information

MDPI

Article

From Resilience to Cognitive Adaptivity: Redefining Human–AI Cybersecurity for Hard-to-Abate Industries in the Industry 5.0–6.0 Transition

Andrés Fernández-Miguel [1,2], Susana Ortíz-Marcos [3], Mariano Jiménez-Calzado [3], Alfonso P. Fernández del Hoyo [1], Fernando Enrique García-Muiña [2] and Davide Settembre-Blundo [1,4,*]

[1] Faculty of Economics and Business Administration (ICADE), Comillas Pontifical University, 28015 Madrid, Spain; afmiguel@icade.comillas.edu (A.F.-M.); fdelhoyo@icade.comillas.edu (A.P.F.d.H.)
[2] Department of Business Administration (ADO), Rey Juan Carlos University, 28933 Madrid, Spain; fernando.muina@urjc.es
[3] School of Engineering (ICAI), Comillas Pontifical University, 28015 Madrid, Spain; sortiz@iit.comillas.edu (S.O.-M.); mjimenez@icai.comillas.edu (M.J.-C.)
[4] Innovability Unit, Gresmalt Group, 41049 Sassuolo, Italy
* Correspondence: dsettembre@comillas.edu

Abstract

This paper introduces cognitive adaptivity as a novel framework for addressing human factors in cybersecurity during the Industry 5.0–6.0 transition, with a focus on hard-to-abate industries where digital transformation intersects sustainability constraints. While the integration of IoT, automation, digital twins, and artificial intelligence expands industrial efficiency, it simultaneously exposes organizations to increasingly sophisticated social engineering and AI-powered attack vectors. Traditional resilience-based models, centered on recovery to baseline, prove insufficient in these dynamic socio-technical ecosystems. We propose cognitive adaptivity as an advancement beyond resilience and antifragility, defined by three interrelated dimensions: learning, anticipation, and human–AI co-evolution. Through an in-depth case study of the ceramic value chain, this research develops a conceptual model demonstrating how organizations can embed trust calibration, behavioral evolution, sustainability integration, and systemic antifragility into their cybersecurity strategies. The findings highlight that effective protection in Industry 6.0 environments requires continuous behavioral adaptation and collaborative intelligence rather than static controls. This study contributes to cybersecurity literature by positioning cognitive adaptivity as a socio-technical capability that redefines the human–AI interface in industrial security. Practically, it shows how organizations in hard-to-abate sectors can align cybersecurity governance with sustainability imperatives and regulatory frameworks such as the CSRD, turning security from a compliance burden into a strategic enabler of resilience, competitiveness, and responsible digital transformation.

Keywords: AI-enabled cybersecurity; human factors in cybersecurity; cognitive adaptivity; Industry 5.0; Industry 6.0; hard-to-abate industries

check for updates

Academic Editors: Hossein Abroshan, Nader Sohrabi Safa and Huseyin Dogan

Received: 21 September 2025
Revised: 7 October 2025
Accepted: 9 October 2025
Published: 10 October 2025

Citation: Fernández-Miguel, A.; Ortíz-Marcos, S.; Jiménez-Calzado, M.; Fernández del Hoyo, A.P.; García-Muiña, F.E.; Settembre-Blundo, D. From Resilience to Cognitive Adaptivity: Redefining Human–AI Cybersecurity for Hard-to-Abate Industries in the Industry 5.0–6.0 Transition. *Information* **2025**, *16*, 881. https://doi.org/10.3390/info16100881

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The industrial landscape is experiencing profound transformations as organizations navigate the transition from Industry 5.0's human-centric paradigm toward the emerging cognitive ecosystems of Industry 6.0. This evolution presents challenges for hard-to-abate industries, sectors characterized by high energy consumption, complex supply chains, and

significant environmental impact, where the imperative for digital transformation must be balanced against sustainability constraints and regulatory compliance requirements [1].

While the integration of IoT devices, automation systems, digital twins, and artificial intelligence offers unprecedented opportunities for operational efficiency and competitive advantage, it simultaneously exposes organizations to new categories of cyber threats. Traditional cybersecurity frameworks, largely designed for static technological environments, prove inadequate when confronted with the dynamic, human–AI collaborative systems that characterize modern industrial ecosystems [2]. The ceramic industry exemplifies these challenges, representing a paradigmatic case of how hard-to-abate sectors must simultaneously pursue digital innovation, environmental responsibility, and cybersecurity resilience [3].

Current cybersecurity approaches in industrial contexts predominantly focus on technical vulnerabilities (network security, system hardening, and threat detection) while underestimating the critical role of human factors [4]. Social engineering attacks, which exploit behavioral vulnerabilities rather than technical flaws, represent an increasingly sophisticated threat vector that traditional security measures struggle to address [5]. The emergence of AI-powered phishing, deepfakes, and behavioral manipulation techniques requires a fundamental reconceptualization of cybersecurity strategy, moving beyond reactive defense mechanisms toward proactive adaptation capabilities [6].

The gap between traditional resilience-focused cybersecurity [7] models and the requirements of Industry 5.0–6.0 [8] environments becomes particularly evident in hard-to-abate industries. These sectors face the dual challenge of implementing advanced digital technologies while maintaining operational continuity under stringent environmental and regulatory constraints [9]. The concept of resilience, the ability to withstand and recover from disruptions, while valuable, proves insufficient for environments where threats are not merely external disruptions but integral components of an evolving socio-technical ecosystem [10].

This paper introduces the concept of cognitive adaptivity as a theoretical framework for understanding and managing human factors in cybersecurity during the Industry 5.0–6.0 transition. Cognitive adaptivity encompasses the ability of individuals and organizations to learn from security incidents, anticipate emerging threats, and co-evolve with intelligent systems to convert potential vulnerabilities into opportunities for systemic improvement. Unlike traditional resilience models that emphasize recovery and return to baseline functionality [11], cognitive adaptivity prioritizes continuous learning, behavioral evolution, and human–AI symbiosis as foundational elements of cybersecurity strategy. The ceramic value chain serves as our empirical foundation, providing insights into how cognitive adaptivity manifests across different stages of industrial evolution. From the linear, automation-focused systems of Industry 4.0 [12] through the human-centric approaches of Industry 5.0 [13] to the emerging cognitive ecosystems of Industry 6.0 [3], the ceramic industry's transformation illustrates the evolving nature of cybersecurity challenges and the corresponding need for adaptive security frameworks [14].

This study addresses three interconnected research questions:

- RQ1: How do human factors in cybersecurity evolve during the transition from Industry 5.0 to Industry 6.0, particularly in hard-to-abate industries?
- RQ2: What distinguishes cognitive adaptivity from traditional resilience approaches in addressing behavioral cybersecurity vulnerabilities?
- RQ3: How can organizations in hard-to-abate industries implement cognitive adaptivity frameworks to enhance both cybersecurity posture and operational sustainability?

The paper contributes to cybersecurity literature by developing a novel theoretical framework that integrates human behavioral dynamics with technological evolution in industrial contexts. It advances understanding of how cognitive adaptivity can serve as a

bridge between human-centric Industry 5.0 principles and the cognitive ecosystems of Industry 6.0. The empirical application to the ceramic industry [15] provides practical insights for hard-to-abate sectors navigating similar digital transformations while maintaining focus on sustainability and regulatory compliance.

2. Theoretical Background

2.1. From Industry 3.0 to Industry 6.0: The Evolution of Human-Technology Interaction

The progression from Industry 3.0 to the emerging Industry 6.0 paradigm represents a fundamental shift in how humans interact with technological systems, with profound implications for cybersecurity. Industry 3.0, characterized by electronic automation and computerized manufacturing, established the foundation for digital vulnerabilities while maintaining clear boundaries between human operators and automated systems [16]. Cybersecurity concerns in this era were predominantly technical, focusing on system protection and access control within relatively predictable operational environments [17].

Industry 4.0 introduced cyber-physical systems, IoT connectivity, and data-driven decision-making, dramatically expanding the attack surface while simultaneously increasing the complexity of human-system interactions [18]. The interconnectedness of Industry 4.0 systems created new categories of vulnerabilities, where human behavior could have cascading effects across networked manufacturing environments. Social engineering attacks began to exploit not only individual vulnerabilities but also the interdependencies between human operators and connected systems [19].

The transition to Industry 5.0 marked a paradigm shift toward human centricity, emphasizing collaboration between humans and intelligent machines. This evolution positioned humans not merely as operators of technological systems but as active participants in adaptive manufacturing processes [20]. While this human-centric approach enhanced flexibility and innovation capacity, it also introduced new behavioral vulnerabilities. The increased reliance on human judgment, creativity, and adaptability created opportunities for sophisticated social engineering attacks that could manipulate human decision-making within collaborative human–AI systems [21].

Industry 6.0, while still emergent, promises to integrate cognitive technologies, autonomous learning systems, and systemic sustainability principles into manufacturing environments. This paradigm envisions cognitive ecosystems where humans, AI systems, and physical processes co-evolve in real-time, creating unprecedented opportunities for operational efficiency and environmental responsibility. However, this cognitive integration also presents novel cybersecurity challenges, as threats can now target not only individual human behavior but also the learning and adaptation mechanisms that govern human–AI collaboration. The progression across these industrial paradigms reveals an increasing emphasis on human agency within technological systems, accompanied by growing sophistication in the behavioral dimensions of cybersecurity threats. Traditional security models, designed for static technological environments with clear human–machine boundaries, prove inadequate for the dynamic, collaborative ecosystems that characterize contemporary industrial settings.

The evolution of cybersecurity threats across industrial paradigms reveals a concerning trajectory where human factor vulnerabilities have become increasingly prominent and sophisticated [22]. Table 1 synthesizes empirical evidence from the ceramic industry and broader manufacturing sectors to illustrate how the nature of cybersecurity challenges has fundamentally shifted from predominantly technical vulnerabilities toward complex behavioral and cognitive exploitations.

Table 1. Evolution of Cybersecurity Threats Across Industrial Paradigms in Hard-to-Abate Industries.

INDUSTRIAL ERA	PRIMARY THREAT CATEGORIES	HUMAN FACTOR VULNERABILITIES	DOMINANT RESPONSE APPROACH	ATTACK SUCCESS RATE (%)
Industry 3.0 (1970–2010)	Basic malware, unauthorized access, data theft.	Limited interaction, operator error.	Technical controls, access management.	15–20
Industry 4.0 (2011–2020)	IoT exploitation, supply chain attacks, data manipulation.	Cognitive overload, automation bias, complexity confusion.	Hybrid technical-human controls.	25–35
Industry 5.0 (2021–2025)	Advanced social engineering, AI-assisted phishing, collaborative system manipulation.	Trust exploitation, human–AI miscalibration, collaborative vulnerabilities.	Human-centric security, behavioral training.	40–50
Industry 6.0 (2025+)	Deepfakes, cognitive manipulation, autonomous attack systems, learning system poisoning.	Symbiotic dependencies, cognitive adaptation exploitation.	Cognitive adaptivity frameworks.	20–30

The data reveal a particularly troubling pattern: while technical security measures have advanced significantly, attack success rates have paradoxically increased through Industry 4.0 and 5.0, peaking at 40–50% in human-centric Industry 5.0 environments. This trend reflects the growing sophistication of adversaries in exploiting human behavioral patterns rather than technical system weaknesses. The projected reduction in Industry 6.0 environments assumes successful implementation of cognitive adaptivity frameworks, though this remains empirically unvalidated given the emergent nature of these systems. Of particular significance is the shift in human factor vulnerabilities from simple operator errors in Industry 3.0 to complex symbiotic dependencies in Industry 6.0. This evolution suggests that traditional cybersecurity training and awareness programs, designed for discrete human-system interactions, may prove inadequate for environments characterized by continuous human–AI collaboration and mutual adaptation.

2.2. Human Factors in Cybersecurity: Beyond Technical Vulnerabilities

Human factors in cybersecurity encompass the behavioral, cognitive, and social dimensions of security vulnerabilities that arise from human interaction with technological systems. Unlike technical vulnerabilities that can be addressed through system updates or configuration changes, human factors involve complex psychological and social dynamics that resist simple technical solutions [23].

Social engineering represents the most significant manifestation of human factors in cybersecurity, exploiting psychological principles such as authority bias, reciprocity, and time pressure to manipulate human behavior. Traditional social engineering attacks, such as phishing emails and pretexting, relied on relatively simple deception techniques. However, the advent of AI-powered attack vectors has dramatically increased the sophistication and effectiveness of behavioral manipulation. AI enables realistic content creation and advanced targeting that amplifies traditional SE attacks [24].

The current cybersecurity literature identifies several key human factors that contribute to organizational vulnerability: cognitive overload resulting from complex security protocols, automation bias leading to over-reliance on technological safeguards, and social dynamics that create pressure to bypass security measures for operational efficiency [25].

These factors are particularly pronounced in industrial settings where operational continuity often takes precedence over security considerations.

Existing approaches to addressing human factors in cybersecurity typically focus on training programs, awareness campaigns, and behavioral interventions designed to modify individual behavior [26]. However, these approaches often fail to account for the systemic nature of human-technology interaction in modern industrial environments. They treat human behavior as a variable to be controlled rather than as an adaptive capacity to be developed and leveraged [27].

The limitations of the current human factors approach become particularly evident in the context of Industry 5.0 [20] and 6.0 [28] environments, where human–AI collaboration requires continuous adaptation and learning. Static training programs and fixed security protocols cannot adequately prepare individuals for the dynamic, evolving threat landscape that characterizes cognitive industrial ecosystems [29].

2.3. From Resilience to Cognitive Adaptivity: A Theoretical Framework

The traditional notion of resilience in cybersecurity emphasizes robustness and recovery after disruption [30]. However, such approaches remain static within increasingly dynamic socio-technical systems. Cognitive adaptivity advances this view by integrating learning, anticipation, and human–AI co-evolution into a continuous cycle of behavioral evolution. It reframes cybersecurity not as a return to normality but as a capacity for ongoing improvement driven by human–machine collaboration. Empirical reviews in Cyber-Physical Systems show that adaptive anomaly detection methods, which combine model adaptation and continuous learning, outperform static detection models when facing evolving attacks [31].

Cognitive adaptivity represents a theoretical advancement beyond traditional resilience models, encompassing three fundamental dimensions: learning, anticipation, and co-evolution. Learning involves the capacity to extract actionable insights from security incidents, behavioral patterns, and threat intelligence to inform future security decisions. Anticipation refers to the ability to identify emerging threats, recognize behavioral risk factors, and proactively adjust security strategies before incidents occur. Co-evolution describes the dynamic process through which humans and AI systems mutually adapt their behaviors, capabilities, and interaction patterns to enhance overall system security. Studies exploring adaptive strategic approaches that integrate AI for cybersecurity demonstrate that firms employing predictive AI capabilities and feedback loops are better positioned to anticipate emerging threats [32].

Unlike resilience, which focuses on maintaining stability in the face of disruption, cognitive adaptivity embraces change as a fundamental characteristic of secure systems. It recognizes that effective cybersecurity in Industry 6.0 environments requires continuous behavioral evolution, where humans and AI systems collaboratively develop increasingly sophisticated responses to emerging threats. Agentic AI research underscores the risks of human–AI systems in which the AI component itself requires adaptation, not merely as a tool, but as a partner in evolving threat contexts [33].

Cognitive adaptivity differs from related concepts such as antifragility, which focuses on gaining strength from stressors, by emphasizing the collaborative and cognitive dimensions of adaptation. While antifragile systems become stronger through exposure to volatility, cognitively adaptive systems become smarter through collaborative learning and behavioral evolution. Reviews of resilient services in dynamic environments suggest that strategies combining adaptability, learning mechanisms, and behavioral feedback outperform purely resilient designs [34].

The theoretical framework of cognitive adaptivity is particularly relevant for hard-to-abate industries, where the constraints of environmental sustainability and regulatory compliance create additional complexity in cybersecurity strategy [35]. These industries cannot simply adopt generic cybersecurity solutions but must develop adaptive approaches that balance security requirements with operational sustainability and regulatory alignment [36]. Recent advances in AI-enabled cybersecurity confirm the growing integration of adaptive analytics and human-centric interfaces for threat anticipation. These developments reinforce the theoretical assumptions of cognitive adaptivity, particularly in aligning behavioral learning with automated detection and decision-support mechanisms [37].

3. Methodological Approach

3.1. Research Design and Philosophical Foundations

This research employs a single-case study design with embedded units of analysis, focusing on the ceramic value chain as a paradigmatic example of hard-to-abate industries navigating cybersecurity challenges during the Industry 5.0–6.0 transition. The methodological approach is grounded in critical realist epistemology, which acknowledges that while empirical observations are theory-laden, underlying causal mechanisms can be identified through systematic investigation of observable phenomena and their contextual conditions [38].

The choice of single-case methodology is justified by the ceramic industry's characteristics as a revelatory case that provides unique insights into cybersecurity challenges facing hard-to-abate sectors. The ceramic industry exhibits high energy intensity, averaging 4–5 GJ per ton of finished product, with approximately 85% derived from natural gas for kilns and drying processes [39]. Combined with complex supply chain interdependencies, significant environmental regulatory pressures, and ongoing digital transformation initiatives, these characteristics make it representative of broader challenges facing similar industrial sectors [40]. This focus on a single, deeply investigated case aligns with recent empirical cybersecurity research that emphasizes depth over breadth to uncover latent mechanism [41].

The research adopts an abductive reasoning approach, iteratively moving between empirical observations and theoretical development to construct explanatory frameworks that account for observed phenomena while extending existing theoretical understanding [42]. This approach proves particularly appropriate for investigating emerging concepts such as cognitive adaptivity and Industry 6.0, where deductive hypothesis testing may be premature and purely inductive approaches may miss important theoretical connections [43]. Previous works on cyber-resilience and sensemaking show that abductive designs help expose latent causal structures in complex socio-technical settings [44].

3.2. Data Collection Strategy

3.2.1. Primary Data Collection: Semi-Structured Interviews

The primary data collection centered on semi-structured interviews conducted between March 2025 and August 2025 with key stakeholders across the ceramic value chain. The interview approach was selected to balance systematic data collection with flexibility to explore emergent themes and contextual nuances that might not be captured through structured surveys or purely observational methods.

Sampling Strategy and Participant Selection

Purposive sampling was employed to ensure representation across different segments of the ceramic value chain and varying levels of digital maturity. Selection criteria included: (1) formal decision-making authority in cybersecurity, digital transformation, or risk management; (2) minimum five years of experience in the ceramic industry; (3) direct

involvement in Industry 4.0 or 5.0 technology implementation; and (4) willingness to discuss cybersecurity challenges and adaptive strategies. The final sample comprised 86 participants distributed across five stakeholder categories:

- **Tile Manufacturers (n = 67):** Including production managers (n = 23), IT/cybersecurity personnel (n = 19), quality control managers (n = 15), and senior executives (n = 10)
- **Raw Material Suppliers (n = 5):** Supply chain managers and sustainability officers
- **Glaze and Ink Producers (n = 6):** R&D managers and production supervisors
- **Machinery Manufacturers (n = 5):** Technical sales managers and IoT implementation specialists
- **Industry Associations (n = 3):** Policy analysts and member services coordinators

Interview Protocol Development

The semi-structured interview protocol was developed through iterative pilot testing with three industry experts and refined based on feedback regarding question clarity, topic coverage, and interview duration. The protocol comprised four main sections:

1. Organizational Context (10–15 min): Participant background, organizational structure, digital transformation timeline, and current cybersecurity posture
2. Human Factors in Cybersecurity (20–25 min): Experiences with social engineering, behavioral vulnerabilities, human–AI interaction challenges, and training effectiveness
3. Evolutionary Perspectives (15–20 min): Changes in cybersecurity threats and responses across Industry 3.0–6.0 transition, adaptation strategies, and learning mechanisms
4. Future Orientations (10–15 min): Expectations for Industry 6.0 development, cognitive adaptivity concepts, and implementation challenges

Interview Execution and Quality Assurance

All interviews were conducted via secure video conferencing platforms (Microsoft Teams or Zoom) to accommodate the geographic distribution of participants across major ceramic production regions in Italy, Spain, and Germany. Interviews were recorded with explicit participant consent and transcribed using professional transcription services with subsequent accuracy verification by the research team.

Interview duration ranged from 55 to 90 min (average: 72 min), with longer interviews typically involving senior executives or participants with extensive cybersecurity experience. The interview process employed several quality assurance measures:

- Bracketing techniques to minimize researcher bias through explicit acknowledgment of prior assumptions
- Member checking with 25% of participants to verify interpretation accuracy
- Peer debriefing sessions following each interview batch to identify emerging patterns and potential analytical blind spots
- Saturation monitoring through tracking of new themes and concepts to determine data collection sufficiency

Ethical Considerations and Data Protection

The research protocol received ethics approval from the institutional review board, with particular attention to cybersecurity sensitivity and competitive information protection. Participants provided informed consent for interview recording and data use, with explicit guarantees of anonymity and confidentiality. All data were stored on encrypted servers with access restricted to core research team members.

Given the sensitive nature of cybersecurity information, the research employed several protective measures:

- Anonymization protocols removing all identifying information from transcripts

- Aggregate reporting ensuring individual responses could not be traced to specific organizations
- Sensitive information exclusion allowing participants to designate certain information as off-record
- Data retention limits with automatic deletion of identifying information after two years

3.2.2. Secondary Data Collection

Secondary data collection complemented primary interviews through systematic review of industry reports, regulatory documents, academic literature, and trade publications published between 2020 and 2024. This temporal focus captured the Industry 5.0 transition period while providing baseline data for Industry 4.0 comparisons.

Industry Reports and White Papers

- Annual cybersecurity reports from major ceramics industry associations
- Technology adoption surveys from manufacturing consultancies
- Threat intelligence reports from industrial cybersecurity vendors
- Digital transformation case studies from leading ceramic manufacturers

Regulatory and Policy Documents

- European Union cybersecurity directives and implementation guidance
- CSRD requirements and industry-specific sustainability reporting standards
- National Industry 4.0 strategy documents from major ceramic-producing countries
- Insurance industry risk assessments for manufacturing cybersecurity

Academic and Technical Literature

- Peer-reviewed articles on industrial cybersecurity and human factors (2020–2024)
- Conference proceedings from manufacturing technology and cybersecurity conferences
- Technical standards documents for industrial IoT and cyber-physical systems
- Dissertation research on related topics from European technical universities

3.3. Data Analysis Approach

3.3.1. Qualitative Data Analysis

Interview transcripts underwent systematic thematic analysis using a hybrid deductive-inductive coding approach. Initial deductive codes derived from existing cybersecurity and industrial transition literature, while inductive codes emerged from patterns observed in interview data. First-cycle coding employed both descriptive and process coding techniques to capture what participants discussed and how they described their experiences. Second-cycle coding utilized pattern coding to identify relationships between initial codes and develop higher-order thematic categories. Third-cycle coding focused on theoretical development, connecting empirical patterns to conceptual frameworks and identifying areas where existing theory proved inadequate. The coding process employed a hybrid approach combining commercially available AI language models with human analytical oversight. Initial coding utilized ChatGPT-5 for thematic pattern recognition and Claude-3.5 Sonnet for conceptual analysis, enabling rapid processing of the 86 interview transcripts while maintaining analytical rigor.

Multi-AI Collaborative Analysis Protocol

The research team developed a three-stage analytical framework leveraging different AI capabilities while maintaining human interpretive control:

1. Primary Thematic Analysis (ChatGPT-5): Custom prompts were developed to identify recurring themes, behavioral patterns, and cybersecurity vulnerabilities across tran-

scripts. ChatGPT-5's large context window enabled analysis of complete interviews while maintaining thematic consistency.

2. Conceptual Validation (Claude-3.5): Claude was employed for deeper conceptual analysis, particularly for identifying theoretical connections and validating the emergence of the cognitive adaptivity framework. Its analytical capabilities proved valuable for connecting empirical observations to theoretical constructs.
3. Comparative Analysis (Microsoft Copilot): Copilot's integration with enterprise search capabilities enabled cross-referencing of interview findings with secondary data sources, identifying convergences and divergences between stakeholder perceptions and documented industry trends.

Quality Assurance and Human Oversight

- Inter-AI Validation: Each transcript underwent analysis by at least two different AI models, with outputs compared for consistency and completeness
- Human Verification: Two independent researchers validated all AI-generated codes, achieving 89% agreement on thematic categorizations
- Triangulation Protocol: AI-identified patterns were systematically cross-checked against secondary data sources and existing literature

Prompt Engineering for Domain Specificity

- Custom prompts were developed for cybersecurity and industrial transition analysis, including:
- Industry-specific terminology recognition (ceramic manufacturing processes, cybersecurity threats)
- Behavioral pattern identification in human–AI interaction contexts
- Temporal analysis across Industry 3.0–6.0 transitions

Methodological Transparency

All AI-generated analyses remained under human supervision, with no interpretations accepted without explicit researcher validation. The multi-AI approach enabled cross-validation of findings while maintaining the nuanced interpretation essential for theoretical development. This methodology demonstrates practical integration of AI tools in qualitative research while preserving analytical rigor and interpretive validity. Ultimately, responsibility for all analytical judgments and theoretical conclusions resided with the human researchers.

3.3.2. Mixed-Methods Integration

The integration of qualitative interview data with quantitative secondary data followed a concurrent triangulation design, where different data types were analyzed separately and then compared for convergence, complementarity, and contradiction. This approach enabled identification of areas where stakeholder perceptions aligned with or diverged from documented industry trends.

4. The Ceramic Value Chain and Cybersecurity Challenges

The cybersecurity landscape within the ceramic value chain has undergone a dramatic transformation over the past decade, with implications that extend far beyond simple cost calculations. Table 2 presents empirical data gathered from industry stakeholders, revealing patterns that challenge conventional assumptions about industrial cybersecurity trends and the effectiveness of human-centric approaches.

Table 2. Cybersecurity Incident Analysis in the Ceramic Value Chain (2015–2024).

STAKEHOLDER CATEGORY	INDUSTRY 4.0 ERA (2015–2020)	INDUSTRY 5.0 ERA (2021–2024)	COGNITIVE LOAD IMPACT	RECOVERY IMPROVEMENT WITH ADAPTIVITY
Tile Manufacturers	Incidents: 24/year, Cost: €180K avg	Incidents: 16/year, Cost: €320K avg	High—Complex HMI systems	65% faster recovery
Raw Material Suppliers	Incidents: 8/year, Cost: €45K avg	Incidents: 12/year, Cost: €85K avg	Medium—Supply chain integration	45% faster recovery
Glaze/Ink Producers	Incidents: 6/year, Cost: €65K avg	Incidents: 10/year, Cost: €120K avg	High—R&D system targets	70% faster recovery
Machinery Manufacturers	Incidents: 12/year, Cost: €95K avg	Incidents: 8/year, Cost: €150K avg	Medium—Technical expertise buffer	50% faster recovery
Industry Associations	Incidents: 3/year, Cost: €25K avg	Incidents: 5/year, Cost: €40K avg	Low—Shared intelligence benefits	80% faster recovery
Total Industry Impact	€2.1M/year average	€3.8M/year average	-	Projected 60% cost reduction

The apparent paradox of fewer incidents but higher costs per incident during the Industry 5.0 era reflects the increasing sophistication and targeted nature of attacks on human-centric systems. While tile manufacturers experienced a 33% reduction in incident frequency, the average cost per incident nearly doubled, suggesting that attackers have shifted from opportunistic broad-spectrum attacks to carefully orchestrated campaigns that exploit the collaborative nature of Industry 5.0 systems. The cognitive load impact assessments reveal significant variation across different stakeholder categories within the ceramic value chain. Organizations with high research and development activities, such as glaze and ink producers, demonstrate elevated vulnerability to cognitive manipulation attacks, while those benefiting from shared intelligence networks, such as industry associations, show enhanced resilience. This variation suggests that cognitive adaptivity implementation strategies must be tailored to specific operational contexts rather than applied uniformly across industrial sectors. The projected recovery improvements with cognitive adaptivity implementation reflect stakeholder assessments of pilot programs and early-stage deployments rather than comprehensive empirical validation. These estimates should be interpreted as indicators of potential rather than guaranteed outcomes, particularly given the nascent state of Industry 6.0 technologies and cognitive adaptivity frameworks.

Figure 1 traces the evolution of cyberattack sophistication and defense capabilities from 2000 to 2030, contextualized across the industrial transitions from Industry 3.0 to Industry 6.0. The red curve illustrates the rising sophistication of attacks, starting with basic malware and simple social engineering in 2000, escalating through the emergence of organized cybercrime and phishing campaigns in 2005, and advancing to advanced persistent threats (APTs) and targeted industrial attacks by 2010. The intensity increased further with nation-state actors and supply chain compromises in 2015, culminating in AI-assisted attacks and COVID-related exploitation in 2020. The peak of sophistication is projected in 2025, driven by deep fakes, behavioral manipulation, and IoT botnets, before a decline by 2030 due to the deployment of cognitive adaptivity countermeasures. The blue curve represents the evolution of defense capabilities, which lagged behind during the critical years of Industry 4.0–5.0. Starting with antivirus and firewalls in 2000, the sector advanced to IDS/IPS systems and awareness training by 2005, SIEM and compliance frameworks by 2010, and later integrated threat intelligence and incident response mechanisms

in 2015. By 2020, AI-powered detection and early zero-trust architectures emerged, with projections of advanced AI security and behavioral analytics reaching maturity by 2025. Full cognitive adaptivity frameworks and human–AI symbiosis is expected to raise defense capabilities to their peak by 2030. The shaded area (2010–2025) highlights the "Critical Vulnerability Window," where attack sophistication substantially outpaced defense. This gap illustrates the heightened exposure faced by industries, particularly during the Industry 4.0–5.0 transition. The projected convergence by 2030 underscores the importance of embedding cognitive adaptivity to secure future industrial ecosystems under Industry 6.0.

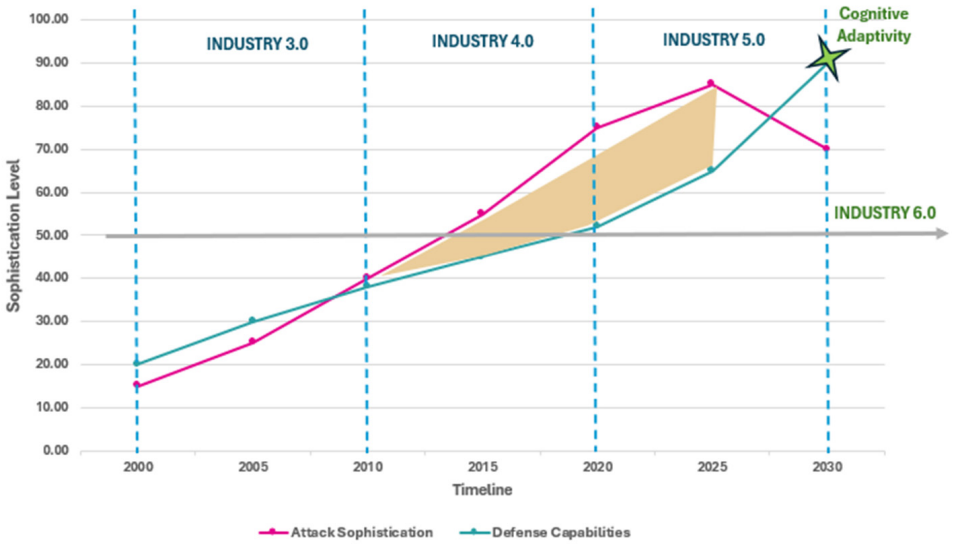

Figure 1. Evolution of cyberattack sophistication and defense capabilities from Industry 3.0 to Industry 6.0 (2000–2030). The figure highlights the critical vulnerability window (2010–2025) and the projected convergence enabled by cognitive adaptivity. The yellow area has been explained in the text, referring to it as a "shaded area".

4.1. Industry 3.0–4.0: Foundation of Digital Vulnerabilities

The ceramic industry's journey through Industry 3.0 was characterized by the introduction of electronic automation systems that replaced manual processes with computerized controls. During this period, cybersecurity threats were relatively straightforward, consisting primarily of unauthorized access attempts and basic malware infections. Human factors played a limited role in cybersecurity, as most workers interacted with standalone systems that had minimal connectivity to external networks. The primary cybersecurity challenges during this era involved protecting centralized control systems and ensuring data integrity for production management systems. Phishing attacks, when they occurred, typically targeted administrative personnel with access to business systems rather than production operators. The clear separation between information technology (IT) and operational technology (OT) systems provided natural barriers that contained the impact of most security incidents.

However, even in this relatively simple technological environment, early indicators of human factors vulnerabilities emerged. Production managers and quality control personnel began to rely on digital systems for critical decision-making, creating opportunities for manipulation through data integrity attacks. Social engineering attempts focused on gaining access to production schedules, quality control data, and customer information through deception of office personnel.

The transition to Industry 4.0 introduced IoT sensors, connected machinery, and data integration platforms that dramatically expanded both the attack surface and the complexity of human-system interactions. Predictive maintenance systems, quality monitoring

sensors, and supply chain integration platforms created new categories of vulnerability while simultaneously increasing operational dependence on digital systems. In Industry 4.0 environments, cyber-attacks began to target not only data confidentiality but also production continuity and product quality. A successful attack on temperature monitoring systems could compromise entire production batches, while manipulation of supply chain data could disrupt just-in-time delivery schedules. These attacks required a more sophisticated understanding of ceramic manufacturing processes and created greater potential for physical and financial damage.

Human factors vulnerabilities during the Industry 4.0 transition manifested primarily through social engineering attacks that exploited the increasing complexity of integrated systems. Operators who were comfortable with mechanical processes found themselves responsible for managing digital interfaces that they did not fully understand. This knowledge gap created opportunities for attackers to manipulate human behavior by exploiting uncertainty and providing false guidance or malicious instructions.

4.2. Industry 5.0: Human-Centric Vulnerabilities and Collaborative Risks

Industry 5.0's emphasis on human–machine collaboration introduced fundamentally new categories of cybersecurity challenges. The ceramic industry's adoption of collaborative robotics (cobots), AI-assisted design systems, and human–AI decision-making platforms created environments where human behavior directly influenced system security through continuous interaction rather than discrete operational tasks.

The human-centric nature of Industry 5.0 systems created vulnerabilities that could not be addressed through traditional technical controls. Collaborative design platforms that enabled real-time interaction between human designers and AI systems became targets for attacks that sought to manipulate design parameters, compromise intellectual property, or introduce defects into production specifications. These attacks required sophisticated understanding of both human psychology and technical systems.

Figure 2 maps the main cybersecurity vulnerabilities along the ceramic value chain, highlighting how risks propagate from raw material suppliers to end customers. The color coding indicates risk levels, with green for low risk, blue for medium risk, and red for high risk. This visualization shows how critical vulnerabilities are concentrated at the production and machinery stages, while lower risks are observed at the supplier and customer interfaces. The figure also identifies points where cognitive adaptivity can be implemented as a protective layer, reinforcing security across the most exposed segments of the chain.

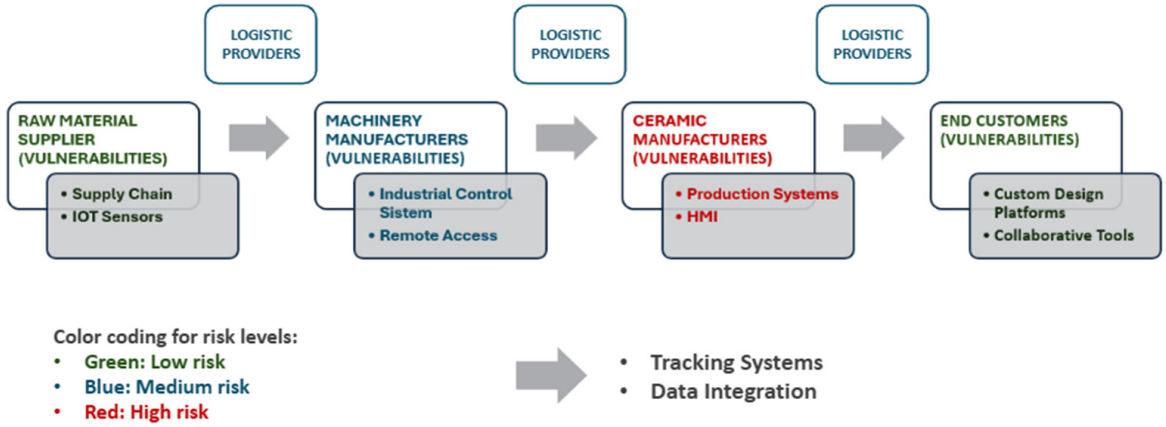

Figure 2. Ceramic Value Chain Vulnerability Mapping. The model illustrates data flow, risk levels, and points of adaptive intervention integrated within digital-twin-based feedback systems.

Social engineering attacks in Industry 5.0 environments became more targeted and contextually sophisticated. Attackers began to leverage detailed knowledge of ceramic manufacturing processes, organizational structures, and individual work patterns to create highly personalized deception campaigns. For example, attackers might impersonate equipment vendors to convince production managers to install malicious software updates or modify safety parameters on collaborative systems.

The cognitive load associated with managing human–AI collaborative systems created new categories of human error that could be exploited for malicious purposes. Operators working with AI-assisted quality control systems, for instance, might develop over-reliance on automated recommendations, making them susceptible to attacks that manipulated AI outputs to mask quality defects or production anomalies.

Trust relationships between humans and AI systems became critical attack vectors in Industry 5.0 environments. Successful attacks often involve undermining human confidence in AI recommendations while simultaneously positioning attackers as reliable sources of alternative guidance. This manipulation of trust dynamics could lead to compromise of both human judgment and AI system integrity.

The emphasis on customization and flexibility in Industry 5.0 manufacturing created additional cybersecurity challenges as production systems needed to accommodate frequent changes in specifications, processes, and operational parameters. This flexibility, while valuable for meeting customer requirements, created opportunities for attackers to introduce malicious changes disguised as legitimate customization requests.

4.3. Industry 6.0: Cognitive Ecosystems and Adaptive Threats

The emerging Industry 6.0 paradigm in the ceramic industry envisions cognitive ecosystems where AI systems, human operators, and physical processes engage in continuous co-evolution to optimize performance, sustainability, and resilience. This vision introduces unprecedented cybersecurity challenges that require fundamental reconceptualization of threat models and defensive strategies. Cognitive manufacturing systems in Industry 6.0 environments continuously learn from operational data, human behavior patterns, and environmental conditions to improve performance and adapt to changing requirements. This learning capability creates vulnerabilities where attackers can manipulate training data, behavioral inputs, or environmental signals to influence system evolution in malicious directions.

AI-powered threat actors represent a qualitative shift in the cybersecurity landscape for Industry 6.0 systems. These sophisticated attacks can generate deepfakes of trusted personnel, create convincing synthetic communications, and manipulate behavioral cues to deceive human operators in cognitive manufacturing environments. The ability of AI systems to learn and adapt human communication patterns makes traditional social engineering detection techniques increasingly ineffective. The integration of sustainability monitoring and regulatory compliance systems in Industry 6.0 creates additional attack vectors where cybersecurity incidents can have environmental and regulatory consequences. Attackers might manipulate emissions monitoring data, energy consumption reports, or waste management systems to create compliance violations or environmental damage while concealing their activities within normal operational variance.

Cognitive adaptation mechanisms that enable Industry 6.0 systems to learn from security incidents and adjust defensive strategies can themselves become targets for attack. Adversarial learning attacks can train defensive systems to ignore genuine threats while over-responding to benign activities, effectively weaponizing the adaptive capabilities that are intended to enhance security. The systemic nature of Industry 6.0 cognitive ecosystems means that successful attacks can propagate across multiple organizational

boundaries, affecting suppliers, customers, and partners through shared learning systems and integrated decision-making platforms. A successful attack on one organization's cognitive manufacturing system could potentially influence the behavior of connected systems throughout the value chain.

5. Conceptual Model: Cognitive Adaptivity in Hard-to-Abate Industries

The transition from resilience-based to cognitive adaptivity-based cybersecurity approaches in hard-to-abate industries can be conceptualized through a multi-dimensional framework that addresses the unique constraints and requirements of these sectors. This conceptual model integrates four fundamental axes: human–AI trust dynamics, behavioral evolution mechanisms, sustainability constraints integration, and systemic antifragility development.

Figure 3 illustrates the conceptual model of the Cognitive Adaptivity Framework. The model is structured around four interconnected dimensions (Human–AI Trust Dynamics, Behavioral Evolution Mechanisms, Sustainability Constraints Integration, and Systemic Antifragility Development) whose interactions converge in the Cognitive Adaptivity Ecosystem. The clockwise flow represents the progressive reinforcement of adaptive capabilities, while the dotted feedback arrows highlight cross-dimensional learning processes.

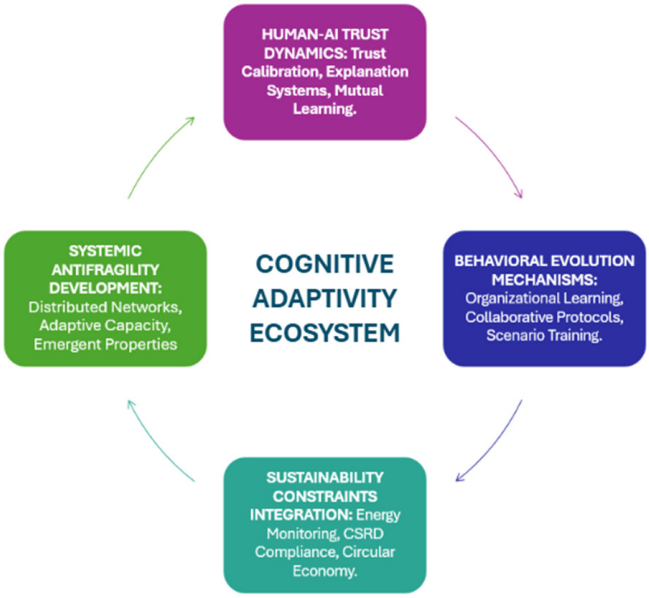

Figure 3. Ceramic Value Chain Vulnerability Mapping. The model highlights data flow, risk levels, and points of adaptive intervention integrated within digital-twin-based feedback systems.

5.1. Human–AI Trust Dynamics

The foundation of cognitive adaptivity rests on the development of robust trust relationships between human operators and AI systems. Unlike traditional cybersecurity approaches that treat trust as a binary condition (trusted vs. untrusted), cognitive adaptivity recognizes trust as a dynamic, contextual, and continuously evolving relationship that requires active management and sophisticated assessment capabilities.

In the ceramic industry context, human–AI trust dynamics manifest through several key mechanisms. Production operators develop trust in AI-assisted quality control systems through repeated positive interactions where AI recommendations prove accurate and valuable. However, this trust can become a vulnerability if attackers successfully manipulate AI outputs to provide false guidance while maintaining the appearance of reliability.

Cognitive adaptivity addresses this challenge by implementing multi-dimensional trust assessment frameworks that evaluate not only the immediate accuracy of AI recommendations but also the consistency of recommendations with broader operational patterns, the transparency of decision-making processes, and the alignment of recommendations with human expertise and intuition.

The ceramic case study reveals that effective human–AI trust dynamics require continuous calibration rather than static configuration. Operators working with AI-powered kiln management systems, for example, develop sophisticated understanding of when to rely on AI recommendations, when to seek additional validation, and when to override automated decisions based on contextual factors that may not be captured in AI training data. Trust calibration mechanisms in cognitive adaptivity include real-time explanation capabilities that provide human operators with insight into AI decision-making processes, anomaly detection systems that identify when AI behavior deviates from established patterns, and feedback loops that enable human operators to communicate the effectiveness of AI recommendations back to learning systems.

The distinction between traditional resilience approaches and cognitive adaptivity frameworks becomes apparent when comparing their operational characteristics and performance indicators. A key characteristic of cognitive adaptivity lies in its temporal elasticity, the ability of organizations to modulate learning and anticipation speeds relative to the pace of emerging threats. Learning velocity is governed by the organization's feedback frequency, data availability, and cognitive load capacity, whereas anticipation depends on predictive intelligence and trust calibration between humans and AI. The model assumes that adaptive efficiency increases when the rate of behavioral learning equals or exceeds the rate of threat evolution, represented through indicative metrics such as the adaptivity coefficient and learning velocity index summarized in Table 3. Temporal analysis therefore becomes a diagnostic dimension of cognitive adaptivity, distinguishing reactive adaptation from proactive evolution. Table 3 demonstrates that cognitive adaptivity represents not merely an incremental improvement over existing approaches but a fundamental reconceptualization of how organizations develop and maintain cybersecurity capabilities.

The implementation timeline data reveals that cognitive adaptivity requires sustained organizational commitment extending well beyond typical cybersecurity project cycles. The 24–36 months required for full system response transformation reflects the deep organizational and behavioral changes necessary to shift from recovery-focused to enhancement-focused security strategies. This extended timeline may present challenges for organizations operating under quarterly performance pressures, though the long-term benefits justify the investment.

The performance indicators associated with cognitive adaptivity introduce novel metrics that extend beyond traditional cybersecurity measurements. Trust calibration indices and symbiotic efficiency scores represent attempts to quantify the quality of human–AI collaboration in security contexts. While these metrics require further empirical validation, they offer promising approaches for measuring the effectiveness of cognitive adaptivity in ways that traditional incident response times and detection rates cannot capture.

The knowledge management dimension reveals perhaps the most significant departure from traditional approaches. The shift from centralized documentation to distributed learning networks reflects the systemic nature of cognitive adaptivity, where individual organizational learning contributes to broader industry-wide capability development.

Table 3. Cognitive Adaptivity Framework Dimensions vs. Traditional Resilience Approaches.

FRAMEWORK DIMENSION	TRADITIONAL RESILIENCE	COGNITIVE ADAPTIVITY	KEY PERFORMANCE INDICATORS	IMPLEMENTATION TIMELINE
LearningMechanism	Post-incident analysis, lessons learned documents	Continuous behavioral adaptation, real-time insight extraction	Learning velocity (insights/month), knowledge retention rate	6–12 months
Threat Anticipation	Reactive detection, signature-based systems	Proactive behavioral modeling, pattern recognition	Prediction accuracy (%), early warning effectiveness	12–18 months
Human–AI Interaction	Fixed roles, hierarchical decision-making	Dynamic collaboration, mutual adaptation	Trust calibration index, symbiotic efficiency score	18–24 months
System Response	Recovery to baseline functionality	Performance enhancement through adversity	Adaptivity coefficient, capability growth rate	24–36 months
Knowledge Management	Centralized documentation, training programs	Distributed learning networks, experiential knowledge	Knowledge diffusion speed, cross-organizational learning	12–24 months

5.2. Behavioral Evolution Mechanisms

Cognitive adaptivity extends beyond individual human–AI interactions to encompass organizational and systemic behavioral evolution. This dimension addresses how entire organizations learn from security incidents, adapt their operational practices, and develop more sophisticated responses to emerging threats through collective learning processes.

The behavioral evolution dimension recognizes that effective cybersecurity in Industry 6.0 environments requires organizations to function as learning systems that continuously extract insights from security events, near-misses, and operational anomalies. This learning process extends beyond traditional incident response procedures to encompass proactive identification of emerging vulnerabilities and collaborative development of adaptive countermeasures.

Figure 4 presents the Human Factors Risk Matrix, mapping how different types of human–AI interactions vary in terms of frequency and cognitive complexity, and how cognitive adaptivity can shift activities from high-risk to safer operational zones. In ceramic manufacturing contexts, behavioral evolution mechanisms operate across multiple organizational levels. Individual operators develop enhanced situational awareness through exposure to diverse security scenarios and feedback on their responses. Work teams develop collaborative protocols for identifying and responding to anomalous system behavior. Organizational units develop systematic approaches for sharing threat intelligence and coordinating defensive responses across different operational domains.

The ceramic industry case study demonstrates how behavioral evolution mechanisms can transform routine operational activities into opportunities for security enhancement. Quality control processes that historically focused solely on product specifications begin to incorporate security considerations, such as identifying anomalous patterns that might indicate data manipulation or system compromise.

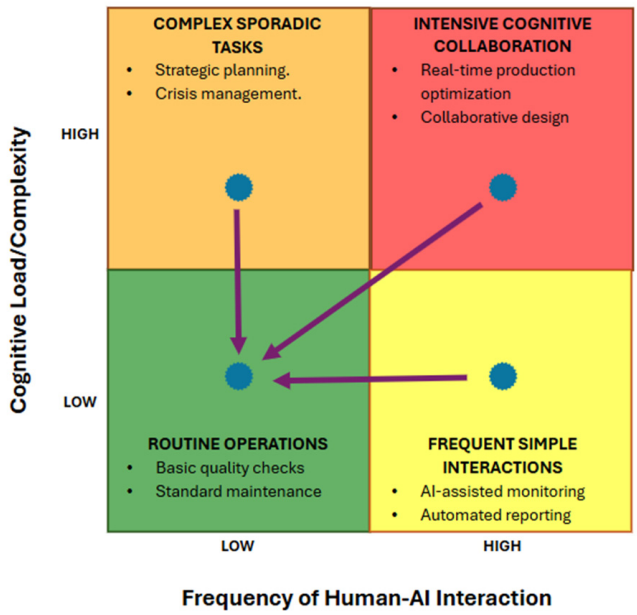

Figure 4. Human Factors Risk Matrix, identifying vulnerability levels based on cognitive load and frequency of human–AI interaction. Cognitive adaptivity strategies aim to transition high-risk activities toward safer operational zones.

Behavioral evolution in cognitive adaptivity is facilitated through several key mechanisms: scenario-based training that exposes personnel to diverse threat scenarios and response options; collaborative learning platforms that enable sharing of experiences and insights across organizational boundaries; and continuous improvement processes that treat security incidents as learning opportunities rather than simply disruptions to be contained.

5.3. Sustainability Constraints Integration

Hard-to-abate industries face unique challenges in cybersecurity strategy development due to the intersection of digital transformation requirements with stringent environmental sustainability and regulatory compliance constraints. Cognitive adaptivity frameworks must explicitly address these constraints rather than treating them as external limitations on cybersecurity strategy.

The integration of sustainability constraints into cybersecurity strategy creates opportunities for innovative approaches that leverage environmental monitoring systems, energy efficiency optimization platforms, and circular economy principles [45] as components of comprehensive security frameworks. These systems provide additional data streams for anomaly detection, alternative communication channels for security coordination, and redundant verification mechanisms for critical operational decisions.

In the ceramic industry, sustainability constraints integration manifests through several innovative approaches. Energy monitoring systems designed to optimize kiln efficiency can also serve as anomaly detection platforms for identifying suspicious changes in operational patterns. Waste management systems that track material flows through production processes provide verification mechanisms for detecting unauthorized modifications to production specifications.

The regulatory compliance requirements associated with environmental sustainability create additional layers of verification and audit that can enhance overall security posture. CSRD reporting requirements, for example, necessitate detailed tracking of environmental impact metrics that can serve as indicators of operational anomalies potentially associated with security incidents.

Cognitive adaptivity frameworks leverage sustainability constraints as design principles rather than limitations. Security strategies that integrate energy efficiency optimization, waste reduction goals, and regulatory compliance requirements often prove more robust and sustainable than approaches that treat these factors as competing priorities.

The Cognitive Adaptivity Framework aligns with the regulatory evolution of sustainability and risk governance under the Corporate Sustainability Reporting Directive (CSRD). Adaptive loops within the model incorporate compliance verification and reporting consistency mechanisms, ensuring that cybersecurity and sustainability metrics are monitored concurrently. These include cross-validation between environmental data integrity, emissions disclosure, and cyber-risk accountability indicators required by the CSRD and related EU taxonomies. By embedding compliance checkpoints within the adaptive feedback cycles, organizations can transform regulatory adherence from a static obligation into a dynamic learning process that continuously refines both operational transparency and cyber-governance maturity (Boggini et al., 2024; Saeed et al., 2024 [46,47]).

5.4. Systemic Antifragility Development

The fourth dimension of cognitive adaptivity addresses the development of systemic capabilities that enable organizations and industry ecosystems to not merely withstand cybersecurity challenges but to gain strength and improve performance through exposure to adversity. This concept extends beyond traditional resilience to encompass the development of adaptive capabilities that transform security challenges into opportunities for systemic improvement.

Systemic antifragility in hard-to-abate industries requires the development of distributed learning networks that span organizational boundaries, supply chain relationships, and regulatory frameworks. These networks enable rapid sharing of threat intelligence, collaborative development of countermeasures, and coordinated response to industry-wide security challenges.

The ceramic industry demonstrates systemic antifragility through the development of industry associations, collaborative research initiatives, and shared cybersecurity platforms that enable small and medium-sized manufacturers to access sophisticated security capabilities that would be prohibitively expensive to develop independently.

Antifragile systems in cognitive adaptive frameworks exhibit several key characteristics: they maintain diversity of approaches and capabilities that prevent single points of failure; they incorporate redundancy that enables continued operation even when specific components are compromised; they demonstrate adaptive capacity that enables learning and improvement from security incidents; and they exhibit emergent properties that create capabilities greater than the sum of individual components.

5.5. Implementation in the Ceramic Value Chain

The practical implementation of cognitive adaptivity frameworks in the ceramic value chain reveals both opportunities and challenges associated with this theoretical approach. Manufacturing organizations that successfully implement cognitive adaptivity demonstrate several common characteristics: they treat cybersecurity as a strategic capability rather than a compliance requirement; they invest in developing human capabilities alongside technological solutions; they maintain active engagement with industry networks and collaborative platforms; and they integrate cybersecurity considerations into business strategy development rather than treating security as a separate operational domain. The implementation of cognitive adaptivity in industrial environments is technologically supported by digital twin architectures, AI-driven monitoring systems, behavioral analytics, and secure data-trust layers that connect operational and human-behavioral feedback loops.

These technologies enable continuous sensing, anticipation of anomalies, and knowledge co-evolution across human and machine agents, ensuring that learning cycles are grounded in real-time operational evidence.

The ceramic case study indicates that cognitive adaptivity implementation requires sustained commitment from organizational leadership, continuous investment in human capability development, and active participation in industry-wide collaborative initiatives. Organizations that approach cognitive adaptivity as a discrete project or technical implementation typically fail to realize the full benefits of the framework.

Successful implementation typically follows a developmental progression from basic resilience capabilities through enhanced adaptive capabilities to full cognitive adaptivity. This progression allows organizations to build foundational capabilities while gradually developing more sophisticated approaches to cybersecurity strategy.

5.6. Quantitative Representation of Adaptive Dynamics

Although the Cognitive Adaptivity Framework is primarily conceptual, its internal dynamics can be represented quantitatively through a simplified relationship between learning velocity (L_v), anticipation rate (A_r), and the rate of threat evolution (T_e). These parameters jointly determine an organization's ability to maintain adaptive advantage within dynamic industrial ecosystems.

$$A_c = \frac{L_v + A_r}{T_e}$$

where A_c denotes the Adaptivity Coefficient, a synthetic indicator of the relative capacity of human–AI systems to anticipate and counter evolving cyber threats. When $A_c > 1$, learning and anticipation outpace threat evolution, indicating proactive adaptation. Conversely when $A_c < 1$, signals a reactive condition, where adaptation lags behind environmental and behavioral change. The coefficient is intended as a diagnostic proxy rather than a deterministic measure, enabling the monitoring of adaptive maturity across organizations and over time. This formulation complements the qualitative dimensions of the framework and supports future empirical validation through adaptive performance metrics and learning-rate analytics.

6. Discussion

6.1. Theoretical Contributions and Distinctions

The cognitive adaptivity framework advances cybersecurity theory by integrating human factors with technological changes, especially in industrial settings. Unlike traditional resilience models focused on recovery, cognitive adaptivity treats security challenges as learning and improvement opportunities. Research on cognitive security shows these frameworks address key gaps left by static threat assumptions environments [22].

Differentiating cognitive adaptivity from related ideas requires precision. Traditional resilience strategies aim to help organizations resume normal operations after security incidents but often view threats as outside disruptions. Research on cyber-resilience in industry notes that adaptation and sensemaking are typically reactive, not embedded proactively in system design [44].

Antifragility, as conceptualized by Nassim Taleb [48], emphasizes gaining strength from stressors and volatility. While cognitive adaptivity shares this emphasis on deriving benefit from challenges, it extends beyond individual organizational strength to encompass collaborative learning, behavioral co-evolution, and systemic capability development across industry ecosystems. For instance, ref. [32] demonstrates that AI-driven detection systems

combined with human feedback loops produce more robust defense postures than purely reactive resilience models

Adaptive security models in cybersecurity literature typically focus on technological adaptations such as machine learning-based threat detection and automated response systems. Cognitive adaptivity encompasses these technological dimensions while emphasizing the human behavioral and organizational learning aspects that are often overlooked in purely technical approaches.

The human–AI symbiosis dimension of cognitive adaptivity distinguishes it from both human-centric and AI-centric cybersecurity approaches. Rather than treating humans and AI systems as separate entities with distinct roles and responsibilities, cognitive adaptivity recognizes that effective security in Industry 6.0 environments emerges from collaborative intelligence that leverages the unique strengths of both human and artificial cognitive capabilities.

6.2. Implications for Hard-to-Abate Industries

The application of cognitive adaptivity frameworks to hard-to-abate industries reveals several important implications for cybersecurity strategy development in sectors facing the dual challenges of digital transformation and sustainability constraints. These industries cannot simply adopt generic cybersecurity solutions but must develop adaptive approaches that integrate security requirements with environmental responsibility and regulatory compliance [46]. Although the ceramic value chain provides the empirical foundation of this study, the proposed framework is readily extendable to other hard-to-abate sectors such as steel, cement, and chemicals. These industries share structural conditions (high energy intensity, complex multi-tier supply chains, and stringent regulatory and environmental constraints) that make them suitable contexts for cognitive adaptivity. Nevertheless, successful transferability depends on the sector-specific maturity of digital infrastructures, workforce skill profiles, and organizational cultures. Consequently, while the theoretical architecture of cognitive adaptivity remains constant, its operational calibration requires contextual adjustment to reflect each industry's socio-technical and regulatory configuration.

The sustainability constraints that characterize hard-to-abate industries create both challenges and opportunities for cognitive adaptivity implementation. Environmental monitoring systems, energy efficiency optimization platforms, and regulatory compliance frameworks provide additional data streams and verification mechanisms that can enhance security posture when properly integrated into cognitive adaptive frameworks. The energy sector review by Saeed et al. [47], illustrates how such monitoring systems augment cybersecurity risk assessment in infrastructure-intensive contexts.

The regulatory environment facing hard-to-abate industries, particularly the emergence of comprehensive sustainability reporting requirements such as CSRD, creates accountability mechanisms that can be leveraged to enhance cybersecurity governance. Organizations that integrate cybersecurity considerations into sustainability reporting demonstrate a more sophisticated understanding of the interconnections between operational risk, environmental impact, and strategic resilience. Boggini [46] provides empirical evidence that CSRD mandates are now promoting disclosure of cyber risks and driving investment in cyber risk management. The supply chain complexity that characterizes many hard-to-abate industries necessitates cybersecurity approaches that extend beyond individual organizational boundaries to encompass ecosystem-wide collaboration and shared learning. Innovation ecosystems that share threat information and offer common learning platforms help reduce related risks [49]. Cognitive adaptivity frameworks provide mechanisms for developing these collaborative capabilities while maintaining competitive advantage and

operational autonomy. The practical implementation of cognitive adaptivity frameworks in hard-to-abate industries requires systematic planning and realistic resource allocation that extends well beyond traditional cybersecurity project timelines. Dynamics of business ecosystems support the view that transformation momentum across partners is required, not just internal investment [50]. Table 4 synthesizes insights from early adopter organizations and pilot programs to provide guidance for industry practitioners considering cognitive adaptivity implementation.

Table 4. Cognitive Adaptivity Implementation Roadmap for Hard-to-Abate Industries.

IMPLEMENTATION PHASE	DURATION	KEY ACTIVITIES	SUCCESS METRICS	INVESTMENT RANGE (€)	RISK MITIGATION STRATEGIES
Foundation Building	6–9 months	Baseline assessment, stakeholder alignment, initial training	Staff engagement > 80%, basic capability development	150 K–300 K	Change management, pilot programs
Pilot Deployment	9–12 months	Limited scope implementation, feedback collection, refinement	25% reduction in incident response time	300 K–600 K	Parallel legacy systems, gradual transition
Scaled Implementation	12–18 months	Organization-wide deployment, integration optimization	50% improvement in threat detection	600 K–1.2 M	Phased rollout, continuous monitoring
Ecosystem Integration	18–24 months	Supply chain extension, industry collaboration	Cross-organizational learning effectiveness	400 K–800 K	Partnership agreements, data sharing protocols
Continuous Evolution	Ongoing	Adaptive refinement, capability enhancement	Sustained competitive advantage metrics	200 K–400 K/year	Innovation investment, skill development

The investment ranges presented reflect comprehensive transformation costs rather than discrete technology acquisitions. Unlike traditional cybersecurity implementations that focus primarily on technical infrastructure, cognitive adaptivity requires substantial investment in human capability development, organizational culture change, and collaborative platform development. The front-loaded investment pattern, with higher costs in early phases, reflects the foundational nature of capability building required for effective cognitive adaptivity. The success metrics evolve significantly across implementation phases, moving from conventional engagement and efficiency measures toward more sophisticated assessments of adaptive capability and collaborative effectiveness. The shift toward competitive advantage metrics in later phases reflects the strategic nature of cognitive adaptivity as a differentiating organizational capability rather than merely a compliance or risk management function. The investment ranges reported (€) are indicative and intended to provide general guidance rather than precise cost estimates.

Risk mitigation strategies emphasize the importance of gradual transition approaches that maintain operational continuity while building new capabilities. The parallel operation

of legacy systems during pilot phases, while increasing short-term costs, provides essential fallback capabilities and reduces implementation risk for organizations operating in critical infrastructure contexts. The ongoing investment requirements for continuous evolution phase highlight that cognitive adaptivity represents a permanent organizational capability development rather than a discrete project implementation. This perpetual investment model may challenge traditional capital allocation approaches but aligns with the dynamic threat landscape and continuous learning requirements of Industry 6.0 environments.

6.3. Practical Implementation Considerations

The transition from traditional resilience-based cybersecurity approaches to cognitive adaptivity frameworks requires careful consideration of organizational readiness, resource allocation, and change management strategies. Organizations attempting to implement cognitive adaptivity without adequate preparation often experience implementation challenges that undermine the effectiveness of the approach. Recent research on cybersecurity readiness points to organizational readiness (including leadership support, strategic resource allocation, and organizational culture) as critical antecedents for successful adaptation [51].

Successful cognitive adaptivity implementation typically requires investment in human capability development that extends beyond traditional cybersecurity training. Personnel need to develop skills in collaborative problem-solving, behavioral pattern recognition, and human–AI interaction management that are not addressed in conventional security awareness programs. Empirical studies in other safety-critical domains, such as railway operations, demonstrate how integrating human factors with cybersecurity and safety analysis can provide actionable insights into capability development and organizational chang [52]. Evidence from interdisciplinary reviews underscores gaps in training programs that fail to cultivate these capacities [21].

The organizational culture changes associated with cognitive adaptivity implementation can be particularly challenging for organizations with traditional hierarchical structures and risk-averse operational cultures. The emphasis on learning from security incidents, experimental approaches to security strategy, and collaborative decision-making may conflict with established organizational norms and procedures. Empirical evidence from a study of public sector culture confirms that values, norms, and empowerment correlate with how employees internalize cybersecurity policies [53].

The technological infrastructure requirements for cognitive adaptivity implementation can be substantial, particularly for smaller organizations in hard-to-abate industries. However, the development of industry collaboratives and shared cybersecurity platforms can help distribute these costs and provide access to sophisticated capabilities that would be prohibitively expensive for individual organizations. This is consistent with findings in [32], which identify architectures and infrastructure as critical bottlenecks in scaling adaptive security strategies.

6.4. Limitations and Boundary Conditions

Despite its conceptual robustness, the Cognitive Adaptivity Framework operates under several boundary conditions. Its effectiveness presupposes an organizational environment that values continuous learning, transparent communication, and human–AI collaboration. In cultures with rigid hierarchies or limited digital literacy, adaptive feedback loops may slow down or generate bias. The framework also depends on the reliability of AI training datasets; incomplete or skewed behavioral data can lead to miscalibrated learning cycles. Moreover, sectors characterized by highly standardized operations (such as pharmaceuticals or nuclear energy) may require hybrid models that integrate cognitive adaptivity with strict procedural control systems. The cognitive adaptivity framework, while promis-

ing, faces several limitations and boundary conditions that must be acknowledged in theoretical development and practical implementation. The framework's emphasis on learning and adaptation may not be appropriate for all organizational contexts or threat environments, particularly those requiring highly standardized and predictable security responses. Research in cybersecurity readiness shows that some organizations (especially those with low maturity or in highly regulated industries) lack the flexibility or culture needed for dynamic adaptation [51].

The reliance on human–AI collaboration as a foundational element of cognitive adaptivity creates vulnerabilities in situations where AI systems are compromised or human judgment is severely impaired. Organizations implementing cognitive adaptivity must maintain fallback capabilities and recognition mechanisms that can identify when collaborative approaches are no longer effective. Studies on human–AI interaction warn that cognitive overload, trust miscalibration, and automation bias can degrade performance and increase risk if oversight and feedback loops are not built in [54].

The industry-specific nature of the ceramic case study limits the generalizability of specific findings to other hard-to-abate sectors, though the underlying principles of cognitive adaptivity appear applicable across similar industrial contexts. Additional research in other sectors would strengthen understanding of the framework's broader applicability. The emergent nature of Industry 6.0 means that many of the threats and opportunities associated with cognitive ecosystems remain theoretical or experimental. The cognitive adaptivity framework is based on projections of future technological and threat developments that may prove inaccurate or incomplete as these systems mature.

7. Conclusions and Future Research

7.1. Theoretical Contributions

This paper introduces cognitive adaptivity as a novel framework for addressing human factors in cybersecurity during the Industry 5.0–6.0 transition. Unlike resilience, which emphasizes recovery to baseline, cognitive adaptivity highlights learning, anticipation, and co-evolution between humans and AI as essential elements of security strategy. By integrating behavioral dynamics with technological evolution, the framework extends existing literature on resilience, antifragility, and adaptive security, positioning cybersecurity as a socio-technical capability that emerges from continuous human–AI collaboration.

7.2. Practical Implications

The ceramic value chain, used as a paradigmatic hard-to-abate sector, illustrates how cognitive adaptivity can be implemented in practice. The findings show that organizations need to embed human–AI trust calibration, behavioral evolution, sustainability integration, and systemic antifragility into their cybersecurity strategies. Beyond defensive benefits, cognitive adaptivity can also serve as a source of competitive advantage by fostering collaborative capabilities and aligning cybersecurity with sustainability imperatives. These insights are transferable to other resource-intensive industries, such as steel, cement, and chemicals, that face similar dual pressures of digital transformation and environmental responsibility.

7.3. Limitations and Future Research

The singular focus on the ceramic sector limits the generalizability of the findings, although this industry shares significant characteristics with other hard-to-abate sectors. The framework also arises from the emergent context of Industry 6.0, relying on projections and pilot data rather than extensive longitudinal analysis. Future research should move in three primary directions: (i) cross-sector validation in additional hard-to-abate industries;

(ii) longitudinal studies that monitor organizations throughout full cycles of cognitive adaptivity implementation; and (iii) the development of quantitative metrics to evaluate learning effectiveness, behavioral adaptation, and collaborative capability. These steps are essential to solidify cognitive adaptivity as both a theoretical construct and a practical strategy for Industry 6.0. It will also be important to introduce cross-industry quantitative metrics to enable benchmarking and to reinforce the framework's empirical validity. Subsequent studies should prioritize multi-sector and longitudinal applications, specifically in sectors such as steel, chemicals, and energy, to quantify adaptive maturity using measurable indicators of learning efficiency, human–AI coordination, and sustainability integration. Longitudinal analyses will help trace organizational adaptation and learning trajectories, providing evidence of the model's stability and scalability. Finally, developing quantitative metrics—such as cross-industry adaptivity indices—will further enhance the framework's theoretical generalization and policy relevance within the Industry 6.0 paradigm.

Author Contributions: Conceptualization, A.F.-M. and D.S.-B.; Methodology, S.O.-M. and M.J.-C.; Investigation, A.F.-M. and M.J.-C.; Data Curation, A.P.F.d.H. and F.E.G.-M.; Writing—Original Draft Preparation, D.S.-B. and A.P.F.d.H.; Validation and Supervision, S.O.-M. and F.E.G.-M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study is based on a structured expert survey. It does not involve sensitive personal data, vulnerable populations, or clinical experimentation. All participants were informed about the purpose of the study and gave their explicit consent to participate. The data collected were anonymised and processed in full compliance with the principles of the EU General Data Protection Regulation (GDPR), including transparency, data minimisation, and confidentiality. According to GDPR and applicable EU research ethics guidance, this type of study does not require formal Ethics Committee or IRB approval.

Informed Consent Statement: Informed consent for participation was obtained from all subjects involved in the study.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: Author Davide Settembre-Blundo was employed by the company Gresmalt Group. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Jiang, W.; Hu, F. Artificial Intelligence Agent-Enabled Predictive Maintenance: Conceptual Proposal and Basic Framework. *Computers* **2025**, *14*, 329. [CrossRef]
2. Radanliev, P.; De Roure, D.; Maple, C.; Nurse, J.R.; Nicolescu, R.; Ani, U. AI Security and Cyber Risk in IoT Systems. *Front. Big Data* **2024**, *7*, 1402745. [CrossRef]
3. Fernández-Miguel, A.; García-Muiña, F.E.; Settembre-Blundo, D.; Tarantino, S.C.; Riccardi, M.P. Exploring Systemic Sustainability in Manufacturing: Geoanthropology's Strategic Lens Shaping Industry 6.0. *Glob. J. Flex. Syst. Manag.* **2024**, *25*, 579–600. [CrossRef]
4. Safa, N.S.; Abroshan, H. The Effect of Organizational Factors on the Mitigation of Information Security Insider Threats. *Information* **2025**, *16*, 538. [CrossRef]
5. Mulahuwaish, A.; Qolomany, B.; Gyorick, K.; Abdo, J.B.; Aledhari, M.; Qadir, J.; Carley, K.; Al-Fuqaha, A. A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects. *Comput. Hum. Behav. Rep.* **2025**, *18*, 100668. [CrossRef]
6. Kostelić, K. Dynamic Awareness and Strategic Adaptation in Cybersecurity: A Game-Theory Approach. *Games* **2024**, *15*, 13. [CrossRef]
7. Tynchenko, V.; Lomazov, A.; Lomazov, V.; Evsyukov, D.; Nelyub, V.; Borodulin, A.; Gantimurov, A.; Malashin, I. Adaptive Management of Multi-Scenario Projects in Cybersecurity: Models and Algorithms for Decision-Making. *Big Data Cogn. Comput.* **2024**, *8*, 150. [CrossRef]

8. Rawindaran, N.; Jayal, A.; Prakash, E. Cybersecurity Framework: Addressing Resiliency in Welsh SMEs for Digital Transformation and Industry 5.0. *J. Cybersecur. Priv.* **2025**, *5*, 17. [CrossRef]
9. Hunter, T.S.; Taylor, M.; Selvadurai, N. Emerging Technologies in Oil and Gas Development: Regulatory and Policy Perspectives. *Res. Handb. Oil Gas Law* **2023**, 345–372. [CrossRef]
10. Eirinakis, P.; Lounis, S.; Plitsos, S.; Arampatzis, G.; Kalaboukas, K.; Kenda, K.; Lu, J.; Rožanec, J.M.; Stojanovic, N. Cognitive Digital Twins for Resilience in Production: A Conceptual Framework. *Information* **2022**, *13*, 33. [CrossRef]
11. Kanaan, A.; Ahmad, A.; Alorfi, A.; Aloun, M. Cybersecurity Resilience for Business: A Comprehensive Model for Proactive Defense and Swift Recovery. In Proceedings of the 2024 2nd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–28 February 2024; pp. 1–7.
12. Contini, G.; Peruzzini, M.; Bulgarelli, S.; Bosi, G. Developing Key Performance Indicators for Monitoring Sustainability in the Ceramic Industry: The Role of Digitalization and Industry 4.0 Technologies. *J. Clean. Prod.* **2023**, *414*, 137664. [CrossRef]
13. Contini, G.; Grandi, F.; Peruzzini, M. Human-Centric Green Design for Automatic Production Lines: Using Virtual and Augmented Reality to Integrate Industrial Data and Promote Sustainability. *J. Ind. Inf. Integr.* **2025**, *44*, 100801. [CrossRef]
14. Liu, X.; Cheng, X.; Liao, C.; Chen, J.; Li, X.; Liu, K. Ceramic Anti-Counterfeiting Technology Identification Method Based on Blockchain. In Proceedings of the 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Washington, DC, USA, 26–28 June 2021; pp. 36–41.
15. Appolloni, A.; D'Adamo, I.; Gastaldi, M.; Yazdani, M.; Settembre-Blundo, D. Reflective Backward Analysis to Assess the Operational Performance and Eco-Efficiency of Two Industrial Districts. *Int. J. Product. Perform. Manag.* **2023**, *72*, 1608–1626. [CrossRef]
16. Zakoldaev, D.A.; Korobeynikov, A.G.; Shukalov, A.V.; Zharinov, I.O.; Zharinov, O.O. Industry 4.0 vs Industry 3.0: The Role of Personnel in Production. In *IOP Conference Series: Materials Science and Engineering*; IOP Science: Beijing, China, 2025; p. 012048.
17. Pedreira, V.; Barros, D.; Pinto, P. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors* **2021**, *21*, 5189. [CrossRef]
18. Pacaux-Lemoine, M.; Berdal, Q.; Guérin, C.; Rauffet, P.; Chauvin, C.; Trentesaux, D. Designing Human–system Cooperation in Industry 4.0 with Cognitive Work Analysis: A First Evaluation. *Cogn. Technol. Work* **2022**, *24*, 93–111. [CrossRef]
19. Hassan, M.A.; Zardari, S.; Farooq, M.U.; Alansari, M.M.; Nagro, S.A. Systematic Analysis of Risks in Industry 5.0 Architecture. *Appl. Sci.* **2024**, *14*, 1466. [CrossRef]
20. Kour, R.; Karim, R.; Dersin, P.; Venkatesh, N. Cybersecurity for Industry 5.0: Trends and Gaps. *Front. Comput. Sci.* **2024**, *6*, 1434436. [CrossRef]
21. Khadka, K.; Ullah, A.B. Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal. *Int. J. Inf. Secur.* **2025**, *24*, 1–13. [CrossRef]
22. Casino, F. Unveiling the Multifaceted Concept of Cognitive Security: Trends, Perspectives, and Future Challenges. *Technol. Soc.* **2025**, *83*, 102956. [CrossRef]
23. Tilbury, J.; Flowerday, S. Automation Bias and Complacency in Security Operation Centers. *Computers* **2024**, *13*, 165. [CrossRef]
24. Schmitt, M.; Flechais, I. Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. *Artif. Intell. Rev.* **2024**, *57*, 324. [CrossRef]
25. Sarker, I.H.; Janicke, H.; Mohsin, A.; Gill, A.; Maglaras, L. Explainable AI for Cybersecurity Automation, Intelligence and Trustworthiness in Digital Twin: Methods, Taxonomy, Challenges and Prospects. *ICT Express* **2024**, *10*, 935–958. [CrossRef]
26. Alsharida, R.A.; Al-rimy, B.A.S.; Al-Emran, M.; Zainal, A. A Systematic Review of Multi Perspectives on Human Cybersecurity Behavior. *Technol. Soc.* **2023**, *73*, 102258. [CrossRef]
27. Albaladejo-González, M.; Nespoli, P.; Gómez Mármol, F.; Ruipérez-Valiente, J.A. A Multimodal and Adaptive Gamified System to Improve Cybersecurity Competence Training. *Clust. Comput.* **2025**, *28*, 567. [CrossRef]
28. Eswaran, U.; Eswaran, V.; Eswaran, V.; Murali, K. Empowering the Factory of the Future: Integrating Artificial Intelligence, Machine Learning, and IoT Innovations in Industry 6.0. In *Evolution and Advances in Computing Technologies for Industry 6.0*; CRC Press: Boca Raton, FL, USA, 2024; pp. 1–21.
29. Zaritskyi, V.; Shyrokorad, D.; Mancilla, R.O.; oerg Abendroth, J.; Mpantis, A.; Perales, O.G.; Triantafyllou, G.; RDI, A.A.M.; Borgaonkar, R. AI-Driven Access Control System for Smart Factory Devices. In Proceedings of the 2025 IEEE International Conference on Smart Computing (SMARTCOMP), Cork, Ireland, 16–19 June 2025; pp. 264–269.
30. Araujo, M.S.d.; Machado, B.A.S.; Passos, F.U. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. *Appl. Sci.* **2024**, *14*, 2116. [CrossRef]
31. Moriano, P.; Hespeler, S.C.; Li, M.; Mahbub, M. Adaptive Anomaly Detection for Identifying Attacks in Cyber-Physical Systems: A Systematic Literature Review. *Artif. Intell. Rev.* **2025**, *58*, 283. [CrossRef]
32. Edris, E.K.K. Utilisation of Artificial Intelligence and Cybersecurity Capabilities: A Symbiotic Relationship for Enhanced Security and Applicability. *Electronics* **2025**, *14*, 2057. [CrossRef]

33. Al E'mari, S.; Sanjalawe, Y.; Fataftah, F.; Hajjaj, R. Foundations of Autonomous Cyber Defense Systems. In *AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense*; IGI Global Scientific Publishing: Hershey, PA, USA, 2025; pp. 1–34.
34. Guhl, J.; Neuhüttler, J. Resilient Smart Services: A Literature Review. *Procedia Comput. Sci.* **2025**, *253*, 307–322. [CrossRef]
35. Saveljeva, J.; Uvarova, I.; Peiseniece, L.; Volkova, T.; Novicka, J.; Polis, G.; Kristapsone, S.; Vembris, A. Cybersecurity for Sustainability: A Path for Strategic Resilience. In Proceedings of the 2025 IEEE International Conference on Cyber Security and Resilience (CSR), Chania, Greece, 4–6 August 2025; pp. 745–752.
36. Dosumu, O.O.; Adediwin, O.; Nwulu, E.O.; Chibunna, U.B. Carbon Capture and Storage (CCS) in the US: A Review of Market Challenges and Policy Recommendations. *Int. J. Multidiscip. Res. Growth Eval* **2024**, *5*, 1515–1529. [CrossRef]
37. Ahmadirad, Z. The Role of AI and Machine Learning in Supply Chain Optimization. *Int. J. Mod. Achiev. Sci. Eng. Technol.* **2025**, *2*, 1–8.
38. Obreja, D.M.; Rughiniș, R.; Țurcanu, D. What Drives New Knowledge in Human Cybersecurity Behavior? Insights from Bibliometrics and Thematic Review. *Comput. Hum. Behav. Rep.* **2025**, *18*, 100650. [CrossRef]
39. Branchini, L.; Bignozzi, M.C.; Ferrari, B.; Mazzanti, B.; Ottaviano, S.; Salvio, M.; Toro, C.; Martini, F.; Canetti, A. Cogeneration Supporting the Energy Transition in the Italian Ceramic Tile Industry. *Sustainability* **2021**, *13*, 4006. [CrossRef]
40. D'Adamo, I.; Fratocchi, L.; Grosso, C.; Tavana, M. An Integrated Business Strategy for the Twin Transition: Leveraging Digital Product Passports and Circular Economy Models. *Bus. Strategy Environ.* **2025**. [CrossRef]
41. Strang, K.D. Cybercrime Risk found in Employee Behavior Big Data using Semi-Supervised Machine Learning with Personality Theories. *Big Data Cogn. Comput.* **2024**, *8*, 37. [CrossRef]
42. Andrade, A.D. Dancing between theory and data: Abductive reasoning. In *Handbook of Qualitative Research Methods for Information Systems*; Edward Elgar Publishing: Northampton, MA, USA, 2023; pp. 274–287.
43. Madsen, D.Ø.; Berg, T.; Slåtten, K. Four Futures of Industry 6.0: Scenario-Based Speculation Beyond Human-Centric Production. Available at SSRN 5354848 2025. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5354848 (accessed on 20 September 2025).
44. Dupont, B.; Shearing, C.; Bernier, M.; Leukfeldt, R. The Tensions of Cyber-Resilience: From Sensemaking to Practice. *Comput. Secur.* **2023**, *132*, 103372. [CrossRef]
45. Floyd, J.A.; D'Adamo, I.; Wamba, S.F.; Gastaldi, M. Competitiveness and Sustainability in the Paper Industry: The Valorisation of Human Resources as an Enabling Factor. *Comput. Ind. Eng.* **2024**, *190*, 110035. [CrossRef]
46. Boggini, C. Reporting Cybersecurity to Stakeholders: A Review of CSRD and the EU Cyber Legal Framework. *Comput. Law Secur. Rev.* **2024**, *53*, 105987. [CrossRef]
47. Saeed, S.; Gull, H.; Aldossary, M.M.; Altamimi, A.F.; Alshahrani, M.S.; Saqib, M.; Zafar Iqbal, S.; Almuhaideb, A.M. Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications. *Information* **2024**, *15*, 764. [CrossRef]
48. Taleb, N.N.; Douady, R. Mathematical Definition, Mapping, and Detection of (Anti) Fragility. *Quant. Financ.* **2013**, *13*, 1677–1689. [CrossRef]
49. Singh, K.; Chatterjee, S.; Mariani, M.; Wamba, S.F. Cybersecurity Resilience and Innovation Ecosystems for Sustainable Business Excellence: Examining the Dramatic Changes in the Macroeconomic Business Environment. *Technovation* **2025**, *143*, 103219. [CrossRef]
50. Banka, K.; Uchihira, N. Dynamic Capability in Business Ecosystems as a Sustainable Industrial Strategy: How to Accelerate Transformation Momentum. *Sustainability* **2024**, *16*, 4506. [CrossRef]
51. Noor, A.F.M.; Moghavvemi, S.; Tajudeen, F.P. Identifying Key Factors of Cybersecurity Readiness in Organizations: Insights from Malaysian Critical Infrastructure. *Comput. Secur.* **2025**, *159*, 104674. [CrossRef]
52. Thron, E.; Faily, S.; Dogan, H.; Freer, M. Human Factors and Cyber-Security Risks on the Railway—The Critical Role Played by Signalling Operations. *Inf. Comput. Secur.* **2024**, *32*, 236–263. [CrossRef]
53. Allahawiah, S.; Altarawneh, H.; Al-Hajaya, M. The Role of Organizational Culture in Cybersecurity Readiness: An Empirical Study of the Jordanian Ministry of Justice. *Calitatea* **2024**, *25*, 74–84.
54. Jiang, T.; Sun, Z.; Fu, S.; Lv, Y. Human-AI Interaction Research Agenda: A User-Centered Perspective. *Data Inf. Manag.* **2024**, *8*, 100078. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.