World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

HUMAN COGNITIVE RESILIENCE IN SECURITY OPERATIONS CENTERS: A STRUCTURED REVIEW AND QUANTITATIVE FRAMEWORK FOR SLEEP, ALERT FATIGUE, WORKLOAD, AND HUMAN-AI CYBER DEFENSE

Stephen Sobulo [1,*], Olajide Dare [1], Adebiyi Adisa [2], Beauty Enobun [1], Isdore Ugochukwu Opara [3], and Ekundayo Peter Buremoh [1]

[1] Department of Computer Science and Engineering, University of Fairfax, Salem, Virginia, USA.
[2] Department of Computer Science and Engineering, Hood College, Maryland, USA.
[3] Department of Business, University of Fairfax, Salem, Virginia, USA.
* Corresponding author; Email: sobulos@students.ufairfax.edu

ORCID Details
Stephen Sobulo: https://orcid.org/0009-0002-9019-7996
Olajide Dare: https://orcid.org/0009-0002-1187-8575
Adebiyi Adisa: https://orcid.org/0009-0002-7298-6713
Isdore Ugochukwu Opara: https://orcid.org/0009-0003-0788-8057
Ekundayo Peter Buremoh: https://orcid.org/0009-0008-5037-0284

World Journal of Advanced Research and Reviews, 2026, 31(03), 1370–1407

Publication history: Received on 10 August 2026; revised on 19 September 2026; accepted on 21 September 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.31.3.2442

ABSTRACT

This review examines how sleep restriction, cumulative fatigue, alert overload, cognitive workload, occupational stress, burnout, and human-AI task allocation shape the cognitive conditions under which Security Operations Center (SOC) analysts and incident responders perform. The review updates and integrates evidence from cybersecurity, cognitive neuroscience, occupational psychology, human factors, and organizational resilience through August 2026. The synthesis distinguishes direct cybersecurity evidence from transferred evidence and identifies a persistent empirical gap: cyber operations clearly exhibit fatigue, workload, burnout, and alert-management pressure, but direct longitudinal evidence connecting objectively measured sleep and cognitive state to operational cyber outcomes remains limited. To move beyond a descriptive human-factors account, we refine the Human Cognitive Resilience Framework (HCRF) as a testable socio-technical model linking operational demands, cognitive load and occupational stress, organizational resources, cognitive resilience, cybersecurity performance, organizational cyber resilience, and organizational learning. The revised framework incorporates 2026 developments in human-centered cybersecurity and human-AI incident management, and introduces a quantitative operationalization for repeated-measures field testing. Recommended measurements combine sleep/actigraphy, psychomotor vigilance, workload and stress instruments, analyst telemetry, objective triage and response metrics, and organizational-resource indicators. Formal mediation, moderation, nonlinear threshold, and multilevel hypotheses are specified. The resulting framework treats human

cognitive capacity neither as a substitute for technical controls nor as an individual responsibility problem, but as an operational resource jointly shaped by work design, staffing, recovery, automation, leadership, and team processes.

Keywords: Alert Fatigue, Burnout, Cognitive Resilience, Cybersecurity Workforce, Human-Centered Cybersecurity, Human-AI Teaming, Security Operations Center, Sleep, Workload.

1 INTRODUCTION

Cybersecurity has become a critical concern for governments, businesses, healthcare systems, financial institutions, and critical infrastructure as digital transformation expands the scale and complexity of organizational exposure to cyber threats. Cloud computing, artificial intelligence, the Internet of Things, remote connectivity, and increasingly interconnected information systems have enlarged organizational attack surfaces and increased dependence on sophisticated defensive technologies. In response, organizations have invested heavily in intrusion detection systems, endpoint detection and response platforms, zero-trust architectures, automated monitoring, and AI-enabled threat intelligence. Yet technological controls alone remain insufficient because cybersecurity outcomes emerge from interactions among technologies, organizational processes, work systems, and human decision-making [12].

The policy and research environment has moved further toward human-centered cybersecurity. In 2026, NIST formalized a concept-paper agenda for human-centered cybersecurity guidelines and resources, emphasizing empirical evidence and the interaction of people, process, and technology [23]. A parallel IEEE Security & Privacy synthesis identified persistent gaps between human-centered cybersecurity research and operational practice [24]. These developments strengthen the argument that workforce cognitive conditions should be evaluated as part of cybersecurity system design rather than as a peripheral wellness issue.

This socio-technical reality is particularly evident in Security Operations Centers (SOCs) and cyber incident-response environments. Cybersecurity professionals must sustain attention over prolonged periods, interpret large volumes of heterogeneous information, distinguish genuine threats from false-positive alerts, prioritize competing incidents, coordinate responses under time pressure, and make consequential decisions under uncertainty. These responsibilities are often performed within continuous operations characterized by rotating shifts, extended working hours, staffing constraints, rapidly changing threats, and persistent information overload. Such conditions create substantial cognitive and emotional demands and can contribute to mental fatigue, occupational stress, and performance deterioration [14].

The significance of these pressures extends beyond employee well-being. Effective cyber defense depends on cognitive functions including sustained attention, working memory, executive control, situational awareness, learning, inhibitory control, and adaptive decision-making. These capabilities enable analysts to identify anomalous activity, interpret ambiguous threat information, prioritize incidents accurately, and respond effectively as conditions change. Their deterioration may therefore increase vulnerability to missed indicators of compromise, delayed threat detection, inappropriate prioritization, analytical errors, slower incident response, and impaired coordination. Human cognitive functioning should consequently be understood not merely as an occupational-health concern but as an operational component of cybersecurity capability.

Sleep and recovery are particularly relevant to this relationship. Evidence from neuroscience and occupational-performance research indicates that insufficient or fragmented sleep can impair executive functioning, vigilance, working memory, reaction time, judgment, learning, and decision-making. Repeated sleep restriction may also produce cumulative impairment even without complete sleep deprivation. These effects are highly relevant to cybersecurity work, which depends on prolonged vigilance and rapid interpretation of complex information. However, much of the evidence linking sleep to cognitive performance originates outside operational cybersecurity settings. Its application to cyber defense is therefore theoretically relevant but requires careful consideration of transferability.

Related concerns arise from security fatigue, occupational stress, cognitive workload, and burnout. Persistent exposure to alert overload, continuous monitoring, complex compliance requirements, high workload, and high-consequence decision-making can progressively strain attentional and psychological resources. Burnout may further affect professional efficacy, collaboration, analytical reasoning, and workforce retention. These conditions suggest that staffing, workload allocation, shift design, leadership support, psychological safety, recovery opportunities, training, and technology design are not peripheral human-resource concerns; they are potential determinants of the conditions under which cybersecurity professionals perform.

1.1 The unresolved problem

Despite increasing recognition of human factors in cybersecurity, the relevant evidence remains conceptually fragmented. Sleep deprivation, cognitive workload, stress, burnout, alert fatigue, security fatigue, human error, organizational resilience, and cyber performance have often been examined as separate phenomena. Consequently,

existing scholarship provides substantial evidence that human conditions matter but offers a less integrated explanation of how operational demands translate into cognitive strain, how organizational conditions buffer or intensify that strain, and how preserved or diminished cognitive functioning may subsequently influence cybersecurity performance and organizational cyber resilience.

Three gaps are particularly important. First, much human-factor research in cybersecurity has historically concentrated on end users, including security awareness, password behavior, policy compliance, phishing susceptibility, and technology adoption. Although these issues remain important, comparatively less attention has been directed toward cybersecurity professionals as cognitively demanding operators whose performance constitutes part of the defense system itself.

Second, evidence concerning sleep, fatigue, executive functioning, psychological recovery, occupational stress, and resilience is distributed across cybersecurity, cognitive neuroscience, occupational psychology, organizational behavior, human factors, healthcare, military performance, and related disciplines. The fragmentation of this evidence limits understanding of how these bodies of knowledge collectively explain human performance in cyber-defense environments.

Third, existing research often identifies associations between demanding working conditions and adverse human outcomes without specifying the mechanisms through which operational demands affect cognitive functioning and, subsequently, cybersecurity outcomes. What remains insufficiently developed is an integrated pathway connecting operational demands, cognitive strain, organizational resources, adaptive cognitive capacity, cybersecurity performance, and organizational cyber resilience.

1.2 Cognitive resilience as the integrative mechanism

This review proposes cognitive resilience as a construct capable of addressing this explanatory gap. Cognitive resilience is conceptualized here as the dynamic capacity to maintain, recover, and adapt the cognitive functioning necessary for effective performance during and following demanding operational conditions. It is not treated as a fixed personal trait or as an expectation that cybersecurity professionals should tolerate excessive workloads. Rather, it emerges from interactions among operational demands, sleep and recovery, organizational support, teamwork, professional learning, and technological design.

This distinction is important because it shifts attention from individual endurance toward the conditions that enable sustainable performance. Excessive workload, inadequate staffing, poorly designed shifts, weak leadership, low psychological safety, insufficient recovery, and cognitively burdensome technologies may constrain the ability of professionals to maintain effective functioning. Conversely, supportive organizational resources may reduce avoidable cognitive strain and facilitate recovery, learning, coordination, and adaptation. Cognitive resilience therefore provides a potential conceptual bridge between individual cognitive functioning and broader organizational cyber resilience.

1.3 Purpose and contribution of the review

Against this background, this review synthesizes interdisciplinary evidence concerning sleep, fatigue, cognitive workload, occupational stress, burnout, cognitive resilience, organizational resources, cybersecurity performance, and organizational cyber resilience. Rather than examining these factors independently, it evaluates their relationships within a unified socio-technical perspective.

The review makes three principal contributions. First, it reframes the cognitive health of cybersecurity professionals as a component of cyber-defense capability rather than treating sleep, fatigue, stress, and burnout solely as occupational well-being outcomes. Second, it integrates evidence from cybersecurity, cognitive neuroscience, occupational psychology, organizational behavior, and human factors to clarify the mechanisms through which operational conditions may influence cybersecurity performance. Third, it develops the Human Cognitive Resilience Framework (HCRF), a theoretically grounded and empirically testable model linking operational demands, cognitive load and occupational stress, organizational resources, cognitive resilience, cybersecurity performance, and organizational cyber resilience.

The HCRF does not seek merely to demonstrate that human factors matter in cybersecurity. Its specific contribution is to explain how operational demands may be translated into cognitive strain, when organizational resources may buffer or mitigate those effects, how cognitive resilience may support the maintenance, recovery, and adaptation of effective cognitive performance, and how cybersecurity performance may provide a pathway between human cognitive functioning and organizational cyber resilience.

1.3.1 Accordingly, the review addresses four research questions:

- RQ1: How do sleep, fatigue, cognitive workload, occupational stress, and burnout influence cognitive functioning relevant to cybersecurity operations?
- RQ2: Which organizational resources help protect or restore cognitive functioning under demanding cybersecurity conditions?
- RQ3: How can cognitive resilience explain the relationship between operational demands and cybersecurity performance?
- RQ4: Through what pathways may cybersecurity professionals' cognitive performance contribute to organizational cyber resilience?

By addressing these questions, the review moves beyond the general proposition that human factors influence cybersecurity toward a more specific explanation of when, why, and through which mechanisms human cognitive functioning may become a determinant of sustainable cyber defense.

2 REVIEW METHODOLOGY

2.1 Review Design

This study employed a structured narrative review to synthesize interdisciplinary evidence concerning sleep, fatigue, cognitive workload, occupational stress, burnout, cognitive resilience, organizational resources, cybersecurity performance, and organizational cyber resilience. A structured narrative approach was selected because the research problem spans cybersecurity, cognitive neuroscience, occupational psychology, organizational behavior, human factors, and information systems, with substantial heterogeneity in study populations, research designs, measurement approaches, and outcomes.

The purpose of the review was not to estimate a pooled effect or provide an exhaustive systematic inventory of all studies. Rather, it was to identify areas of convergence and disagreement, evaluate the methodological strength and contextual relevance of available evidence, assess the transferability of findings across disciplines, and integrate these findings into an explanatory framework for human cognitive functioning in cyber defense. The structured approach was intended to increase transparency and consistency while retaining the conceptual breadth required for interdisciplinary theory development.

2.2 Information Sources and Search Strategy

The literature search covered publications from January 2015 to August 2026, while selected earlier studies were retained where they provided foundational theoretical or empirical evidence necessary for interpreting more recent research. The principal sources were Scopus, Web of Science, PubMed, IEEE Xplore, and the ACM Digital Library. Google Scholar was used as a supplementary source for citation tracking and identification of potentially relevant studies not captured through the principal database searches.

The core Boolean search structure combined terms representing the target occupational population, human cognitive and occupational factors, and relevant performance outcomes:

("cybersecurity professional*" OR "cyber security professional*" OR "security operations cent*" OR "SOC analyst*" OR "security analyst*" OR "incident responder*")

AND

("sleep" OR "sleep deprivation" OR "fatigue" OR "alert fatigue" OR "security fatigue" OR "burnout" OR "occupational stress" OR "cognitive load" OR "cognitive resilience")

AND

("performance" OR "decision making" OR "human performance" OR "threat detection" OR "incident response" OR "cyber resilience")

Supplementary searches examined narrower combinations of concepts, particularly sleep and cognition, fatigue and alert overload, occupational stress and burnout, cognitive resilience, organizational resources, human-AI interaction, and cybersecurity performance. Reference lists of highly relevant empirical studies and recent reviews were also examined to identify additional literature.

This broader search strategy was necessary because the constructs examined in this review are distributed across disciplinary literatures and are not consistently indexed using cybersecurity-specific terminology. At the same time, recent cybersecurity scholarship includes focused reviews of individual components. For example, Tariq et al. [18] systematically examined alert fatigue in Security Operations Centers and associated technological mitigation approaches. The present review therefore adopts a broader analytical scope by examining how alert fatigue and related operational demands connect with cognitive strain, organizational resources, cognitive resilience, cybersecurity performance, and organizational cyber resilience.

2.3 Eligibility Criteria

Sources were considered eligible when they satisfied one or more of the following substantive criteria:

- examined cybersecurity professionals, SOC analysts, incident responders, or comparable high-demand occupational populations;
- investigated sleep, fatigue, cognitive workload, occupational stress, burnout, cognitive resilience, or related cognitive mechanisms;
- examined organizational conditions or resources such as staffing, leadership, psychological safety, workload management, recovery, teamwork, training, shift design, or technology design; or
- provided evidence relevant to cybersecurity performance, decision-making, threat detection, incident response, or organizational cyber resilience.

Eligible sources included empirical studies, systematic and scoping reviews, theoretical and conceptual studies, and selected authoritative institutional or professional reports published in English. Peer-reviewed research was prioritized. Earlier studies were retained selectively where they established concepts or relationships necessary for the theoretical synthesis. For example, Stanton et al. [17] was retained because it provided an early empirical characterization of security fatigue and its behavioral consequences.

Sources were excluded when they were editorials or unsupported opinion pieces, non-scholarly web materials, duplicate publications, or purely technical cybersecurity studies without a relevant human-performance, cognitive, occupational, or organizational dimension. Sources were also excluded when their contribution was insufficiently relevant to the review questions or the development of the proposed conceptual framework.

2.4 Study Selection and Data Extraction

Records identified through the searches were assessed in stages. Titles and abstracts were initially examined for relevance to the review questions and eligibility criteria. Publications considered potentially relevant were subsequently examined in greater detail, and their full texts were assessed for substantive relevance, methodological contribution, and applicability to the interdisciplinary synthesis. Reference lists of highly relevant studies and recent reviews were additionally examined to identify literature that may not have been captured through the principal searches.

Because this study was designed as a structured narrative review rather than a systematic review, selection was guided by relevance, methodological quality, conceptual contribution, and applicability to the research questions rather than by an objective of exhaustive study identification or quantitative pooling. Particular emphasis was placed on evidence obtained directly from cybersecurity professionals and operational cyber environments.

Where cybersecurity-specific evidence was limited, findings from cognitive neuroscience, occupational psychology, shift-work research, human factors, and other high-demand occupational settings were considered when they provided theoretically relevant evidence concerning plausible cognitive or organizational mechanisms. Such evidence was not treated as equivalent to direct cybersecurity evidence. Its transferability to cybersecurity settings was explicitly considered during interpretation.

For each included source, the synthesis considered the author and year, study population and setting, research design, human or organizational factor examined, cognitive or performance outcome, principal findings, methodological limitations, directness of cybersecurity relevance, and contribution to the development or evaluation of the Human Cognitive Resilience Framework (HCRF).

A central analytical distinction was maintained between direct evidence and transferred evidence. Direct evidence referred to studies involving cybersecurity professionals, SOC analysts, incident responders, or operational cyber environments. Transferred evidence referred to findings derived from adjacent populations or disciplines that informed plausible cognitive or occupational mechanisms but had not been demonstrated directly within cybersecurity operations. Maintaining this distinction reduced the risk of presenting findings established in other occupational settings as though they had been empirically confirmed in cyber-defense environments.

2.5 Quality and Relevance Appraisal

Given the methodological diversity of the evidence base, studies were appraised using criteria appropriate to their design and source type rather than a single aggregate quality score.

Empirical studies were considered in relation to research design, sample characteristics and adequacy, measurement validity, analytical approach, transparency of reporting, and strength of inference. Greater evidential weight was assigned to studies using objective measures, validated instruments, longitudinal or experimental designs, and populations directly relevant to cybersecurity operations.

Review articles were considered according to the transparency of their search and selection procedures, breadth and relevance of the evidence base, and appropriateness of the synthesis. Theoretical and conceptual studies were evaluated according to conceptual clarity, theoretical grounding, internal coherence, and explanatory relevance to the research questions.

Authoritative institutional and professional sources were used selectively where they provided contemporary information about cybersecurity practice, workforce conditions, or human-centered security that was not adequately represented in peer-reviewed research. Such sources were used principally to support contextual or practice-oriented claims rather than as substitutes for empirical evidence.

Directness of evidence formed an additional appraisal dimension. Findings obtained from cybersecurity professionals and operational cyber environments were considered more directly applicable to cyber defense than findings transferred from healthcare, aviation, military, neuroscience, or general occupational populations. Indirect evidence was retained when it provided credible insight into relevant mechanisms, but conclusions based on such evidence were qualified accordingly.

No formal meta-analytic weighting or aggregate numerical quality score was applied because of substantial heterogeneity in populations, research designs, constructs, measurement instruments, and outcomes. Instead, methodological strength, directness, and contextual relevance informed the evidential weight assigned to individual findings during synthesis.

2.6 Evidence Synthesis and Framework Development

Evidence was synthesized thematically across five interconnected domains: (1) human factors and operational demands; (2) sleep, fatigue, and cognitive performance; (3) cognitive resilience; (4) security fatigue, occupational stress, and burnout; and (5) organizational resources supporting human-centered cyber defense.

The synthesis moved beyond sequential description of individual studies by comparing findings according to consistency, methodological strength, directness of evidence, contextual relevance, and transferability. Particular attention was given to areas in which cybersecurity-specific findings converged with evidence from adjacent disciplines, as well as areas in which direct cyber evidence remained limited or findings could not be transferred confidently.

Table 1: Representative evidence informing the human cognitive resilience framework

Study	Population / Context	Evidence / Design	Main Finding Relevant to Review	Evidence Status	HCRF Contribution
Van Dongen et al. [20]	Controlled sleep-restriction participants	Experimental	Repeated sleep restriction produced cumulative neurobehavioral impairment	Transferred evidence	Sleep/recovery influences available cognitive resources
García et al. [10]	Non-cybersecurity participants	Experimental cognitive research	Sleep deprivation impaired attention, working memory, and executive functioning	Transferred evidence	Mechanistic link between inadequate sleep and performance vulnerability

Study	Population / Context	Evidence / Design	Main Finding Relevant to Review	Evidence Status	HCRF Contribution
Robbins et al. [16]	Shift workers	Systematic review	Non-standard schedules create continuing challenges for adequate sleep and recovery	Transferred evidence	Recovery and work scheduling as organizational considerations
Arnold et al. [2]	Digital/work information environments	Review	Information overload is associated with attentional fragmentation, stress, impaired decisions, and reduced performance	Transferred evidence	Information overload as an operational demand
Galy et al. [9]	Workplace resilience literature	Theoretical/review evidence	Resilience is dynamic and shaped by individual, collective, and organizational resources	Transferred theoretical evidence	Dynamic and multilevel conception of cognitive resilience
Vestberg et al. [21]	Non-cybersecurity population	Empirical	Cognitive flexibility was associated with resilience-related functioning	Transferred evidence	Cognitive flexibility as a candidate resilience dimension
Banks et al. [3]	Repeated sleep-restriction participants	Experimental	Prior sleep-wake history continued to influence vigilant attention across subsequent restriction	Transferred evidence	Cumulative sleep/recovery effects
Stanton et al. [17]	40 general computer users	Qualitative empirical study	Repeated security demands were associated with resignation, loss of control, risk minimization, and decision avoidance	Cybersecurity-related but indirect	Establishes security-fatigue concept; not direct evidence among cyber professionals
Dykstra and Paul [8]	Tactical cyber operations, including NSA-related studies	Cyber-operations empirical research	Fatigue, frustration, and cognitive workload can be measured directly during cyber operations	Direct cyber evidence	Cognitive load and occupational strain as operational cyber concerns
Nepal et al. [13]	35 cybersecurity incident responders	Mixed-methods study	Burnout was associated with workload, time pressure, limited control, poor teamwork, recognition, sleep quality, and extended work hours	Direct cyber evidence	Interaction between demands and organizational resources

Study	Population / Context	Evidence / Design	Main Finding Relevant to Review	Evidence Status	HCRF Contribution
Chhetri et al. [4]	Security Operations Centers	Human-AI teaming framework	Human-AI task allocation may help address SOC alert fatigue while preserving human judgment	Cybersecurity-specific conceptual evidence	Human-centered automation as an organizational resource
Tariq et al. [18]	SOC alert-fatigue literature	Review	Alert volume, false positives, system complexity, staffing, and repetitive investigation contribute to alert fatigue	Directly cyber-relevant synthesis	Alert overload and technology design as operational demands
Colabianchi et al. [5]	Human-centered cybersecurity	Delphi study	Culture, responsibilities, continuous learning, and managerial practices contribute to human-centered cybersecurity	Direct cyber evidence	Leadership, culture, learning, and organizational resources
Tsen et al. [19]	110 cyber practitioners	Empirical	Relationships between cyber-resilience dimensions and incident outcomes were not uniformly intuitive	Direct cyber evidence	Caution regarding the final organizational-resilience pathway

Framework development proceeded through the identification and integration of recurring relationships across the evidence base. Operational demands were conceptualized as antecedent conditions; cognitive load and occupational stress as explanatory mechanisms through which sustained demands may generate cognitive strain; organizational resources as potential buffering and enabling conditions; cognitive resilience as the central adaptive mechanism concerned with maintaining or recovering effective cognitive functioning; cybersecurity performance as the proximal operational outcome; and organizational cyber resilience as the broader system-level outcome.

These relationships formed the basis of the HCRF. The framework was developed as a theoretically grounded synthesis of the reviewed evidence rather than as an empirically validated causal model. Accordingly, relationships incorporated into the HCRF are treated as propositions requiring subsequent longitudinal, multilevel, experimental, and field-based testing.

Table 1 makes explicit the evidential asymmetry underlying the HCRF: sleep, recovery, and several cognitive mechanisms are supported primarily by transferred evidence, whereas fatigue, burnout, alert overload, and human-AI task allocation have a growing base of cybersecurity-specific evidence. This distinction informs the weighting of claims throughout the review and prevents mechanisms established in adjacent fields from being presented as if they were already validated in operational cyber settings.

Figure 1 summarizes how the review preserves the distinction between transferred and direct cybersecurity evidence while allowing both streams to inform the HCRF. The convergence step is deliberately interpretive rather than equivalent-weight pooling: direct cyber evidence receives greater contextual weight, while transferred evidence supports mechanisms that remain to be validated in operational cyber settings.

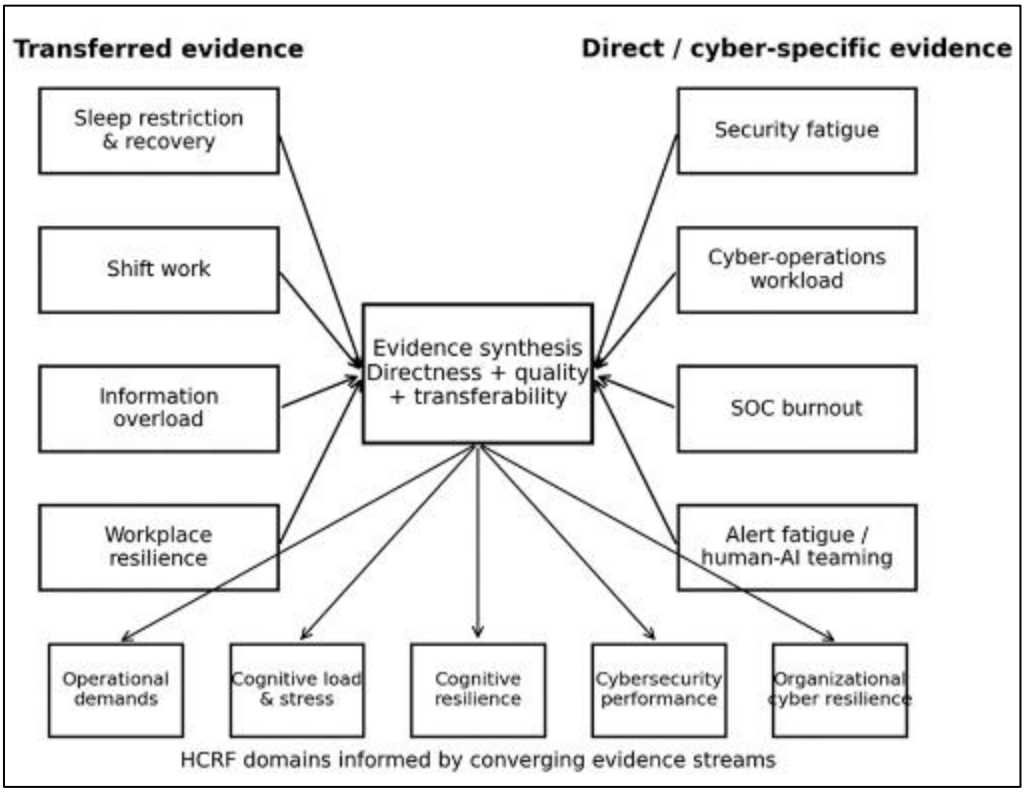

Figure 1: Evidence-convergence logic linking transferred and direct cybersecurity evidence to the principal HCRF domains.

3 HUMAN FACTORS IN MODERN CYBER DEFENSE

Cybersecurity is increasingly understood as a socio-technical system in which security outcomes emerge from interactions among people, technologies, organizational structures, and operational processes. This perspective challenges approaches that treat human actors primarily as sources of error or vulnerability. Cybersecurity professionals are active components of defensive systems whose attention, judgment, expertise, communication, and adaptive capacity influence how effectively technological controls are interpreted and applied. Recent interdisciplinary evidence consequently supports treating human factors as integral to cybersecurity resilience rather than as secondary concerns addressed primarily through awareness and compliance training [12].

This perspective is particularly relevant to Security Operations Centers (SOCs), where analysts must continuously interpret security alerts, distinguish genuine threats from false positives, integrate information from multiple systems, prioritize incidents, and make rapid decisions under uncertainty. Automation has increased the capacity to process large volumes of security data, but it has not eliminated the need for human judgment. Instead, analysts increasingly operate within complex human-machine systems in which automated technologies filter, prioritize, and present information that still requires interpretation, validation, and action.

Alert fatigue illustrates the interaction between technological conditions and human cognitive capacity. Tariq et al. [18], in a comprehensive review of SOC research, identified excessive alert volume, false-positive alerts, inadequate contextual information, repetitive investigation, staffing constraints, and increasing system complexity as interconnected contributors to alert fatigue. These conditions can increase cognitive burden and make sustained prioritization more difficult, creating circumstances in which consequential threats may be overlooked or inadequately investigated [18]. Alert fatigue should therefore not be interpreted solely as an individual attentional limitation; it emerges partly from the design of technologies, workflows, staffing arrangements, and operational processes.

Technological mitigation requires similar caution. Automation and artificial intelligence can reduce repetitive processing, support alert prioritization, and improve information handling, but greater automation does not necessarily translate into lower cognitive demand. Chhetri et al. [4] address this issue through a human-AI teaming perspective that distinguishes automated, augmented, and collaborative forms of SOC activity. Their approach emphasizes complementary roles for automated systems and human expertise rather than wholesale replacement of analysts [4]. This distinction is important because poorly designed automation may redistribute rather than reduce cognitive

workload by requiring analysts to verify opaque recommendations, resolve ambiguous outputs, monitor automated processes, or retain responsibility for high-consequence decisions.

The available evidence therefore suggests that the relationship between technology and human performance is conditional rather than uniformly beneficial. Technologies that reduce low-value processing and improve the quality or prioritization of information may preserve cognitive resources. Conversely, systems that generate excessive alerts, increase verification demands, or provide inadequate contextual information may intensify cognitive burden. From a human-factors perspective, the relevant question is therefore not simply whether security processes are automated, but how technological design changes the cognitive work required of cybersecurity professionals.

Organizational conditions further shape this relationship. Human-centered cybersecurity cannot be reduced to individual vigilance or technical competence because professionals apply those capabilities within work systems that influence workload, communication, learning, recovery, and decision-making. Colabianchi et al. [5], for example, identified organizational culture, clearly defined responsibilities, continuous learning, and related managerial practices as important components of human-centered cybersecurity. Similarly, interdisciplinary evidence indicates that organizational behavior, cybersecurity culture, adaptive education, and socio-technical design influence whether human capabilities function predominantly as sources of vulnerability or resilience [12].

These findings also challenge conventional interpretations of human error. An analyst who misses a critical alert after prolonged exposure to large volumes of low-value alerts may technically have committed an error, but attributing the outcome solely to individual failure obscures the conditions under which that error occurred. Alert design, workload distribution, staffing levels, shift arrangements, organizational expectations, automation quality, communication practices, and recovery opportunities may collectively shape the probability of performance deterioration. Human error is therefore more appropriately examined as an outcome emerging within a work system than as an isolated characteristic of the individual analyst.

This systems perspective does not remove individual responsibility or imply that all performance failures originate in organizational design. Rather, it recognizes that individual expertise and decision-making operate within conditions that can either support or constrain effective performance. This distinction is particularly important in cyber defense because the same analyst may perform differently as alert volume, sleep and recovery, time pressure, team support, system usability, and incident complexity change. Human performance should therefore be conceptualized as dynamic and context dependent rather than as a fixed property of the professional.

Despite growing recognition of these relationships, an important limitation remains in the literature. Alert fatigue, cognitive workload, burnout, human-machine interaction, organizational culture, and related human factors are frequently examined as separate constructs. Tariq et al. [18], for example, provide substantial insight into alert fatigue and its mitigation, while Chhetri et al. [4] focus more specifically on human-AI collaboration. These studies advance understanding of particular components of SOC performance but do not fully explain how operational demands generate cognitive strain, how organizational resources modify that relationship, or how changes in cognitive functioning may subsequently affect cybersecurity performance and organizational cyber resilience.

The evidence reviewed in this section can therefore be organized across three interconnected analytical levels. The first is the operational level, comprising conditions such as alert volume, information complexity, workload, shift demands, time pressure, staffing constraints, and incident complexity. The second is the cognitive level, comprising attention, working memory, executive control, situational awareness, judgment, learning, and adaptive decision-making. The third is the organizational level, comprising staffing, leadership, teamwork, culture, training, recovery opportunities, work design, and technological configuration.

These levels are analytically distinct but operationally interdependent. Operational conditions influence the cognitive demands placed on cybersecurity professionals; cognitive functioning affects how effectively threats are interpreted and managed; and organizational conditions can intensify, buffer, or reshape those demands. This three-level relationship establishes the conceptual foundation for examining sleep, fatigue, cognitive workload, occupational stress, and cognitive resilience in the sections that follow and ultimately for specifying their relationships within the Human Cognitive Resilience Framework.

4 SLEEP, FATIGUE, AND COGNITIVE PERFORMANCE

Sleep is a fundamental determinant of cognitive functioning and is particularly relevant to cybersecurity professionals whose work requires sustained attention, rapid information processing, judgment, and decision-making under uncertainty. In Security Operations Centers (SOCs), these demands may be intensified by continuous monitoring, shift work, high alert volumes, incident escalation, and prolonged vigilance. Sleep and fatigue are therefore relevant to cyber

defense not simply as occupational-health concerns but because they may alter the cognitive resources available for security-critical performance. However, the strength and directness of the supporting evidence vary substantially, requiring a distinction between established cognitive mechanisms and relationships demonstrated specifically in cybersecurity settings.

4.1 Sleep Loss and Cognitive Function

Controlled experimental evidence provides a strong basis for understanding how inadequate sleep can affect cognitive functioning. García et al. [10] found that acute sleep deprivation adversely affected components of attention, working memory, and executive functioning, although the magnitude of impairment differed across cognitive domains. This variation is important because sleep loss should not be interpreted as producing a uniform decline across all aspects of cognition. Rather, particular functions relevant to complex performance may differ in their susceptibility to inadequate sleep [10].

These findings have plausible relevance to cyber defense. SOC analysts depend on sustained and selective attention to distinguish meaningful indicators from large volumes of routine information, working memory to integrate information across systems, and executive control to prioritize competing threats and adjust decisions as new evidence emerges. Impairment in these functions could therefore affect activities central to threat monitoring and incident response. Nevertheless, this represents a mechanism-based inference rather than direct evidence that sleep deprivation produces specific cybersecurity failures.

The effects of inadequate sleep may also accumulate over time. The controlled experiment by Van Dongen et al. [20] demonstrated dose-dependent neurobehavioral deficits during chronic sleep restriction, showing that repeated inadequate sleep can progressively impair waking performance. Importantly, subjective awareness did not necessarily correspond to the degree of objective deterioration, suggesting that individuals may underestimate accumulating impairment. Although this study predates the principal review period, it is retained because it established a foundational dose-response relationship between chronic sleep restriction and neurobehavioral functioning [20].

More recent evidence strengthens the relevance of cumulative sleep history. Banks et al. [3] demonstrated that neurobehavioral impairment accumulated across repeated periods of sleep restriction and that responses during subsequent restriction remained influenced by prior sleep-wake history despite intervening changes in sleep opportunity. These findings indicate that cognitive functioning may reflect accumulated sleep history rather than only the immediately preceding sleep period [3].

Taken together, Van Dongen et al. [20] and Banks et al. [3] suggest that repeated inadequate sleep may have cumulative consequences that are not necessarily eliminated by short-term recovery opportunities. This possibility is particularly relevant to cybersecurity environments involving repeated night shifts, prolonged incidents, on-call responsibilities, or irregular working hours. However, neither study directly examined cybersecurity professionals. Their contribution to the present review is therefore mechanistic: they establish credible relationships between sleep restriction and cognitive functioning that require direct testing within cyber-operational environments.

4.2 Fatigue and Cybersecurity Operations

The transfer of general sleep science to cybersecurity requires caution. Most controlled sleep-deprivation studies have been conducted in laboratory or non-cybersecurity populations, whereas direct studies involving operational cybersecurity professionals remain comparatively limited. Nevertheless, the cognitive functions most consistently implicated in sleep research, particularly vigilance, attention, working memory, and executive control, overlap substantially with capabilities required for threat monitoring and incident response.

Cybersecurity-specific research provides evidence that fatigue and cognitive workload are genuine operational concerns. Dykstra and Paul [8] developed the Cyber Operations Stress Survey (COSS) and applied it across four cyber-operations studies involving the U.S. National Security Agency. Their work examined fatigue, frustration, and cognitive workload during tactical cyber operations and demonstrated that these factors can be assessed within cyber-operational environments rather than treated solely as general occupational well-being variables [8].

This evidence is important because it establishes the presence and measurability of cognitive strain within cyber operations. However, it does not by itself establish that sleep loss causes poorer operational cybersecurity outcomes. The distinction between the existence of fatigue and workload in cyber operations and the causal consequences of sleep restriction for objective cyber performance must therefore be maintained.

Alert fatigue provides a second cybersecurity-specific evidence stream. Tariq et al. [18] identified excessive alert volumes, false positives, repetitive investigations, staffing constraints, and increasing SOC complexity as contributors to analyst fatigue and burnout. Their synthesis further indicates that alert fatigue is intertwined with cognitive workload

and the difficulty of maintaining effective attention during continuous monitoring [18]. Unlike experimental sleep studies, this literature locates fatigue within the technological and organizational conditions of cybersecurity work.

The evidence consequently supports an important distinction between sleep-related fatigue and task-induced cognitive fatigue. Sleep-related fatigue reflects inadequate or disrupted recovery, whereas task-induced cognitive fatigue may develop through prolonged exposure to demanding tasks, excessive information, repetitive alerts, and sustained vigilance. These mechanisms are conceptually distinct but may interact operationally. An analyst experiencing inadequate sleep while simultaneously managing high alert volumes may have fewer cognitive resources available to meet task demands than a well-rested analyst facing comparable conditions.

This interaction is theoretically important for the HCRF because it suggests that cognitive strain cannot be attributed to a single exposure. Sleep history, workload, alert characteristics, task duration, and organizational conditions may combine to influence the cognitive resources available at a given point in time. Future cyber-specific studies should therefore examine these factors jointly rather than treating sleep, fatigue, and workload as independent predictors.

4.3 Shift Work, Recovery, and Sustained Performance

The continuous nature of many cybersecurity operations introduces an additional challenge. SOCs and incident-response teams may require night work, rotating shifts, on-call responsibilities, extended incident response, and work outside conventional hours. Such arrangements can restrict or disrupt opportunities for sleep and recovery.

Evidence from shift-work research demonstrates the difficulty of maintaining adequate sleep under non-standard work schedules. Robbins et al. [16], in a systematic review of workplace interventions intended to improve sleep duration among shift workers, highlighted persistent challenges in protecting adequate sleep within shift-based employment. This evidence supports the broader proposition that work organization can shape opportunities for recovery rather than sleep being determined solely by individual behavior [16].

The relevance to cybersecurity is plausible but should not be overstated. The available evidence does not establish that particular SOC shift schedules cause cybersecurity incidents or that modifying shifts will necessarily improve objective cyber outcomes. Instead, two evidence streams currently converge at different levels. Sleep and shift-work research identifies mechanisms through which irregular schedules and inadequate recovery may affect cognitive functioning, while cybersecurity-specific research establishes that fatigue, workload, prolonged vigilance, and irregular operational demands occur in cyber environments. Direct studies connecting these mechanisms to objective cybersecurity outcomes remain limited.

This evidential gap has practical implications. Recommendations concerning shift design, protected recovery time, or fatigue management in cybersecurity should be framed as risk-reduction strategies supported by plausible cognitive mechanisms rather than as interventions already proven to reduce cyber incidents. Stronger evidence will require longitudinal and field-based studies comparing work schedules, objective sleep or recovery measures, cognitive functioning, and operational cybersecurity performance within the same populations.

4.4 Implications for Cyber Defense and the HCRF

Taken together, the evidence supports a theoretically plausible pathway in which sleep restriction and sustained operational demands contribute to fatigue and cognitive strain, which may reduce the cognitive capacity available for effective cyber performance:

Sleep restriction and sustained operational demands → fatigue and cognitive strain → reduced attentional and executive capacity → increased vulnerability to performance deterioration

The evidential strength is not equivalent across this pathway. The relationship between sleep loss and cognitive impairment is supported by controlled experimental research, whereas the direct relationship between measured sleep loss and objective cybersecurity outcomes remains comparatively under-investigated. Cybersecurity-specific research establishes that fatigue, cognitive workload, alert overload, and prolonged vigilance occur in cyber operations, but it does not yet provide equally strong causal evidence connecting sleep restriction to operational security failures.

This distinction is central to the HCRF. Sleep and recovery are therefore best conceptualized not as isolated determinants of cybersecurity performance but as conditions that influence the cognitive resources available to professionals operating under demanding circumstances. Their effects are likely to interact with workload, alert exposure, occupational stress, task duration, staffing, shift design, and other organizational resources.

Within the HCRF, inadequate sleep and insufficient recovery may therefore increase susceptibility to cognitive strain, whereas adequate recovery may help preserve or restore the cognitive capacity required for sustained attention,

flexible reasoning, and effective decision-making. This interpretation avoids reducing cyber performance either to individual sleep behavior or to organizational conditions alone. Instead, it positions sleep and recovery within the wider socio-technical system that shapes human performance.

The central unresolved question is consequently not whether sleep matters for cognition, which is comparatively well established, but how much variation in cybersecurity performance can be attributed to sleep and recovery once operational demands, cognitive workload, occupational stress, individual differences, and organizational resources are considered simultaneously. Addressing this question requires direct measurement within operational cybersecurity environments and provides a clear empirical bridge from the sleep and fatigue literature to the concept of cognitive resilience developed in the next section.

5 COGNITIVE RESILIENCE IN CYBERSECURITY

Cognitive resilience refers to the capacity to maintain, recover, and adapt the cognitive functioning required for effective performance when individuals are exposed to stress, fatigue, uncertainty, and sustained operational demands. Contemporary resilience research increasingly conceptualizes resilience as a dynamic process rather than a fixed personal trait, emphasizing interactions among individual capabilities, workplace resources, organizational support, and environmental demands [9], [22].

This perspective is particularly relevant to cybersecurity. Professionals routinely work under high cognitive workload, information overload, time pressure, continuous vigilance, and rapidly changing threat conditions. Analysts must interpret ambiguous indicators, distinguish genuine threats from false positives, prioritize competing incidents, integrate information from multiple systems, and make consequential decisions under uncertainty. Effective performance therefore depends not only on technical expertise but also on the capacity to sustain attention, adapt reasoning, regulate responses, and recover cognitive functioning following periods of intense operational demand.

Within this review, cognitive resilience is not proposed as immunity to fatigue or stress. Nor does it imply that effective professionals should maintain unchanged performance regardless of workload. Rather, it describes a dynamic performance-related capacity whose expression depends partly on the relationship between operational demands and the resources available to manage and recover from those demands.

5.1 Distinguishing Cognitive Resilience from Related Constructs

Conceptual clarity is essential because cognitive resilience overlaps with, but is not equivalent to, several established constructs.

Psychological resilience broadly concerns successful psychological adaptation to adversity. Cognitive resilience has a narrower performance-related focus: the maintenance, recovery, or adaptation of cognitive functions required for effective task performance. A professional may therefore report psychological well-being while still experiencing deterioration in vigilance, working memory, or decision accuracy under sustained cognitive demand.

Cognitive reserve, primarily developed within neuroscience and aging research, refers to the capacity to maintain cognitive functioning despite age-related or pathological brain changes. Although both concepts concern preserved functioning, cognitive reserve addresses resistance to neurological deterioration and is therefore conceptually different from the dynamic response to occupational demands examined here.

Coping refers to cognitive or behavioral strategies used to manage stressful circumstances. Coping strategies may contribute to cognitive resilience by reducing or regulating demands, but the strategies themselves are not equivalent to the resulting capacity to sustain or restore cognitive functioning.

Well-being describes an important psychological state or outcome but does not necessarily indicate preserved operational cognitive performance. Similarly, the absence of burnout or distress cannot by itself demonstrate that attention, executive control, working memory, or decision-making remain effective under demanding conditions.

For the purposes of this review, cognitive resilience is therefore defined as:

- The dynamic capacity of cybersecurity professionals to maintain, recover, and adapt the cognitive functions necessary for effective performance during and following demanding operational conditions.
- Three elements of this definition are important. Maintenance concerns sustaining adequate cognitive functioning while demands are occurring. Recovery concerns restoring functioning after deterioration or intense cognitive strain. Adaptation concerns modifying cognitive strategies, mental models, or decision processes when changing conditions make previous approaches inadequate.

This definition establishes cognitive resilience as a dynamic performance-related construct rather than a personality trait, general state of well-being, or synonym for coping. It also provides the conceptual basis for operationalizing the construct within the HCRF.

5.2 Cognitive Mechanisms Underlying Resilience

Cognitive resilience is expressed through several interconnected functions, particularly sustained attention, executive control, working memory, cognitive flexibility, emotional regulation, and adaptive decision-making. These functions are directly relevant to cyber defense. Analysts must maintain attention during prolonged monitoring, retain and integrate information from multiple sources, inhibit premature conclusions, switch between competing incidents, revise hypotheses as new evidence emerges, and make decisions despite uncertainty.

Cognitive flexibility is particularly relevant because resilient performance requires more than resisting deterioration. Cybersecurity professionals must modify strategies when familiar approaches no longer correspond to changing threat conditions. Evidence from non-cybersecurity populations suggests that the capacity to modify cognitive strategies is associated with resilience-related outcomes, supporting cognitive flexibility as one potential component of resilient functioning [21]. However, its specific contribution to resilience among cybersecurity professionals has not yet been established directly.

The same caution applies to the other proposed cognitive components. Their relevance to cybersecurity tasks is theoretically strong, but evidence demonstrating that they collectively constitute a distinct cognitive-resilience construct in cyber professionals remains limited. The HCRF therefore treats these functions as candidate dimensions whose relationships require empirical validation rather than as an already established measurement model.

Cognitive resilience can consequently be understood as involving three related responses to operational demands. First, functioning may be maintained, with sufficient attentional and executive capacity preserved during manageable strain. Second, functioning may recover after temporary deterioration or intense demand. Third, functioning may adapt, allowing strategies and mental models to change in response to new information, technologies, threats, or operational conditions.

Figure 2 depicts the temporal interpretation implied by this definition. Cognitive resilience is not a static score: performance may be maintained during manageable demand, deteriorate as strain accumulates, recover when resources and sleep opportunity are restored, and adapt when learning changes subsequent decision strategies.

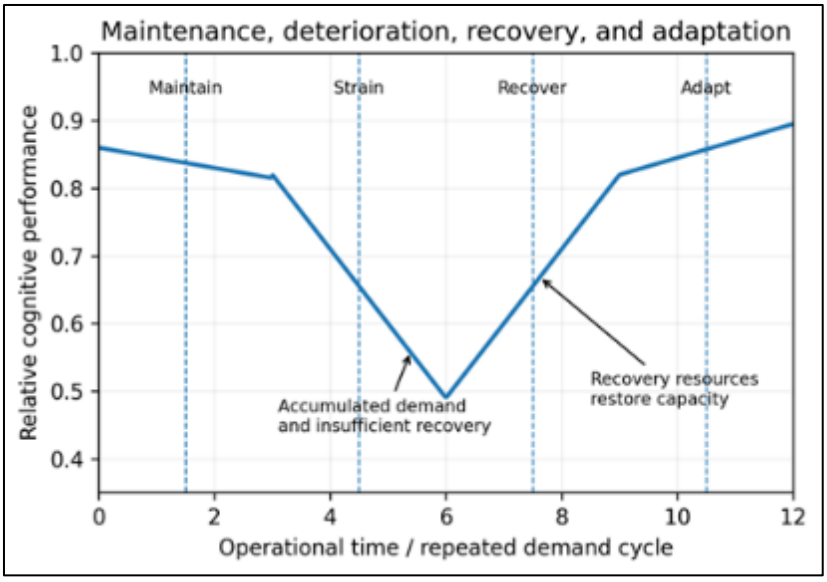

Figure 2: Conceptual temporal cycle of maintenance, deterioration, recovery, and adaptation in cognitive resilience. The trajectory is illustrative rather than an estimated empirical curve.

5.3 Information Overload and Cognitive Resilience

Information overload presents a direct challenge to resilient cognitive functioning. Digital work environments can expose individuals to information volumes that exceed immediate processing capacity, contributing to attentional fragmentation, stress, impaired decision-making, and reduced performance [2]. This problem is particularly relevant to

cybersecurity, where professionals may simultaneously encounter alerts, logs, dashboards, threat intelligence, automated recommendations, communications, and multiple active incidents.

When information supply persistently exceeds available attentional resources, cognitive strain may accumulate. Cognitive resilience may therefore involve the capacity to allocate limited cognitive resources effectively, distinguish high-value information from noise, preserve situational awareness, and maintain decision quality under information pressure [2].

However, this capacity is necessarily bounded. Cognitive resilience should not be interpreted as an unlimited ability to absorb increasing information demands. If workload consistently exceeds recoverable limits, deterioration cannot reasonably be addressed through greater individual effort alone. Organizational and technological interventions become necessary to reduce unnecessary cognitive demands, improve information prioritization, or increase the resources available to manage them.

This boundary is central to the HCRF. Resilience is meaningful only in relation to the demands placed on professionals and the resources available to meet those demands.

5.4 Cognitive Resilience Through a Job Demands–Resources Perspective

The Job Demands–Resources (JD-R) model provides an important theoretical basis for explaining why cognitive resilience should not be conceptualized independently of the work environment. The model distinguishes job demands requiring sustained physical, psychological, or cognitive effort from job resources that support goal attainment, reduce the costs associated with demands, and facilitate effective functioning [6].

Within cybersecurity, operational demands may include alert overload, incident complexity, information density, time pressure, prolonged vigilance, shift work, and staffing constraints. These conditions require sustained cognitive and emotional effort. Relevant organizational resources may include manageable workloads, adequate staffing, recovery opportunities, supportive leadership, psychological safety, effective teamwork, professional development, appropriate shift design, and technologies that reduce unnecessary cognitive burden.

From this perspective, cognitive resilience is not simply an individual characteristic brought into the workplace. Its expression depends partly on the balance between demands and available resources. Organizational resources may operate in at least two ways: by reducing or buffering the cognitive strain generated by operational demands and by supporting the recovery, learning, coordination, and adaptation required for resilient functioning.

This interpretation is consistent with resilience-at-work research emphasizing that resilience emerges through interactions among individual, collective, and organizational resources rather than from personal characteristics alone [9].

The JD-R perspective also establishes an important boundary condition. Cognitive resilience should not imply that well-trained analysts can compensate indefinitely for chronic understaffing, that short recovery periods can completely offset repeated excessive workloads, that psychological resilience eliminates the cognitive consequences of inadequate sleep, or that individual coping can correct poorly designed security systems.

Cyber-operations research already demonstrates that fatigue, frustration, and cognitive workload occur among defenders [8]. The organizational objective should therefore not be to develop professionals who are unaffected by stress, but to maintain operational demands within conditions from which effective cognitive functioning can reasonably be sustained or restored. Chronic excessive workload, inadequate staffing, insufficient recovery, and cognitively burdensome technologies are system conditions requiring system-level responses.

5.5 Adaptive Learning as a Dimension of Cognitive Resilience

Cybersecurity resilience requires more than maintaining current performance or recovering from temporary strain. Cybersecurity professionals must also learn and adapt because threats, attack techniques, vulnerabilities, defensive technologies, and adversarial strategies continually evolve.

Resilient analysts must therefore update threat models, incorporate new intelligence, learn from incidents, and revise decision strategies as operational conditions change. Cognitive flexibility and learning capacity are consequently relevant to the adaptive dimension of cognitive resilience. Effective adaptation may involve not simply returning to a previous level of functioning but developing improved mental models or decision strategies following experience.

This adaptive dimension distinguishes recovery from adaptation. Recovery restores effective functioning after disruption, whereas adaptation modifies functioning in response to what has been learned from that disruption. The distinction also connects individual cognitive resilience with broader cyber-resilience scholarship, in which resilience encompasses preparation, response, recovery, adaptation, and learning rather than prevention alone.

5.6 From Cognitive Resilience to Organizational Cyber Resilience

Cognitive resilience and organizational cyber resilience operate at different analytical levels and should not be treated as equivalent constructs.

Cognitive resilience operates primarily at the individual level and concerns the capacity of cybersecurity professionals to maintain, recover, and adapt the cognitive functioning required for effective performance. Organizational cyber resilience operates at the system level and concerns an organization's capacity to prepare for, withstand, respond to, recover from, and adapt following cyber disruption. This broader conception is consistent with cyber-resilience scholarship that conceptualizes resilience as extending beyond prevention to encompass the capacity to respond to, recover from, and adapt to cyber-related disruptions [1], [7].

The theoretical significance of the HCRF lies partly in explaining how these levels may be connected without assuming that cognitively resilient employees automatically produce a resilient organization. The proposed pathway is:

Cognitive resilience → cybersecurity performance → organizational cyber resilience

Cognitive resilience may support more reliable threat detection, incident prioritization, analytical judgment, collaboration, and response. These performance outcomes may subsequently contribute to organizational capacity to manage and recover from cyber disruption. However, organizational cyber resilience also depends on technical architecture, governance, resources, processes, leadership, and other system-level capabilities. Individual cognitive resilience is therefore proposed as one contributing mechanism rather than a sufficient condition for organizational resilience.

This cross-level relationship remains a theoretical proposition requiring empirical validation.

5.7 Empirical Evidence Gap and Implications for the HCRF

Despite its theoretical relevance, cognitive resilience has not yet been established as a distinct, validated empirical construct among cybersecurity professionals. Cybersecurity research has examined related phenomena including cognitive workload, fatigue, occupational stress, burnout, security fatigue, alert fatigue, and task performance. Dykstra and Paul [8], for example, directly examined fatigue, frustration, and cognitive workload during cyber operations. However, such studies do not measure the multidimensional cognitive-resilience construct proposed here.

This distinction is critical. Evidence that cybersecurity professionals experience fatigue, workload, or occupational stress does not establish that cognitive resilience mediates the relationship between these conditions and cybersecurity performance. Likewise, evidence that particular cognitive functions are associated with resilience-related outcomes outside cybersecurity does not establish that those functions operate identically within cyber-defense environments.

The present review therefore treats cognitive resilience as a theoretically grounded but empirically under-tested construct. Existing cybersecurity research establishes the presence of demanding operational conditions and relevant performance pressures, while occupational and resilience research provides theoretical support for maintenance, recovery, and adaptation under demanding conditions. The HCRF integrates these evidence streams by proposing cognitive resilience as a testable mechanism connecting cognitive strain with cybersecurity performance.

Within the framework, operational demands are expected to influence cognitive load and occupational stress; organizational resources may buffer these effects and support recovery and adaptation; and cognitive resilience may influence whether effective threat detection, prioritization, analytical judgment, decision-making, and incident response can be sustained or restored.

The immediate research priority is therefore not to assume the validity of cognitive resilience as a cybersecurity construct, but to establish it empirically. This requires development and validation of measures capable of distinguishing cognitive resilience from psychological resilience, coping, cognitive reserve, fatigue, burnout, and general well-being, followed by testing of its relationships with objective cognitive and cybersecurity-performance outcomes. Until such evidence is available, cognitive resilience should be interpreted as the central testable mechanism proposed by the HCRF rather than as an established determinant of cyber performance.

6 SECURITY FATIGUE, BURNOUT, AND ORGANIZATIONAL CYBER RISK

Security fatigue, alert fatigue, cognitive fatigue, occupational stress, and burnout describe related but distinct responses to demanding cybersecurity work. Cybersecurity professionals frequently operate under conditions of sustained vigilance, high information density, time pressure, incident uncertainty, and continuous responsibility for protecting organizational systems. When these demands are persistent and recovery is insufficient, they may contribute to cognitive strain, emotional exhaustion, reduced motivation, and diminished capacity to sustain effective performance. Cyber-operations research has directly documented fatigue, frustration, and cognitive workload as relevant operational concerns, reinforcing the need to examine these conditions as potential cybersecurity-performance risks rather than solely as employee well-being issues [8].

Conceptual distinction is important because these conditions operate at different levels. Security fatigue concerns weariness or disengagement arising from repeated security-related demands and decisions. Alert fatigue refers more specifically to the attentional and decision burden created by repeated exposure to security alerts. Cognitive fatigue reflects reduced cognitive efficiency following sustained mental effort. Occupational stress concerns the psychological and physiological strain associated with demanding work conditions, whereas burnout represents a broader and more persistent occupational response to chronic workplace stress. These constructs may coexist and interact, but they should not be treated as interchangeable.

6.1 Security Fatigue: Concept and Evidence

Security fatigue describes weariness, frustration, or reluctance associated with repeated cybersecurity demands and decisions. Stanton et al. [17] provided one of the foundational empirical examinations of the construct through semi-structured interviews with 40 computer users. Participants described resignation, loss of control, risk minimization, decision avoidance, and related responses consistent with security fatigue. Their findings demonstrated that repeated cybersecurity demands can shape how individuals interpret and respond to security requirements [17].

An important limitation, however, concerns the population studied. Stanton et al. [17] examined general computer users rather than cybersecurity professionals. The study therefore provides evidence for the broader behavioral concept of security fatigue but does not establish how the construct manifests among SOC analysts, incident responders, or other cybersecurity practitioners.

Subsequent scholarship has increasingly recognized stress, burnout, and security fatigue as important human-factor issues within cybersecurity. Nobles [14], for example, argues that these conditions represent persistent challenges that are insufficiently addressed by approaches focused predominantly on technological controls. Much of this literature, however, remains conceptual or descriptive. Direct empirical evidence establishing the prevalence, predictors, and performance consequences of security fatigue among cybersecurity professionals remains limited.

This evidential limitation is important for the HCRF. Security fatigue should currently be treated as a plausible manifestation of repeated cybersecurity demands rather than as a validated mediator between operational conditions and cyber performance.

6.2 Alert Fatigue in Security Operations Centers

Alert fatigue is more directly situated within SOC operations. Analysts may receive large numbers of alerts that vary substantially in reliability, severity, and contextual quality. Each alert can require decisions concerning investigation, prioritization, escalation, dismissal, or further validation. When alert volume and complexity exceed available attentional resources, sustained prioritization may become increasingly difficult.

Tariq et al. [18], in a comprehensive review of alert fatigue in SOCs, identified multiple interacting causes and examined mitigation approaches involving automation, augmentation, and human-AI collaboration. Their synthesis indicates that alert fatigue arises not simply from analyst limitations but from interactions among alert characteristics, technological design, operational processes, staffing, and human workload [18].

This socio-technical interpretation is important because it locates alert fatigue partly within system design. Increasing the number of automated security tools does not necessarily reduce fatigue if those tools generate excessive false positives, provide inadequate context, or create additional verification requirements. Automation may therefore reduce some forms of workload while creating others.

Chhetri et al. [4] address this problem through a human-AI teaming approach that assigns different roles to automated and human actors. Routine or repetitive processing may be delegated to automated systems, while human judgment is retained for ambiguous, complex, or high-consequence decisions [4]. Such an approach may reduce unnecessary

cognitive burden, but its effectiveness depends on how tasks, information, and responsibility are distributed between humans and automated systems.

Alert fatigue therefore illustrates a broader HCRF principle: operational demands emerge partly from how technologies and workflows are configured. The relevant concern is not simply the number of alerts presented to an analyst, but whether the total informational and decision burden remains within sustainable cognitive limits.

6.3 Burnout Among Cybersecurity Professionals

Burnout differs from security fatigue and alert fatigue in both scope and persistence. Whereas fatigue may develop during repeated or prolonged cognitive demands, burnout represents a broader occupational response to chronic workplace stress. Treating these constructs as equivalent would obscure differences in their antecedents, duration, and potential consequences.

Direct cybersecurity evidence is beginning to clarify factors associated with burnout. Nepal et al. [13] conducted a mixed-methods study involving 35 cybersecurity incident responders and combined self-reported occupational and personal characteristics with digital activity data. Nineteen participants, representing more than half of the sample, experienced burnout. Burnout was associated with greater workload, time pressure, limited control, poor teamwork, inadequate recognition, poor sleep quality, and working more than 40 hours per week. Burned-out participants also demonstrated greater email, meeting, and after-hours collaborative activity [13].

This study is particularly valuable because it examines cybersecurity incident responders directly and combines self-report data with behavioral indicators. At the same time, its small sample size limits generalizability, and the observational design does not establish that the identified working conditions caused burnout. The findings therefore provide direct cybersecurity-specific associations rather than population-wide causal estimates.

Nevertheless, the pattern is theoretically important. Burnout was associated not with a single individual characteristic but with combinations of workload, time pressure, job control, teamwork, recognition, sleep quality, and working hours. This is consistent with the HCRF's broader proposition that sustained strain emerges from interactions between operational demands and available organizational resources.

6.4 From Occupational Strain to Cybersecurity Performance

The relationship between occupational strain and cybersecurity performance remains one of the most important unresolved issues in the literature. It is plausible that persistent fatigue, stress, or burnout could affect threat detection, decision quality, collaboration, prioritization, and incident response, but direct empirical evidence connecting these conditions with objective cybersecurity outcomes remains limited.

Dykstra and Paul [8] provide part of the empirical pathway. Their Cyber Operations Stress Survey measured fatigue, frustration, and cognitive workload during tactical cyber operations across four studies involving U.S. National Security Agency operations. Their findings establish that these factors can be examined directly in operational cyber settings and support treating them as relevant human-performance variables.

Research on alert fatigue provides complementary evidence that excessive alert demands can create substantial cognitive burden in SOC environments, while broader cognitive research indicates that sustained fatigue and workload can impair attention and executive functioning. These evidence streams converge on a plausible pathway:

Operational demands → fatigue, cognitive strain, and burnout-related outcomes → potential degradation of cybersecurity performance → increased vulnerability to organizational cyber risk

However, the evidential strength declines along this pathway. The existence of operational strain within cybersecurity is supported directly, while the final links to objective cyber performance and organizational risk remain incompletely tested. The pathway should therefore be interpreted as theoretically supported rather than empirically established.

This distinction is important to the HCRF because it prevents fatigue or burnout from being treated as direct causes of cyber incidents. Cyber incidents are multi-causal events shaped by technical vulnerabilities, adversarial actions, organizational processes, technological design, and human decisions.

6.5 Organizational Antecedents and Protective Resources

Available cybersecurity evidence increasingly suggests that organizational conditions shape the likelihood that operational demands develop into sustained strain. Nepal et al. [13] identified workload, time pressure, job control, teamwork, recognition, working hours, and sleep quality among factors associated with burnout in incident responders.

Alert-fatigue research similarly identifies technological and organizational conditions that shape the cognitive burden placed on SOC personnel [18].

These findings challenge interventions that locate responsibility primarily within individual workers. Stress-management training, mindfulness, coping strategies, and individual resilience development may have value, but they cannot compensate indefinitely for persistent overload, chronic understaffing, poorly designed alert systems, inadequate recovery opportunities, or weak managerial support.

A more defensible organizational response is to reduce avoidable demands while strengthening relevant resources. Potential measures include realistic workload allocation, adequate staffing, protected recovery periods, supportive supervision, effective teamwork, recognition, greater job control, and technologies designed to reduce rather than redistribute cognitive burden.

These measures should nevertheless be described as evidence-informed strategies rather than universally established solutions. Cybersecurity-specific intervention studies testing their direct effects on burnout, cognitive performance, and objective cyber outcomes remain limited.

6.6 Implications for Organizational Cyber Risk and the HCRF

Security fatigue, alert fatigue, cognitive fatigue, occupational stress, and burnout are relevant to cybersecurity governance because they affect the human capabilities through which technical information is interpreted, prioritized, and acted upon. Their importance does not imply that a fatigued or burned-out analyst will necessarily cause a security incident. Cyber incidents remain multi-causal and cannot defensibly be attributed to employee strain alone.

The more supportable proposition is that persistent strain may reduce the reliability of human performance when accurate and timely judgment is required. Depleted cognitive resources may increase vulnerability to delayed investigation, inconsistent prioritization, reduced collaboration, impaired situational awareness, or diminished decision quality. Whether these vulnerabilities translate into measurable cybersecurity failures depends on the wider socio-technical system.

Within the HCRF, these constructs should therefore occupy different conceptual positions. Cognitive load and occupational stress remain the principal explanatory mechanisms linking operational demands with cognitive strain. Security fatigue, alert fatigue, cognitive fatigue, and burnout are better interpreted as related manifestations or outcomes of sustained demands, repeated decision burden, insufficient recovery, or inadequate organizational resources rather than as interchangeable formal mediators.

This distinction prevents the framework from becoming conceptually overloaded. It also preserves cognitive resilience as the central adaptive mechanism concerned with whether effective cognitive functioning can be maintained, recovered, or adapted despite operational strain.

The organizational implication is therefore not that cybersecurity professionals should simply become more resilient. Sustainable cognitive functioning depends partly on whether workloads, technologies, staffing arrangements, leadership practices, recovery opportunities, and other organizational resources remain within conditions that permit effective performance. This provides the transition from identifying human-performance risks to examining the organizational resources that may mitigate those risks in the following section.

7 BUILDING HUMAN-CENTERED CYBER DEFENSE

Human-centered cyber defense recognizes that effective cybersecurity depends on the interaction of people, processes, technologies, and organizational conditions. Rather than treating cybersecurity professionals primarily as potential sources of error, this perspective regards them as active components of the defense system whose cognitive capabilities must be supported through appropriate work, organizational, and technology design. This interpretation is consistent with NIST's human-centered cybersecurity approach, which emphasizes empirically grounded solutions designed around interactions among people, processes, and technology [11].

Within the Human Cognitive Resilience Framework (HCRF), human-centered cyber defense is particularly important because organizational resources may influence whether operational demands remain manageable or develop into sustained cognitive strain. The objective is not to eliminate demanding work, which is neither realistic nor necessarily desirable in cybersecurity, but to create conditions that enable professionals to perform, recover, adapt, and learn under pressure.

Organizational resources are therefore considered here not as peripheral workforce benefits but as components of the socio-technical environment that may shape cognitive functioning and cyber performance. The principal resources identified across the reviewed literature include workload and staffing arrangements, supportive leadership and teamwork, human-centered automation, continuous professional development, and opportunities for sleep and recovery.

7.1 Workload, Staffing, and Work Design

Workload and staffing represent foundational organizational conditions because they influence the intensity and duration of cognitive demands placed on cybersecurity professionals. Direct evidence from cybersecurity incident responders indicates that burnout is associated with high workload, time pressure, limited job control, poor teamwork, inadequate recognition, poor sleep quality, and work extending beyond 40 hours per week [13].

These findings suggest that workforce resilience cannot be reduced to the number of personnel employed. Staffing adequacy also depends on how work is distributed, whether operational demand corresponds with available personnel, how frequently professionals work beyond scheduled hours, and whether sufficient recovery occurs between high-intensity periods.

Work design should therefore seek to reduce persistent mismatches between operational demands and available cognitive resources. Potential strategies include realistic workload allocation, appropriate shift scheduling, protected recovery periods, task rotation, sufficient staffing, and greater control over work organization.

However, an important evidential limitation remains. Although these practices are consistent with occupational and cybersecurity evidence concerning workload and burnout, cybersecurity-specific intervention studies testing whether particular staffing or scheduling arrangements improve objective cognitive or cyber-performance outcomes remain limited. These measures should therefore be presented as evidence-informed organizational strategies rather than established causal solutions.

Within the HCRF, workload and staffing may influence cognitive resilience through two pathways. First, they may affect the level of cognitive load and occupational stress generated by operational demands. Second, they may determine whether sufficient time and capacity remain available for recovery following intense work.

7.2 Leadership, Teamwork, and Supportive Communication

Human-centered cyber defense also depends on social and organizational conditions that support communication, coordination, and help-seeking. Cybersecurity decisions rarely occur in isolation. Analysts frequently depend on information exchange, escalation procedures, shared situational awareness, peer consultation, and coordinated decision-making during complex incidents.

Direct evidence from cybersecurity incident responders associates poor teamwork with burnout, while managerial support has also been identified as relevant to occupational strain [13]. These findings suggest that leadership and teamwork may influence not only employee experience but also the conditions under which professionals manage uncertainty and operational pressure.

Supportive leadership can shape workload expectations, staffing decisions, access to recovery, communication norms, training opportunities, and the extent to which employees can acknowledge uncertainty or seek assistance without inappropriate blame. Team environments may similarly influence whether emerging concerns are shared early, whether expertise is distributed effectively, and whether errors or ambiguous findings can be discussed before they develop into larger operational problems.

Psychological safety is relevant within this context because cybersecurity professionals may sometimes need to challenge assumptions, report uncertainty, request assistance, or acknowledge mistakes during high-pressure operations. However, the available cybersecurity-specific evidence directly linking psychological safety to objective cyber outcomes remains limited. Its role within the HCRF should therefore be treated as theoretically and organizationally plausible rather than conclusively established.

Within the framework, leadership and teamwork are proposed to function as social resources that may reduce avoidable occupational stress and support coordination, recovery, learning, and adaptive decision-making.

7.3 Human-Centered Automation and AI

Automation and artificial intelligence can potentially reduce cognitive burden by removing repetitive processing, improving alert prioritization, and presenting relevant information more efficiently. However, automation is not

inherently human-centered. Poorly designed systems may generate additional alerts, create new verification requirements, reduce transparency, or introduce additional monitoring responsibilities.

Recent incident-management research sharpens this point. Kincl, Adam, and Pavleska [25] show that industry-aligned AI integration depends on task allocation, human oversight, contextual constraints, and recovery/governance requirements rather than algorithmic capability alone. Security-operations research has likewise begun to emphasize evidence-backed, human-verifiable AI support rather than opaque automation [28]. Accordingly, the HCRF treats AI as a conditional organizational resource: it can preserve cognitive capacity when it reduces low-value processing and improves context, but it can become an additional demand when it creates verification burden, automation bias, or poorly calibrated trust.

Chhetri et al. [4] address this problem through a human-AI teaming model for Security Operations Centers. Their framework differentiates among automated, augmented, and collaborative modes of operation, allowing routine tasks to be automated while preserving human expertise for ambiguous, uncertain, and high-consequence decisions [4].

The critical issue is therefore not simply whether automation is present, but how cognitive work is redistributed between humans and machines. Automation that removes repetitive low-value processing may preserve attentional resources. In contrast, automation that produces opaque recommendations or requires continuous verification may simply shift cognitive demand from one activity to another.

From the perspective of cognitive resilience, the relevant design question is:

- Which allocation of tasks between humans and AI best preserves attention, situational awareness, judgment, and adaptive capacity while reducing unnecessary cognitive burden?
- This question moves human-centered automation beyond efficiency alone. A system may improve processing speed while simultaneously weakening situational awareness, increasing automation bias, or creating dependence on opaque recommendations. Human-centered design should therefore consider both technical performance and the cognitive consequences of automation.
- Within the HCRF, technology design functions as an organizational resource when it reduces avoidable cognitive load, improves information quality, and preserves meaningful human judgment. Conversely, poorly configured technologies may become operational demands in their own right.

Figure 3 translates this conditional view of automation into a task-allocation heuristic. As ambiguity and consequence increase, the recommended role shifts from automation toward augmentation, collaboration, and human-led judgment. The matrix is a design aid rather than a validated decision rule, but it makes the HCRF's human-AI proposition operationally interpretable.

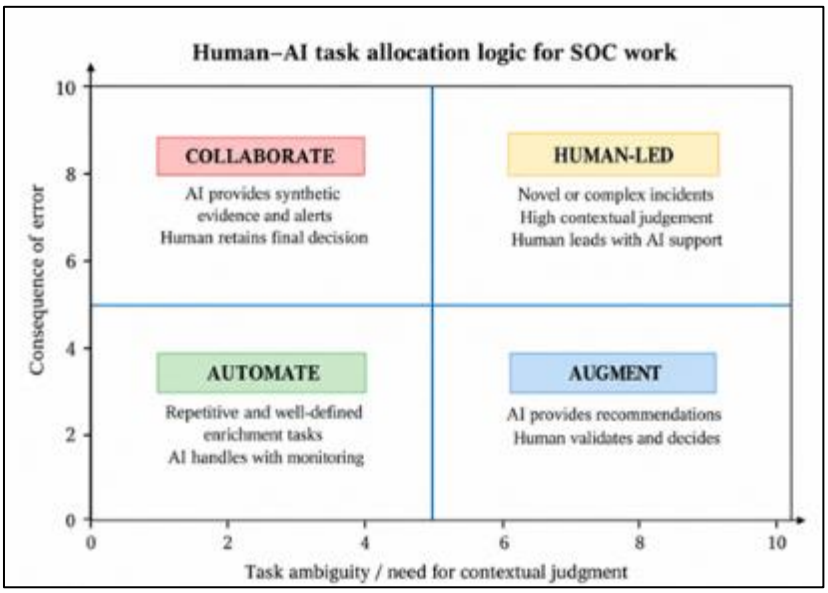

Figure 3: Human-AI task-allocation logic for Security Operations Center work. The matrix is conceptual and does not represent an empirically validated decision rule.

7.4 Training and Adaptive Expertise

Continuous professional development represents another important organizational resource because cybersecurity operates in an environment of rapidly evolving threats, attack techniques, vulnerabilities, technologies, and defensive practices. Static technical knowledge is therefore insufficient for sustained performance.

Training should extend beyond the acquisition of technical knowledge to include scenario-based decision-making, incident simulation, collaborative problem-solving, adaptive reasoning, and effective use of AI-supported tools. Recent human-factor scholarship similarly emphasizes adaptive education, socio-technical integration, and human-centered approaches to cybersecurity capability development [12].

Within the HCRF, training is particularly relevant because cognitive resilience includes adaptation as well as maintenance and recovery. Professionals must be able not only to return to effective functioning after demanding events but also to revise mental models and strategies when threats or technologies change.

Post-incident reviews, simulations, mentoring, knowledge sharing, and reflective practice may therefore contribute to both individual expertise and organizational learning. These activities can help convert operational experience into improved future performance rather than treating recovery simply as a return to the previous state.

Nevertheless, cybersecurity-specific evidence establishing which forms of training most effectively strengthen cognitive resilience remains limited. Training should therefore be treated as a plausible resilience-supporting resource whose effects require direct empirical evaluation.

7.5 Sleep, Recovery, and Sustainable Performance

Sleep and recovery should be incorporated into cybersecurity workforce design rather than treated solely as personal responsibilities. As discussed in Section 4, sleep restriction can impair cognitive functions relevant to cyber operations, while cybersecurity-specific evidence indicates that poor sleep quality and extended working hours occur alongside burnout among incident responders.

Organizations operating continuous SOCs should therefore consider whether shift structures, on-call expectations, overtime practices, incident escalation procedures, and staffing arrangements permit sufficient recovery. The objective is not to prescribe a single optimal schedule across all organizations but to recognize recovery capacity as an operational resource.

This distinction is important because recommendations directed only at individual sleep behavior may overlook organizational conditions that restrict recovery opportunities. Encouraging employees to obtain adequate sleep while maintaining chronic overtime, unpredictable on-call demands, or insufficient staffing places responsibility on individuals for conditions that are partly shaped by the organization.

Within the HCRF, recovery may operate as a resource that helps restore cognitive functioning following periods of sustained strain. However, recovery should not be assumed to offset unlimited exposure to excessive demands. Persistent workload or repeated sleep disruption may exceed the capacity of short-term recovery practices to restore effective functioning.

7.6 Designing an Integrated System for Cognitive Resilience

The organizational resources examined above should not be treated as independent interventions. Their effects are likely to depend on how they interact within the wider work system.

A well-staffed SOC may still produce excessive cognitive strain if alert systems are poorly designed. Effective AI may provide limited benefit when personnel are chronically sleep deprived. Strong technical training may not produce optimal performance where communication and teamwork are weak. Similarly, supportive leadership cannot fully compensate for persistent alert overload or inadequate staffing.

Human-centered cyber defense therefore requires a systems approach in which staffing, workload, leadership, teamwork, recovery, training, and technology design function as interconnected organizational resources. This interpretation is consistent with interdisciplinary cybersecurity research emphasizing organizational behavior, cybersecurity culture, human-centered design, adaptive education, and responsible AI as interconnected components of effective security systems [12].

This systems perspective also implies that organizational resources may have complementary effects. The benefit of one resource may depend on the presence of others. For example, improved staffing may create recovery opportunities,

while supportive leadership may determine whether those opportunities are actually used. Similarly, effective automation may reduce cognitive load, but adequate training may be required for professionals to interpret and challenge automated recommendations appropriately.

The HCRF therefore does not assume that any single intervention produces cognitive resilience. Resilient functioning is more plausibly supported by combinations of resources that keep operational demands within manageable and recoverable limits.

7.7 From Human-Centered Defense to the HCRF

The central implication of the reviewed evidence is that organizations do not merely experience variation in cognitive resilience among their cybersecurity professionals; they help create the conditions under which resilient functioning can be supported or undermined.

Within the HCRF, organizational resources are therefore proposed to perform two related functions.

First, they may buffer the relationship between operational demands and cognitive strain. Adequate staffing, manageable workload, appropriate technology design, leadership support, and effective coordination may reduce the cognitive load and occupational stress generated by demanding operational conditions.

Second, they may support cognitive resilience directly by facilitating recovery, learning, coordination, adaptation, and sustained access to cognitive resources.

These functions are conceptually distinct. Buffering reduces the extent to which demands generate strain, whereas resilience support strengthens the conditions under which effective cognitive functioning can be maintained, recovered, or adapted after strain occurs.

The distinction provides the bridge between the evidence synthesized in Sections 3–7 and the formal conceptual framework developed in Section 8. Rather than treating sleep, fatigue, burnout, workload, leadership, training, automation, and resilience as separate cybersecurity concerns, the HCRF integrates them into a testable socio-technical pathway linking operational demands, cognitive strain, organizational resources, cognitive resilience, cybersecurity performance, and organizational cyber resilience.

8 A HUMAN COGNITIVE RESILIENCE FRAMEWORK FOR MODERN CYBER DEFENSE

The preceding sections demonstrate that cybersecurity performance is shaped by more than technical capability. Operational demands, sleep and recovery, cognitive workload, occupational stress, fatigue, burnout, organizational resources, and adaptive functioning interact to influence how effectively cybersecurity professionals detect, interpret, prioritize, and respond to threats. Yet these factors are frequently examined independently, limiting understanding of the mechanisms through which working conditions influence cognitive functioning and how these effects may extend to cybersecurity performance and organizational cyber resilience.

To integrate these relationships, this review proposes the Human Cognitive Resilience Framework (HCRF). The HCRF is a socio-technical conceptual model explaining how operational demands may influence cybersecurity performance through cognitive load, occupational stress, and cognitive resilience, while organizational resources may buffer cognitive strain and support the maintenance, recovery, and adaptation of cognitive functioning.

The framework does not position human cognition as an alternative to technical cybersecurity controls. Rather, cognitive functioning is treated as one component of a wider socio-technical defense system in which people, technologies, organizational structures, and operational processes interact. This interpretation is consistent with contemporary human-factors research emphasizing interactions among behavior, organizational culture, technology, and adaptive capacity rather than treating people primarily as sources of cybersecurity vulnerability [12].

8.1 Theoretical Foundations of the HCRF

The HCRF draws on three complementary theoretical perspectives: socio-technical systems thinking, the Job Demands–Resources (JD-R) model, and contemporary resilience theory.

The socio-technical perspective provides the broadest theoretical foundation. Cybersecurity outcomes emerge from interactions among people, technologies, organizational structures, procedures, and operating environments. Analyst performance therefore cannot be explained solely by individual competence or technical infrastructure. Socio-technical cybersecurity research similarly emphasizes that human behavior, organizational conditions, and technological systems

must be considered together when explaining security outcomes [12], [15]. Khadka and Ullah [12], for example, integrate psychological resilience, adaptive education, socio-technical design, organizational behavior, and ethical AI within a broader human-centered cybersecurity perspective.

The JD-R model provides the demand-resource logic underlying the framework. The model proposes that sustained job demands require continuing psychological, physical, or cognitive effort, while job resources can reduce the costs associated with those demands and support effective functioning [6]. Within the HCRF, alert overload, information overload, shift work, time pressure, prolonged vigilance, staffing constraints, and incident complexity represent operational demands. Organizational resources such as adequate staffing, supportive leadership, recovery opportunities, teamwork, training, appropriate work design, and human-centered automation may reduce the strain associated with these demands or provide resources needed to recover from them.

Contemporary resilience theory provides the adaptive component. Resilience-at-work research increasingly conceptualizes resilience as dynamic, multilevel, and dependent on interactions among individual, collective, and organizational resources rather than as a fixed personal characteristic [9]. The HCRF applies this logic specifically to cognitive functioning in cyber defense by asking how the cognitive capabilities required for effective performance are maintained, recovered, and adapted under operational pressure.

These perspectives perform distinct but complementary roles. Socio-technical theory identifies the system within which cybersecurity performance occurs. JD-R logic explains how operational demands and organizational resources may generate or mitigate strain. Resilience theory explains how effective functioning may be maintained, restored, and adapted over time. Their integration provides the theoretical basis for the HCRF.

8.2 Why a New Framework Is Needed

Existing human-centered cybersecurity frameworks already recognize that people, organizational culture, training, technology, and resilience influence cybersecurity. The novelty of the HCRF should therefore not be framed as the first attempt to incorporate human factors into cybersecurity theory. Its contribution is narrower and more specific.

First, the HCRF places cognitive functioning at the center of the pathway between working conditions and cybersecurity performance. Rather than treating human factors as a broad category, it identifies the cognitive processes through which operational conditions may become relevant to cyber-defense outcomes.

Second, the HCRF distinguishes operational demands from the mechanisms through which those demands may affect functioning. Alert overload, shift work, time pressure, or incident complexity are not equivalent to cognitive impairment. The framework proposes that such demands may generate cognitive strain primarily through cognitive load and occupational stress, while fatigue, sleep disruption, security fatigue, alert fatigue, and burnout represent related conditions or manifestations that may accompany sustained demands and inadequate recovery.

Third, the HCRF distinguishes cognitive resilience from organizational cyber resilience. Cognitive resilience operates primarily at the individual level and concerns the maintenance, recovery, and adaptation of cognitive functioning required for effective performance. Organizational cyber resilience operates at the system level and concerns the capacity of an organization to prepare for, withstand, respond to, recover from, and adapt following cyber disruption.

Fourth, the framework specifies a cross-level pathway connecting these constructs:

Operational demands → cognitive load and occupational stress → cognitive resilience → cybersecurity performance → organizational cyber resilience

Organizational resources are positioned both as buffers against the development of cognitive strain and as direct supporters of cognitive resilience.

This architecture is more specific and empirically testable than the general proposition that human factors influence cybersecurity. It identifies distinct constructs, proposes relationships among them, and preserves the analytical distinction between individual cognitive functioning and organizational outcomes.

8.3 Components of the Framework

8.3.1 Operational Demands

Operational demands refer to features of cybersecurity work that require sustained cognitive, emotional, or behavioral effort. They include alert overload, information overload, shift work, prolonged working hours, time pressure, incident complexity, continuous vigilance, staffing constraints, and rapid technological change.

These demands are not inherently harmful. Complexity, uncertainty, vigilance, and time-sensitive decision-making are unavoidable features of many cyber-defense roles. Risk is expected to increase when the intensity, duration, frequency, or accumulation of demands exceeds the cognitive and organizational resources available to manage them.

The HCRF therefore predicts variation rather than assuming that all exposure to demanding work produces impairment. Moderate or short-duration demands may remain manageable and may sometimes stimulate effective engagement, whereas persistent or excessive demands may contribute to cumulative cognitive strain.

8.3.2 Cognitive Load and Occupational Stress

Cognitive load and occupational stress represent the principal explanatory mechanisms through which operational demands are proposed to influence cognitive resilience.

Cognitive load refers to the mental effort required to process information, maintain situational awareness, manage competing tasks, retain relevant information, and make decisions. Occupational stress refers to the psychological and physiological strain that may develop when work demands challenge or exceed the resources available for coping and recovery.

Within cybersecurity environments, sustained cognitive load and occupational stress may be accompanied by fatigue, attentional depletion, sleep disruption, emotional exhaustion, and reduced decision capacity. These related conditions are important indicators of strain but are not treated as interchangeable constructs within the framework.

The HCRF does not assume that temporary increases in cognitive load or occupational stress inevitably reduce performance. Performance deterioration is expected to become more likely when strain is persistent, cumulative, or insufficiently offset by recovery and organizational resources.

8.3.3 Organizational Resources

Organizational resources are the structural, social, technological, and managerial conditions that support effective functioning under demanding circumstances. They include adequate staffing, realistic workload allocation, supportive leadership, psychological safety, effective teamwork, protected recovery opportunities, appropriate scheduling, continuous professional development, human-centered technology design, and intelligent automation.

Within the HCRF, organizational resources perform two theoretically distinct functions.

First, they may exert a buffering effect by weakening the extent to which operational demands generate cognitive load and occupational stress. Improved alert prioritization, for example, may reduce unnecessary information processing, while adequate staffing and appropriate scheduling may reduce cumulative workload and recovery deficits.

Second, they may exert a resilience-supporting effect by directly strengthening the conditions necessary for maintenance, recovery, learning, coordination, and adaptation. Training may improve adaptive expertise, supportive teams may facilitate distributed problem-solving, and recovery opportunities may help restore cognitive functioning following periods of intense demand.

This dual role is consistent with resilience-at-work research emphasizing that resilience emerges through interactions among individual, collective, and organizational resources [9].

8.3.4 Cognitive Resilience

Cognitive resilience is the central adaptive construct within the HCRF. It is defined as:

The dynamic capacity of cybersecurity professionals to maintain, recover, and adapt the cognitive functions necessary for effective performance during and following demanding operational conditions.

Cognitive resilience is therefore conceptualized as a dynamic performance-related process rather than a fixed antecedent trait. Candidate dimensions include sustained attention, executive functioning, cognitive flexibility, emotional regulation, adaptive decision-making, learning capacity, and recovery of decision capability following periods of strain.

These dimensions should not yet be interpreted as an empirically validated measurement model. As established in Section 5, cognitive resilience remains a theoretically grounded but under-tested construct within cybersecurity. Future empirical research must determine whether these dimensions form a coherent construct and whether that construct

can be distinguished reliably from psychological resilience, coping, fatigue, burnout, cognitive reserve, and general well-being.

Importantly, the HCRF does not conceptualize resilience as tolerance of chronic overload. A cognitively resilient analyst is not one who remains unaffected regardless of workload. Rather, resilience concerns the capacity to preserve essential functioning under manageable demands, recover following periods of strain, and adapt cognitive strategies when operational conditions change, particularly when appropriate organizational resources are available.

8.4 Cybersecurity Performance

Cybersecurity performance represents the proximal operational outcome within the HCRF. It concerns how effectively cybersecurity professionals translate cognitive functioning and expertise into security-relevant action.

For future empirical testing, cybersecurity performance may be operationalized through indicators such as threat-detection accuracy, incident prioritization, decision quality, response speed, analytical judgment, collaboration and coordination, and operational error rates. Where possible, objective or behaviorally anchored measures should be preferred over reliance solely on self-reported performance.

The framework proposes that higher cognitive resilience should be associated with greater reliability of cybersecurity performance under demanding conditions. Conversely, deterioration in cognitive functioning may increase vulnerability to attentional lapses, delayed response, inaccurate prioritization, or analytical errors.

This relationship remains a testable proposition rather than an established universal causal relationship because direct empirical studies linking measured cognitive resilience with objective SOC or incident-response performance remain limited.

8.5 Organizational Cyber Resilience

Organizational cyber resilience is positioned as the higher-level outcome of the HCRF and concerns the capacity of an organization to prepare for, withstand, respond to, recover from, and adapt following cyber disruption. This interpretation is consistent with broader cyber-resilience scholarship emphasizing resilience as a multidimensional capacity extending beyond prevention to include response, recovery, and adaptation [1], [7].

The framework does not assume that employee well-being or individual cognitive resilience directly produces organizational cyber resilience. Rather, the proposed cross-level mechanism operates through cybersecurity performance:

Cognitive resilience → cybersecurity performance → organizational cyber resilience

This distinction is important because individual cognition and organizational resilience operate at different levels of analysis. Organizational cyber resilience additionally depends on technical architecture, governance, redundancy, resources, procedures, leadership, and other system-level capabilities. Cognitive resilience is therefore proposed as one contributing human-performance mechanism rather than a sufficient condition for organizational resilience.

Resilience-at-work research similarly emphasizes that individual, team, and organizational resilience may interact but should not be collapsed into a single construct [9]. Emerging cybersecurity research also indicates that empirical evidence linking organizational cyber resilience directly with cyber-incident outcomes remains limited. Tsen et al. [19], in a study involving 110 cyber practitioners, similarly identified limitations in the available empirical evidence connecting organizational cyber resilience with incident outcomes.

8.6 Relationships Among the Framework Components

The framework proposes that operational demands influence cognitive load and occupational stress, which in turn affect cognitive resilience. Cognitive resilience supports cybersecurity performance, through which individual and team-level cognitive functioning may contribute to organizational cyber resilience. Organizational resources perform two functions: they buffer the relationship between operational demands and cognitive strain and directly support the maintenance, recovery, and adaptation of cognitive functioning. A feedback pathway represents organizational learning through which incident experience may subsequently influence staffing, training, work design, leadership practices, and technology configuration.

The HCRF consists of a core sequential pathway:

Operational demands → cognitive load and occupational stress → cognitive resilience → cybersecurity performance → organizational cyber resilience

Organizational resources influence this pathway through two principal mechanisms:

Buffering pathway: Organizational resources weaken the positive relationship between operational demands and cognitive load and occupational stress.

Resilience-supporting pathway: Organizational resources directly strengthen the conditions under which cognitive functioning can be maintained, recovered, and adapted. Figure 4 summarizes the framework.

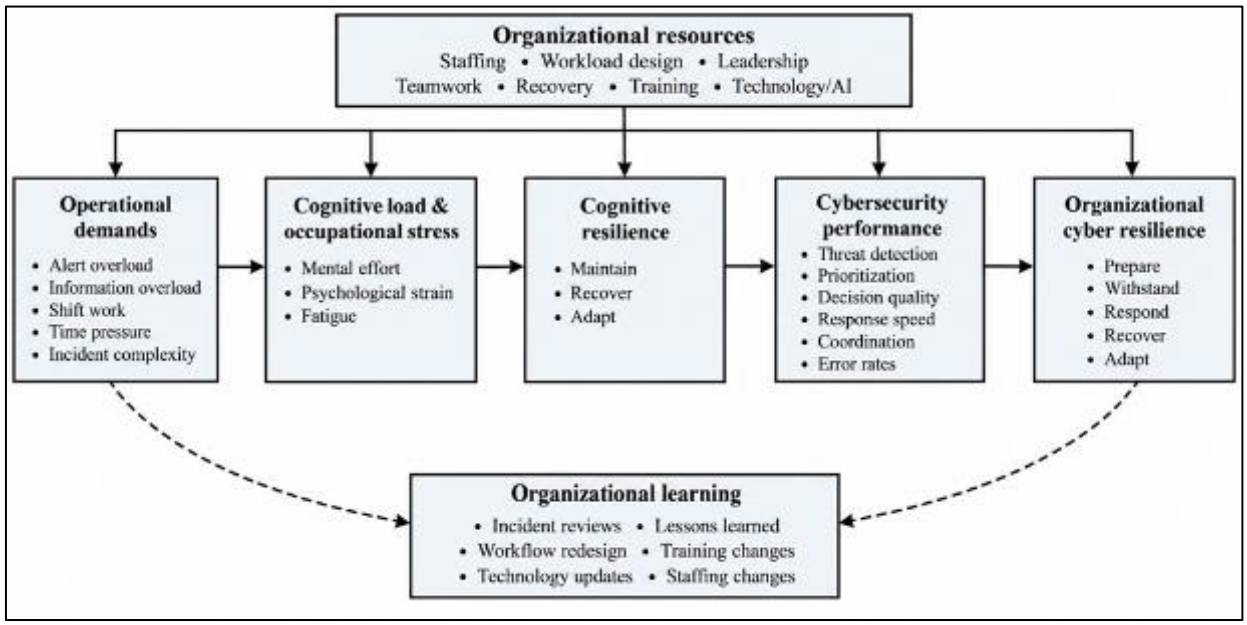

Figure 4: Human Cognitive Resilience Framework (HCRF) for modern cyber defense.

The framework also incorporates an organizational learning feedback loop. Lessons generated through incidents, post-incident reviews, operational failures, recovery processes, and successful responses may inform subsequent staffing, training, workflows, leadership practices, and technology design. Organizational cyber resilience is therefore not conceptualized solely as a terminal outcome but as part of an adaptive learning cycle capable of reshaping the resources and conditions influencing future performance.

8.7 Research Propositions

The HCRF generates the following propositions for empirical testing:

- P1. Higher operational demands are associated with greater cognitive load and occupational stress among cybersecurity professionals.
- P2. Sustained cognitive load and occupational stress are negatively associated with cognitive resilience among cybersecurity professionals.
- P3. Organizational resources moderate the relationship between operational demands and cognitive load and occupational stress, such that the positive relationship is weaker when organizational resources are stronger.
- P4. Organizational resources are positively associated with cognitive resilience.
- P5. Cognitive resilience is positively associated with cybersecurity performance.
- P6. Cybersecurity performance is positively associated with organizational cyber resilience.
- P7. Cognitive resilience mediates the relationship between cognitive load and occupational stress and cybersecurity performance.
- P8. Cybersecurity performance mediates the relationship between cognitive resilience and organizational cyber resilience.
- P9. Organizational learning following cyber incidents strengthens subsequent organizational resources and the conditions supporting cognitive resilience.

These propositions should be interpreted as theoretically derived relationships rather than empirically confirmed hypotheses. Their purpose is to make the HCRF falsifiable and to provide a structured basis for future longitudinal, multilevel, experimental, and field-based research.

8.8 Theoretical Contribution of the HCRF

The HCRF contributes to human-centered cybersecurity theory in three principal ways.

First, it moves beyond the broad category of human factors by specifying cognitive mechanisms through which operational conditions may influence cybersecurity performance. This creates a more precise theoretical pathway between work design and security-relevant outcomes.

Second, it connects individual cognitive functioning with organizational cybersecurity outcomes without collapsing levels of analysis. Cognitive resilience is positioned as an individual-level adaptive mechanism, cybersecurity performance as the proximal operational pathway, and organizational cyber resilience as the higher-level system outcome.

Third, the framework reconceptualizes organizational resources as cybersecurity-relevant variables rather than treating staffing, leadership, recovery, training, teamwork, and technology design solely as employee-well-being interventions. These resources may affect the reliability of cyber operations by influencing both the strain generated by operational demands and the capacity to maintain, recover, and adapt cognitive functioning.

The HCRF therefore complements rather than replaces existing human-centered cybersecurity models. Khadka and Ullah's [12] framework adopts a broader emphasis encompassing psychological resilience, adaptive education, socio-technical integration, organizational behavior, and ethical AI. The HCRF narrows the analytical focus to the cognitive pathway through which operational demands and organizational resources may influence cybersecurity performance and, ultimately, organizational cyber resilience.

Its principal theoretical contribution is therefore not the assertion that human factors matter in cybersecurity, but the specification of how, through which mechanisms, and under what organizational conditions human cognitive functioning may contribute to sustainable cyber-defense performance.

9 FUTURE RESEARCH DIRECTIONS

The Human Cognitive Resilience Framework (HCRF) provides a structured basis for moving human-centered cybersecurity research from conceptual integration toward empirical testing. Future research should therefore move beyond isolated examinations of sleep, fatigue, burnout, workload, alert fatigue, or human error and investigate the relationships among operational demands, cognitive load and occupational stress, organizational resources, cognitive resilience, cybersecurity performance, and organizational cyber resilience within integrated empirical models.

The immediate research challenge is not to generate additional conceptual frameworks but to establish whether the constructs and relationships proposed by the HCRF can be observed reliably in operational cybersecurity environments. This requires stronger construct measurement, longitudinal and field-based designs, objective performance indicators, multilevel analysis, organizational interventions, and careful examination of emerging human-AI configurations.

9.1 Construct Development and Measurement

A primary research priority is the development and validation of a measure of cognitive resilience specifically suited to cybersecurity professionals. Existing studies commonly assess fatigue, stress, cognitive workload, burnout, or general psychological resilience, but these constructs do not directly capture the proposed capacity to maintain, recover, and adapt cognitive functioning during and following demanding cyber operations.

Future research should determine whether cognitive resilience can be represented reliably through candidate dimensions including sustained attention, executive functioning, cognitive flexibility, emotional regulation, adaptive decision-making, learning capacity, and recovery of decision capability. These dimensions should not be assumed to form a single construct without empirical validation.

Measurement development should therefore proceed through appropriate psychometric stages, including examination of construct structure, reliability, convergent validity, discriminant validity, and criterion-related validity. Particular attention should be given to distinguishing cognitive resilience from psychological resilience, cognitive reserve, coping, fatigue, burnout, and general well-being.

Self-report measures alone are unlikely to capture the full construct. Where feasible, researchers should combine subjective assessments with objective or behaviorally anchored indicators such as reaction time, psychomotor vigilance, decision accuracy, error rates, sustained-attention performance, cognitive-flexibility tasks, sleep and recovery measures, and operational cybersecurity performance.

The central measurement question is whether cognitive resilience can predict meaningful variation in cyber performance beyond what is already explained by fatigue, stress, workload, technical expertise, and general psychological resilience.

9.2 Longitudinal and Temporal Testing of the HCRF

Much of the existing cybersecurity human-factors evidence is cross-sectional or based on relatively short operational periods. Dykstra and Paul [8], for example, demonstrated that fatigue, frustration, and cognitive workload can be measured during tactical cyber operations, but evidence concerning how these conditions develop and recover over time remains limited.

Longitudinal studies should follow cybersecurity professionals across repeated shifts, incident-response periods, periods of heightened alert activity, and subsequent recovery cycles. Such designs could determine whether cumulative workload, sleep restriction, alert exposure, and occupational stress predict subsequent changes in cognitive functioning, resilience, and operational performance.

Cybersecurity-specific evidence concerning burnout, workload, sleep quality, and extended working hours reinforces the importance of examining these relationships temporally rather than treating them as static characteristics [13].

Repeated-measures designs would also help distinguish maintenance, deterioration, recovery, and adaptation, which are central to the definition of cognitive resilience. Researchers could examine whether performance remains stable during manageable demand, declines after accumulated strain, returns following recovery, or improves through learning and adaptation after repeated experience.

Longitudinal evidence is particularly important for establishing temporal ordering. Cross-sectional associations cannot determine whether operational demands reduce cognitive resilience, whether lower resilience increases perceptions of workload and stress, or whether both relationships operate simultaneously.

9.3 Testing Mediation, Moderation, and Nonlinear Effects

The propositions specified in Section 8 require direct empirical testing. Particular attention should be given to the mediation and moderation mechanisms at the center of the HCRF.

Researchers should examine whether cognitive load and occupational stress explain how operational demands become associated with changes in cognitive resilience; whether organizational resources weaken the effects of operational demands on cognitive strain; whether cognitive resilience explains variation in cybersecurity performance under strain; and whether cybersecurity performance provides the pathway through which individual cognitive functioning contributes to organizational cyber resilience.

Structural equation modelling may be useful for examining several of these relationships simultaneously, provided that sample size, measurement quality, and model assumptions are adequate. Longitudinal mediation models would be particularly valuable because they could test whether changes in one construct precede changes in another rather than inferring mediation from cross-sectional data.

Researchers should also avoid assuming uniformly linear relationships. Moderate workload or time pressure may sometimes support engagement and alertness, whereas persistent or excessive exposure may contribute to deterioration. Threshold, curvilinear, or cumulative effects should therefore be examined.

Similarly, organizational resources may not exert equal effects across all levels of demand. Strong teamwork or effective automation may be sufficient under moderate operational pressure but unable to compensate for extreme or prolonged workloads. Testing such boundary conditions would strengthen the explanatory precision of the HCRF.

9.4 Field-Based and Multilevel Cybersecurity Research

A major weakness in the current evidence base is the reliance on mechanisms transferred from neuroscience, occupational psychology, healthcare, military operations, and other high-demand professions. These literatures remain valuable, but the HCRF ultimately requires testing among cybersecurity professionals themselves.

Future studies should increasingly recruit SOC analysts, incident responders, threat hunters, malware analysts, digital forensic personnel, and other operational cybersecurity professionals. Research conducted within real or high-fidelity cyber environments would improve ecological validity and clarify whether relationships established in adjacent fields generalize to cyber defense.

Performance measures should extend beyond perceived stress and self-reported effectiveness. Relevant outcomes may include threat-detection accuracy, missed alerts, false escalation, incident prioritization, response latency, decision accuracy, analytical errors, escalation quality, collaboration, and coordination.

The HCRF also spans multiple levels of analysis. Operational demands may be experienced by individuals but shaped by organizational staffing, technology, and policies. Cognitive resilience primarily concerns individual cognitive functioning but may be supported by team processes. Cybersecurity performance may occur at individual or team level, whereas organizational cyber resilience is fundamentally a system-level construct.

Future research should therefore use multilevel designs where appropriate rather than treating all HCRF constructs as though they exist at the same analytical level. Multilevel modelling could examine how organizational resources influence individual cognitive functioning and how individual or team performance aggregates into wider cyber-resilience capability.

This distinction is particularly important because emerging evidence does not support every intuitive relationship concerning organizational cyber resilience. Tsen et al. [19], for example, reported that organizations without reported attacks demonstrated higher levels of several cyber-resilience dimensions, while greater cyber resilience did not necessarily predict lower post-incident outcomes. Such findings reinforce the need to test rather than assume the final HCRF pathway.

9.5 Organizational Intervention Studies

The HCRF proposes that organizational resources may buffer cognitive strain and support cognitive resilience, but direct intervention evidence within cybersecurity remains limited. Future research should therefore move beyond identifying associations and test whether changes in organizational conditions actually produce measurable improvements.

Relevant interventions could examine shift scheduling and fatigue-risk management, staffing and workload redistribution, protected recovery periods, alert prioritization, leadership practices, psychological safety, team coordination, simulation-based training, and human-centered automation.

Where randomized controlled trials are impractical, stronger quasi-experimental approaches should be considered, including interrupted time-series designs, matched comparison groups, natural experiments, longitudinal case studies, and pre-post evaluations incorporating comparison conditions.

Importantly, interventions should assess both human and cybersecurity outcomes. An intervention may improve well-being without improving operational reliability, while another may reduce error rates without improving recovery or burnout. Evaluating both domains would help determine whether organizational resources produce the dual effects proposed by the HCRF.

Studies should also examine combinations of interventions rather than assuming that resources operate independently. Improved staffing, for example, may create recovery opportunities, while leadership practices may determine whether those opportunities are protected and used. Human-centered automation may reduce alert burden, but appropriate training may be required to prevent automation bias or overreliance.

9.6 Human-AI Collaboration and Cognitive Resilience

The expanding use of artificial intelligence in SOCs creates a particularly important research agenda. Existing work suggests that human-AI teaming may help mitigate alert fatigue, while reviews of SOC operations continue to identify limitations in alert-management approaches [4], [18].

Future research should assess not only whether AI improves technical efficiency or threat detection but also how it redistributes cognitive work across analysts, teams, and workflows. Systems that automate repetitive processing may preserve attentional resources, whereas systems that generate additional alerts, opaque recommendations, or continuous verification requirements may increase cognitive demand.

Relevant outcomes include automation bias, trust calibration, vigilance, situational awareness, decision confidence, cognitive flexibility, independent reasoning, workload, and recovery following sustained human-AI interaction.

Research should also compare different forms of task allocation. Automated, augmented, and collaborative configurations may have different consequences for cognitive resilience. The appropriate allocation may also vary according to task complexity, analyst expertise, threat uncertainty, and the consequences of error.

The central research question is therefore not simply whether AI improves cybersecurity performance, but whether particular human-AI configurations preserve or degrade the cognitive capabilities required for sustained cyber defense over time.

9.7 Generalizability, Organizational Learning, and Priority Research Design

The HCRF should be tested across different cybersecurity contexts, including healthcare, finance, critical infrastructure, government, military cyber units, managed security service providers, and private-sector SOCs. Workload, regulation, threat exposure, staffing, organizational culture, technological maturity, and recovery practices may vary considerably across these environments.

Cross-sector and cross-national research could therefore determine which HCRF relationships generalize broadly and which depend on organizational or cultural context. Such research would also help identify whether different forms of operational demand or organizational resources become more important in particular cybersecurity environments.

The framework's feedback pathway also requires empirical investigation. Organizations that conduct structured post-incident reviews, encourage open reporting, revise workflows, redesign alert systems, adjust staffing, and incorporate lessons into training may strengthen the organizational conditions supporting future cognitive and cyber resilience. This interpretation is consistent with broader cyber-resilience research emphasizing the capacity to withstand, recover from, and adapt following disruption [7].

The most valuable next step, however, is a direct longitudinal field test of the HCRF. A particularly informative design would recruit SOC analysts across repeated operational periods and integrate:

objective sleep and recovery measures + workload and occupational-stress measures + validated cognitive-resilience measures + cognitive-performance testing + operational cybersecurity metrics + organizational-resource measures

Such a design would permit simultaneous examination of temporal relationships, moderation, mediation, recovery patterns, and cross-level outcomes. It could determine whether cognitive resilience contributes explanatory value beyond established measures of fatigue, workload, stress, and technical competence.

The primary research priority is therefore clear: the HCRF should now be tested rather than further elaborated conceptually. Its scientific value will ultimately depend on whether its constructs can be measured reliably, whether the proposed pathways withstand empirical testing, and whether they explain meaningful variation in cybersecurity performance across real operational environments.

10 QUANTITATIVE OPERATIONALIZATION AND EMPIRICAL TEST PROTOCOL

The principal weakness of the current literature is not the absence of plausible mechanisms but the lack of integrated measurement within real cyber operations. We therefore specify a quantitative form of the HCRF that can be tested using repeated shifts nested within analysts and analysts nested within SOCs. The purpose is not to claim that the coefficients below are already known; rather, the equations define falsifiable relationships and the minimum measurements needed to estimate them.

10.1 Time-Varying Operational Demand

For analyst i during operational interval t, normalized cumulative demand can be represented as:

$$D_{it} = w_1 A_{it} + w_2 I_{it} + w_3 T_{it} + w_4 S_{it} + w_5 C_{it}, \quad \Sigma w_j = 1$$

where A is alert burden, I is incident complexity, T is time pressure, S is shift/recovery burden, and C is contextual information complexity. The weights should be estimated empirically or set prospectively and sensitivity-tested. This formulation makes explicit that workload is multidimensional; alert count alone is insufficient.

10.2 Cognitive Strain and Resource Buffering

$$L_{it} = \alpha D_{it} - \beta R_{it} + u_i + v_o + \varepsilon_{it}$$

L represents cognitive load/occupational strain; R is the organizational-resource index; u_i is an analyst-level random effect; v_o is a SOC-level random effect; and ε_{it} is interval-specific error. The coefficient β operationalizes the HCRF buffering proposition.

10.3 Dynamic Cognitive Resilience

$$CR_{i,t+1} = \rho CR_{it} - \gamma L_{it} + \delta Rec_{it} + \eta Learn_{it} + \zeta AI_{it} + e_{it}$$

CR is latent cognitive resilience; Rec captures recovery opportunity and sleep quality; Learn captures adaptive learning and post-incident knowledge acquisition; and AI captures the net effect of human-AI task configuration. ζ is not assumed positive: AI can reduce or increase cognitive demand depending on transparency, context quality, analyst control, and verification requirements [25], [28].

10.4 Cybersecurity Performance Link

$$logit[P(Y_{it} = 1)] = \theta_0 + \theta_1 CR_{it} - \theta_2 L_{it} + \theta_3 E_i + \theta_4 Q_{it}$$

Y may represent correct triage, timely escalation, or successful incident handling; E represents analyst expertise; and Q represents task quality/context. Continuous outcomes such as response latency can be estimated with generalized linear mixed models. The key empirical question is whether CR explains performance beyond fatigue, workload, expertise, and general psychological resilience. Figure 5 illustrates the proposed measurement architecture.

Table 2: Recommended Operationalization of HCRF Constructs

Construct	Example measures	Sampling cadence	Primary role
Sleep/recovery	Actigraphy; sleep duration/efficiency; self-reported sleep quality	Daily/shift	Exposure/resource
Operational demand	Alert volume; false-positive burden; incident severity; shift length; concurrent cases	Minute/hour/shift	Antecedent
Cognitive load	NASA-TLX; COSS; task-switch count; interface interaction burden	Task/shift	Mediator
Stress/burnout	Validated occupational stress and burnout measures; after-hours activity	Weekly/monthly	Strain/outcome
Cognitive resilience	PVT; sustained attention; working-memory/flexibility tasks; recovery slope across shifts	Pre/post shift; repeated	Central adaptive construct
Cyber performance	Detection accuracy; triage precision; escalation quality; MTTD/MTTR; error rate	Event/shift	Proximal outcome
Organizational resources	Staffing ratio; leadership support; psychological safety; recovery opportunity; training; AI transparency	Weekly/monthly	Moderator/support
Cyber resilience	Service continuity; incident containment; recovery time; lessons implemented	Incident/quarter	System-level outcome

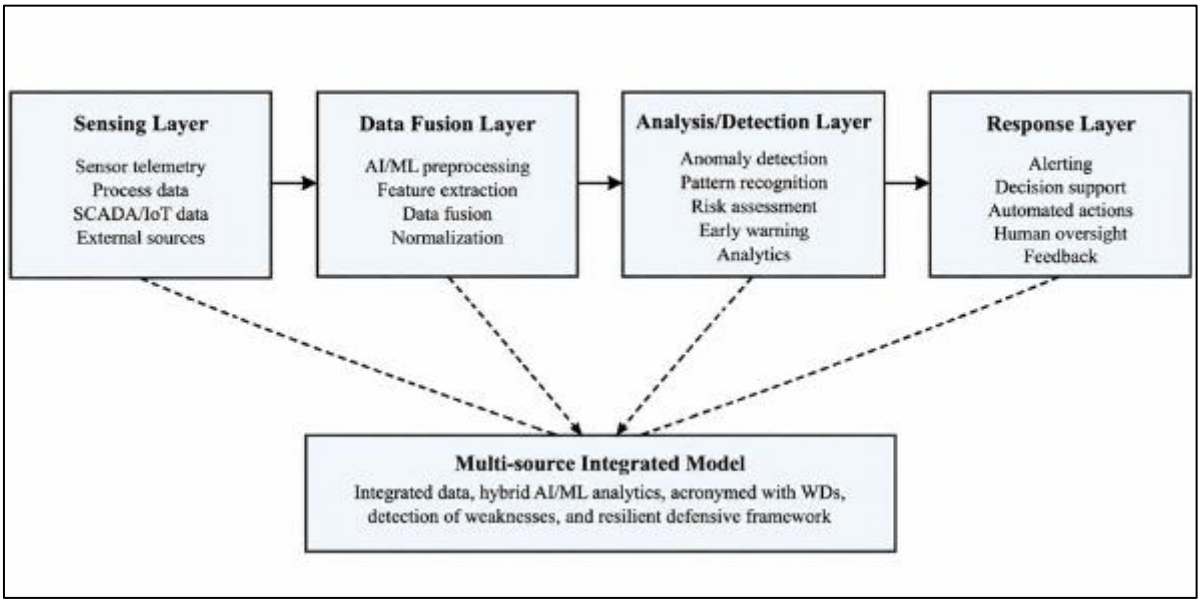

Figure 5: Proposed multilevel measurement architecture for empirical validation of the HCRF.

10.5 Nonlinearity, Thresholds, and Recovery Debt

The framework should not assume that demand-performance relationships are linear. Moderate workload can support engagement, while prolonged or cumulative demands may produce abrupt deterioration once recovery capacity is exceeded. Piecewise regression, generalized additive models, or change-point models should therefore be compared with purely linear specifications. A cumulative recovery-debt term can also represent repeated insufficient recovery across consecutive shifts. This is particularly important because controlled sleep research shows cumulative neurobehavioral impairment that is not fully reflected in subjective sleepiness [3], [20]. Figure 6 illustrates this conceptual relationship.

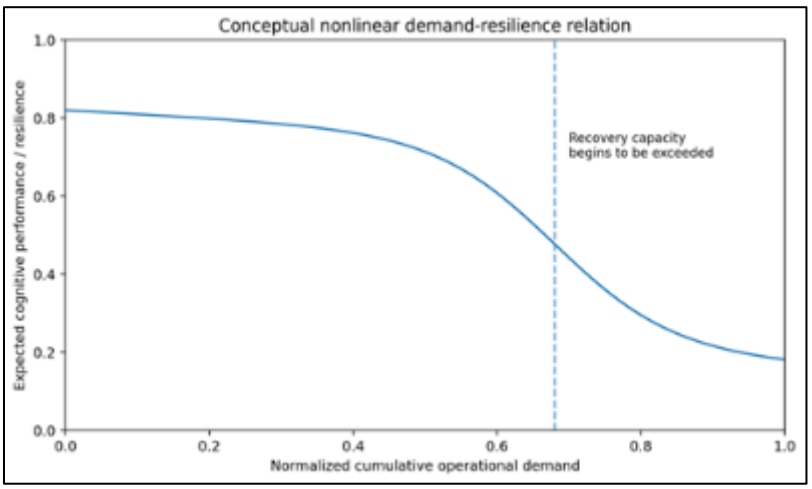

Figure 6: Conceptual nonlinear relation between cumulative operational demand and cognitive performance/resilience; the curve is illustrative and requires empirical estimation.

10.6 Proposed Field Validation Design

A defensible next-stage study would recruit analysts from multiple SOCs for 8-12 weeks, collecting repeated measures across ordinary shifts and elevated incident periods. Objective operational metrics should be linked to human-state measurements using de-identified analyst identifiers. Ethical design is essential: fatigue-risk research should not become employee-surveillance infrastructure. Data minimization, purpose limitation, separation from disciplinary performance management, and transparent consent/governance are necessary, particularly because recent evidence identifies surveillance itself as a distinct source of stress for cybersecurity professionals [26].

Table 3: Recommended Longitudinal Validation Protocol

Design component	Recommended specification	Reason
Population	SOC analysts, incident responders, threat hunters, digital forensics personnel across ≥3 organizations	Improves ecological and cross-organizational validity
Duration	8-12 weeks with repeated shifts and at least one high-demand period where feasible	Captures accumulation, recovery, and adaptation
Human measures	Actigraphy/sleep, PVT, NASA-TLX/COSS, validated stress/burnout and resilience-related measures	Separates subjective strain from objective cognitive performance
Cyber outcomes	Triage accuracy, false escalation, missed alerts, response latency, escalation quality, analyst handoffs	Creates behaviorally anchored performance endpoints
Modeling	Multilevel longitudinal mediation/moderation; nonlinear demand terms; sensitivity analysis	Matches HCRF temporal and cross-level structure
AI condition	Record task allocation, explanation quality, analyst override, verification time, confidence calibration	Tests whether AI reduces or redistributes cognitive work
Governance	Consent, de-identification, role-based access, no disciplinary reuse without explicit policy	Reduces surveillance-stress and ethics risk

11 2026 EVIDENCE UPDATE AND IMPLICATIONS FOR THE HCRF

The 2026 literature provides stronger support for three revisions to the HCRF. First, NIST's current human-centered cybersecurity agenda explicitly calls for practical, empirically grounded guidance that considers interactions among people, process, and technology [23], while Rangarajan et al. [24] identify continuing research-practice gaps. This supports treating organizational resources and work-system design as cyber-governance variables rather than optional wellness benefits.

Second, human-AI integration is becoming a core feature of incident management. Kincl et al. [25] emphasize task alignment, human oversight, operational context, and risk management, while evidence-backed SOC-agent work illustrates a shift from manual correlation toward analyst validation and strategic judgment [28]. These developments strengthen the HCRF requirement to measure not only whether AI is deployed but how it redistributes cognitive work.

Third, the occupational-strain construct is broadening. Singh et al. [26] identify surveillance stress among cybersecurity professionals as a distinct strain involving ethical ambiguity, relational tension, and emotional fatigue. This finding suggests that future HCRF tests should include role-specific stressors beyond conventional workload and alert volume. The updated framework therefore treats cognitive resilience as contingent on both task demand and the social/ethical context of cyber work.

The HCRF is principally a human-centered cybersecurity framework, but its emphasis on socio-technical integration is consistent with broader digital-system research. Distributed IoT-security and edge-intelligence studies demonstrate how sensing, computation, and decision support become interdependent in decentralized cyber-physical systems [30], [31]. Cross-domain work on data-driven quality assessment, cloud adoption in healthcare, digital-twin risk detection, and wireless integrity monitoring similarly illustrates that digital technologies create value only when technical outputs remain traceable to domain outcomes and human decisions [32]-[35]. These studies are not evidence for cognitive resilience itself; they provide methodological context for treating human, technical, and organizational layers as an integrated system.

Recent 2026 evidence materially strengthens the framework's human-AI and governance components. NIST has explicitly advanced a human-centered cybersecurity agenda grounded in the interaction of people, process, and technology [23], while Rangarajan et al. identify persistent research-practice gaps in human-centered cybersecurity [24]. Incident-management and SOC research increasingly treats AI as a collaborative rather than autonomous control layer, emphasizing human oversight, task allocation, trust calibration, explainability, and operational context [25], [36]. Empirical work also shows that cybersecurity professionals can experience role-specific surveillance stress [26], while mixed-methods SOC research identifies distinct risks of cognitive offloading, cognitive tethering, and automation bias across analyst profiles [45]. These findings are consistent with established human-automation research showing that appropriate reliance depends on calibrated trust, maintained situation awareness, and preserved human agency rather than maximal automation [38]-[44]. Finally, emerging human-centered security frameworks that integrate behavioral

and physiological state estimation demonstrate both the potential and the ethical sensitivity of using human-state signals for adaptive cyber-risk controls [46].

Additional sources retained in the framework provide complementary context on human-centered cybersecurity practice, workforce conditions, and socio-technical automation. NIST workshop synthesis [27] and cybersecurity-workforce evidence [29] support the practice context; cloud and digital-twin studies [33]-[34] are retained as cross-domain methodological context; and research on incident-management teaming, SOC structure, automation bias, situation awareness, trust, and human-centered AI [37], [39]-[43] supports the framework's treatment of technology as a conditional organizational resource.

12 LIMITATIONS

This study remains a structured narrative review rather than a systematic review or meta-analysis. Although database searching, explicit eligibility criteria, direct-versus-transferred evidence classification, and methodological appraisal increase transparency, the design does not guarantee exhaustive retrieval. Several key mechanisms - especially sleep-related cognitive impairment - are supported more strongly outside cybersecurity than within operational SOC populations. The HCRF remains conceptual and the quantitative equations introduced here are specifications for future estimation, not fitted causal models. The proposed construct of cognitive resilience also requires psychometric validation and discriminant testing against fatigue, burnout, coping, cognitive reserve, and psychological resilience. Finally, the increasing use of analyst telemetry creates a governance tension: measurements intended to protect cognitive performance could themselves create surveillance stress or chill help-seeking if implemented without strict purpose limitation and psychological safety [26].

13 CONCLUSION

Modern cyber defense is sustained by a socio-technical system in which analyst cognition, organizational design, automation, and technical controls interact. The evidence reviewed here supports treating sleep, fatigue, alert burden, workload, stress, burnout, recovery, leadership, staffing, teamwork, training, and human-AI configuration as conditions that can influence the reliability of security-critical cognitive work. The revised HCRF contributes a more precise pathway from operational demands to cognitive strain, cognitive resilience, cybersecurity performance, organizational cyber resilience, and organizational learning. Its value now depends on empirical testing. The next research step should therefore be longitudinal, multilevel, and field-based, combining objective sleep and cognitive measures with real operational performance while protecting analysts from inappropriate surveillance. Human-centered cyber resilience should ultimately be evaluated not by whether professionals can tolerate unlimited pressure, but by whether work systems preserve the capacity to detect, reason, coordinate, recover, learn, and adapt when cyber operations become demanding.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

Author Contributions

Stephen Sobulo led conceptualization of the Human Cognitive Resilience Framework, review synthesis, human-factors interpretation, and original manuscript development. Olajide Dare and Beauty Enobun contributed socio-technical systems interpretation, critical-infrastructure operational context, quantitative framework development, and critical revision. Adebiyi Adisa contributed Security Operations Center practice, cyber-risk governance, human-AI incident-management interpretation, and critical revision. Isdore Ugochukwu Opara contributed organizational-risk, governance, workforce-risk, and resilience interpretation and critical revision. Ekundayo Peter Buremoh contributed cybersecurity analytics, technical framework validation, human-AI systems interpretation, and critical revision. All authors reviewed and approved the final manuscript.

Data Availability and Ethics Statement

This article is a structured narrative review and conceptual/quantitative framework paper; no human-participant dataset was collected or analyzed by the authors for this manuscript. The equations and figures are theoretical specifications for future empirical testing. Any future field validation involving analyst sleep, cognitive state, telemetry, or work-performance data should obtain appropriate ethics review, informed consent where required, data minimization, de-identification, purpose limitation, and safeguards against inappropriate disciplinary reuse.

REFERENCES

[1] M. S. de Araujo, B. A. S. Machado, and F. U. Passos, "Resilience in the context of cyber security: A review of the fundamental concepts and relevance," Applied Sciences, vol. 14, no. 5, art. 2116, 2024, doi: 10.3390/app14052116.

[2] M. Arnold, M. Goldschmitt, and T. Rigotti, "Dealing with information overload: A comprehensive review," Frontiers in Psychology, vol. 14, art. 1122200, 2023, doi: 10.3389/fpsyg.2023.1122200.

[3] S. Banks et al., "Long-term influence of sleep/wake history on the dynamic neurobehavioural response to sustained sleep restriction," Journal of Sleep Research, vol. 33, no. 4, e14117, 2024, doi: 10.1111/jsr.14117.

[4] M. B. Chhetri, S. Tariq, R. Singh, F. Jalalvand, C. Paris, and S. Nepal, "Towards human-AI teaming to mitigate alert fatigue in Security Operations Centres," ACM Transactions on Internet Technology, vol. 24, no. 3, art. 12, pp. 1-22, 2024, doi: 10.1145/3670009.

[5] S. Colabianchi, F. Costantino, F. Nonino, and G. Palombi, "Transforming threats into opportunities: The role of human factors in enhancing cybersecurity," Journal of Innovation & Knowledge, vol. 10, no. 3, art. 100695, 2025, doi: 10.1016/j.jik.2025.100695.

[6] E. Demerouti, A. B. Bakker, F. Nachreiner, and W. B. Schaufeli, "The job demands-resources model of burnout," Journal of Applied Psychology, vol. 86, no. 3, pp. 499-512, 2001, doi: 10.1037/0021-9010.86.3.499.

[7] B. Dupont, "The cyber-resilience of financial institutions: Significance and applicability," Journal of Cybersecurity, vol. 5, no. 1, tyz013, 2019, doi: 10.1093/cybsec/tyz013.

[8] J. Dykstra and C. L. Paul, "Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations," in Proc. 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET), 2018.

[9] A. Galy, D. Chênevert, E. Fouquereau, and P. Groulx, "Toward a new conceptualization of resilience at work as a meta-construct?" Frontiers in Psychology, vol. 14, art. 1211538, 2023, doi: 10.3389/fpsyg.2023.1211538.

[10] A. García, J. Del Angel, J. Borrani, C. Ramirez, and P. Valdez, "Sleep deprivation effects on basic cognitive processes: Which components of attention, working memory, and executive functions are more susceptible to the lack of sleep?" Sleep Science, vol. 14, no. 2, pp. 107-118, 2021, doi: 10.5935/1984-0063.20200049.

[11] J. Jacobs and J. Haney, "Learning, sharing, and exploring with NIST's Human-Centered Cybersecurity Community of Interest," National Institute of Standards and Technology, 2024.

[12] K. Khadka and A. B. Ullah, "Human factors in cybersecurity: An interdisciplinary review and framework proposal," International Journal of Information Security, vol. 24, art. 119, 2025, doi: 10.1007/s10207-025-01032-0.

[13] S. Nepal et al., "Burnout in cybersecurity incident responders: Exploring the factors that light the fire," Proc. ACM Human-Computer Interaction, vol. 8, CSCW1, pp. 1-35, 2024, doi: 10.1145/3637304.

[14] C. Nobles, "Stress, burnout, and security fatigue in cybersecurity: A human factors problem," HOLISTICA - Journal of Business and Public Administration, vol. 13, no. 1, pp. 49-72, 2022, doi: 10.2478/hjbpa-2022-0003.

[15] A. Pollini et al., "Leveraging human factors in cybersecurity: An integrated methodological approach," Cognition, Technology & Work, vol. 24, no. 2, pp. 371-390, 2022, doi: 10.1007/s10111-021-00683-y.

[16] R. Robbins et al., "A systematic review of workplace-based employee health interventions and their impact on sleep duration among shift workers," Workplace Health & Safety, vol. 69, no. 11, pp. 525-539, 2021, doi: 10.1177/21650799211020961.

[17] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security fatigue," IT Professional, vol. 18, no. 5, pp. 26-32, 2016, doi: 10.1109/MITP.2016.84.

[18] S. Tariq, M. B. Chhetri, S. Nepal, and C. Paris, "Alert fatigue in Security Operations Centres: Research challenges and opportunities," ACM Computing Surveys, vol. 57, no. 9, art. 224, pp. 1-38, 2025, doi: 10.1145/3723158.

[19] E. Tsen, R. K. L. Ko, and S. Slapničar, "The effect of organizational cyber resilience on cyber incident outcomes," Journal of Cybersecurity, vol. 11, no. 1, tyaf040, 2025, doi: 10.1093/cybsec/tyaf040.

[20] H. P. A. Van Dongen, G. Maislin, J. M. Mullington, and D. F. Dinges, "The cumulative cost of additional wakefulness: Dose-response effects on neurobehavioral functions and sleep physiology from chronic sleep restriction and total sleep deprivation," Sleep, vol. 26, no. 2, pp. 117-126, 2003, doi: 10.1093/sleep/26.2.117.

[21] T. Vestberg et al., "Cognitive flexibility is associated with sickness resilience," Frontiers in Psychology, vol. 15, art. 1253152, 2024, doi: 10.3389/fpsyg.2024.1253152.

[22] C. E. Waugh and A. W. Sali, “Resilience as the ability to maintain well-being: An allostatic active inference model,” Journal of Intelligence, vol. 11, no. 8, art. 158, 2023, doi: 10.3390/jintelligence11080158.

[23] National Institute of Standards and Technology, “Human-Centered Cybersecurity Guidelines and Resources Concept Paper,” NIST, Aug. 2026.

[24] A. Rangarajan et al., “Advancing Human-Centered Cybersecurity: Challenges and Pathways Forward,” IEEE Security & Privacy, vol. 24, no. 3, pp. 81-87, May-Jun. 2026, doi: 10.1109/MSEC.2026.3676927.

[25] J. Kincl, M. T. P. Adam, and T. Pavleska, “Human-AI Integration in Cybersecurity: An Industry-Aligned Perspective on Incident Management,” International Journal of Information Security, vol. 25, art. 103, 2026, doi: 10.1007/s10207-026-01259-5.

[26] T. Singh, A. C. Johnston, M. Hudnall, and G. J. Bott, “Understanding surveillance stress in cybersecurity professionals: A stage model perspective,” Computers & Security, vol. 164, art. 104859, 2026, doi: 10.1016/j.cose.2026.104859.

[27] J. Haney et al., “Workshop Summary Report for ConnectCon 2024: ‘Minding the Gaps in Human-Centered Cybersecurity’,” NIST Special Publication 1332, Apr. 2025, doi: 10.6028/NIST.SP.1332.

[28] S. Sheikhi, P. Kostakos, and L. Loven, “Cognitive SOC: Evidence-Backed Narrative Generation for Security Operations with Multi-Agent LLM Architecture,” in Proc. 2025 IEEE International Conference on Big Data (BigData), Macau, China, pp. 7027-7036, 2025, doi: 10.1109/BigData66926.2025.11401968.

[29] A. Reeves, M. Pattinson, and M. Butavicius, “The sleepless sentinel: factors that predict burnout and sleep quality in cybersecurity professionals,” Information and Computer Security, vol. 32, no. 4, pp. 477-491, 2024, doi: 10.1108/ICS-11-2023-0222.

[30] A. Falayi, Q. Wang, W. Liao, and W. Yu, "Survey of distributed and decentralized IoT securities: Approaches using deep learning and blockchain technology," Future Internet, vol. 15, no. 5, art. 178, 2023.

[31] A. Falayi, Q. Wang, and W. Yu, "Edge intelligence in smart transportation CPS," in Edge Intelligence in Cyber-Physical Systems, Academic Press, 2025, pp. 193-219.

[32] O. Akande, A. Falayi, T. Oguntuga, E. Taiwo, T. Adegoke, and D. Ajewole, "Sustainable insect proteins vs. conventional proteins as fillings in gluten-free oat-based breakfast wraps: Nutritional, microbial, and sensory quality," Exploration of Foods and Foodomics, vol. 3, art. 101078, 2025.

[33] O. A. Olorunfemi, K. O. Falayi, T. A. Oriolowo, S. A. John, A. Falayi, and C. O. Obi, "Assessment of the adoption of cloud computing system in the Nigeria healthcare sector," World Journal of Advanced Research and Reviews, vol. 21, no. 1, pp. 929-941, 2024.

[34] T. B. Falayi, J. E. Balota, A. I. Falayi, O. A. Olorunfemi, and A. Olugbade, "Simulate. Optimize. Succeed: Integrating Digital Twin Technology for Real-Time Risk Detection and Decision Support in IT Projects Management Lifecycle," Advances in Consumer Research, vol. 2, pp. 2427-2441, 2025.

[35] O. Olatunde, B. Adebayo, P. Wordie, F. Oladoyin, O. Abegunde, and M. Jegede, "Assessment of blood sample integrity using wireless signal distortion and biochemical degradation markers during transportation delays," World, vol. 4, no. 3, 2025.

[36] M. Kumar, R. Rani, G. Epiphaniou, and C. Maple, "Adaptive Trust-Aware SOC Human-AI Teaming for resilient operations," Computers & Security, vol. 169, art. 104971, 2026, doi: 10.1016/j.cose.2026.104971.

[37] G. Romeo and D. Conti, "Exploring automation bias in human-AI collaboration: A review and implications for explainable AI," AI & Society, vol. 41, pp. 259-278, 2026, doi: 10.1007/s00146-025-02422-7.

[38] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security Operations Center: A systematic study and open challenges," IEEE Access, vol. 8, pp. 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[39] R. Parasuraman and V. Riley, "Humans and automation: Use, misuse, disuse, abuse," Human Factors, vol. 39, no. 2, pp. 230-253, 1997.

[40] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," Human Factors, vol. 37, no. 1, pp. 32-64, 1995.

[41] J. D. Lee and K. A. See, "Trust in automation: Designing for appropriate reliance," Human Factors, vol. 46, no. 1, pp. 50-80, 2004.

[42] B. Shneiderman, "Human-Centered Artificial Intelligence: Reliable, Safe & Trustworthy," International Journal of Human-Computer Interaction, vol. 36, no. 6, pp. 495-504, 2020, doi: 10.1080/10447318.2020.1741118.

[43] E. Glikson and A. W. Woolley, "Human trust in artificial intelligence: Review of empirical research," Academy of Management Annals, vol. 14, no. 2, pp. 627-660, 2020, doi: 10.5465/annals.2018.0057.

[44] I. Seeber et al., "Machines as teammates: A research agenda on AI in team collaboration," Information & Management, vol. 57, no. 2, art. 103174, 2020, doi: 10.1016/j.im.2019.103174.

[45] J. Tilbury, S. Flowerday, G. Bott, Y. T. Chua, E. Olson, and B. Foltz, "Human-factor vulnerabilities of automation in SOCs: A mixed-methods multigroup analysis," Computers & Security, vol. 166, art. 104871, 2026, doi: 10.1016/j.cose.2026.104871.

[46] D. A. Ta, F. Farid, F. Ahamed, A. Al-Areqi, R. Beutel, T. Watson, and A. Maurushat, "BioEnvSense: A human-centred security framework for preventing behaviour-driven cyber incidents," Cybersecurity, vol. 9, art. 177, 2026, doi: 10.1186/s42400-026-00609-z.