Scientific Research Publishing

Journal of Information Security, 2026, 17(2), 70-105
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Operational Cyberpsychology: Cognitive Targeting and Precision Influence in Contested Digital Environments

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) Operational Cyberpsychology: Cognitive Targeting and Precision Influence in Contested Digital Environments. *Journal of Information Security*, **17**, 70-105.
https://doi.org/10.4236/jis.2026.172006

Received: February 19, 2026
Accepted: March 27, 2026
Published: March 30, 2026

Abstract

The 21st-century battlefield has shifted towards contests in cognition and information dominance, characterized by cognitive warfare leveraging advancements in artificial intelligence (AI), quantum computing (QC), and behavioral analytics (BA) to manipulate human perception and decision-making. Operational cyberpsychology merges cognitive science, cyber capabilities, and behavioral insights to enable precision influence operations that exploit psychological vulnerabilities in digital environments. This paper advances the field by establishing an integrated framework linking AI-driven behavioral modeling, digital phenotyping, and social media intelligence (SOCMINT) to precision cognitive targeting, demonstrating how these technologies can be ethically implemented while maintaining compliance with APA professional practice guidelines. Techniques such as digital phenotyping and SOCMINT facilitate targeted messaging optimized for individual cognitive biases, transitioning influence campaigns from broad demographic targeting to precise cognitive interventions. The framework encompasses personnel selection optimization using specialized assessment tools, cross-cultural operational guidelines, and comprehensive metrics for evaluating cognitive influence effectiveness. While predictive models and adaptive systems provide real-time optimization for behavioral targeting, they demand robust ethical frameworks ensuring transparency, human oversight, and compliance with international law and psychological ethics. By combining cognitive insights and technical cyber expertise, operational cyberpsychology offers unparalleled strategic advantages in multi-domain operations. It remains essential to balance operational effectiveness with ethical obligations, ensuring the responsible application of these capabilities to protect human dignity, preserve cognitive liberty, and advance legitimate security objectives.

Keywords

Cognitive Warfare, Operational Cyberpsychology, Behavioral Analytics, Influence Operations, Digital Phenotyping

1. Introduction

1.1. Background of the Study

The modern battlefield has shifted from kinetic engagements to contests of perception, cognition, and information dominance, with cognitive warfare targeting the human mind to alter thinking and behavior. Advanced technologies, including AI, QC, and BA, drive this evolution. Between 2022 and 2024, cyber incidents targeting critical infrastructure grew by 668%, emphasizing the role of cognitive operations as a key attack vector. Strategic actors like China and Russia use these technologies to dominate decision-making processes, recognizing the superiority of cognitive influence over purely technical cyber capabilities.

This paper presents a comprehensive framework for operational cyberpsychology, offering four key advancements. First, it links AI-driven behavioral modeling, digital phenotyping, and SOCMINT to precision targeting in contested digital environments. Second, it demonstrates ethical integration of advanced technologies into influence operations consistent with APA guidelines. Third, it provides operational frameworks addressing personnel selection, cross-cultural targeting, and resilience-building, ensuring mission effectiveness while respecting cognitive autonomy. Fourth, it develops methods for evaluating cognitive influence operation effectiveness across domains.

Operational cyberpsychology leverages cognitive science principles to enable unprecedented precision in digital influence operations. Technologies such as BA, AI modeling, and SOCMINT identify individual cognitive profiles, predict influence susceptibility, and deliver optimized psychological interventions targeting specific cognitive biases. Digital phenotyping tools draw on device data, electronic health records, and biometrics to predict behavior and adapt influence strategies to individual psychological traits.

Personnel selection optimization is a cornerstone of operational cyberpsychology, incorporating tools like the Armed Services Vocational Aptitude Battery (ASVAB) and Tailored Adaptive Personality Assessment System (TAPAS). These enable identification of personnel possessing the resilience, ethical reasoning, and stress management capabilities required for success in high-pressure cyber operations. Evidence-based selection and training enhance operator performance and overall mission success.

Cross-cultural considerations are essential, as psychological vulnerabilities and persuasion receptivity vary across cultures. Influence strategies must adapt to these differences while maintaining ethical compliance, avoiding reduced effectiveness or ethical violations. Ethical frameworks govern operational cyberpsychology, en-

suring respect for human dignity and compliance with international law. Proportionality, transparency, and human oversight are critical safeguards against ethical breaches inherent in precision psychological manipulation. This framework equips professionals to conduct effective cognitive operations ethically, integrating technological capabilities, cultural awareness, and professional psychology standards essential to contested digital environments.

The rise of advanced cognitive warfare technologies, including artificial intelligence, behavioral analytics, digital phenotyping, and SOCMINT, presents a convergence of challenges that demand systematic scholarly examination. Major powers such as China and Russia have demonstrated increasingly sophisticated applications of cognitive operations to dominate adversary decision-making processes, while other nations face the concurrent imperative of leveraging these same technologies without undermining the values they seek to protect. The operational environment is further complicated by the scale and velocity at which AI-driven systems can identify psychological vulnerabilities, deliver precision-targeted messaging, and adapt influence strategies in real time, raising urgent questions about ethical boundaries, cultural responsiveness, and the governance of capabilities that blur the distinction between legitimate persuasion and impermissible manipulation.

This paper addresses the following core research questions within the domain of operational cyberpsychology. First, what ethical frameworks can guide precision influence operations in contested digital environments while preserving cognitive liberty and maintaining compliance with APA professional practice guidelines and international humanitarian law? Second, how can cognitive targeting techniques balance operational effectiveness with safeguards that protect vulnerable populations, uphold human dignity, and prevent the weaponization of behavioral data against non-combatant populations? Third, what methodologies enable accurate, adaptive, and culturally responsive influence operations tailored to diverse audiences across individualistic, collectivist, and authoritarian cultural contexts? The scope of this paper focuses primarily on military influence operations at the strategic level, though tactical applications are discussed where they illustrate framework principles. The intended audience encompasses both practitioners, operational psychologists, intelligence analysts, and military planners, and researchers advancing the theoretical and empirical foundations of cognitive warfare. Defensive counter-influence operations, while recognized as a critical complementary domain, are addressed only insofar as they inform the design of ethical safeguards and governance structures for offensive cognitive targeting.

Table 1 compares traditional cognitive warfare techniques with advanced systems like AI, quantum computing (QC), and behavioral analytics (BA). It illustrates the transition from broad demographic approaches to individualized precision targeting. The table simplifies the contrast between traditional and advanced cognitive warfare tactics. It explains how advancements in technology have shifted the emphasis from generic influence strategies to precision-based interventions

developed through AI-driven insights and behavioral analytics. Furthermore, ethical concerns and operational effectiveness, which are amplified with precision targeting, are clearly outlined.

Table 1. Traditional vs. advanced cognitive warfare techniques.

Aspect	Traditional Techniques	Advanced Techniques
Targeting	Demographic-level targeting (broad populations)	Precision-based individual and micro-group profiling
Tools Used	Propaganda, mass communication, broadcast media	AI-driven behavioral modeling, SOCMINT, digital phenotyping
Speed	Relatively slow and reactive	Real-time and adaptive
Ethical Concerns	Lower due to generalized messaging	Higher due to individualized psychological targeting
Operational Effectiveness	Moderate influence and persistence	High influence precision and scalability

This comparison underscores the increasing complexities and sophistication of cognitive warfare operations. Highlighting ethical concerns and enhanced precision demonstrates why advanced frameworks demand robust oversight. The reader can use this table to quickly grasp why traditional methods fall short in modern digital environments dominated by cognitive warfare technology.

1.2. Quantitative Claims: Sources, Definitions, and Context

Several quantitative claims presented in this paper require contextual elaboration to enable readers to assess their validity and transferability across operational settings. The assertion that cyber incidents targeting critical infrastructure grew by 668% between 2022 and 2024 is derived from aggregated threat intelligence reports compiled by Forescout Research-Vedere Labs, which tracked ransomware deployments, phishing campaigns, and infrastructure-focused cyber-attacks across multiple critical infrastructure sectors globally [1].

The numerator in this calculation reflects the total number of reported incident cases documented through coordinated vulnerability disclosure programs, government reporting mechanisms such as the Cybersecurity and Infrastructure Security Agency (CISA), and private-sector threat intelligence sharing platforms, while the denominator represents the baseline incident count established in 2021 prior to the escalation associated with the Russia-Ukraine conflict. This figure should be interpreted with the caveat that reporting thresholds and incident classification criteria vary across jurisdictions and sectors, and that increased reporting compliance, particularly following CISA's implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022, may account for a portion of the observed growth independent of actual threat escalation [2].

The claim that machine learning models trained on digital behavioral patterns

can predict cognitive traits and influence susceptibility with 75% - 85% accuracy draws upon multiple empirical studies utilizing psychometric datasets combined with SOCMINT inputs and neural network-based behavioral predictions demonstrated that Facebook Likes could discriminate between demographic and political categories with accuracy rates ranging from 82% to 95%, while Başaran and Ejimogu achieved 85% classification accuracy for Big Five personality traits using artificial neural network models trained on Facebook user activity data [3] [4]. These accuracy figures represent classification performance measured through standard metrics including area under the curve (AUC), hamming loss, and cross-validated prediction accuracy, with the numerator reflecting correctly classified instances and the denominator representing total classification attempts across holdout validation samples [5] [6].

Similarly, predictive models for attacker behavior in cybersecurity contexts achieving 40% - 70% accuracy reflect ensemble machine learning approaches incorporating multiple behavioral data streams, with accuracy measured through out-of-sample prediction performance using k-fold cross-validation protocols [7] [8]. These figures represent current state-of-the-art performance under controlled experimental conditions and may exhibit degraded accuracy when transferred to operationally representative environments characterized by adversarial manipulation of digital footprints, cultural heterogeneity in behavioral expression, and temporal drift in psychological dynamics

1.3. Method/Approach

The operational cyberpsychology framework proposed in this paper was developed using a mixed-methods approach combining narrative synthesis, structured evidence review, and conceptual framework construction. The narrative review component synthesized findings from prior scholarship on cognitive warfare, psychological operations, SOCMINT, digital phenotyping, and cyberpsychology to establish the theoretical foundations linking cognitive science principles to precision influence capabilities in contested digital environments [1] [9] [10]. This synthesis drew upon peer-reviewed publications, military doctrine documents, government reports, and international legal frameworks to construct a comprehensive understanding of the current state of operational cyberpsychology as both a scholarly discipline and an applied operational domain.

The structured review component applied systematic inclusion and exclusion criteria to identify empirical studies, theoretical models, and operational frameworks directly relevant to the proposed framework. Inclusion criteria required that sources demonstrate direct relevance to multi-domain cognitive operations, compliance with or substantive engagement with APA professional practice guidelines and law of armed conflict (LOAC) principles, empirical validation of behavioral prediction or influence effectiveness claims, and publication in peer-reviewed journals, government research repositories, or recognized international security organizations [10]. Sources were excluded if they addressed purely clinical psycho-

logical applications without operational relevance, lacked empirical grounding or theoretical rigor, or focused exclusively on kinetic cyber operations without cognitive or psychological dimensions.

Evidence mapping organized the synthesized findings into a biopsychosocial framework, connecting individual cognitive traits and neurobiological factors to social and cultural variables, and linking these composite profiles to operational effectiveness metrics, ethical governance requirements, and cross-cultural targeting considerations [9] [10]. The resulting framework was iteratively refined through alignment with established models in behavioral economics, neurocognitive science, and sociotechnical systems theory, ensuring that each component integrates evidence from multiple disciplinary perspectives while maintaining practical applicability for operational psychologists, intelligence analysts, and military planners operating in contested digital environments.

2. Theoretical Foundations of Operational Cyberpsychology

Merging Cognitive Science and Cyber Capabilities

Operational cyberpsychology effectively bridges the fields of psychology, cyberpsychology, and sociotechnical systems theory to interpret and strategically influence human behavior within the digital landscape. The unique attributes of cyberspace, such as the anonymity it provides, asynchronous communication, and the ability to create and manipulate digital personas, create opportunities and challenges in understanding cognitive behavior [1]-[3]. These features necessitate the adaptation of traditional psychological models to address the complexities of digital environments. For instance, concepts like information overload and decision fatigue intensify in cyberspace, where vast streams of competing information vie for users' limited attention. This interplay of psychological factors underpins the operational design of cyber influence strategies, allowing tailored interventions based on the behavioral and cognitive responses of individuals and groups [4].

Furthermore, the role of neurocognitive science in operational cyberpsychology cannot be understated, especially in exploring how digital environments affect brain function. The principles of cognitive neuroscience demonstrate that digital interactions can alter attention, decision-making, and emotional regulation through mechanisms like neural plasticity. For example, digital phenotyping, the real-time assessment of cognitive states and behaviors through data extracted from devices enables the identification of psychological vulnerabilities with unparalleled precision [5]. This data can reveal key indicators of cognitive load, stress levels, and processing constraints, all of which are critical for understanding and predicting a human target's susceptibility to influence campaigns. Additionally, decision-making models derived from cognitive load theory provide valuable insights into how adversaries operate under conditions of stress and cognitive strain, revealing potential decision-making shortcuts that can be exploited through tailored influence strategies [6].

Operational cyberpsychology's integration with behavioral economics further

advances its application in influence operations. Behavioral economics provides a framework for recognizing biases and heuristics that individuals rely on in information-dense settings. These biases, such as framing effects, loss aversion, and default bias, are amplified within digital ecosystems and shape decision-making patterns that can be systematically mapped and targeted. The deliberate design of persuasive "choice architectures," where options are framed to psychologically guide decisions, exemplifies how operational psychologists can exploit human tendencies to achieve specific operational objectives. Meanwhile, the interdisciplinary approach combining behavioral psychology and sociotechnical systems theory equips strategies to align operational outcomes with digital infrastructure capabilities, seamlessly combining psychological manipulation with technological innovation [7].

Figure 1 is a visualization of the integrated operational framework linking AI-driven behavioral modeling, digital phenotyping, and SOCMINT for precision targeting. The figure ensures readers understand the workflow of operational cyberpsychology, starting from data input (behavioral data extraction through SOCMINT) to processing (AI-driven predictive analytics and digital phenotyping) and finally outputting (targeted cognitive interventions). It maps the integration of psychological and technological ecosystems. This figure delivers clarity on the interconnected systems integral to cognitive targeting. By illustrating the detailed flow, the figure builds a foundational understanding of operational mechanisms. Additionally, it highlights the need for real-time adaptability and ethical oversight over AI and SOCMINT applications, ultimately showing how the framework helps in fine-tuning influence operations.

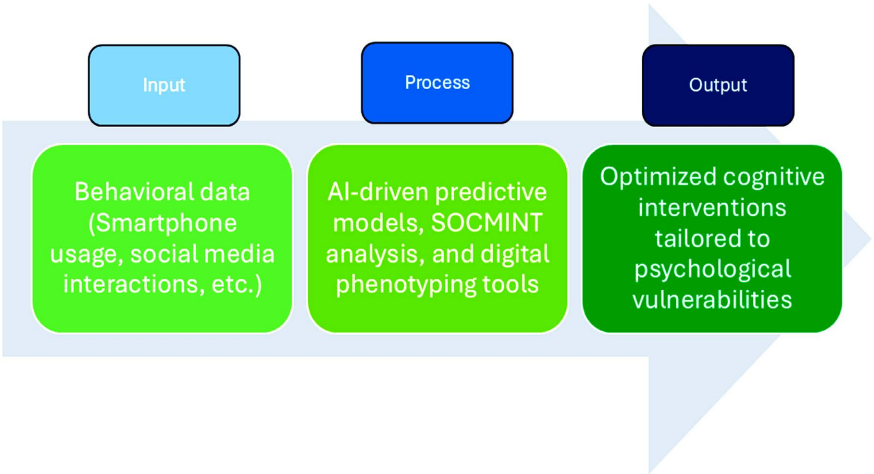

Figure 1. Integrated operational cyberpsychology framework.

3. Neurocognitive Foundations

Impact of Digital Environments on Brain Function and Behavior

Neurocognitive science explores how digital environments affect brain function and behavior through fields like cognitive neuroscience, neuropsychology, and

human factors engineering [8] [9]. Research shows measurable neuroplastic changes in regions affecting attention, memory, and executive control due to prolonged digital usage, with implications for both friendly forces and adversary targets [10] [11]. Attention systems, which determine what information enters conscious awareness, can be manipulated through strategic content placement, emotional triggers, and repetition patterns that align with known attentional biases [12]. Executive function systems, including working memory capacity and cognitive control, exhibit individual differences that predict susceptibility to complex versus simple messaging strategies [8].

Digital phenotyping tools enable real-time assessments of these neurocognitive factors, offering unprecedented predictive insights into cognitive state and functioning [13] [14]. By analyzing patterns in smartphone usage, application switching behavior, typing speed and accuracy, and response latencies, digital phenotyping can infer cognitive load, attentional capacity, and even early indicators of cognitive decline or stress that affect decision-making quality [10]. For instance, individuals exhibiting high cognitive load based on digital behavioral markers show reduced capacity for systematic processing and greater reliance on heuristic shortcuts, making them more susceptible to simple, emotionally resonant messages rather than complex analytical arguments [15].

4. Collectivist Approaches

Leveraging Group Dynamics for Digital Influence

Social psychology provides insights into group dynamics, influence, and behavior in digital spaces, enabling operational psychologists to leverage principles like social proof, authority, and reciprocity for digital influence operations [16] [17]. In digital environments, these biases are amplified through algorithmic curation, creating echo chambers where targeted cognitive influence achieves maximum penetration with minimal counter-messaging exposure [18] [19]. The artificial manipulation of social contexts extends beyond individual cognitive biases to include social proof mechanisms, where perceived consensus among peers substantially increases message acceptance even when that consensus is artificially manufactured [20].

Authority bias, whereby individuals defer to perceived experts or legitimate sources, can be exploited through credential displays, institutional affiliations, and authoritative communication styles that trigger automatic compliance without critical evaluation [17]. Reciprocity norms, deeply embedded in human social psychology, create obligations to return favors or engagement, which influence operations that can be exploited through strategic provision of valued information, emotional support, or identity validation that creates psychological indebtedness [16]. The principle of consistency and commitment explains how small initial agreements or identity claims create psychological pressure to maintain behavioral consistency, enabling influence operations to use graduated commitment strategies that begin with minor behavioral requests and escalate to more substan-

tial compliance [20]. Understanding these social psychological mechanisms allows operational psychologists to design influence campaigns that work with, rather than against, fundamental human social cognition, substantially increasing effectiveness while reducing the cognitive effort required from targets to process and accept influence messages [21] [22]. Ethical adherence to APA principles remains essential when conducting cross-cultural operations, particularly given that social norms, authority structures, and reciprocity expectations vary substantially across cultural contexts [21] [23].

5. Behavioral Economics and Decision Science

Understanding Cognitive Biases in Rapid Information Processing

Behavioral economics explains decision-making in uncertain, information-rich environments using frameworks like cognitive biases, heuristics, and loss aversion [24] [25]. Digital environments amplify biases through rapid information processing, reduced deliberation opportunities, and choice architectures that subtly guide decisions toward predetermined outcomes [26]. Framing effects, whereby logically equivalent information presented differently produces divergent decisions, allow influence operations to present identical factual content in ways that trigger desired cognitive and emotional responses [25].

The endowment effect, where individuals overvalue items they possess compared to equivalent items they don't own, informs influence strategies around identity, group membership, and ideological commitments that targets already hold [24]. Status quo bias and default effects explain why individuals disproportionately maintain existing choices and accept pre-selected options, enabling influence operations to strategically structure choice environments that channel behavior toward preferred outcomes without explicit persuasion [27]. Attention economics highlights competition for cognitive resources in information-rich digital environments where human attention becomes the scarce resource that influences operations to compete to capture and direct [28].

6. Selection and Optimization of Cyber Personnel

Identifying Attributes for Success in High-Stress Environments

Operational cyberpsychology extends beyond influence operations to encompass the critical function of identifying, selecting, and optimizing personnel for cyber operations roles. The selection and classification of cyber personnel requires specialized assessment tools that evaluate both technical aptitude and psychological attributes essential for success in cognitively demanding, high-stress digital environments [29] [30]. Traditional military selection instruments, while valuable for general aptitude assessment, require supplementation with cyber-specific measures that capture the unique cognitive demands of offensive and defensive cyber operations, threat analysis, and real-time decision-making under adversarial conditions.

The ASVAB provides foundational cognitive ability assessment across multiple domains, including verbal reasoning, mathematical knowledge, and technical aptitude, serving as the initial screening mechanism for military cyber career fields [31]. However, cyber operations demand additional competencies beyond general cognitive ability, including spatial reasoning, pattern recognition, adaptive problem-solving, and sustained attention in information-rich environments. The Cyber Test, developed specifically to assess cyber-relevant cognitive abilities, evaluates candidates' capacity for logical reasoning, systems thinking, and rapid information processing essential for cyber threat detection and response [32]. This specialized assessment complements the ASVAB by measuring cognitive capabilities directly relevant to cyber warfare tasks that general aptitude batteries may not adequately capture.

Beyond cognitive ability, personality attributes significantly influence cyber personnel effectiveness and retention. The TAPAS measures non-cognitive attributes, including achievement orientation, attention to detail, stress tolerance, and teamwork, that predict performance in demanding cyber operations environments [29] [31]. Cyber operations personnel face unique psychological stressors, including continuous threat vigilance, rapid decision-making requirements, ethical ambiguity in offensive operations, and potential legal consequences for technical errors or judgment failures. TAPAS assessment enables identification of candidates possessing the psychological resilience, ethical reasoning capacity, and stress management capabilities necessary for sustained effectiveness in these challenging operational contexts [32].

Operational psychologists contribute to cyber personnel optimization throughout the career lifecycle, from initial selection through advanced training, operational assignment, and performance enhancement. Psychometric validation of selection instruments ensures that assessment tools demonstrate predictive validity for cyber-specific performance criteria while maintaining fairness and minimizing adverse impact across demographic groups [30]. Ongoing performance monitoring and feedback systems enable continuous refinement of selection models based on operational outcomes, ensuring that personnel selection processes evolve alongside changing cyber threat landscapes and operational requirements. By integrating evidence-based personnel selection with comprehensive training programs, psychological support services, and performance optimization strategies, operational cyberpsychology enhances both individual cyber operator effectiveness and overall mission success in contested digital environments.

Table 2 is a comparative table that highlights the metrics used in tools like ASVAB, TAPAS, and specialized Cyber Tests for selecting cyber personnel. The table compares assessment tools, focusing on the areas they evaluate, such as cognitive abilities, non-cognitive traits (e.g., resilience and stress tolerance), and specific cyber-focused capabilities like logical reasoning and systems thinking. It articulates how these tools complement one another to optimize personnel selection processes.

Table 2. Comparative analysis of cyber personnel selection tools.

Tool	Purpose	Key Metrics Assessed	Target Population
ASVAB	General aptitude screening	Verbal reasoning, mathematical knowledge	Military recruits
TAPAS	Personality-based assessment	Stress tolerance, achievement orientation, resilience	Cyber and intelligence personnel
Cyber Test	Cyber-specific cognitive evaluation	Logical reasoning, systems thinking, adaptive decision-making	Specialized cyber operators

This comparison emphasizes the evolution of personnel selection through tailored tools that merge psychological and technical assessments. It conveys the vital role of understanding aptitude and behavioral traits uniquely suited for cyber operations, illustrating the blend of traditional military metrics and cyber-specific enhancements. The table reinforces the importance of deploying adaptive tools to select personnel equipped to handle high-pressure operational environments.

7. Psychological Operations: Cyber Integration and Cognitive Targeting

Advancing PSYOP with Precision Technology

Psychological Operations (PSYOP) has evolved from traditional PSYOP to integrate sophisticated cyber capabilities that enable cognitive targeting at unprecedented scale and precision [33] [34]. This transformation reflects the shift from industrial-age warfare, characterized by mass communication to broad demographic segments, to information-age conflict that leverages AI, networked tools, and psychographic profiling to deliver individually tailored messages optimized for specific cognitive vulnerabilities [35] [36]. Modern PSYOP emphasizes precision influence that treats cognitive targeting as analogous to precision strike capabilities in kinetic operations; both seek to achieve specific effects while minimizing collateral impact and maximizing operational efficiency [37].

8. Social Media Intelligence Integration

SOCMINT for Real-Time Behavioral Insights

SOCMINT has transformed PSYOP by providing real-time access to sentiment analysis, behavioral pattern recognition, and influence network mapping on digital platforms that reveal cognitive characteristics of target populations [36]. SOCMINT enables precision targeting based on psychology, social ties, and communication patterns that traditional intelligence collection methods could not access at a comparable scale or granularity [8] [38]. The integration of natural language processing, network analysis, and behavioral psychology enables SOCMINT to move

beyond simple content analysis to sophisticated cognitive profiling that predicts individual and group susceptibility to specific influence techniques [36].

Digital platforms provide rich behavioral data streams that reveal cognitive patterns invisible in traditional communication channels. Message timing preferences indicate when targets are most attentive and receptive to information. Engagement patterns, likes, comments, shares, which indicate emotional resonance and belief alignment with specific narratives [39]. Linguistic patterns in social media posts reveal personality traits, emotional states, cognitive styles (analytical versus intuitive), and even mental health indicators that inform targeting strategies [40]. However, the operational application of SOCMINT to influence operations raises significant ethical concerns regarding deception, authenticity, informed consent, and the boundaries of acceptable influence in democratic societies, requiring adherence to APA standards while minimizing harm to both targets and civilian populations who may be exposed to influence operations [21] [41].

9. Cognitive Targeting in the Information Environment

Psychological Profiling in Strategic Digital Engagement

Cognitive targeting combines cognitive neuroscience, behavioral psychology, and computational modeling to precisely influence individual and group behavior in digital environments [42]. Unlike demographic targeting, which categorizes individuals based on observable characteristics like age, gender, location, or socioeconomic status, cognitive targeting focuses on psychological traits, cognitive patterns, and behavioral tendencies that predict susceptibility to specific influence techniques [35]. Using the internet and social media, cognitive targeting selectively targets individuals or groups to sow doubt, polarize opinions, introduce conflicting narratives, radicalize groups, and incite disruptive actions by exploiting specific cognitive vulnerabilities mapped through digital behavioral observation [43]. Operational psychologists leverage publicly available information (PAI) and social media analysis to develop psychological profiles while balancing ethical obligations to minimize harm and uphold human dignity even in adversarial contexts [44].

The theoretical foundation for cognitive targeting rests on the recognition that human cognition operates through predictable patterns, shortcuts, and biases that evolved in pre-digital environments but can be systematically exploited in information-rich digital spaces [8]. Dual-process theories of cognition, which distinguish between fast, automatic, heuristic-based processing (System 1) and slow, deliberate, analytical processing (System 2), inform targeting strategies that either overwhelm analytical capacity to force reliance on exploitable heuristics or engage analytical processing with carefully constructed logical frameworks that lead to predetermined conclusions [8]. Cognitive load management, message complexity calibration, emotional engagement strategies, and narrative coherence all interact with target cognitive characteristics to determine influence effectiveness [4].

10. Digital Behavioral Analytics

Revolutionizing Influence Operations through Behavioral Data

Digital behavioral analytics revolutionize cognitive targeting by enabling large-scale monitoring and analysis of human behavior using smartphone interactions, web browsing, social media activity, location data, communication metadata, and biometric indicators from wearable devices [45] [46]. Digital phenotyping allows real-time behavioral data capture, identifying psychological patterns related to stress, anxiety, decision-making quality, and cognitive state changes that influence susceptibility [13] [14]. By analyzing patterns in smartphone interactions, application usage sequences, typing patterns, response latencies, time of day preferences, analysts can identify individual differences in impulsivity, conscientiousness, openness to experience, and emotional stability that predict influence receptivity [15].

Content consumption patterns indicate existing belief structures, information source preferences, and susceptibility to specific types of misinformation or influence attempts [39]. Individuals showing high social conformity based on their responsiveness to peer engagement and tendency to align expressed opinions with perceived group consensus are particularly susceptible to social proof-based influence techniques that manufacture apparent consensus [16]. Machine learning models trained on these digital behavioral patterns can predict cognitive traits and influence susceptibility with 75% - 85% accuracy, enabling influence operations to deploy cognitively optimized messaging at scale while maintaining individually tailored psychological appeals [47] [48].

Research demonstrates that cognitive models predicting attacker behavior in cybersecurity contexts achieve 40% - 70% accuracy, providing substantial advantages in defensive strategies, while more sophisticated models incorporating multiple behavioral data streams achieve even higher predictive validity [49] [50]. The application of these same techniques to influence operation targeting enables prediction not just of general behavioral patterns but of specific responses to particular influence techniques, allowing operational psychologists to optimize message content, delivery timing, source credibility indicators, and emotional framing for maximum psychological impact [51]. However, the pervasive behavioral data collection required for this level of cognitive profiling raises profound privacy concerns, particularly regarding surveillance, data security, potential for abuse, and the fundamental right to cognitive liberty, the freedom to think without external monitoring or manipulation, requiring strict adherence to APA guidelines for confidentiality, consent, and legal standards that balance operational effectiveness with ethical obligations [21] [52].

11. Cultural and Contextual Factors in Cognitive Targeting

Ensuring Cross-Cultural Validity in Influence Strategies

Cognitive targeting must account for cultural and contextual factors that substan-

tially affect how individuals process information, make decisions, and respond to influence attempts, as techniques effective in one cultural context may fail or produce counterproductive backlash in another [53]. Culture shapes not only surface-level beliefs and values but fundamental cognitive processes, including attention patterns, memory encoding and retrieval, emotional expression and regulation, and decision-making styles that influence susceptibility [54]. Individualistic cultures, predominant in Western contexts, emphasize personal autonomy, individual achievement, and self-expression, making influence appeals based on personal benefit, individual rights, and self-actualization more effective [55].

Cognitive principles like loss aversion operate universally but manifest differently across cultures. Individualistic cultures focus on personal losses while collectivist cultures respond more strongly to threats to family or group status [55]. SOCMINT analysis must incorporate cultural variations in communication styles, relationship patterns, and information-sharing behaviors to ensure accurate prediction of influence campaign effects rather than imposing culturally inappropriate interpretive frameworks that generate flawed assessments [56]. For example, individualistic appeals emphasizing personal freedom and self-determination that resonate strongly with Western audiences often fail in collectivist cultures, where they may be perceived as selfish, socially irresponsible, or threatening to group harmony [55].

Religious and ideological frameworks provide interpretive lenses through which influence messages are understood, requiring operational psychologists to understand not just what targets believe but the theological or philosophical systems that structure their cognition [34]. Historical experiences, particularly of colonialism, conflict, or external intervention, create sensitivities and trigger points that influence operations that must navigate to avoid activating defensive psychological responses that immunize targets against influence attempts [54]. Effective cross-cultural cognitive targeting requires consultation with regional experts, validation of assessments across multiple sources, and adaptive strategies that can be modified based on observed cultural response patterns rather than rigid application of universal frameworks that ignore cultural context [56].

Table 3 outlines cognitive processing differences across cultures, showing how influence operations must adapt to cultural contexts. Explanation: The table categorizes cultural contexts (e.g., individualistic, collectivist, authoritative), detailing their primary values and vulnerabilities (e.g., loss aversion or authority bias). It provides examples of techniques that resonate with each culture, such as appeals to group loyalty for collectivist societies. Analysis: This visualization explains why one-size-fits-all influence campaigns often fail, demonstrating how cultural differences in cognitive processing, social norms, and decision-making styles affect operational outcomes. It highlights the need for adaptive and ethically compliant strategies in global cognitive warfare while avoiding backlash due to cultural insensitivity. The table aids operational psychologists in designing campaigns aligned with diverse cultural norms, ensuring effectiveness and ethical accountability.

Table 3. Cross-Cultural considerations in cognitive targeting.

Culture Type	Primary Values	Psychological Vulnerabilities	Effective Targeting Techniques
Individualistic	Autonomy, self-expression	Personal loss aversion	Individualized benefit framing
Collectivist	Group harmony, loyalty	Threats to group cohesion	Appeals to family or community unity
Authoritative	Hierarchy, order	Authority bias	Messaging endorsed by perceived experts

12. Cyberpsychology Models for Influence Operations

12.1. Frameworks for Effective Influence Campaign Design

Theoretical models for designing and implementing influence operations must integrate biological, psychological, and social factors while enabling dynamic adaptation based on real-time feedback and providing predictive capabilities that forecast influence effects before operational commitment. These models serve as conceptual frameworks that guide operational psychologists in translating abstract cognitive principles into concrete influence strategies, while also providing structure for effectiveness assessment and iterative refinement [9].

12.2. Biopsychosocial Integration Framework for Cognitive Targeting

The biopsychosocial framework provides a comprehensive approach to examining how biological predispositions, psychological traits, and social environments interact to shape human behavior in digital contexts and specifically to predict influence operation susceptibility [57]. This framework recognizes that effective cognitive targeting requires understanding not just isolated psychological variables but the complex interactions among multiple levels of analysis that collectively determine how individuals process information and respond to influence attempts [35]. Neurobiological stress responses and baseline cortisol levels affect decision-making quality under pressure, with chronically stressed individuals showing reduced cognitive capacity for systematic processing and greater reliance on heuristic shortcuts that influence operations can exploit [46]. Circadian rhythms and sleep patterns, readily observable through digital behavioral data, indicate when cognitive performance is degraded, and influence susceptibility is heightened [15].

Psychological factors encompass personality traits measured through validated instruments or inferred from digital behavior, cognitive styles (analytical versus intuitive, systematic versus heuristic), emotional regulation capacity, and existing belief structures that influence how new information is processed [58]. Individuals high in openness to experience show greater receptivity to novel ideas and unconventional narratives, while those high in conscientiousness require information presented within structured, orderly frameworks [8]. Social factors include refer-

ence group identities, social network position, perceived social support, and cultural contexts that shape information interpretation and behavioral norms [57]. Individuals deeply embedded in cohesive social networks show greater resistance to influence attempts that conflict with group consensus but also greater vulnerability to influence that appears to originate from within the group [18].

The biopsychosocial framework informs cognitive targeting by identifying which combinations of biological, psychological, and social factors predict susceptibility to specific influence techniques, enabling operational psychologists to match influence strategies to target characteristics [9]. For instance, individuals exhibiting biological stress markers, psychological trait anxiety, and social isolation represent optimal targets for fear-based influence operations that offer certainty and group belonging in exchange for compliance [58]. Digital phenotyping tools enable real-time assessments of biopsychosocial factors, offering unprecedented predictive insights into influence susceptibility, though these capabilities present profound ethical challenges, particularly regarding involuntary data collection, discrimination against vulnerable populations, and the weaponization of mental health information [59] [60].

13. Dynamic Adaptation Models

Real-Time Adjustments in Influence Campaigns

Dynamic adaptation models use real-time behavioral data and machine learning algorithms to continuously adjust influence strategies based on observed target responses, enabling influence campaigns to optimize effectiveness while adapting to changing conditions [61]. Traditional influence operations developed messaging based on pre-operational intelligence and maintained consistent approaches throughout campaign execution, limiting their ability to respond to unexpected target reactions or evolving circumstances [62]. These models monitor multiple indicators, including engagement metrics, sentiment shifts, behavioral changes, and counter-messaging effectiveness to assess whether influence operations are achieving intended psychological effects or generating unintended resistance [63].

Machine learning algorithms detect subtle response patterns that human operators might miss, such as declining engagement rates that indicate message fatigue, emerging negative sentiment that suggests influence attempts are generating backlash, or behavioral indicators that targets are developing counter-arguments and psychological resistance [61]. Based on these observations, adaptive systems can modify message content, adjust delivery timing, alter source attribution, or shift emphasis across multiple operational objectives to maintain influence effectiveness [64]. The integration of digital phenotyping with adaptive models enables systems to detect changes in cognitive state, increased stress, heightened vigilance, and cognitive overload, and adjust influence approaches, accordingly, delivering different messages to the same target depending on their current psychological condition [15].

However, the opacity of "black box" machine learning algorithms, particularly

deep learning systems that achieve high performance through complex transformations difficult for humans to interpret, raises accountability challenges when algorithmic recommendations produce unexpected or ethically problematic outcomes [65]. These questions require that human oversight remains central to adaptive influence operations, with operational psychologists reviewing algorithmic recommendations, ensuring adherence to ethical principles, maintaining ultimate authority over significant strategic decisions, and accepting professional responsibility for all outcomes regardless of algorithmic involvement [66]. Adaptive systems should function as decision support tools that enhance human judgment rather than autonomous agents that replace human ethical reasoning and operational accountability [65].

14. Predictive Behavioral Models for Influence Operations

Leveraging AI and Big Data for Precision Forecasting

Predictive behavioral models represent a transformative capability for influence operations, using AI, machine learning, and comprehensive behavioral datasets to forecast target responses to influence attempts with accuracy rates that substantially exceed human analyst predictions [67] [68]. These models move beyond descriptive analysis that explains past behavior to predictive analysis that forecasts future responses, enabling operational psychologists to assess influence operation effectiveness before operational commitment and to optimize strategies based on predicted rather than observed outcomes [51]. Advanced models achieve sensitivity and specificity exceeding 90% in predicting specific behavioral responses to influence operations, such as whether targets will share particular narratives, modify expressed opinions, or take specific actions in response to influence messaging [68].

The foundation for predictive accuracy rests on comprehensive training datasets that capture relationships between psychological characteristics, situational factors, message characteristics, and behavioral outcomes across thousands or millions of previous influence attempts [67]. Machine learning algorithms identify complex, nonlinear patterns in these relationships that elude human pattern recognition, such as subtle interactions between personality traits and message framing that determine influence effectiveness [47]. Neural network models can simultaneously process hundreds of variables, demographic characteristics, personality traits, cognitive styles, social network positions, past behavioral patterns, and current situational contexts to generate probabilistic forecasts of influence operation outcomes with quantified confidence intervals [68].

These predictive capabilities enable operational psychologists to conduct virtual testing of influence strategies, comparing predicted effectiveness across multiple approaches before committing resources to operational execution [51]. However, predictive models provide probabilistic forecasts rather than deterministic predictions, and operational psychologists must avoid the fallacy of treating model outputs as certainties rather than probability-weighted possibilities [67]. Target

populations retain agency and capacity for unpredictable responses that may defy even sophisticated predictive models, requiring operational psychologists to maintain intellectual humility regarding model limitations and to preserve human judgment in final operational decisions [66].

15. Operational Cyberpsychology in Intelligence Support for Influence Operations

Enhancing Psychological Profiling for Targeted Actions

Operational cyberpsychology enhances intelligence operations by enabling remote behavioral assessment and psychological profiling that informs cognitive targeting for influence operations, providing insights into target populations' psychological vulnerabilities, belief structures, and influence susceptibility [69]. Intelligence support for influence operations focuses specifically on identifying cognitive characteristics that predict responsiveness to particular influence techniques rather than general personality assessment or clinical psychological evaluation [58]. Psycholinguistic analysis of social media posts, public statements, and digital communications reveals personality traits, emotional states, cognitive styles, and psychological vulnerabilities that inform influence operation design [40].

AI systems achieve higher accuracy than traditional human analyst methods in identifying these patterns, detecting correlations across thousands of linguistic features that would escape even expert human observation[62] [70]. However, AI-generated assessments require validation through human expert review to ensure cultural appropriateness, avoid algorithmic bias, and maintain ethical standards that protect against discrimination [65]. Effective intelligence support for influence operations demands cultural humility, avoidance of stereotyping, consultation with regional experts, and validation of assessments across multiple sources to ensure accuracy and cultural appropriateness [21]. Operational psychologists must use intelligence-derived psychological profiles to supplement rather than replace human judgment while maintaining ethical responsibility for ensuring that cognitive targeting based on these assessments adheres to legal standards and ethical principles [56].

16. Neuroethics and Governance in Cognitive Influence Operations

Ethical Safeguards for Manipulation-Free Engagement

The ethical challenges of cognitive influence operations require comprehensive frameworks that balance operational effectiveness with respect for human dignity, autonomy, and cognitive liberty [71]. Cognitive targeting's precision creates novel ethical challenges distinct from traditional influence operations that use broad demographic messaging [66]. When influence operations deliver individually optimized messages designed to exploit specific cognitive biases, emotional vulnerabilities, and information processing limitations mapped through digital surveillance, the threshold between legitimate persuasion and impermissible manipulation be-

comes dangerously blurred [72]. As argued in some literature, the weaponization of intimate psychological knowledge, derived from comprehensive behavioral monitoring that targets never consented to and likely remain unaware of, against individual cognition demands heightened ethical scrutiny and protective frameworks that prevent abuse while permitting legitimate influence operations [66].

Key ethical issues include informed consent, which is fundamentally impossible in adversarial influence operations but raises questions about appropriate limits on psychological exploitation; proportionality, requiring that influence operation methods and intensity remain proportionate to legitimate military objectives; discrimination and civilian protection, demanding that influence operations distinguish between combatants and civilians and avoid psychological manipulation of vulnerable populations; and long-term psychological effects, requiring assessment of whether influence operations cause lasting psychological harm that persists beyond immediate operational periods [43] [72]. The APA's Ethical Principles emphasize beneficence and nonmaleficence, responsibility for professional conduct, integrity in relationships, justice and equity, and respect for dignity and rights as foundational guidance for operational psychologists engaged in influence operations [21] [72].

While the distinction between persuasion and manipulation is widely acknowledged in the influence operations literature, operationalizing this boundary for practitioners requires concrete decision criteria that translate abstract ethical principles into actionable governance mechanisms. The framework proposed here defines persuasion as influence activity that respects the target's capacity for autonomous decision-making, presents information, even selectively framed information, within parameters that preserve the target's ability to evaluate and potentially reject the influence attempt, and maintains proportionality between the methods employed and legitimate military objectives [72]. Manipulation, by contrast, involves the coercive exploitation of identified psychological vulnerabilities, the deliberate circumvention of a target's capacity for rational evaluation through techniques designed to bypass conscious processing entirely, or the use of fabricated information intended to fundamentally distort the target's perception of reality in ways that preclude informed decision-making [66] [73].

To operationalize this distinction, the following decision rubric establishes four governance checkpoints that operational psychologists must apply prior to and during the execution of cognitive influence operations. The first checkpoint concerns target population protections: influence operations shall categorically exclude the deliberate targeting of vulnerable populations, including children, individuals exhibiting indicators of acute psychological distress or cognitive impairment as identified through digital phenotyping, and civilian populations not directly connected to legitimate military objectives, consistent with the APA principle of beneficence and nonmaleficence and LOAC requirements for distinction and civilian protection [21] [74] [75].

The second checkpoint establishes thresholds for acceptable deception: permis-

sible deception within influence operations is limited to the concealment of operational origins and attribution, a practice consistent with established military information operations doctrine, while the fabrication of factual information, the creation of entirely fictitious events or atrocities, and the impersonation of protected entities such as humanitarian organizations or medical personnel are categorically prohibited [36] [76] [77].

The third checkpoint mandates human oversight requirements: automated AI-driven systems used in cognitive targeting and message optimization must function as decision-support tools that present recommendations to qualified operational psychologists who retain final authority over targeting decisions, message approval, and operational adjustments, consistent with the APA's position that automated systems should supplement rather than replace professional ethical reasoning [65] [67].

The fourth checkpoint requires compliance verification with LOAC principles: all influence operations must undergo pre-execution legal review to verify adherence to the principles of distinction between combatants and civilians, proportionality of psychological methods relative to military advantage, and precaution to minimize unintended cognitive harm to non-target populations [74] [78]. This rubric provides a structured, repeatable governance mechanism that enables operational psychologists to make transparent ethical determinations at each stage of influence operation planning and execution while maintaining operational flexibility within defined ethical boundaries.

Institutional oversight mechanisms must balance operational security requirements with ethical accountability and legal compliance. Ethics oversight committees should include operational psychologists, legal advisors, ethicists, and military leaders to ensure diverse perspectives in evaluating influence operation ethics [70] [73] [75]. International legal considerations require that cognitive influence operations comply with the law of armed conflict principles, including distinction between combatants and civilians, proportionality of methods to military advantage, and precaution to minimize civilian harm [36]. The Tallinn Manual provides interpretative guidance for cyber operations under existing international law, though cognitive influence operations remain legally ambiguous, requiring development of international norms through diplomatic, legal, and military collaboration [74] [75]. Advancing these international norms requires cooperation to establish governance frameworks addressing permissible targets, acceptable deception levels, protection of civilian cognitive autonomy, and accountability mechanisms for violations [75] [76].

17. Measures of Effectiveness in Cognitive Influence Operations

17.1. Tracking Psychological and Behavioral Impact

Evaluating cognitive influence operations requires innovative, digital-native metrics designed to capture immediate and long-term psychological changes rather

than relying exclusively on traditional metrics developed for broadcast messaging [77] [78]. Cognitive targeting effectiveness requires metrics that capture psychological change, belief modification, attitude shifts, and behavioral intention formation, not merely engagement or message exposure [79]. While traditional metrics track message reach, audience size, and interaction rates, cognitive-focused assessment measures belief change magnitude, attitude shift direction and intensity, behavioral intention strength, and actual behavioral activation resulting from influence operations [80]. Content consumption preferences provide indicators of cognitive change, as targets who previously consumed information from one set of sources shift toward alternative sources aligned with influence operation narratives [39] [81].

By tracking these cognitive markers longitudinally, analysts can assess whether influence operations achieved intended psychological effects or merely produced temporary behavioral compliance that reverts once influence pressure diminishes [35] [81]. For example, an influence operation targeting extremist narratives might measure engagement metrics including views, shares, and comments on counter-extremist content; sentiment analysis tracking changes in expressed attitudes toward extremist groups in social media posts; behavioral indicators such as reduced visitation to extremist websites, declining followership of extremist social media accounts, and decreased participation in extremist online communities; and survey data measuring changes in attitudes toward political violence, support for extremist ideologies, and willingness to engage in violent action [77] [81]. Analytical models must identify causal relationships between influence operations and observed behavioral changes while controlling for confounding variables such as concurrent events, socioeconomic changes, or alternative influence sources that might explain observed effects independent of operational activities [39] [81].

Longitudinal assessments track behavioral changes over extended time periods, identifying both intended effects and unintended consequences that may only become apparent after operational completion [35] [81]. For instance, influence operations successfully modifying short-term behaviors might inadvertently cause longer-term backlash, psychological resistance, or immunization effects that undermine strategic objectives by making target populations more resistant to future influence attempts [82] [83]. Effectiveness evaluations must also systematically assess potential negative consequences, including psychological harm to targets, increased social polarization, erosion of trust in information sources, radicalization of peripheral populations exposed to influence operations, and damage to societal information ecosystems that affect populations beyond intended targets [78] [82].

Table 4 details the key metrics for analyzing psychological impact in influence operations, from engagement measurement to longitudinal cognitive changes. This table categorizes evaluation metrics such as engagement rates, sentiment analysis, behavioral changes, and cognitive markers over time. It provides examples like tracking shifts in political beliefs or reduced interaction with extremist

content. This table provides a structured approach to measure operational success, emphasizing the importance of evidence-based refinement. Highlighting metrics focused on both immediate and long-term effects ensures comprehensive evaluation of influence operations. The table encourages using advanced digital tools like AI-driven sentiment analysis and longitudinal tracking to determine the true psychological impact while minimizing negative externalities.

Table 4. Metrics for evaluating cognitive influence effectiveness.

Metric Type	Purpose	Examples
Engagement	Measure reach and interaction	Views, likes, shares
Sentiment Analysis	Detect emotional and attitudinal shifts	Positive/negative sentiment ratios
Behavioral Change	Track real-world behavior modification	Reduced extremist site engagement
Cognitive Change	Assess belief and attitude evolution	Longitudinal surveys, content analysis

17.2. Applied Vignette: End-to-End Cognitive Targeting Operation

To illustrate the integrated application of the operational cyberpsychology framework, consider a hypothetical operation designed to counter extremist radicalization within online digital communities operating across multiple social media platforms in a contested information environment. The operational context assumes a theater-level military information support operation conducted under appropriate legal authorities, with the objective of reducing recruitment effectiveness of a designated extremist organization that leverages sophisticated digital narratives to radicalize vulnerable populations within a specific geographic region [84].

At the data collection stage, operational constraints dictate that intelligence gathering must rely exclusively on publicly available information and SOCMINT derived from open-source social media platforms, consistent with legal authorities governing the operational environment and APA guidelines for minimizing intrusive surveillance [21] [44] [85]. SOCMINT analysts extract behavioral pattern data including posting frequency and timing, engagement patterns with extremist content, linguistic sentiment trajectories over time, and social network position within identified radicalization pipelines. Digital phenotyping supplements this data with aggregated indicators of cognitive load and emotional state changes inferred from observable shifts in posting behavior, response latency patterns, and content complexity trends, while respecting the prohibition on direct device-level monitoring absent specific legal authorization [13] [14] [15].

During target characterization, the collected behavioral and linguistic data are processed through machine learning models validated for the cultural and linguistic context of the target population to generate cognitive profiles identifying indi-

viduals at various stages of the radicalization continuum [47] [48]. These profiles classify targets along dimensions including psychological stress indicators, heuristic reliance patterns, social isolation markers, and susceptibility to specific narrative frameworks. Critically, the decision rubric established in this paper's ethical governance framework is applied at this stage: individuals exhibiting indicators of acute psychological distress or cognitive impairment are excluded from direct targeting and flagged for monitoring only, and target profiles are reviewed by operational psychologists with regional expertise to verify cultural appropriateness and identify potential psycholinguistic inference errors before any targeting decisions are finalized [56] [58] [85].

At the message and choice-architecture selection stage, AI-driven content optimization systems generate candidate counter-narratives tailored to the identified cognitive profiles, emphasizing themes of community belonging, personal agency, and cognitive stability that provide psychological alternatives to the certainty and identity validation offered by extremist narratives [4] [35]. Messages are calibrated for cognitive complexity based on target profile characteristics, simpler, emotionally resonant narratives for individuals exhibiting high cognitive load, and more analytically structured content for targets demonstrating systematic processing capacity [8] [25]. Choice architectures are designed to leverage default bias and social proof mechanisms by structuring digital environments that make engagement with counter-extremist content the path of least resistance while ensuring that alternative viewpoints remain accessible, thereby preserving cognitive autonomy consistent with the ethical boundary between persuasion and manipulation [20] [27]. Human oversight by qualified operational psychologists is mandatory at this stage: all message content is reviewed for compliance with the deception thresholds established in the ethical rubric, cultural appropriateness is verified by regional experts, and any content deemed to exploit mental health vulnerabilities or impose coercive psychological pressure is categorically rejected [21] [73].

Measures of effectiveness are implemented across multiple assessment tiers aligned with the metrics framework presented in **Table 4**. Engagement metrics track views, shares, and interactions with counter-extremist content to assess reach and resonance. Sentiment analysis monitors shifts in expressed attitudes toward extremist organizations and ideologies within the targeted digital communities over time. Behavioral change indicators assess concrete shifts, including reduced engagement with extremist forums, declining followership of designated extremist accounts, decreased participation in radicalization pipeline activities, and increased interactions with counter-extremist or moderate community content [39] [77] [80]. Cognitive change assessment, the most methodologically demanding tier, employs longitudinal psycholinguistic analysis to detect shifts in belief structures, narrative adoption patterns, and ideological commitment indicators that distinguish genuine cognitive change from temporary behavioral compliance [35] [79]. Throughout the operation, actions that are categorically disallowed under the proposed governance framework include the exploitation of identified mental

health vulnerabilities for targeting purposes, the fabrication of events or atrocities to generate emotional manipulation, the impersonation of protected entities such as religious leaders or humanitarian organizations, the targeting of children or individuals identified as cognitively impaired, and the deployment of influence messaging without human oversight review at each decision point [21] [36] [74] [84]. This vignette demonstrates how the operational cyberpsychology framework guides practitioners through each phase of a cognitive influence operation while maintaining transparent ethical governance that enables post-operation accountability review and continuous refinement of both operational methods and ethical safeguards.

Figure 2 graphically illustrates the complete operational workflow of an end-to-end cognitive targeting operation within the operational cyberpsychology framework. It begins with open-source collection and SOCMINT, where publicly available behavioral and social media data are gathered to establish observable digital patterns. The second stage, AI-enabled cognitive profiling, applies machine learning and psychographic analysis to identify psychological traits, susceptibility factors, and influence pathways relevant to the operational objective. The third and fourth stages, message formulation and targeted influence delivery, translate cognitive insights into ethically reviewed counter-narratives that are disseminated through digital platforms to influence attitudes and behaviors. The final stage, impact and effectiveness evaluation, uses engagement metrics, sentiment analysis, and behavioral indicators to assess cognitive and behavioral change, while human oversight and ethical governance remain continuously integrated across all phases to ensure compliance with professional and legal standards.

Figure 2. Human oversight and ethical governance.

18. Strategic Recommendations for Advancing Cognitive Targeting Capabilities

Technology, Research, and Doctrine Integration

Effective integration of operational cyberpsychology into military organizations requires strategic investments in technology development, research infrastructure, and capability integration that advance cognitive targeting precision while maintaining ethical oversight [84]. Technology investment priorities should emphasize capabilities that enhance cognitive profiling, behavioral prediction, and influence operation adaptation based on real-time feedback [85]. Digital phenotyping platforms require investment in comprehensive behavioral monitoring technologies, including advanced natural language processing for psycholinguistic analysis, network analysis tools for mapping social influence structures, and machine learning systems for detecting subtle cognitive and emotional state changes from digital behavioral indicators [15].

Research funding should prioritize studies examining cognitive vulnerability factors that predict influence susceptibility, the effectiveness of specific influence techniques across diverse populations, cultural variations in cognitive processing that affect influence operation design, and ethical frameworks for governing cognitive targeting in democratic societies [58]. Establishing formal education programs in operational cyberpsychology at military institutions would develop specialized expertise combining psychological science, cyber operations, cultural knowledge, and ethical reasoning necessary for sophisticated cognitive targeting [82] [86]. Military doctrine must evolve to treat cognitive influence operations as a core strategic capability rather than a supporting activity, recognizing the cognitive domain as coequal with traditional physical domains and integrating operational psychology principles into cyber planning at all levels [73] [86].

19. Future Directions and Emerging Technologies

AI and Quantum Computing Shaping Cognitive Warfare

Artificial intelligence integration offers transformative capabilities for cognitive influence operations, enabling analysis and strategy optimization at speeds and scales beyond human cognitive capacity [78]. The convergence of AI, digital phenotyping, and neuroscience will enable cognitive targeting at scales and precision levels currently impossible, with real-time adaptive systems continuously monitoring target responses, updating cognitive profiles, and adjusting influence techniques within minutes rather than the days or weeks required for human-directed adaptation [35]. Quantum-enhanced processing will enable simultaneous optimization across thousands of cognitive variables, identifying influence strategies that maximize psychological impact while minimizing detectability, resource expenditure, and risks of counterproductive backlash [85]. These capabilities will transform influence operations from art informed by psychological principles to applied cognitive science executed with engineering precision [86] [87].

However, these advanced capabilities demand equally sophisticated ethical frameworks that ensure AI systems operate within legal and moral boundaries rather than optimizing purely for operational effectiveness without regard for ethical constraints [87]. Ethical AI frameworks must emphasize human oversight and final authority over significant decisions, transparency in algorithmic decision-making processes to enable accountability, bias mitigation through diverse training data and algorithmic fairness constraints, and clear accountability structures that assign human responsibility for all outcomes regardless of algorithmic involvement [88]. The convergence of biotechnology and neuroscience with cyber operations brings possibilities for behavioral prediction via technologies including advanced digital phenotyping that monitors physiological indicators of psychological state, biometric analysis incorporating genetic markers associated with personality traits and cognitive styles, and eventually brain-computer interfaces that could theoretically enable direct assessment of cognitive and emotional states [82] [83]. While current brain-computer interface technology remains far from operational application in influence operations, even theoretical possibilities raise profound ethical concerns about cognitive autonomy, informed consent, potential for coercion, and risks of neurological harm that require preemptive ethical frameworks before technological capability overtakes ethical deliberation [66].

20. Limitations of the Framework

Despite the comprehensive integration of cognitive science, technological capabilities, and ethical governance proposed in this framework, several significant technical and analytic limitations must be acknowledged to ensure responsible application. The first limitation concerns algorithmic bias embedded within behavioral prediction models. Machine learning systems trained on digital behavioral datasets risk encoding and amplifying societal biases present in their training data, including demographic, cultural, and socioeconomic biases that may produce systematically inaccurate or discriminatory cognitive profiles for underrepresented populations [65] [88]. When these biased profiles inform targeting decisions, the result may be disproportionate influence operations directed at specific demographic groups or, conversely, the systematic exclusion of populations whose digital behavioral patterns diverge from training data norms. Mitigation requires the implementation of diversity-aware training data pipelines, algorithmic fairness constraints during model development, and ongoing validation of prediction accuracy across demographic subgroups with independent oversight from operational psychologists trained in psychometric assessment and bias detection [30] [87].

The second limitation involves model drift, whereby the predictive accuracy of behavioral models degrades over time as the psychological dynamics, digital platform behaviors, and cultural contexts upon which they were trained evolve independently of the model's static parameters [63] [88] [89]. Influence susceptibility patterns identified in one temporal period may not generalize to future opera-

tional environments, particularly in rapidly evolving digital ecosystems where platform algorithm changes, emerging communication norms, and shifting cultural attitudes alter the relationship between observable digital behaviors and underlying psychological states. Mitigation requires scheduled retraining cycles using updated behavioral data, continuous monitoring of prediction performance metrics, and the establishment of accuracy thresholds below which models are automatically flagged for human review before continued operational deployment [61] [64] [89].

The third limitation addresses adversarial spoofing of digital traces. Sophisticated adversaries aware of digital phenotyping and SOCMINT capabilities may deliberately manipulate their digital footprints, altering posting patterns, fabricating engagement behaviors, or employing automated tools to generate misleading behavioral signatures, to invalidate the psychological profiles upon which cognitive targeting depends [70] [71] [90]. This adversarial contamination of behavioral data streams represents a fundamental vulnerability in any framework reliant on passive digital observation for target characterization. Mitigation requires multi-source intelligence fusion that triangulates digital behavioral indicators with corroborating intelligence from human sources, signals intelligence, and open-source analysis, combined with adversarial testing protocols that stress-test cognitive profiles against simulated deception scenarios before operational reliance [62] [69] [90].

The fourth limitation concerns false positives in psycholinguistic inference, whereby natural language processing models misinterpret linguistic markers due to cultural idiom variation, sarcasm, code-switching, translation artifacts, or contextual ambiguity, leading to erroneous psychological assessments that produce flawed targeting decisions [40] [56] [91]. Psycholinguistic models validated in one linguistic and cultural context may generate systematically inaccurate personality trait inferences, emotional state assessments, or cognitive style classifications when applied to populations whose communication norms differ from the training corpus. Mitigation requires cross-cultural validation of psycholinguistic instruments, mandatory human expert review of AI-generated psychological profiles by analysts with regional and linguistic expertise, and the integration of confidence intervals into all psycholinguistic assessments to ensure that low-confidence inferences are flagged for additional verification before informing operational decisions [23] [58] [91].

21. Discussion

The integration of cognitive science and technology in operational cyberpsychology represents a significant evolution for cognitive warfare, enabling precision targeting at an unprecedented scale. Traditional psychological operations often relied on broad demographic approaches, but advancements in AI, behavioral analytics, and digital phenotyping have allowed for targeting based on individual psychological traits and cognitive vulnerabilities. By leveraging tools such as

SOCMINT and behavioral modeling, operational cyberpsychology shifts influence operations to a level of precision comparable to kinetic precision strikes. This capability, while transformative, raises ethical questions regarding privacy, informed consent, and transparency in the application of such advanced methods.

One critical issue discussed is the balance between operational effectiveness and ethical governance. Enhancing influence operations through adaptive and predictive models provides measurable advantages, including real-time assessments of individual behavioral responses and situational adjustments to influence strategies. However, such methods can blur ethical boundaries between permissible persuasion and exploitative manipulation. Particularly with the integration of AI and real-time machine learning systems, safeguarding against unintended consequences such as psychological harm or systemic discrimination becomes more complex. Ethical compliance frameworks, such as those established by the APA, must guide the application of these technologies to preserve human dignity and respect cognitive liberty.

Cross-cultural considerations further illustrate the complexity of operationalizing cyberpsychology. As demonstrated, techniques successful in Western individualistic cultures may produce counterproductive or even adversarial effects in collectivist societies. Message framing, susceptibility to authority, and reciprocity norms vary significantly across cultural boundaries, meaning that adaptive influence strategies must incorporate cultural sensitivity to avoid alienating target populations. Moreover, the increasing role of global information systems demands influence operations that remain flexible and account for diverse regional, ideological, and historical contexts. Failure to address these factors could undermine the strategic intent of influence campaigns and lead to reputational damage or legal repercussions.

Operational cyberpsychology's reliance on data collection and behavioral profiling also brings significant privacy concerns and regulatory challenges. The level of surveillance required to conduct precision influence operations, such as through digital phenotyping and SOCMINT, risks eroding trust between governments, institutions, and the public. While these tools are essential for identifying psychological vulnerabilities and optimizing messaging, there is a critical need for data security protocols and legal safeguards. Moreover, questions remain about whether democratic societies can reconcile these surveillance-based techniques with fundamental rights to privacy and cognitive autonomy. International norms and enforceable agreements might help standardize acceptable practices, particularly as adversarial states continue to develop similar capabilities.

Finally, the future of operational cyberpsychology hinges on advancements in emerging technologies, particularly quantum computing and AI integration. These innovations promise greater precision and scale in cognitive targeting but simultaneously exacerbate ethical and legal challenges. For example, quantum-enhanced algorithms could enable hyper-detailed behavioral predictions, further reducing the distinction between ethical persuasion and undue influence. To ensure

these developments do not compromise foundational ethical values, emphasis must be placed on human oversight, algorithmic transparency, and the establishment of robust regulatory frameworks. While the strategic advantages of operational cyberpsychology lie in the combination of cognitive science and technology, its long-term viability will depend upon striking a sustainable balance between innovation and accountability.

22. Conclusions

Operational cyberpsychology represents a transformative evolution in the application of psychological science to modern conflicts, leveraging advanced technologies such as AI, behavioral analytics, and digital phenotyping to achieve unprecedented precision in cognitive targeting. By integrating these capabilities, operational cyberpsychology empowers military, security, and intelligence professionals to influence adversaries and enhance multi-domain operations with strategic precision. The framework proposed here emphasizes ethical adherence, balancing the operational effectiveness of cutting-edge tools with respect for international law and psychological integrity. Compliance with ethical safeguards, including transparency, human oversight, and proportionality, ensures these techniques serve legitimate security objectives without compromising cognitive liberty or human dignity.

As this field continues to evolve, significant challenges demand further exploration. The global nature of cognitive warfare necessitates the development of culturally adaptive approaches to influence operations, ensuring strategies are effective across diverse populations while avoiding unintended backlash. Simultaneously, addressing privacy concerns and potential misuse is paramount, particularly when leveraging vast behavioral data streams required for digital phenotyping and SOCMINT applications. Without robust oversight mechanisms and international collaboration, such technologies have the potential to erode public trust and exacerbate ethical vulnerabilities. Therefore, operational cyberpsychology must prioritize ethical innovation to align with democratic values, even within contested environments.

The implications of operational cyberpsychology extend beyond military applications, offering valuable insights for public health, cybersecurity, and counterterrorism efforts. Technologies such as digital phenotyping can enable early detection of psychological stress or behavioral vulnerabilities, improving resilience among cybersecurity teams or identifying individuals at risk of radicalization. Cross-disciplinary collaboration will be essential for adapting these tools to non-military contexts, ensuring their responsible and effective use in broader societal applications. The dual-use nature of many of these technologies places even greater responsibility on practitioners to maintain ethical rigor and prioritize human well-being.

Future advancements in AI and quantum computing will further redefine the capabilities of operational cyberpsychology, making it essential to establish global

norms and legal frameworks to prevent misuse. The ability to simultaneously optimize thousands of cognitive variables promises significant gains in influence precision, yet also increases risks, including the potential for abuse by authoritarian regimes. International collaboration will play a critical role in balancing security objectives with the protection of cognitive autonomy and privacy rights. Ethical AI frameworks, emphasizing transparency, accountability, and stringent oversight, will be necessary to govern these revolutionary capabilities effectively.

In conclusion, operational cyberpsychology merges psychological science and cyber expertise to address the challenges of cognitive warfare, offering unparalleled strategic advantages while emphasizing the need for ethical application. Balancing innovation with ethical accountability will ensure cognitive targeting advances national security goals without compromising fundamental human rights. As the field matures, the continued alignment of technological power with legal, cultural, and ethical principles is essential to sustain its role as a critical capability in contested digital environments. By fostering interdisciplinary research and establishing robust governance, operational cyberpsychology can evolve responsibly, safeguarding human dignity and cognitive liberty in an increasingly complex world.

Conflicts of Interest

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

References

[1] Forescout Research-Vedere Labs (2025) Since Stuxnet: A History of Critical Infrastructure Attacks. https://www.forescout.com/blog/since-stuxnet-a-brief-history-of-critical-infrastructure-attacks/

[2] Staal, M.A., Corey, D.M., Dean, P.J., DeMatteo, D., Krauss, D.A., Lewis, L.K., *et al.* (2025) Professional Practice Guidelines for Operational Psychology: An Executive Summary. *American Psychologist*, **80**, 844-855. https://doi.org/10.1037/amp0001499

[3] American Psychological Association (2024) Artificial Intelligence and the Field of Psychology. https://www.apa.org/about/policy/artificial-intelligence-psychology

[4] U.S. Government Accountability Office (2024) High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation (GAO-24-107231). https://www.gao.gov/products/gao-24-107231

[5] Cohen, D. and Bar'el, O. (2017) The Use of Cyberwarfare in Influence Operations. Yuval Ne'eman Workshop for Science, Technology, and Security. Tel Aviv, Tel-Aviv University. https://en-cyber.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/cyber%20center/cyber-center/Cyber_Cohen_Barel_ENG.pdf

[6] Kritika, M. (2025) A Comprehensive Study on Navigating Neuroethics in Cyberspace. *AI and Ethics*, **5**, 93-100. https://doi.org/10.1007/s43681-024-00486-7

[7] Emond, B. and West, R.L. (2003) Cyberpsychology: A Human-Interaction Perspective Based on Cognitive Modeling. *CyberPsychology & Behavior*, **6**, 527-536. https://doi.org/10.1089/109493103769710550

[8] McNeese, M.D. and Hall, D.L. (2017) The Cognitive Sciences of Cyber-Security: A Framework for Advancing Socio-Cyber Systems. In: Liu, P., Jajodia, S. and Wang, C., Eds., *Theory and Models for Cyber Situation Awareness*, Springer, 173-202. https://doi.org/10.1007/978-3-319-61152-5_7

[9] Wiederhold, B.K. (2025) The Rise of Synthetic Societies: Is There a Role for Humans? *Cyberpsychology, Behavior, and Social Networking*, **28**, 224-226. https://doi.org/10.1089/cyber.2025.0067

[10] Gutzwiller, R.S., Hunt, S.M. and Lange, D.S. (2016) A Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts. 2016 *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support* (*CogSIMA*), San Diego, 21-25 March 2016, 14-20. https://doi.org/10.1109/cogsima.2016.7497780

[11] De Zoysa, S. (2024) Neuroscience of Persuasion: Understanding Brain Mechanisms in Psychological Operations. https://www.researchgate.net/profile/Sayonara-De-Zoysa/publication/383157275_Neurosci-ence_of_Persuasion_Understanding_Brain_Mechanisms_in_Psychological_Operations/links/66bf30d0311cbb09493eb528/Neuroscience-of-Persuasion-Understanding-Brain-Mechanisms-in-Psychological-Operations.pdf

[12] Steeds, M. and Clinch, S. (2025) On Cyberpsychology and Human-Computer Interactions. In: Wright, M.F., Ed., *Research Handbook on Cyberpsychology*, Edward Elgar Publishing, 8-54. https://doi.org/10.4337/9781803929484.00006

[13] Piazza, J. and Bering, J.M. (2009) Evolutionary Cyber-Psychology: Applying an Evolutionary Framework to Internet Behavior. *Computers in Human Behavior*, **25**, 1258-1269. https://doi.org/10.1016/j.chb.2009.07.002

[14] Parsons, T.D. (2017) Cyberpsychology and the Brain: The Interaction of Neuroscience and Affective Computing. Cambridge University Press. https://doi.org/10.1017/9781316151204

[15] Tovo, K., Spitaletta, J., Rhem, S., Linera, R., Seese, G., Martin, M. and Greenlee, M. (2016) White Paper on Bio Psycho Social Applications to Cognitive Engagement (No. SECDEFSMA). https://apps.dtic.mil/sti/html/tr/AD1092269/

[16] Camacho, E., Brady, R.O., Lizano, P., Keshavan, M. and Torous, J. (2021) Advancing Translational Research through the Interface of Digital Phenotyping and Neuroimaging: A Narrative Review. *Biomarkers in Neuropsychiatry*, **4**, Article ID: 100032. https://doi.org/10.1016/j.bionps.2021.100032

[17] Parker, S., Gupta, S. and Lee, H. (2024) Digital Cognitive Enhancement and Decline: A Neuropsychological Perspective. *Journal of Cognitive Neuroscience*, **36**, 789-805.

[18] ElSayary, A. and Ragab, J.K. (2025) Digital Neuroplasticity: How Prolonged Technology Use Reshapes Neural Pathways over Time. *Proceedings of the International Multi-Conference on Complexity, Informatics and Cybernetics*, 25-28 March 2025, 158-164. https://doi.org/10.54808/imcic2025.01.158

[19] Insel, T.R. (2017) Digital Phenotyping: Technology for a New Science of Behavior. *JAMA*, **318**, 1215-1216. https://doi.org/10.1001/jama.2017.11295

[20] Onnela, J. and Rauch, S.L. (2016) Harnessing Smartphone-Based Digital Phenotyping to Enhance Behavioral and Mental Health. *Neuropsychopharmacology*, **41**, 1691-1696. https://doi.org/10.1038/npp.2016.7

[21] Yang, Z., Heaukulani, C., Sim, A., Buddhika, T., Abdul Rashid, N.A., Wang, X., *et al.* (2025) Utility of Digital Phenotyping Based on Wrist Wearables and Smartphones in Psychosis: Observational Study. *JMIR mHealth and uHealth*, **13**, e56185.

https://doi.org/10.2196/56185

[22] Liu, Y., Yue, K. and Liu, Y. (2024) Behavioral Analysis in Immersive Learning Environments: A Systematic Literature Review and Research Agenda. arXiv: 2405.03442.

[23] Nonum, E.O., Avwokuruaye, O. and Umar, A.M. (2025) Social Engineering: Understanding Human Factors in Cyber Security. *International Journal of Convergent and Informatics Science Research*, **7**, 155-171. https://doi.org/10.70382/hijcisr.v07i9.032

[24] Costa Netto, Y. and Maçada, A.C.G. (2019) The Influence of Social Media Filter Bubbles and Echo Chambers on Its Identity Construction. https://aisel.aisnet.org/ecis2019_rip/65

[25] Janhonen, J. (2023) Socialisation Approach to AI Value Acquisition: Enabling Flexible Ethical Navigation with Built-In Receptiveness to Social Influence. *AI and Ethics*, **5**, 527-553. https://doi.org/10.1007/s43681-023-00372-8

[26] Fogg, B.J. (2002) Persuasive Technology: Using Computers to Change What We Think and Do. *Ubiquity*, **2002**, 2. https://doi.org/10.1145/764008.763957

[27] American Psychological Association (2023) Professional Practice Guidelines for Operational Psychology. https://www.apa.org/about/policy/operational-psychology.pdf

[28] Levine, M. (2025) A Golden Age of Behavioural Social Psychology? Towards a Social Psychology of Power and Intergroup Relations in the Digital Age. *British Journal of Social Psychology*, **64**, e12896. https://doi.org/10.1111/bjso.12896

[29] Hofstede, G. (2011) Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture*, **2**, Article 8. https://doi.org/10.9707/2307-0919.1014

[30] Chen, Y. (2025) The Impact of Behavioral Economics on Consumer Decision-Making in the Digital Era. *Advances in Management and Intelligent Technologies*, **1**, 1-9. https://doi.org/10.62177/amit.v1i3.391

[31] Obioha-Val, O.A., Olaniyi, O.O., Gbadebo, M.O., Balogun, A.Y. and Olisa, A.O. (2025) *Asian Journal of Research in Computer Science*, **18**, 184-204. https://doi.org/10.9734/ajrcos/2025/v18i1557

[32] Zhang, J., Song, W. and Liu, Y. (2025) Cognitive Bias in Generative AI Influences Religious Education. *Scientific Reports*, **15**, Article No. 15720. https://doi.org/10.1038/s41598-025-99121-6

[33] Shevchenko, Y., von Helversen, B. and Scheibehenne, B. (2014) Change and Status Quo in Decisions with Defaults: The Effect of Incidental Emotions Depends on the Type of Default. *Judgment and Decision Making*, **9**, 287-296. https://doi.org/10.1017/s1930297500005817

[34] Marković, S., Popović, G. and Andjelković, L. (2024) Mastering the Attention Economy: Strategies for Competing on Digital Platforms. *Fusion of Multidisciplinary Research, An International Journal*, **5**, 568-578. https://doi.org/10.63995/pgje3232

[35] Nye, C.D., Drasgow, F., Chernyshenko, O.S., Stark, S., Kubisiak, U.C., White, L.A. and Jose, I. (2012) Assessing the Tailored Adaptive Personality Assessment System (TAPAS) as an MOS Qualification Instrument (No. ARITR1312). https://apps.dtic.mil/sti/tr/pdf/ADA566090.pdf

[36] Society for Industrial and Organizational Psychology (2018) Principles for the Validation and Use of Personnel Selection Procedures (5th ed.). https://www.researchgate.net/profile/Frederick-Oswald/publication/330544995_Princi-ples_for_the_Validation_and_Use_of_Personnel_Selection_Procedures/links/5d0c1164a6fdcc246297bb60/Principles-for-the-Validation-and-Use-of-Personnel-Selection-Procedures.pdf

[37] Trippe, D.M., Moriarty, K.O., Russell, T.L., Carretta, T.R. and Beatty, A.S. (2014) Development of a Cyber/information Technology Knowledge Test for Military Enlisted Technical Training Qualification. *Military Psychology*, **26**, 182-198. https://doi.org/10.1037/mil0000042

[38] Shewach, O.R., Ingerick, M., Butterfuss, R., Carretta, T.R. and Persing, C. (2023) Optimizing Qualification to US Space Force Spacepower Disciplines. https://apps.dtic.mil/sti/trecms/pdf/AD1212816.pdf

[39] Lingfeng, H. (2024) Military Information Support Operations. In: Kan, Z., Ed., *The ECPH Encyclopedia of Psychology*, Springer, 920-922. https://doi.org/10.1007/978-981-97-7874-4_1303

[40] White, M.M. (2025) Terrorism: Psychological Warfare Of. In: Shackelford, T., Ed., *Encyclopedia of Religious Psychology and Behavior*, Springer, 1-3. https://doi.org/10.1007/978-3-031-38971-9_1917-1

[41] Martins, G.D.G., Caricati, V.V., Barbugli, B.C., da Silva Ribeiro, C.M., Lobato, F.B.H., Scatena, A., *et al.* (2021) The Biopsychosocial Impact of Abusive Use of Digital Media. In: De Micheli, D., Andrade, A.L.M., Reichert, R.A., Silva, E.A.D., Pinheiro, B.D.O. and Lopes, F.M., Eds., *Drugs and Human Behavior*, Springer, 459-468. https://doi.org/10.1007/978-3-030-62855-0_33

[42] 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

[43] Vandegrift, S., Canan, M. and Shives, T. (2025) The Roles of PA and MISO in Modern Warfare. *International Conference on Cyber Warfare and Security*, **20**, 476-483. https://doi.org/10.34190/iccws.20.1.3500

[44] Omand, D., Bartlett, J. and Miller, C. (2019) Introducing social media intelligence (SOCMINT). In: Andrew, C., Aldrich, R.J. and Wark, W.K., Eds., *Secret Intelligence*, Routledge, 77-94. https://doi.org/10.4324/9780429029028-7

[45] Yu, S. (2023) Cyber Profiling: Predicting Political Orientation with SOCMINT. *Telematics and Informatics Reports*, **10**, Article ID: 100058. https://doi.org/10.1016/j.teler.2023.100058

[46] Torous, J., Linardon, J., Goldberg, S.B., Sun, S., Bell, I., Nicholas, J., *et al.* (2025) The Evolving Field of Digital Mental Health: Current Evidence and Implementation Issues for Smartphone Apps, Generative Artificial Intelligence, and Virtual Reality. *World Psychiatry*, **24**, 156-174. https://doi.org/10.1002/wps.21299

[47] Graphika & Stanford Internet Observatory (2022) Unheard Voice: Evaluating Five Years of Pro-Western Covert Influence Operations. Stanford Digital Repository. https://stacks.stanford.edu/file/druid:nj914nx9540/unheard-voice-tt.pdf

[48] Boyd, B. and Lin, H. (2019) Affecting the Cognitive Dimension of the Information Environment through Cyber-Enabled Information Operations. *Journal of Information Warfare*, **18**, 49-66. https://www.jstor.org/stable/26894681

[49] Tariq, M.U., Babar, M., Poulin, M., Khattak, A.S., Alshehri, M.D. and Kaleem, S. (2021) Human Behavior Analysis Using Intelligent Big Data Analytics. *Frontiers in Psychology*, **12**, Article 686610. https://doi.org/10.3389/fpsyg.2021.686610

[50] Cacioppo, J.T., Cacioppo, S. and Petty, R.E. (2017) The Neuroscience of Persuasion: A Review with an Emphasis on Issues and Opportunities. *Social Neuroscience*, **13**, 129-172. https://doi.org/10.1080/17470919.2016.1273851

[51] Gokhman, D., Harris, K.D., Carmi, S. and Greenbaum, G. (2025) Predicting the Direction of Phenotypic Difference. *Nature Communications*, **16**, Article No. 6898. https://doi.org/10.1038/s41467-025-62355-z

[52] Vankhede, P. and Kumar, S. (2024) Predictive Analytics for Website User Behavior Analysis. 2024 *IEEE International Students' Conference on Electrical, Electronics and Computer Science* (*SCEECS*), Bhopal, 24-25 February 2024, 1-6. https://doi.org/10.1109/sceecs61402.2024.10482298

[53] Venkateswaran, P.S. and Mm, S. (2025) Predictive Analytics: Utilizing Machine Learning and Big Data for Forecasting Future Trends in Business and Consumer Behavior. In: Hussain, Z., Salehhuddin Sharipudin, M.N., Albattat, A. and Khan, A., Eds., *Strategic Brand Management in the Age of AI and Disruption*, IGI Global, 463-492. https://doi.org/10.4018/979-8-3693-9461-8.ch019

[54] Moreira, T. and Carvalho, L. (2024) Legal and Regulatory Considerations in Cybersecurity and Information Assurance: Managing Privacy, Responsibility, and Compliance in Digital Systems. *Journal of Applied Computational Science, Numerical Methods, and Scientific Computing in Engineering*, **14**, 1-15. https://soloncouncil.com/index.php/JACSNMSCE/article/download/2024-nov-04/8

[55] Kshetri, N. and Alcantara, L.L. (2015) Cyber-Threats and Cybersecurity Challenges: A Cross-Cultural Perspective. In: Holden, N., Michailova, S. and Tietze, S., Eds., *The Routledge Companion to Cross-Cultural Management*, Routledge, 285-293.

[56] White, C.J., Baimel, A. and Norenzayan, A. (2021) How Cultural Learning and Cognitive Biases Shape Religious Beliefs. *Current Opinion in Psychology*, **40**, 34-39. https://doi.org/10.1016/j.copsyc.2020.07.033

[57] Hedrih, V. (2019) Adapting Psychological Tests and Measurement Instruments for Cross-Cultural Research: An Introduction. Routledge. https://doi.org/10.4324/9780429264788

[58] Troublefield, T.C. (2025) The Cyberpsychology of Small and Medium-Sized Enterprises Cybersecurity: A Human-Centric Approach to Policy Development. *Journal of Information Security*, **16**, 158-183. https://doi.org/10.4236/jis.2025.161009

[59] Ohu, F. and Jones, L. (2025) The Intersection of Cyberwarfare, Social Media, and Adolescent Self-Esteem: A Forensic Cyberpsychology Analysis. *International Conference on Cyber Warfare and Security*, **20**, 332-344. https://doi.org/10.34190/iccws.20.1.3375

[60] Maynard, A., Corey, C., Greaves, A., Kozar, M., Kwon, K.H. and Scragg, M. (2022) Conducting Socially Responsible and Ethical Counter Influence Operations Research: A Practical Guide for Researchers and Practitioners. https://apps.dtic.mil/sti/html/trecms/AD1221500/

[61] Bodenstein, K.C., Paquin, V., Sekhon, K., Lesage, M., Cinalioglu, K., Rej, S., *et al.* (2023) Digital Markers of Mental Health Problems: Phenotyping across Biological, Psychological, and Environmental Dimensions. In: Teixeira, A.L., Rocha, N.P. and Berk, M., Eds., *Biomarkers in Neuropsychiatry*, Springer, 105-122. https://doi.org/10.1007/978-3-031-43356-6_7

[62] Hudon, A., Harvey, E., Nicolas, S., Dufour, M., Guérin-Thériault, C., Bérubé-Fortin, J., *et al.* (2025) Cyberpsychopathy: A Multidimensional Framework for Understanding Psychopathic Traits in Digital Environments. *European Journal of Investigation in Health, Psychology and Education*, **15**, Article 107. https://doi.org/10.3390/ejihpe15060107

[63] Razian, M., Fathian, M., Bahsoon, R., Toosi, A.N. and Buyya, R. (2022) Service Composition in Dynamic Environments: A Systematic Review and Future Directions. *Journal of Systems and Software*, **188**, Article ID: 111290. https://doi.org/10.1016/j.jss.2022.111290

[64] Larson, E.V., Darilek, R.E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz,

L.H. and Thurston, C.Q. (2009) Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities. https://apps.dtic.mil/sti/html/tr/ADA503375/

[65] Patchipala, S.G. (2023) Tackling Data and Model Drift in AI: Strategies for Maintaining Accuracy during ML Model Inference. *International Journal of Science and Research Archive*, **10**, 1198-1209. https://doi.org/10.30574/ijsra.2023.10.2.0855

[66] Klos, V., Gothel, T. and Glesner, S. (2016) Formal Models for Analysing Dynamic Adaptation Behaviour in Real-Time Systems. 2016 *IEEE 1st International Workshops on Foundations and Applications of Self Systems* (*FAS*W*), Augsburg, 12-16 September 2016, 106-111. https://doi.org/10.1109/fas-w.2016.34

[67] American Psychological Association (2023) Informing the Role of Congress in Artificial Intelligence Regulation. https://www.apaservices.org/advocacy/news/congress-artificial-intelligence-regulation

[68] Kritika, E.M. (2024) Neuroethical Quandaries at the Crossroads of Cyberspace. *Scientific Practical Cyber Security Journal*, **8**, 57-63. https://journal.scsa.ge/wp-content/uploads/2024/04/0017_neuroethical-quandaries-at-the-crossroads-of-cyberspace.pdf

[69] Bose, R. and Glasgow, K. (2025) AI-Based Replication of Human Moral Judgements: Moral Proxies for Multidomain Operations. *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications VII*, Orlando, 14-17 April 2025, 9-20. https://doi.org/10.1117/12.3053725

[70] Minici, M., Luceri, L., Fabbri, F. and Ferrara, E. (2025) IOHunter: Graph Foundation Model to Uncover Online Information Operations. *Proceedings of the AAAI Conference on Artificial Intelligence*, **39**, 28258-28266. https://doi.org/10.1609/aaai.v39i27.35046

[71] Spitaletta, J.A. (2021) Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations. https://apps.dtic.mil/sti/html/trecms/AD1154566/

[72] Jensen, B. (2025) Cyber Crisis Management in Non-Military Warfare. In: Jonsson, O. and Käihkö, I., Eds., *Non-Military Warfare*, Routledge, 90-118. https://doi.org/10.4324/9781003616993-5

[73] Rich, M. (2025) Cyberpsychology: Integrating Cyber Behavioral Sciences with Adaptive Environments for Enhanced Cyber Deception. *Proceedings of the Annual Hawaii International Conference on System Sciences*, Hawaii, 7-10 January 2025, 1136-1145. https://doi.org/10.24251/hicss.2025.135

[74] Claverie, B. and Du Cluzel, F. (2022) The Cognitive Warfare Concept. https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf

[75] Herberger, K. (2025) Mind Warfare: Psychological Operations and the Inducement of Psychosis in Military Strategy. Kathlene Herberger.

[76] Schmitt, M.N. (2013) Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. https://www.penncerl.org/wp-content/uploads/2021/12/6481-tallinn-manual-on-the-international-law-applicable.pdf

[77] Schmitt, M.N. (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. https://csrcl.huji.ac.il/sites/default/files/csrcl/files/9781107177222_frontmatter.pdf

[78] Pagallo, U. (2014) Cyber Force and the Role of Sovereign States in Informational Warfare. *Philosophy & Technology*, **28**, 407-425.

https://doi.org/10.1007/s13347-014-0177-4

[79] Yager, M. (2018) What Do Others Think/How Do We Know What the Think? NSI. https://www.nsiteam.com/nsi-publications/what-do-others-think-how-dow-we-know-what-they-think

[80] Roberts, A. and Venables, A. (2024) Military Psychological Operations in the Digital Battlespace: A Practical Application of the Legal Framework. 2024 16*th International Conference on Cyber Conflict*: *Over the Horizon* (*CyCon*), Tallinn, 28-31 May 2024, 281-296. https://doi.org/10.23919/cycon62501.2024.10685605

[81] Tims, F.M., Sorensen, R.C., Mushal, F.C. and Morgan Jr., J.T. (1975) New Indicators of Psychological Operations Effects (No. OADACR114). https://apps.dtic.mil/sti/html/tr/ADA015004/

[82] Santa Maria, S.D. (2013) Improving Influence Operations by Defining Influence and Influence Operations (No. ATZLSWV). https://apps.dtic.mil/sti/html/tr/ADA606282/

[83] Gupta, P., Sharma, S. and Sharma, T. (2025) Big Data Analytics in Behavior Analysis. In: Chhabra, G., Singh, T. and Kumar, M., Eds., *Mapping Human Data and Behavior with the Internet of Behavior* (*IoB*), IGI Global, 205-238. https://doi.org/10.4018/979-8-3693-7545-7.ch009

[84] Kim, K., Sin, S.J. and Yoo-Lee, E. (2021) Use and Evaluation of Information from Social Media: A Longitudinal Cohort Study. *Library & Information Science Research*, **43**, Article ID: 101104. https://doi.org/10.1016/j.lisr.2021.101104

[85] Pijpers, P. (2022) Towards a Legal Framework for Influence Operations in Cyberspace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4112370

[86] Staal, M.A. (2026) Operational Psychology and National Security. Routledge. https://doi.org/10.4324/9781003564195

[87] Wallace, R. (2019) Cognitive Dynamics on Clausewitz Landscapes: The Control and Directed Evolution of Organized Conflict. Springer. https://doi.org/10.1007/978-3-030-26424-6

[88] Couretas, J.M. (2022) Measures of Cyber Performance and Effectiveness. In: Couretas, J.M., Ed., *An Introduction to Cyber Analysis and Targeting*, Springer, 197-219. https://doi.org/10.1007/978-3-030-88559-5_9

[89] Kosinski, M., Stillwell, D. and Graepel, T. (2013) Private Traits and Attributes Are Predictable from Digital Records of Human Behavior. *Proceedings of the National Academy of Sciences of the United States of America*, **110**, 5802-5805. https://doi.org/10.1073/pnas.1218772110

[90] Başaran, S. and Ejimogu, O.H. (2021) A Neural Network Approach for Predicting Personality from Facebook Data. *Sage Open*, **11**. https://doi.org/10.1177/21582440211032156

[91] Orrù, G., Monaro, M., Conversano, C., Gemignani, A. and Sartori, G. (2020) Machine Learning in Psychometrics and Psychological Research. *Frontiers in Psychology*, **10**, Article 2970. https://doi.org/10.3389/fpsyg.2019.02970