specific platform affordances, audience compositions, and social norms [18]. Identity performance theory, drawing on Goffman's foundational framework and its extensions into digital environments by Markman, holds that individuals manage impressions across different social stages by selectively displaying identity facets appropriate to each audience and context. For multinational cybersecurity organizations, identity multiplicity creates both an analytical opportunity and a systematic risk in threat actor attribution, employee security monitoring, and social engineering detection [19].

The opportunity is that multi-platform monitoring can access identity facets that together provide more comprehensive threat understanding than any single platform reveals: a threat actor's technical community identity may reveal capability indicators and operational orientation, their ideological community identity may reveal motivation and target selection criteria, and their personal social network identity may reveal organizational affiliations and operational security practices. [20] demonstrated that identity linkage across platforms can be achieved through behavioral signature analysis, linguistic pattern matching, temporal activity correlation, and social network overlap analysis with accuracy rates sufficient for intelligence-grade attribution under controlled conditions, though with non-trivial false positive rates that impose confidence limitations on multi-platform profile construction in operational environments.

The risk is particularly significant for multinational organizations monitoring employees across multiple jurisdictions with different legal frameworks governing workplace monitoring and privacy rights. Constructing a psychological profile from multiple identity facets without accounting for their context-specificity may produce falsely coherent assessments that generalize context-specific performances into cross-situation characterizations of stable underlying psychology. An employee who presents differently on a professional network, a personal social platform, and a hobbyist community is exhibiting normal identity multiplicity, not evidence of deceptive intent. Multinational organizations must develop cross-jurisdictional governance frameworks for BICD-based employee monitoring that are compliant with General Data Protection Regulation (GDPR) requirements in EU jurisdictions, national security monitoring legislation in partner-nation con-

texts, and applicable employment law across the full operational geography [21].

The BICD framework operationalizes identity multiplicity analysis for cybersecurity contexts through a four-stage procedure: attribution methodology that employs behavioral signatures, linguistic stylometric features, temporal activity patterns, and network connections to link platform identities to individuals or organizations with explicitly stated confidence levels derived from the number and independence of corroborating indicators; integration analysis that synthesizes identified identity facets into a composite threat profile specifying capability indicators, motivation structures, and operational security practices; activation prediction that assesses which identity facets will be operative in specific targeting contexts; and authenticity stratification that distinguishes stable characteristics from context-specific performances that may not generalize to behavioral prediction.

5.4. Mechanism Three: Algorithmic Belief Environment Formation and Organizational Social Engineering Vulnerability

Digital platform algorithms, designed primarily to maximize engagement metrics, systematically shape the information environments in which individuals form beliefs by selectively curating content toward attitude-consistent, emotionally arousing, and socially validated material [22]. For multinational cybersecurity organizations, algorithmic belief environment formation creates both a direct organizational vulnerability and an analytical challenge for threat intelligence programs monitoring social engineering campaigns targeting employees and partner networks.

The direct organizational vulnerability operates through the radicalization and grievance amplification pathways that algorithmically curated environments facilitate. Employees who engage with workplace grievance content on algorithmically curated platforms will be systematically served additional grievance content that confirms and intensifies negative organizational attitudes, potentially accelerating the grievance-to-insider-threat pipeline through mechanisms that operate largely outside the employee's reflective awareness [23]. Social engineering threat actors deliberately exploit this dynamic by seeding grievance content in platforms frequented by target organization employees, anticipating algorithmic amplification that will reach susceptible individuals without direct adversarial contact that might trigger security detection.

The analytical challenge for threat intelligence programs is a representativeness problem with direct security implications. Social media monitoring of threat actor campaigns and employee behavioral dynamics captures the attitudinal distribution of individuals who are behaviorally active on the monitored platforms in the monitored time period. This is not the same as the attitudinal distribution of the organizational population or the true prevalence of threat actor narratives in the target environment. Content that is algorithmically visible reflects algorithmic amplification decisions rather than organic sentiment distribution. Intelligence

products derived from unanalyzed social media monitoring may systematically overestimate the prevalence of security-relevant attitudes, misattribute algorithmic amplification artifacts as organic organizational consensus around grievances or threat narratives, and conflate platform-specific demographically skewed user populations with the broader organizational population of security interest.

[24] demonstrated that false information spreads faster and further than true information on social media platforms, a finding with direct implications for social engineering threat assessment: the threat narratives and deceptive content most prevalent in social media monitoring data are systematically biased toward what platform algorithms reward for engagement rather than toward what accurately represents the threat actor's organic reach or operational capability. The BICD framework addresses representativeness bias through platform algorithm modeling, demographic correction, and adversarial contamination detection as mandatory analytical prerequisites before social media monitoring data informs organizational security decisions.

5.5. Mechanism Four: Social Proof Dynamics and Adversarial Influence Network Assessment

Social proof, the cognitive tendency to infer the appropriateness of a belief or action from the apparent beliefs and actions of others, operates differently in digital environments than in conventional social contexts because digital platforms make social proof signals quantifiable, visible, and technically manipulable at scale [25]. For multinational cybersecurity organizations, social proof manipulation by adversarial actors constitutes a direct threat to organizational decision-making quality and a significant amplification mechanism for social engineering campaigns targeting employees, partners, and external stakeholders.

[26] demonstrated through randomized experimentation that artificial positive ratings produced herding effects that significantly inflated subsequent organic engagement, providing direct experimental evidence that manufactured social proof produces genuine attitude and behavior change in exposed populations. Applied to cybersecurity contexts, this finding means that adversaries who successfully manufacture apparent consensus around security-irrelevant narratives (to divert attention), false crisis signals (to induce panic-driven security bypasses), or apparent peer endorsement of malicious content (to increase click-through rates) achieve direct behavioral effects on organizational security posture through mechanisms that bypass technical defenses entirely.

[27] demonstrated that coordinated inauthentic behavior designed to manufacture social proof can be detected through temporal dynamics analysis: organic content adoption follows predictable sigmoid diffusion curves characteristic of peer-to-peer information spread, while bot-driven amplification produces anomalous spike patterns inconsistent with organic diffusion that reflect coordinated simultaneous action rather than sequential social influence. Network topology analysis provides a complementary detection method: inauthentic amplification networks exhibit centralized, low-reciprocity structural signatures distinct from

the distributed, high-reciprocity structures of organic peer-to-peer information diffusion.

The BICD framework operationalizes social proof assessment for multinational cybersecurity contexts through a procedure that integrates temporal dynamics analysis with network topology examination to produce authenticity ratings for observed social proof signals. This authentication assessment has direct applications to business email compromise detection, executive impersonation identification, and false authority social engineering detection, attack vectors that rely on manufactured social proof of organizational legitimacy to induce security-bypassing employee behavior. [28] provide empirical support for the distinction between genuine organizational influencers, whose social proof signals reflect authentic network authority, and imitators who amplify existing content without generating independent influence, a distinction critical for identifying executive impersonation and authority-fabrication social engineering attempts.

5.6. Mechanism Five: Digital Cognitive Bias Amplification and Organizational Security Culture

A substantial cyberpsychology literature documents that digital information environments systematically amplify the effects of well-established cognitive biases, with direct implications both for understanding organizational vulnerability to social engineering and for managing the analytical quality of security professionals' own threat assessment processes [29]. Confirmation bias, the tendency to seek, process, and recall attitude-consistent information while discounting contradictory evidence, intensifies in algorithmically curated environments that selectively present attitude-consistent content, creating reinforcing loops between individual cognitive bias and platform algorithmic amplification. For multinational cybersecurity organizations, this mechanism operates at two levels of organizational vulnerability.

At the employee behavioral level, cognitively biased information environments make individuals more susceptible to targeted social engineering that exploits existing attitudes and beliefs, a phenomenon. [8] documented in the context of spear-phishing susceptibility, demonstrating that cognitive load and existing attitude structures significantly moderate phishing response rates. Employees embedded in high-confirmation-bias digital environments are more likely to accept social engineering content that confirms existing attitudes (organizational distrust, security skepticism, urgency about particular topics) and less likely to apply critical evaluation to requests that fit their existing belief structures.

At the analytical level, security professionals who routinely monitor threat actor content, extremist material, and high-arousal cybersecurity incident data are exposed to the same availability and confirmation bias amplification dynamics that affect the populations they analyze [30]. Without explicit institutional recognition of this dual exposure and structured debiasing protocols, threat intelligence products may systematically reflect analyst cognitive bias alongside genuine threat indicators, a compounding error source whose effects cannot be distinguished from

authentic intelligence signals in the absence of structured quality controls. Multinational organizations, whose security teams operate across multiple cultural contexts that may themselves shape cognitive bias expression differently, face additional cross-cultural complexity in designing analyst debiasing programs that address both universal cognitive bias mechanisms and culturally specific manifestations.

The BICD framework addresses cognitive bias amplification through a dual-channel debiasing procedure operating simultaneously on the threat analysis and analyst sides. Threat-side bias mapping models the specific algorithmic and social environments in which monitored threat actors and organizational populations form beliefs, estimating the degree to which observed behavioral patterns reflect bias amplification rather than stable underlying dispositions. Analyst-side debiasing applies structured analytical techniques, alternative competing hypotheses generation, mandatory cross-team review, and periodic analytical assumption auditing, to counteract the cognitive bias amplification that sustained exposure to threat content induces in security analysts [31].

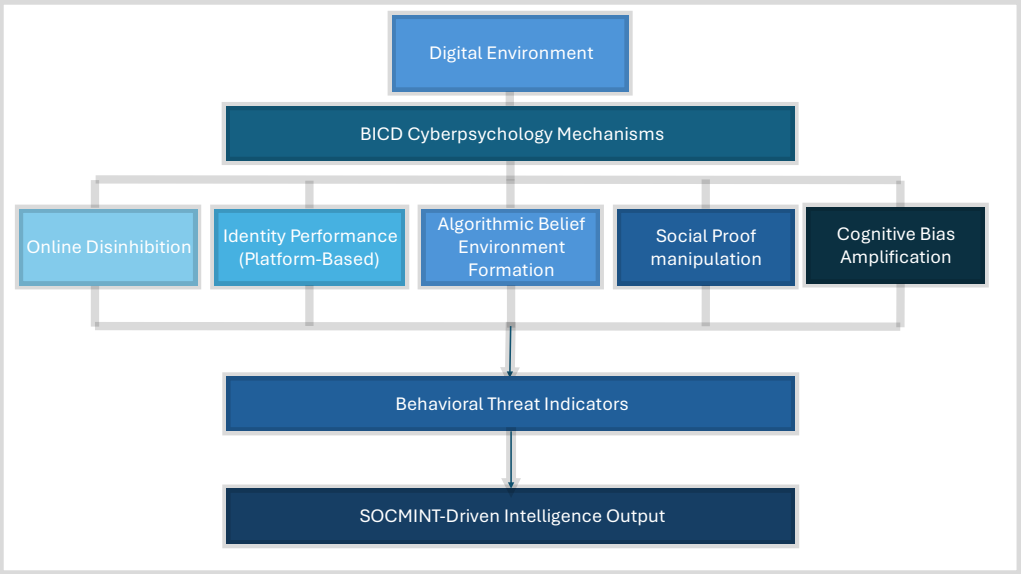

Figure 1. BICD cyberpsychology mechanism model.

Figure 1 illustrates the conceptual architecture of the BICD framework, showing how human behavior in digital spaces is transformed into actionable cybersecurity intelligence. At the top of the model, the digital environment represents the total ecosystem of online platforms, social media, communication systems, and algorithmically mediated spaces, where human interaction occurs. This environment is not neutral; it actively shapes behavior through anonymity, platform design, and algorithmic curation. As such, it serves as the originating condition from which all subsequent behavioral dynamics emerge.

The second layer introduces the BICD cyberpsychology mechanisms, which function as the core explanatory drivers of digital behavior. These five mecha-

nisms, online disinhibition, platform-conditioned identity performance, algorithmic belief environment formation, social proof manipulation, and digital cognitive bias amplification, operate in parallel rather than sequentially. Each mechanism captures a distinct way in which digital contexts systematically alter cognition, emotion, and social interaction. Importantly, these mechanisms are interdependent; for example, algorithmic environments can intensify cognitive biases, while social proof dynamics can reinforce identity performance.

From these mechanisms emerge behavioral expressions, represented in the model as distributed outputs flowing downward from each mechanism. These expressions include observable signals such as shifts in tone, engagement patterns, identity inconsistencies, or coordinated amplification behaviors. However, the model emphasizes that these signals are not direct reflections of intent; they are mediated outputs shaped by the mechanisms above, requiring careful interpretation.

These outputs converge into the behavioral threat indicators layer, where raw behavioral data is synthesized into analytically meaningful patterns. At this stage, individual signals are aggregated, contextualized, and evaluated for their relevance to cybersecurity threats such as insider risk, social engineering susceptibility, or influence operations. The convergence visually reinforces that no single mechanism is sufficient on its own; reliable threat indicators emerge only through integrated, multi-mechanism analysis.

Finally, the model culminates in SOCMINT-driven intelligence output, representing the transformation of behavioral indicators into structured intelligence products. This output supports decision-making in cybersecurity operations by providing explanatory and predictive insights into human vulnerabilities and adversarial influence strategies. Crucially, the model underscores that effective intelligence production depends on interpreting behavioral data through a cyberpsychology lens rather than treating it as traditional documentary evidence.

Overall, **Figure 1** conveys a layered, systems-based understanding of cybersecurity in which the human cognitive domain is both the primary attack surface and a critical source of intelligence. It demonstrates that behavioral data, when properly contextualized through cyberpsychology mechanisms, becomes a powerful tool for anticipating and mitigating complex, human-centric cyber threats.

Table 1 presents the five core cyberpsychology mechanisms that form the analytical foundation of the Behavioral Intelligence in the Cognitive Domain (BICD) framework. Each mechanism represents a distinct way in which digital environments systematically alter human behavior, producing observable indicators that can be leveraged for cybersecurity intelligence. Online disinhibition explains why individuals express amplified or atypical emotions in high-anonymity environments, necessitating careful validation before interpreting such signals as genuine intent. Platform-conditioned identity performance highlights the multiplicity of digital identities, emphasizing both the opportunity for richer behavioral profiling and the risk of misattribution when context is ignored. Algorithmic belief environment formation demonstrates how platform curation shapes perception and

can artificially inflate or distort threat-relevant narratives. Social proof manipulation reveals how adversaries exploit perceived consensus to influence behavior at scale, particularly in phishing and influence operations. Finally, digital cognitive bias amplification underscores that both targets and analysts are susceptible to reinforced biases in digital environments. Collectively, these mechanisms transform raw behavioral data into structured threat indicators while also defining the analytical constraints necessary to avoid systematic misinterpretation. The table therefore serves as both a diagnostic model and a cautionary framework, ensuring that behavioral intelligence is interpreted with appropriate epistemological rigor.

Table 1. BICD Mechanisms.

Mechanism	Core Concept	Observable Indicators	Cybersecurity Relevance	Explanation
Online Disinhibition	Reduced behavioral restraint in digital environments	Hostile posts, grievance expression, emotional volatility	Insider threat detection	High-anonymity environments distort authenticity, requires cross-platform validation
Identity Performance	Individuals present different identities across platforms	Inconsistent personas, role-based behavior shifts	Attribution & profiling	Enables multi-layer threat profiling but risks false attribution if misinterpreted
Algorithmic Belief Formation	Platforms shape user beliefs via content curation	Echo chambers, repeated narratives	Social engineering vulnerability	Artificial amplification can mimic real sentiment, misleading analysts
Social Proof Manipulation	Perceived consensus influences behavior	Viral trends, engagement spikes, bot activity	Phishing & influence ops	Adversaries manufacture legitimacy to trigger compliance
Cognitive Bias Amplification	Digital environments intensify biases	Confirmation loops, selective perception	Analyst + employee vulnerability	Affects both targets AND analysts, requires debiasing protocols

6. The Intelligence-to-Defense Pipeline

Before detailing each stage, the crosswalk below specifies the direct analytical contribution of each of the five BICD mechanisms to each of the four pipeline stages. This mapping makes explicit the connective logic between the cyberpsychology mechanisms developed in Section 5 and the operational outputs described in Sections 6.1 through 6.4, enabling security practitioners to identify which mechanisms are load-bearing for which pipeline stage and to diagnose where analytical gaps will degrade pipeline output quality. Mechanism 1, Online Disinhibition Effect: Informs Stage 1 (behavioral risk segmentation) by identifying individuals whose platform expression patterns exceed contextually expected norms, signaling reduced self-monitoring and elevated social engineering susceptibility; informs Stage 4 (adaptive feedback) by flagging anomalous expression spikes that may indicate adversary-induced disinhibition in targeted segments. Mechanism 2, Platform-Conditioned Identity Performance: Informs Stage 1 by enabling identity multiplicity analysis that distinguishes between-platform role variability from deceptive identity manipulation; informs Stage 2 (countermeasure design) by providing the identity structure parameters that determine which security narrative frameworks will achieve maximum audience identification in each behavioral

segment. Mechanism 3, Algorithmic Belief Environment Formation: Informs Stage 1 by characterizing the information ecosystems in which different organizational populations form security-relevant beliefs; informs Stage 2 by providing the content environment parameters for security awareness design; informs Stage 3 (cross-jurisdictional threat communication) by identifying platform-specific amplification dynamics that determine how threat communications will propagate across partner networks. Mechanism 4, Social Proof Manipulation: Informs Stage 1 by identifying high-authenticity influence nodes whose behavioral patterns determine segment-level norm formation; informs Stage 2 by providing the trust network architecture for peer-credibility-based security countermeasure design; informs Stage 3 by identifying the genuine influence nodes through which cross-jurisdictional threat communications should be routed to achieve processing depth rather than pro forma receipt. Mechanism 5, Digital Cognitive Bias Amplification: Informs Stage 1 by identifying the specific bias profiles, confirmation bias, availability heuristic, temporal discounting, that characterize different behavioral risk segments and predict differential vulnerability to specific social engineering and influence operation tactics; informs Stage 2 by specifying debiasing and bias-awareness parameters for security narrative design; informs Stage 4 by providing the baseline behavioral bias profile against which anomalous post-incident response patterns can be detected as potentially adversary-induced. This crosswalk is not merely organizational. It specifies that Stages 1 and 2 draw most heavily on Mechanisms 1- 3 (identity- and environment-focused mechanisms), Stage 3 draws primarily on Mechanism 4 (trust network architecture), and Stage 4 draws on all five mechanisms as feedback signals, with Mechanism 5 providing the baseline against which anomalous behavioral responses are assessed. Where analytical capacity requires prioritization, mechanisms should be sequenced accordingly.

6.1. One: Behavioral Risk Segmentation of Organizational Populations

Conventional organizational security risk assessment employs role-based or access-level segmentation that groups employees by their technical privileges or organizational function, privileged users, system administrators, external partners, end users, and designs security controls and awareness interventions calibrated to assumed shared characteristics within those groups. This approach generates administratively convenient segments that are behaviorally heterogeneous: the role-based categories that organize conventional security risk assessment do not correspond reliably to the psychological variables that determine differential susceptibility to social engineering, insider threat development, or cognitive influence operations [2].

BICD-based behavioral risk segmentation replaces role-based with psychographic grouping derived from the framework's analytical outputs. Identity multiplicity analysis produces psychological profiles specifying the belief configura-

tions, identity structures, and psychological needs that characterize individuals within the organizational population; these profiles are clustered into behavioral risk segments that group individuals by the characteristics that predict differential susceptibility to specific threat vectors. Algorithm bias environment analysis identifies the information environments different segments inhabit, enabling targeted security awareness interventions calibrated to actual behavioral vulnerability rather than assumed role-based risk. Social proof authenticity analysis identifies the genuine organizational influence nodes and trust network structures through which security-relevant information organically spreads within different segments, enabling strategic engagement of real organizational opinion leaders in security culture change efforts rather than relying on formal authority structures that may lack behavioral influence in practice.

[32] identify audience analysis as the foundational competency for effective influence operations, an insight that translates directly to the design of organizational security awareness and behavioral countermeasure programs: failure to understand target population psychology at operational depth produces interventions that are technically executed but behaviorally uninformed. BICD-based behavioral risk segmentation operationalizes audience analysis at the psychological depth that effective security culture change requires, moving beyond role-based and demographic approaches toward behavioral intelligence-based segmentation that captures the mechanisms through which different organizational populations form and update security-relevant beliefs.

6.2. Stage Two: Security Countermeasure Design Parameter Derivation

Narrative transportation theory, the psychological process through which story immersion suspends critical evaluation and produces attitude change congruent with narrative themes, provides the primary mechanism through which BICD-informed behavioral intelligence is converted into effective organizational security countermeasures [33]. Transportation effects are moderated by the degree to which narratives engage the specific psychological characteristics of the target audience: security awareness content featuring identifiable protagonists, addressing psychological needs salient to the audience, and resolving in ways consistent with the audience's existing belief frameworks achieves greater transportation and stronger behavioral effects than generic security training content that lacks these audience-specific properties. BICD intelligence products provide the audience-specific parameters that transportation-maximizing security countermeasure design requires.

From identity multiplicity analysis, security awareness designers derive the identity structures and professional self-concepts of target segments, enabling protagonist design in security scenarios that maximizes employee identification and narrative engagement. From algorithmic bias environment analysis, designers derive the informational narrative environment in which employees habitually

operate, the stories, framings, and interpretive contexts through which they process new security-relevant information. From behavioral authenticity analysis, designers derive the psychological needs, meaning, belonging, significance, professional competence, that motivate the expressed behaviors and attitudes of target segments, enabling security narrative resolution mechanisms that address those needs while directing employees toward desired security behaviors.

[34] narrative identity theory provides an additional design parameter with specific organizational security relevance: individuals who internalize narrative identity frameworks, stories about who they are and what their roles mean, generate the behaviors consistent with those identities as expressions of self-concept rather than as responses to external compliance requirements. Security awareness content that offers employees an identity framework as organizational protector, trusted guardian, or security culture leader will generate security-consistent behaviors more durably and with greater generalization across novel threat contexts than compliance-framed training that relies on regulatory obligation as its primary motivational mechanism. BICD analysis identifies which identity frameworks are available to and attractive for specific organizational segments by analyzing the identity facets they perform and the professional self-concepts they project across their digital identity performances.

6.3. Stage Three: Cross-Jurisdictional Threat Communication Architecture

BICD social proof analysis provides the intelligence basis for cross-jurisdictional threat communication decisions that conventional multinational security coordination addresses primarily through formal reporting channels and established liaison relationships. Identifying genuine high-authenticity influence nodes, the individuals, communities, and organizations through which security-relevant information organically spreads within partner networks, enables communication strategies that leverage existing trust relationships rather than relying on formal authority channels that may lack credibility in specific cultural or organizational contexts. This distinction is operationally significant for multinational cybersecurity organizations: threat intelligence shared through trusted network relationships achieves higher processing depth, greater organizational response, and more durable behavioral effects than formally mandated threat reporting received from unfamiliar or distrusted institutional sources.

Multinational cybersecurity coordination frameworks, including ENISA's European cyber crisis coordination framework, the Five Eyes intelligence sharing architecture, and regional cybersecurity coordination mechanisms, establish formal channels for cross-jurisdictional threat communication that are necessary but insufficient for the behavioral threat intelligence exchange that BICD-informed security operations require [35]. Behavioral threat intelligence, including psychographic risk assessments, social engineering campaign characterizations, and insider threat behavioral indicator profiles, requires additional governance frame-

works addressing data minimization, purpose limitation, and cross-jurisdictional data protection obligations that standard technical threat indicator sharing arrangements do not encompass.

[36] demonstrated that effective contemporary influence operations require platform-specific content adaptation rather than cross-platform content repurposing, a finding that translates directly to multinational security communication design: threat communication that is effective in one organizational cultural context may be ineffective or counterproductive in another if it relies on platform assumptions, communication style expectations, or authority framing that does not translate across cultural boundaries. BICD platform-specific behavioral environment analysis provides the intelligence basis for culturally adapted threat communication design by characterizing the communication patterns, trust network structures, and authority dynamics that govern how different national and organizational cultures process and respond to security-relevant information.

6.4. Stage Four: Adaptive Organizational Learning through Behavioral Feedback

The final stage of the intelligence-to-defense pipeline exploits the behavioral intelligence collection capacity inherent in multinational security countermeasure execution. Security awareness programs, phishing simulation exercises, incident response communications, and policy compliance monitoring generate continuous behavioral response data, engagement metrics, behavioral change indicators, incident response patterns, and policy deviation rates, that can be analyzed through BICD procedures to update behavioral risk models and refine countermeasure design parameters in near real time [37].

This feedback architecture transforms security program management from a planning-and-execution sequence into an adaptive organizational learning process. Tactical adaptation, adjusting security awareness content, communication timing, and targeting parameters in response to behavioral performance data, enables rapid identification of failed assumptions before they propagate through extended program timelines into systematic security culture failures. Strategic adaptation, revising behavioral risk segment definitions, countermeasure design parameters, and threat communication architecture in response to accumulated behavioral evidence, enables security program evolution over extended operational timelines as organizational behavioral models are refined by empirical response data. Organizational learning, capturing insights from multiple security program cycles in systematic, policy-level form, enables institutional advancement of behavioral security capabilities beyond individual program cycles, building organizational knowledge about which behavioral population characteristics predict differential response to which security countermeasure approaches in which cross-jurisdictional contexts.

The adaptive feedback loop also provides early warning indicators of adversary counter-security activity. Anomalous patterns in organizational behavioral response data, sudden security compliance drops, sentiment reversals not predicted

by model updates, unexpected network topology shifts in security incident reporting, may indicate adversary counter-operation targeting the same organizational segments. BICD mechanism analysis applied to these anomalous patterns can distinguish natural organizational response variation from adversary-induced disruption, enabling responsive counter-operation before adversary influence achieves significant penetration in target organizational populations.

Table 2. Intelligence-to-Defense pipeline stages.

Stage	Function	Inputs	Outputs	Explanation
Stage 1: Behavioral Risk Segmentation	Classify users by psychological vulnerability	Mechanism analysis (identity, bias, behavior)	Risk profiles (psychographic segments)	Replaces role-based security with behavior-based segmentation
Stage 2: Countermeasure Design	Develop targeted interventions	Segment profiles + narrative insights	Tailored security awareness & defenses	Uses narrative psychology for behavioral influence
Stage 3: Threat Communication	Deliver intelligence across networks	Social proof + influence mapping	Trusted dissemination pathways	Focuses on who people trust, not just formal channels
Stage 4: Adaptive Learning				

Table 2 outlines the four-stage intelligence-to-defense pipeline that operationalizes BICD-derived behavioral intelligence into actionable cybersecurity outcomes within multinational environments. The pipeline begins with behavioral risk segmentation, which replaces traditional role-based models with psychographically informed groupings based on cognitive and behavioral vulnerability. This enables a more precise understanding of which individuals or groups are susceptible to specific threat vectors. The second stage, countermeasure design, translates these insights into targeted interventions, often leveraging narrative and psychological alignment to influence behavior more effectively than compliance-based approaches. The third stage, cross-jurisdictional threat communication, addresses the complexities of multinational environments by emphasizing trust networks and culturally adaptive communication strategies rather than relying solely on formal reporting structures. The final stage, adaptive learning, establishes a continuous feedback loop in which outcomes from implemented countermeasures inform future intelligence assessments and organizational responses. Together, these stages form an integrated, iterative system that connects behavioral analysis to real-world security decision-making. The table illustrates how cybersecurity shifts from a reactive, technically focused model to a proactive, behaviorally informed framework capable of adapting to evolving human-centric threats.

Figure 2 depicts the operational backbone of the BICD framework: a four-stage pipeline that converts behavioral intelligence into coordinated cybersecurity action within multinational environments. Where Figure 1 explains how behavior becomes intelligence, this model explains how intelligence becomes defense.

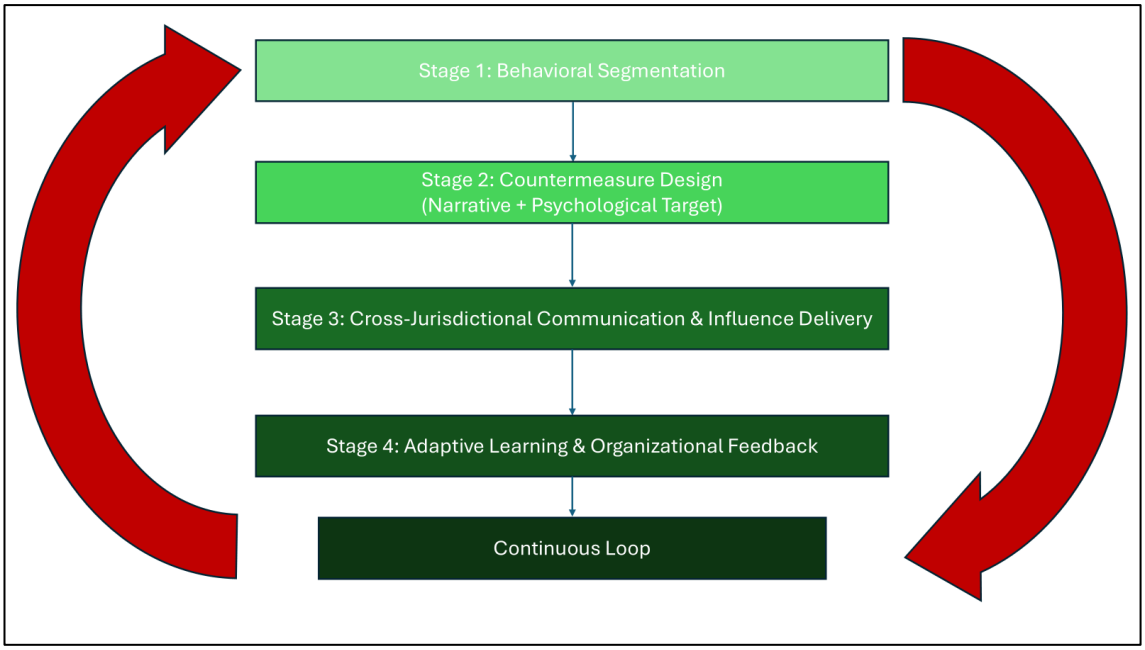

Figure 2. Intelligence defense pipeline.

The pipeline begins with Stage 1: Behavioral Segmentation, which replaces conventional role- or access-based security models with psychologically informed grouping. Instead of treating users as "administrators," "employees," or "partners," this stage classifies individuals according to behavioral patterns, cognitive vulnerabilities, and identity structures derived from BICD analysis. The purpose is precision: different populations are susceptible to different forms of social engineering, insider threat development, or influence operations. By segmenting based on how people think and behave, rather than what role they occupy, organizations gain a far more accurate risk map.

This segmentation feeds directly into Stage 2: Countermeasure Design, where intelligence is translated into targeted interventions. Here, the framework departs from traditional compliance-based security training and instead emphasizes narrative and psychological alignment. Security measures, whether awareness campaigns, phishing defenses, or insider threat interventions, are designed to resonate with the specific motivations, beliefs, and identity frameworks of each segment. The inclusion of narrative reflects a key insight: people do not change behavior through instruction alone, but through meaning, identification, and perceived relevance.

The third stage, Cross-Jurisdictional Communication and Influence Delivery, addresses the realities of multinational cybersecurity environments. Organizations operating across borders must navigate differences in culture, language, legal frameworks, and trust structures. This stage ensures that both threat intelligence and countermeasures are communicated through trusted networks and culturally appropriate channels, rather than relying solely on formal authority or standardized messaging. It recognizes that influence, and therefore security effectiveness,

depends heavily on who delivers the message and how it is perceived, not just on the content itself.

The final stage, Adaptive Learning and Organizational Feedback, closes the loop by integrating outcomes back into the system. Behavioral responses, incident results, and communication effectiveness are continuously monitored and analyzed to refine segmentation models, improve countermeasure design, and recalibrate communication strategies. This creates a dynamic system in which the organization learns from its own interactions with the threat environment, rather than remaining static.

The continuous loop at the bottom of the model is not merely symbolic; it represents a fundamental shift from reactive cybersecurity to an adaptive, intelligence-driven posture. Instead of responding to isolated incidents, the organization evolves in parallel with the behavioral dynamics of both its workforce and its adversaries. The Show that there is a continual feedback loop from stage 1 to stage 4, indicating that organization continues to learn and adapt throughout the different stages.

7. Discussion

Operationalizing the BICD framework in multinational cybersecurity contexts requires organizational and technical adaptations that exceed current standard capabilities across multiple dimensions. At the personnel level, behavioral threat intelligence analytical requirements cannot be met by security analysts trained exclusively in technical threat indicator analysis or by security awareness professionals trained in conventional compliance-based program design. BICD analytical competencies require genuine theoretical grounding in cyberpsychology, the ability to apply mechanism-specific interpretive procedures, recognize their epistemological limitations, construct confidence-calibrated behavioral threat intelligence products, and identify the conditions under which those products support or do not support specific security decisions.

Developing BICD competencies at scale in multinational organizations requires either dedicated recruitment of behavioral scientists with digital environments expertise into security team structures, or sustained multi-year investment in advanced training programs that integrate cyberpsychology into security professional development at a foundational rather than supplementary level. Professional certification standards for behavioral threat intelligence analysis, distinct from general OSINT certification and from technical security certifications, provide the quality assurance architecture that the epistemological distinctiveness of SOCMINT requires. Academic partnerships with cyberpsychology research programs provide one institutional mechanism for maintaining analytical competency currency as platform dynamics and behavioral research findings evolve.

At the technology level, BICD requires integrated analytical platforms supporting longitudinal behavioral tracking across platforms, algorithmic environment modeling, AI-generated content detection, social network topology analysis, and

real-time behavioral response monitoring. These capabilities exist in component form in commercial social media analytics platforms and security orchestration tools but require substantial integration, interoperability engineering, and cross-jurisdictional data governance architecture to achieve the reliability and compliance requirements of multinational security applications. [38] provide frameworks for human-machine teaming architecture in complex analytical environments that are directly applicable to BICD deployment: AI and machine learning systems can automate pattern detection components of mechanism analysis, but the interpretive judgment required to translate detections into confidence-calibrated behavioral threat intelligence products requires human analytical expertise that current systems cannot substitute for at operational quality standards.

The cross-jurisdictional legal landscape governing behavioral monitoring in multinational organizations represents the most significant implementation challenge for BICD deployment. The General Data Protection Regulation (GDPR) in EU jurisdictions imposes stringent requirements on the collection, processing, and retention of personal behavioral data, including social media monitoring of employees per European Parliament, 2016. Article 22 constraints on automated decision-making with significant effects on individuals impose specific procedural requirements on any BICD-based system that produces behavioral risk assessments contributing to employment-consequential security decisions. Equivalent but non-identical privacy and monitoring legislation in jurisdictions including the United Kingdom (post-Brexit), the United States, Canada, Australia, Japan, and Singapore creates a complex compliance matrix that varies by jurisdiction, employment relationship type, and the specific behavioral data categories collected.

The principle of data minimization, which requires that data collected be limited to what is necessary for the specified purpose, imposes specific design constraints on BICD behavioral monitoring architecture in multinational contexts. Behavioral threat intelligence programs that collect comprehensive social media behavioral data across all organizational employees without purpose-specific justification for each data category will face significant legal exposure in GDPR jurisdictions regardless of their security justification. Designing BICD deployment architectures that achieve meaningful behavioral threat intelligence while satisfying data minimization requirements across multiple jurisdictions simultaneously requires legal expertise that most security teams do not currently possess and that cybersecurity governance scholarship has not yet addressed with sufficient specificity to guide multinational organizational practice.

Cross-jurisdictional data transfer restrictions, including GDPR Chapter V restrictions on personal data transfers to third countries without adequate protection mechanisms, impose additional constraints on the multinational intelligence sharing architectures that BICD Stage Three envisions. Behavioral threat intelligence that includes personal behavioral data derived from SOCMINT collection about identified or identifiable individuals requires transfer mechanisms, Standard Contractual Clauses, Binding Corporate Rules, or adequacy decisions, that in-

troduce procedural requirements and liability frameworks into what technical security architectures often treat as purely operational data exchange.

Several conditions define the boundaries of the BICD framework's analytical reliability and require explicit acknowledgment to support calibrated deployment. Cross-Cultural Transferability. The five cyberpsychology mechanisms underlying the BICD framework were predominantly validated in research conducted in Western, English-language, and WEIRD (Western, Educated, Industrialized, Rich, Democratic) digital environments. Platform use norms, identity performance conventions, social proof dynamics, and disinhibition thresholds vary significantly across cultural contexts, with documented differences in collectivist versus individualist settings, high-power-distance versus low-power-distance organizational cultures, and digital communication contexts shaped by non-Western platform ecologies (e.g., WeChat, VKontakte, LINE, or Telegram-dominant environments).

Mechanism-to-indicator mappings developed from Western empirical research may not transfer without cultural calibration to multinational security operations involving Asian, African, Middle Eastern, or Eastern European partner organizations. The framework identifies this cross-cultural validation gap as an explicit research priority; practitioners deploying BICD in non-Western operational contexts should treat all mechanism-to-indicator mappings as hypotheses requiring local validation rather than established analytical procedures. False Positives in Identity Linkage. Platform-conditioned identity performance analysis requires cross-platform identity linkage, the attribution of multiple accounts or behavioral profiles to a single individual, which is a technically and analytically uncertain inference even under favorable data conditions. [20] report linkage precision rates that, while competitive in research settings, produce non-trivial false positive rates when generalized to operational environments with diverse user populations, overlapping linguistic communities, and adversary-managed deceptive accounts. False positive identity linkages produce behavioral profiles attributed to the wrong individual, potentially generating insider threat flags against innocent organizational members. Human review is mandatory before any identity linkage-based behavioral assessment contributes to personnel security decisions; the BICD framework does not authorize automated identity linkage as a basis for consequential security determinations. Sparse and Synthetic Data Environments.

The BICD framework's analytical reliability degrades in two specific data conditions. In sparse data environments, where an individual, account, or organizational population has a limited digital behavioral record across the monitored platforms, the longitudinal behavioral baselines required for mechanism analysis are unavailable, and inferences about psychological state, identity multiplicity, or social influence positioning are correspondingly unreliable. Analysts should designate sparse-data assessments as low-confidence or indeterminate regardless of the behavioral indicators present. In synthetic data environments, where the behavioral record being analyzed is partially or wholly generated by AI-controlled accounts or coordinated inauthentic behavior, applying BICD mechanism analy-

sis to detected behavioral patterns risks producing intelligence assessments of adversary-controlled personas rather than genuine organizational members. AI-generated content detection and coordinated inauthentic behavior analysis must precede or run concurrently with mechanism analysis to bound this inferential risk. The authenticity confidence tier assigned at the conclusion of BICD analysis is the primary output variable for calibrating how much weight any BICD product should carry in downstream security decisions.

The ethical dimensions of BICD application in multinational cybersecurity contexts extend beyond legal compliance frameworks to the fundamental question of organizational legitimacy in behavioral monitoring and influence operations directed at employees, partners, and organizational populations. Cognitive sovereignty, the right of individuals to form their own beliefs through processes that engage their rational capacities rather than circumvent them, provides the appropriate ethical frame for evaluating BICD-based security countermeasure design that deliberately targets identified psychological vulnerabilities to produce behavior change through non-rational mechanisms.

The manipulation versus persuasion distinction is the operationally relevant version of the cognitive sovereignty question in organizational security contexts. Security awareness interventions that engage employees' rational capacities, providing accurate information about threats, making transparent arguments for security behaviors, offering narratives that employees can consciously evaluate, are categorically different from interventions that bypass rational evaluation by exploiting identified cognitive biases, emotional vulnerabilities, or social proof susceptibilities identified through BICD mechanism analysis. Organizations that deploy BICD capabilities for the latter are engaged in manipulation of their own employees, a practice that raises organizational legitimacy questions independent of its legal permissibility and operational effectiveness.

[39] provided an ethical framework for AI applications that is directly applicable to BICD deployment in organizational contexts, identifying the principles of beneficence, non-maleficence, autonomy, justice, and explicability as essential constraints on organizational systems that analyze and influence human behavior [39]. The explicability principle is particularly relevant: employees subject to BICD-based behavioral monitoring and countermeasure design have legitimate interests in understanding that their behavioral data is being collected and analyzed for security purposes, what data categories are involved, how resulting assessments influence organizational decisions about them, and what procedural rights they have regarding those assessments. Transparency requirements that satisfy explicability standards may require disclosure practices that are inconsistent with security program effectiveness in some operational contexts, creating genuine organizational tensions that require executive-level governance resolution rather than technical-level security decision-making [40].

Operational Guardrails for BICD Deployment is the ethical and legal analysis in this Discussion establishes the conceptual obligations governing BICD deploy-

ment. The following operational guardrails translate those obligations into specific implementation boundaries applicable to multinational security organizations. These guardrails are intended as minimum governance standards rather than comprehensive legal advice; organizations must obtain jurisdiction-specific legal review before operational deployment.

Guardrail 1, permissible data sources, in which BICD behavioral collection is restricted to: 1) publicly accessible social media content where no account-level authentication is required for access; 2) organizational communication data for which employees have been provided clear notice consistent with applicable monitoring law and have not been subject to unlawful inducement to consent; and 3) anonymized or pseudonymized behavioral analytics from security systems where individual attribution is not the primary analytical objective. BICD does not authorize covert infiltration of private or closed social media communities, collection from platforms requiring deceptive identity creation, or access to private communications content without lawful intercept authority. Data collected under permissible sources must be retained only as long as operationally necessary and must be subject to data minimization review at each collection reauthorization cycle.

Guardrail 2, mandatory human review points, which is an automated BICD scoring and behavioral pattern detection outputs must not flow directly into consequential security decisions without human analyst review at each of the following decision points: 1) initial designation of an individual as a behavioral threat indicator subject for sustained monitoring; 2) any upward revision of an individual's insider threat risk classification; 3) any referral of a behavioral assessment to human resources, legal, or law enforcement for action; and 4) any cross-jurisdictional sharing of a behavioral assessment that identifies or permits identification of a specific individual. Human review at these points must be conducted by an analyst with documented BICD competency, not solely by automated system output reviewers.

Guardrail 3, decisions excluded from automated behavioral coring, which means that decisions must not rely on automated behavioral scoring alone and require human deliberation with access to primary evidence: employment-consequential security determinations (access revocation, investigation initiation, employment action); assignment of high-confidence insider threat designation without corroborating non-behavioral evidence; cross-jurisdictional intelligence sharing of personally identifiable behavioral profiles; and any security communication strategy that deliberately targets identified psychological vulnerabilities without executive-level review and documented organizational legitimacy determination.

Guardrail 4, manipulation-persuasion boundary, which are the security countermeasures designed using BICD behavioral intelligence must be reviewed against the manipulation-persuasion distinction before deployment: countermeasures that engage employees' rational capacities through accurate information, transparent argument, and consciously evaluable narrative are operationally permissible; countermeasures that bypass rational evaluation by exploiting identified cognitive biases, emotional vulnerabilities, or social proof susceptibilities without

employee awareness require executive authorization and legal review before deployment. The organizational norm is that employees are subjects of security education, not targets of psychological operations.

Guardrail 5, transparency and explicability, are employees in jurisdictions governed by GDPR or equivalent privacy frameworks must be notified that behavioral monitoring for security purposes is conducted, which data categories are collected, how long data is retained, and what procedural rights they hold regarding security assessments derived from their behavioral data. Notification must occur prior to collection, must be specific rather than general, and must be documented in a form that satisfies audit requirements. The explicability standard extends to cross-jurisdictional partner organizations: behavioral threat intelligence products shared with partner organizations must include documentation of the analytical procedure, confidence tier, data source categories, and human review status of each assessment.

8. Conclusions

The BICD framework, applied to multinational cybersecurity contexts in this article, addresses a specific, consequential, and undertheorized gap in organizational security practice: the absence of analytically rigorous, operationally specified methods for extracting behavioral and psychological threat intelligence from social media and organizational communication data that account for the cyberpsychology mechanisms through which digital environments systematically mediate human behavior. The framework's contributions to multinational cybersecurity scholarship and practice are organized around three core claims.

The epistemological claim that SOCMINT requires a behavioral epistemology distinct from OSINT's documentary epistemology, with different analytical procedures, quality standards, and error modes, has direct operational consequences for multinational security organizations that collect social media data as part of insider threat programs, threat actor monitoring, and supply chain security assessment. Applying documentary analytical assumptions to behavioral data produces systematic errors, overconfident threat assessments from disinhibited expression, false attribution from platform-specific identity performances, and misattribution of algorithmic amplification as organic threat activity that erode the credibility and operational value of behavioral threat intelligence programs regardless of their technical sophistication.

The analytical claim that five cyberpsychology mechanisms can be operationalized into specific analytical procedures producing theoretically grounded and epistemologically distinguished behavioral threat intelligence, argued to be superior in explanatory and predictive precision to undifferentiated documentary SOCMINT analysis, a claim that awaits controlled empirical validation as identified in the Future research section. Previous scholarship has established that psychology is relevant to cybersecurity; BICD establishes how that relevance translates into specific threat detection procedures, organizational vulnerability assessments, and se-

curity countermeasure design parameters for defined categories of threat intelligence products applicable to the multinational operating environment.

The operational claim, that BICD intelligence products provide specific, actionable inputs to a four-stage intelligence-to-defense pipeline connecting behavioral threat analysis to organizational security countermeasure design, creates a coherent analytical and operational architecture applicable to the governance and operational structures of multinational organizations across the full range of their cybersecurity mission sets, from insider threat programs and social engineering countermeasures to cross-jurisdictional threat communication and adaptive organizational security culture development.

Against these contributions, this article has argued that BICD's analytical precision intensifies rather than resolves the ethical challenges of behavioral monitoring and influence in organizational contexts. Cognitive sovereignty, manipulation ethics, and democratic legitimacy constraints, including the specific legal obligations that GDPR and equivalent privacy frameworks impose on multinational organizations, do not become less demanding when behavioral security programs become more analytically rigorous; they become more urgent because the monitoring and influence mechanisms are more precisely calibrated to target the specific psychological structures through which individuals exercise autonomous judgment. Multinational organizations that develop BICD-level capabilities must simultaneously develop the ethical governance architecture, embedded in authorization processes, legally compliant across jurisdictions, staffed with relevant behavioral and ethical expertise, and transparent to employees subject to behavioral monitoring, that can ensure those capabilities are deployed consistently with the organizational values and legal obligations that define legitimate security operations as distinct from cognitive surveillance.

The challenge of securing multinational organizations in the cognitive domain is ultimately a challenge of institutional integrity. The analytical tools that enable more effective behavioral threat intelligence can also enable more sophisticated organizational control. The distinction between legitimate and illegitimate applications of these capabilities is not inherent in the capabilities themselves; it is constituted by the institutional commitments, oversight mechanisms, legal compliance frameworks, and ethical constraints within which they are deployed. Future research priorities include controlled experimental validation of BICD analytical procedures against conventional SOCMINT methods in cybersecurity-specific threat assessment tasks, cross-cultural replication studies examining mechanism-to-indicator mappings in non-Western digital environments relevant to multinational operations, and legal-technical governance framework development addressing the cross-jurisdictional compliance architecture that responsible BICD deployment requires.

Conflicts of Interest

The author declares no conflict of interest regarding the publication of this paper.

References

[1] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015) Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, **22**, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

[2] Workman, M. (2008) Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, **59**, 662-674. https://doi.org/10.1002/asi.20779

[3] La Polla, M.N. (2014) Social Media Analytics and Open Source Intelligence: The Role of Social Media in Intelligence Activities. https://tesidottorato.depositolegale.it/bitstream/20.500.14242/139718/1/LaPollaTesiDottorato.pdf

[4] Dover, R. (2020) SOCMINT: A Shifting Balance of Opportunity. *Intelligence and National Security*, **35**, 216-232. https://doi.org/10.1080/02684527.2019.1694132

[5] Troublefield, T.C. (2025) Strategic Military Information Support Operations for Countering Digital Terrorist Threat Networks. *Journal of Applied Security Research*, **20**, 586-602. https://doi.org/10.1080/19361610.2025.2498446

[6] Torraco, R.J. (2005) Writing Integrative Literature Reviews: Guidelines and Examples. *Human Resource Development Review*, **4**, 356-367. https://doi.org/10.1177/1534484305278283

[7] Heartfield, R. and Loukas, G. (2015) A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, **48**, 1-39. https://doi.org/10.1145/2835375

[8] Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R. (2011) Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, **51**, 576-586. https://doi.org/10.1016/j.dss.2011.03.002

[9] Verizon (2024) 2024 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[10] Deppe, C. and Schaal, G.S. (2024) Cognitive Warfare: A Conceptual Analysis of the NATO ACT Cognitive Warfare Exploratory Concept. *Frontiers in Big Data*, **7**, Article 1452129. https://doi.org/10.3389/fdata.2024.1452129

[11] Fenstermacher, L.H., Uzcha, D., Larson, K.G., Vitiello, C.A. and Shellman, S.M. (2023) New Perspectives on Cognitive Warfare. *Signal Processing, Sensor/Information Fusion, and Target Recognition XXXII*. https://doi.org/10.1117/12.2666777

[12] Loch, K.D., Carr, H.H. and Warkentin, M.E. (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, **16**, 173-186. https://doi.org/10.2307/249574

[13] Akhgar, B., Bayerl, P.S. and Sampson, F. (2016) Open Source Intelligence Investigation: From Strategy to Implementation. Springer. https://doi.org/10.1007/978-3-319-47671-1

[14] Goldstein, J.A., Sastry, G., Musser, M., DiResta, R., Gentzel, M. and Sedova, K. (2023) Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations. arXiv: 2301.04246. https://arxiv.org/abs/2301.04246

[15] Hazell, J. (2023) Spear Phishing with Large Language Models. arXiv: 2305.06972. https://arxiv.org/abs/2305.06972

[16] Fredheim, R. and Pamment, J. (2025) Assessing the Risks and Opportunities Posed

by AI-Enhanced Influence Operations on Social Media. *Place Branding and Public Diplomacy*, **21**, 319-326. https://doi.org/10.1057/s41254-023-00322-5

[17] Suler, J. (2004) The Online Disinhibition Effect. *CyberPsychology & Behavior*, **7**, 321-326. https://doi.org/10.1089/1094931041291295

[18] Ancis, J.R. (2025) The Cyberpsychology Influence on Modern Computing. *Communications of the ACM*, **68**, 72-79. https://doi.org/10.1145/3720535

[19] Markman, K.M. (2012) A Networked Self: Identity, Community and Culture on Social Network Sites. *New Media & Society*, **14**, 1240-1242. https://doi.org/10.1177/1461444812453432

[20] Chatzakou, D., Soler-Company, J., Tsikrika, T., Wanner, L., Vrochidis, S. and Kompatsiaris, I. (2020) User Identity Linkage in Social Media Using Linguistic and Social Interaction Features. *Proceedings of the* 12*th ACM Conference on Web Science*, Southampton, 6-10 July 2020, 295-304.

[21] Friedl, P. (2025) The General Data Protection Regulation. In: *Reasonable Expectations of Privacy*: *With Special Regard to European Privacy and Data Protection Law*, Springer Nature Switzerland, 295-344. https://doi.org/10.1007/978-3-031-84881-0_11

[22] Pariser, E. (2011) The Filter Bubble: What the Internet Is Hiding from You. Penguin Press.

[23] Sunstein, C.R. (2017) #Republic: Divided Democracy in the Age of Social Media. Princeton University Press. https://doi.org/10.1515/9781400884711

[24] Vosoughi, S., Roy, D. and Aral, S. (2018) The Spread of True and False News Online. *Science*, **359**, 1146-1151. https://doi.org/10.1126/science.aap9559

[25] O'Keefe, D.J. (2025) Persuasion. In: Hargie, O., Ed., *The Handbook of Communication Skills*, Routledge, 371-390. https://doi.org/10.4324/9781003367796

[26] Muchnik, L., Aral, S. and Taylor, S.J. (2013) Social Influence Bias: A Randomized Experiment. *Science*, **341**, 647-651. https://doi.org/10.1126/science.1240466

[27] Biagio, M.S., Acquaviva, R., Mazzonello, V., La Mattina, E. and Morreale, V. (2021) A New SOCMINT Framework for Threat Intelligence Identification. 2021 *International Conference on Computational Science and Computational Intelligence* (*CSCI*), Las Vegas, 15-17 December 2021, 692-697. https://doi.org/10.1109/csci54926.2021.00180

[28] Susarla, A., Oh, J. and Tan, Y. (2016) Influentials, Imitables, or Susceptibles? Virality and Word-of-Mouth Conversations in Online Social Networks. *Journal of Management Information Systems*, **33**, 139-170. https://doi.org/10.1080/07421222.2016.1172454

[29] Nickerson, R.S. (1998) Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, **2**, 175-220. https://doi.org/10.1037/1089-2680.2.2.175

[30] Kahneman, D. (2011) Thinking, Fast and Slow. Farrar, Straus and Giroux. https://grahamseibert.com/Reviews/Psychometric/thinking%20fast%20and%20slow.pdf

[31] Heuer, R.J. (1999) Psychology of Intelligence Analysis. Center for the Study of Intelligence, Central Intelligence Agency.

[32] Pote, M., Elmas, T., Flammini, A. and Menczer, F. (2025) Coordinated Reply Attacks in Influence Operations: Characterization and Detection. *Proceedings of the International AAAI Conference on Web and Social Media*, **19**, 1586-1598. https://doi.org/10.1609/icwsm.v19i1.35889

[33] Green, M.C. and Brock, T.C. (2000) The Role of Transportation in the Persuasiveness

of Public Narratives. *Journal of Personality and Social Psychology*, **79**, 701-721. https://doi.org/10.1037/0022-3514.79.5.701

[34] McAdams, D.P. (2018) Narrative Identity: What Is It? What Does It Do? How Do You Measure It? *Imagination, Cognition and Personality*, **37**, 359-372. https://doi.org/10.1177/0276236618756704

[35] ENISA (2023) Blueprint for Coordinated Response to Large-Scale Cybersecurity Incidents and Crises in the EU. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

[36] Dash, S. and Mitra, T. (2024) Decoding the Playbook: Multi-Modal Characterization of Coordinated Influence Operations on Indian Social Media. *ACM Journal on Computing and Sustainable Societies*, **2**, 1-19. https://doi.org/10.1145/3675760

[37] Goldman, J. (2023) Influence Operations and the Role of Intelligence. In: Arcos, R., Chiru, I. and Ivan, C., Eds., *Routledge Handbook of Disinformation and National Security*, Routledge, 84-94. https://doi.org/10.4324/9781003190363

[38] Chen, D., Yoon, H.J., Wan, Z., Alluru, N., Lee, S.W., He, R., Moore, T.J., *et al.* (2025) Advancing Human-Machine Teaming: Concepts, Challenges, and Applications. arXiv: 2503.16518. https://arxiv.org/abs/2503.16518

[39] Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., *et al.* (2018) AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, **28**, 689-707. https://doi.org/10.1007/s11023-018-9482-5

[40] Ferrara, E. (2023) Social Bots, Deepfakes, and Disinformation in the Age of Large Language Models. arXiv: 2311.01790. https://arxiv.org/abs/2311.01790