ISSN: 2831-6789

Research Article

Journal of Robotics and Automation Research

Towards a Human-Centric Physical Internet: The Next Digital Transition

Franco Maciariello[1,2*], Fabrizio Benelli[3] and Redvin Marku[4]

[1]*New Generations Sensors, 56024, Italy*

[2]*Marketing Area, Santa Maria la Fossa (CE,) Italy*

[3]*Zetta Software Tlc Shpk, Albania*

[4]*Department of Economics and Business, Tirana Business University College, Albania*

[*]Corresponding Author
Franco Maciariello, New Generations Sensors, 56024, Italy.

Submitted: 2025, Nov 24; **Accepted:** 2025, Dec 22; **Published:** 2025, Dec 30

Citation: Maciariello, F., Benelli, F., Marku, R. (2025). Towards a Human-Centric Physical Internet: The Next Digital Transition. *J Robot Auto Res, 6*(4), 01-09.

Abstract

The coming wave of digital transformation will be defined less by technological acceleration in automation and more by the strategic convergence between physical infrastructures, human capabilities and explainable artificial intelligence. Over the past decade, industries have progressively implemented increasingly automated architectures, from smart manufacturing to predictive analytics and robotic platforms. Yet the macro-trend that now emerges across critical infrastructures suggests a shift toward a more distributed, interoperable and ethically driven ecosystem where the Physical Internet, originally conceived for logistics, evolves into a transversal organizational paradigm. In such a view, infrastructures become cognitive systems capable of enabling the secure exchange of information, energy, skills and operational decisions across heterogeneous domains. The Human-centric Physical Internet represents an evolution of digital infrastructures that moves beyond pure automation, aiming instead to preserve the centrality of human agency through transparent and explainable digital mechanisms. This evolution requires a revision of organizational models, business governance and cross-sector digital capabilities in order to ensure trustworthiness, resilience and compliance with emerging regulatory frameworks. Moreover, the need for distributed intelligence and interoperability across energy, public services and industrial ecosystems calls for new human-AI collaboration patterns, where decision-making is shared, explainable and auditable. The article proposes a conceptual framing of this transition, with particular emphasis on human-in-the-loop operational models, distributed infrastructures, and digital sovereignty across the European context

Keywords: Human-AI, Cognitive Enterprise, Physical Internet, Digital Transition, Explainable Intelligence, Human-Centric Infrastructures, Distributed Digital Systems

Acronyms

AI – Artificial Intelligence
XAI – Explainable Artificial Intelligence
PI – Physical Internet
EPI – Energy Physical Internet
IoE – Internet of Energy
DER – Distributed Energy Resources
DSO – Distribution System Operator
TSO – Transmission System Operator
SCADA – Supervisory Control and Data Acquisition
HIL – Human-in-the-Loop
HCI – Human-Centric Infrastructure
DT – Digital Twin
CPS – Cyber-Physical Systems
GDPR – General Data Protection Regulation
NIS – Network and Information Security Directive
KPI – Key Performance Indicator
ENTSO-E – European Network of Transmission System Operators for Electricity
ENISA – European Union Agency for Cybersecurity

IEA – International Energy Agency
WHO – World Health Organization
OECD – Organisation for Economic Co-operation and Development
IEEE – Institute of Electrical and Electronics Engineers
WEF – World Economic Forum
JRC – Joint Research Centre

1. Introduction and Business Context

Digital transition has reached a point where the traditional boundaries between computational systems, industrial infrastructures and human decision-making are increasingly blurred. The acceleration of artificial intelligence and edge-based analytics within critical infrastructures, combined with growing cyber-physical convergence, is redefining the nature of enterprise architectures [1]. Historically, technological innovation in industrial systems followed a trajectory predominantly focused on automation and operational efficiency. However, efficiency-driven automation has proven insufficient to address systemic resilience, sustainability and socio-technical complexity in domains such as energy distribution, healthcare infrastructures and public administration. The transformation underway demands more than incremental technology upgrades. It requires a fundamental reconceptualization of how physical assets, digital platforms and human expertise interact to create value, ensure safety and maintain societal legitimacy.

Over the past five years, multiple reports by European and international institutions have recognized that digital infrastructures must incorporate not only advanced automation capabilities but also explicit mechanisms of explainability, transparency and human empowerment. European regulatory frameworks such as the emerging AI-related directives, the new cyber-resilience strategies and sector-specific digital grid initiatives highlight the need for infrastructures that retain human oversight, accountability and ethical alignment [2,3]. These policy developments reflect a broader shift in industrial expectations, where operational efficiency must be balanced against societal trust, regulatory compliance and long-term resilience. Organizations operating in critical sectors are therefore compelled to integrate cognitive governance mechanisms into their digital transformation roadmaps, ensuring that automation serves human decision-makers rather than displacing them.

This changing scenario reveals the emergence of a strategic driver: designing infrastructures that enable human and artificial intelligence to interact as co-decision makers, particularly in critical sectors where risk exposure, societal impact and ethical responsibility are structurally higher. The Physical Internet paradigm, traditionally associated with logistics and supply chain interoperability, now offers a broader conceptual foundation to articulate a multi-sector, distributed and human-centric transformation of digital infrastructures. By extending the Physical Internet beyond logistics into energy systems, healthcare networks and public service platforms, organizations can envision a future where distributed intelligence operates within transparent governance frameworks, preserving human authority while enabling autonomous coordination across complex systems.

The objective of this article is to define a conceptual framing for a Human-centric Physical Internet, providing executives, technology leaders and policy stakeholders with an interpretative model capable of explaining how the next phase of digital transformation could evolve beyond traditional automation. The focus is therefore managerial and strategic, adopting the perspective of industrial organization, business governance and ING-IND/35 conceptual frameworks. This article does not propose a technical implementation blueprint but rather articulates a vision that can guide strategic planning, investment decisions and organizational transformation initiatives across sectors. In this sense, the Physical Internet can be interpreted as a structural enabler of distributed infrastructures, while explainable AI acts as the cognitive layer. The interaction of these two dimensions generates a shift from isolated operational platforms to ecosystems capable of supporting distributed decision-making while preserving human agency and societal accountability.

1.1 The Convergence of Automation, AI and Physical Infrastructures

Automation has historically been perceived as the principal path toward digital maturity. Industrial robotics, automated operations management and algorithmic optimization have delivered substantial productivity gains in multiple sectors, particularly in manufacturing and logistics. Nonetheless, the last decade has demonstrated that automation alone is not the endpoint of digital transformation. Instead, infrastructures are increasingly expected to incorporate mechanisms of trust, interoperability, resilience and human-AI alignment, particularly in critical sectors where failures have cascading societal consequences. The evolution toward cognitive infrastructures reflects a recognition that technology must serve broader organizational, ethical and societal objectives beyond pure operational efficiency.

Recent analyses by global consultancies show that digital transformation success increasingly depends on explainability, accountability and governance capabilities rather than on purely technological deployment. For example, energy utilities deploying automated grid balancing systems must also guarantee explainability for regulatory compliance and public trust. Healthcare systems adopting predictive analytics must ensure human oversight and ethical validation of clinical decision paths. These real-world constraints reveal that purely automated infrastructures are structurally unable to ensure societal and regulatory sustainability, especially when decisions have a direct impact on citizens, urban planning, environmental sustainability or national security. Consequently, organizations must integrate cognitive governance mechanisms into their transformation strategies, ensuring that digital systems remain auditable, transparent and aligned with human values [4-6].

The transformation toward the Physical Internet therefore requires a revision of organizational assumptions, shifting from automated infrastructures to human-centric cognitive infrastructures. Such a transition is not only technical; it entails substantial governance redesign. For instance, the implementation of interoperable and distributed infrastructures necessitates new cross-sector governance models, shared data architectures and convergent policy frameworks capable of supporting multi-domain decision-making under uncertainty. In this sense, EU digital grid initiatives, ENTSO-E development routes and national cybersecurity frameworks provide a contextual environment in which the Human-centric Physical Internet can gradually evolve [7,8]. These institutional frameworks create the regulatory scaffolding necessary for organizations to adopt distributed cognitive architectures while maintaining accountability, digital sovereignty and societal legitimacy. Organizations that successfully navigate this transition will position themselves as leaders in the next generation of digital infrastructure management.

1.2 Human-AI Collaboration in Critical Infrastructures

A fundamental element of the Human-centric Physical Internet is the explicit inclusion of human-AI collaboration mechanisms. While traditional automation focuses on reducing human intervention, the Human-centric Physical Internet explicitly re-introduces human expertise as a strategic asset. This paradigm shift recognizes that complete automation is neither technically feasible nor socially desirable in domains where decisions carry significant ethical, safety or societal implications. Instead, human-AI collaboration enables organizations to leverage the computational power of artificial intelligence while preserving the contextual judgment, ethical reasoning and strategic oversight that only human operators can provide.

In energy infrastructures, for example, human operators must supervise AI-driven balancing systems, particularly when the system operates near critical thresholds or under high uncertainty caused by variable renewable energy. In healthcare infrastructures, human clinicians must validate AI-driven diagnostic recommendations, ensuring that algorithmic outputs are consistent with clinical evidence, patient history and ethical medical practice. In logistics, human experts may supervise and reassess autonomous routing under unexpected disruptions, such as extreme weather events, geopolitical instability or supply chain shocks. These scenarios illustrate that human oversight is not a temporary concession to technological immaturity but a permanent structural requirement for trustworthy and accountable digital infrastructures.

The reason is not technological immaturity alone. Rather, human oversight is structurally required as a mechanism of responsibility, trust, social acceptability and ethical legitimacy. As international institutions emphasize, the absence of human explainability would render digital infrastructures incompatible with democratic, regulatory and societal expectations. This requirement reshapes the strategic meaning of digital infrastructure maturity. Whereas traditional maturity models prioritized automation and performance indicators, future maturity must integrate explainability, accountability, sovereignty and human-centric resilience as foundational dimensions. Organizations that embrace this shift will be better positioned to secure regulatory approval, public trust and long-term operational sustainability in an increasingly complex and interconnected digital ecosystem [9].

1.3 Light Literature and Practice Review

Emerging literature identifies the growing need for multi-layer digital infrastructures combining distributed sensing, edge analytics and explainable AI governance. Academic contributions have progressively recognized the limitations of purely automated cyber-physical infrastructures, stressing resilience, human-centric design and explainability as prerequisites for ethical AI adoption. These scholarly works provide important conceptual foundations for understanding how digital infrastructures must evolve to meet societal expectations, regulatory requirements and ethical standards. However, the literature remains largely fragmented across disciplinary boundaries, with limited integration between engineering, organizational science and policy analysis perspectives [10-12].

Reports from global organizations such as the European Commission, ENISA and WHO consistently observe that critical infrastructures must adopt new digital resilience paradigms that explicitly integrate human oversight and transparency. Additionally, industrial whitepapers highlight that explainability and transparency are increasingly considered business requirements rather than optional technical features. These institutional and industry reports reflect a growing consensus that digital transformation in critical sectors must prioritize trust, accountability and human empowerment alongside traditional metrics of efficiency and automation. Organizations that fail to address these dimensions risk regulatory non-compliance, public backlash and operational vulnerabilities [13-16].

Recent energy studies show that interoperable and explainable grid architectures significantly improve resilience and operational safety under distributed generation conditions. In logistics, Physical Internet research confirms the advantages of interoperable and shared infrastructures for cost reduction, resilience and sustainability. The extension of these principles beyond logistics, into energy and public services, introduces an organizational interpretation of the Physical Internet, evolving from an operational concept to a strategic infrastructure paradigm. This evolution suggests that the Physical Internet can serve as a unifying framework for conceptualizing the next generation of distributed, interoperable and human-centric digital infrastructures across multiple sectors [17-21].

Consultancy reports converge in identifying explainability, trust, and governance as key drivers of digital adoption, particularly in organizations operating critical infrastructures or regulated domains [22,23]. At the same time, early industrial deployments of distributed architectures, digital grids and explainable analytics reveal the feasibility of human-centric models at operational scale, although implementation remains

heterogeneous across sectors. Collectively, these contributions suggest that Physical Internet evolution requires interoperability, distributed cognitive architectures, human-AI collaboration, trust-enhancing explainability and cross-sector governance. Yet, academic formalization remains at an early stage, and the literature primarily offers domain-specific insights rather than cross-sector frameworks. The purpose of this article is to fill this analytical gap by proposing an integrated conceptualization of Physical Internet as a multi-sector, cognitive and human-centric infrastructure paradigm.

2. Business Methodology and Conceptual Framework

2.1 Conceptualizing the Human-Centric Physical Internet

The Human-centric Physical Internet can be defined as an interconnected ecosystem of physical infrastructures, digital platforms, and explainable cognitive mechanisms capable of coordinating distributed operations across multiple domains while preserving human authority, ethical alignment and societal trust. This interpretation extends the traditional notion of the Physical Internet beyond logistics toward an integrated socio-technical paradigm where infrastructure nodes interact through transparent, auditable and interoperable mechanisms. These mechanisms are cognitive rather than purely operational, embedding human context, ethical considerations and regulatory constraints into digital decision paths.

In practice, the Human-centric Physical Internet requires that physical infrastructures adopt new digital architectures that support distributed intelligence while guaranteeing explainability at every level of decision-making, from local edge nodes to regional supervisory systems. Organizations implementing this paradigm must redesign their governance structures, operational workflows and technological platforms to ensure that human oversight remains structurally embedded throughout the system. This approach represents a fundamental departure from traditional automation strategies, which typically sought to minimize human involvement in operational processes. Instead, the Human-centric Physical Internet positions human expertise as an indispensable component of system intelligence, enabling contextual interpretation, ethical validation and strategic decision-making that cannot be delegated to algorithms alone.

2.2 Dimensions of the Conceptual Framework

The framework proposed by this article is articulated along six foundational dimensions that collectively define the maturity and effectiveness of human-centric digital infrastructures. Each dimension represents a critical capability that organizations must develop to successfully implement the Physical Internet paradigm across critical sectors.

Interoperability describes the capacity of infrastructures to interact across domains, standards and regulatory contexts. Interoperability is not limited to data exchange; it includes semantic, operational and governance interoperability enabling cross-sector decision-making. Organizations must adopt common protocols, shared data models and coordinated governance frameworks that facilitate seamless information flow across organizational and sectoral boundaries. Without robust interoperability mechanisms, distributed infrastructures remain fragmented silos incapable of achieving system-level optimization or resilience.

Explainability refers to the capacity of infrastructures to expose decision processes in transparent, auditable and human-understandable formats. Explainability should be conceived as a governance function, not merely a technical requirement. Organizations must implement explainability mechanisms that enable human operators, regulators and stakeholders to understand how and why specific decisions were made by digital systems. This capability is essential for maintaining trust, ensuring accountability and complying with emerging regulatory frameworks that mandate transparent algorithmic decision-making.

Human-in-the-loop emphasizes the presence of human decision-makers within critical workflows. Human involvement becomes a structural element of cognitive validation, ethical oversight and contextual interpretation. Rather than relegating humans to passive monitoring roles, human-in-the-loop architectures position human expertise at strategic intervention points where contextual judgment, ethical reasoning and experience-based intuition provide value that algorithms cannot replicate.

Distributed infrastructures refer to the architecture of sensing, computation and decision-making distributed across edge and cloud systems, rather than centralized automation. Distributed architectures enable local intelligence, reduce latency, enhance resilience and improve responsiveness to dynamic conditions. Organizations adopting distributed infrastructures must develop new capabilities in edge computing, federated learning and distributed coordination protocols.

Resilience highlights the capacity of infrastructures to preserve operational continuity under uncertainty, variability or cyber-physical risk, leveraging distributed cognition and human oversight. Resilient infrastructures can adapt to unexpected disruptions, recover from failures and maintain essential services even under adverse conditions. This capability requires not only technical redundancy but also cognitive flexibility, enabling human operators and AI systems to collaboratively respond to novel challenges.

Digital sovereignty refers to the strategic necessity of maintaining technological autonomy, governance control and regulatory alignment, particularly across infrastructures considered critical for public security and national resilience. Organizations must ensure that their digital infrastructures remain under their own control, free from undue external influence or dependency on foreign technologies that could compromise security, privacy or strategic interests. Together, these dimensions enable the transition from automated infrastructures to cognitive infrastructures capable of negotiating multi-domain interactions while preserving human responsibility and societal legitimacy.

2.3 Human-Centric Maturity Model

The maturity model is articulated into four levels. Although described linearly, these levels should not be interpreted as rigid stages; sectors may evolve asymmetrically and exhibit hybrid configurations. Nonetheless, the model provides a conceptual scaffold to analyze cross-sector readiness and alignment with emerging European policy directions and industrial digitalization trajectories.

2.3.1 Level 1 – Traditional Digital: At this stage infrastructures are partially digitalized but remain siloed, fragmented and often characterized by legacy systems designed for cost efficiency or automation within narrow functional domains. Human operators retain central responsibility, while digital systems provide limited situational awareness. Data access, interoperability and explainability remain marginal attributes, typically addressed through ad-hoc integration initiatives. Traditional digital infrastructures enhance operational performance but do not enable cognitive decision-making across domains or critical sectors. Organizations at this level face significant challenges in scaling digital initiatives beyond departmental boundaries and struggle to achieve system-level optimization.

2.3.2 Level 2 – Interoperable Infrastructures: This level corresponds to an evolution in which infrastructures begin to expose interoperable interfaces, shared data schemas and real-time interconnection across heterogeneous nodes. For instance, energy distribution networks may integrate with distributed generation data, logistics platforms may exchange information with urban mobility systems, and healthcare infrastructures may adopt shared data standards for cross-institutional diagnosis. Yet explainability and human-in-the-loop mechanisms are still partial; decision-making relies predominantly on automation and performance-driven algorithms, without structured governance mechanisms for human oversight. Organizations at this level benefit from improved coordination and data sharing but lack the transparency and accountability mechanisms necessary for sustainable operation in high-stakes environments.

2.3.3 Level 3 – Explainable Infrastructures: At this stage infrastructures introduce human-AI collaboration and transparent decision-making, enabling human supervision through explainable outputs, auditable logs and ethical safeguards. Explainability becomes a design principle rather than a compliance afterthought. This level represents the shift in which digital infrastructures must demonstrate trustworthiness, fairness and accountability to institutional and regulatory stakeholders. Moreover, distributed decisioning capabilities begin to emerge, particularly through edge intelligence and domain-specific cognitive mechanisms such as local grid balancing or context-aware triage, creating the foundations for distributed resilience. Organizations at this level can justify their decisions to regulators, earn public trust and operate with greater confidence in complex, uncertain environments.

2.3.4 Level 4 – Cognitive Infrastructures: The highest level is characterized by autonomous but human-supervised infrastructures capable of anticipatory reasoning, context learning and socio-technical alignment. Human-AI interaction becomes systemic, with operators assuming strategic oversight rather than direct operational control. Digital sovereignty is not a peripheral concern but a structural component of governance frameworks, particularly in critical sectors exposed to geopolitical, cyber and regulatory risks. The Physical Internet becomes a distributed cognitive ecosystem where infrastructures negotiate decisions within human-defined boundaries and under transparent governance constraints. Organizations at this level represent the future state of digital infrastructure management, where technology serves human objectives while maintaining societal legitimacy and ethical alignment.

3. Comparative Evidence

The following tables provide indicative values and conceptual comparisons derived from primary and secondary data sources, including EU digitalization indicators, ENTSO-E and IEA assessments, McKinsey and BCG studies, and industrial whitepapers associated with energy, logistics and healthcare infrastructures. These values must be interpreted as qualitatively indicative rather than statistically exhaustive. Their purpose is to illustrate macro-level sectoral differences relevant from a strategic and ING-IND/35 lens. The evidence suggests that different sectors exhibit varying levels of digital maturity, interoperability and explainability readiness, reflecting structural differences in regulatory frameworks, legacy systems and organizational culture.

Domain	Current Digital Level	Interoperability Status	Explainability Readiness
Energy Distribution	Level 2-3 (Interoperable to Explainable)	Advanced (smart grids, DER integration)	Medium (regulatory push for transparency)
Healthcare Systems	Level 1-2 (Traditional to Interoperable)	Limited (privacy constraints, data silos)	High need (clinical validation required)
Logistics Networks	Level 2-3 (Interoperable to Explainable)	Advanced (Physical Internet pioneers)	Medium (operational transparency valued)
Public Services	Level 1-2 (Traditional to Interoperable)	Emerging (institutional fragmentation)	High need (democratic accountability)

Table 1: Digitalization Levels Across Physical Domains (Indicative)

The evidence presented in Table 1 indicates that energy distribution and logistics networks have achieved higher levels of digital maturity compared to healthcare and public services. This disparity reflects differences in regulatory pressure, investment priorities and organizational culture. Energy systems benefit from strong European policy support for smart grid development and renewable integration, while logistics networks have been early adopters of interoperable platforms driven by competitive pressure and efficiency imperatives. In contrast, healthcare systems face significant barriers to interoperability due to privacy regulations, institutional fragmentation and risk-averse clinical cultures. Public services struggle with legacy systems, budget constraints and complex multi-stakeholder governance structures that slow digital transformation.

Notably, all sectors demonstrate growing recognition of the need for explainability, though implementation remains uneven. Healthcare and public services face particularly strong explainability requirements due to ethical and democratic accountability concerns, while energy and logistics systems are increasingly adopting transparency mechanisms to comply with regulatory frameworks and build stakeholder trust. These sectoral patterns suggest that the evolution toward cognitive infrastructures will proceed at different paces across domains, with energy and logistics likely leading the transition while healthcare and public services follow as governance frameworks mature and enabling technologies become more accessible.

PI Principle	Value for Utilities	Value for Public Admin	Value for Citizens
Interoperability	Operational continuity, reduced integration costs	Service integration, cross-agency coordination	Better access, seamless services
Distributed Intelligence	Enhanced resilience, faster response	Emergency management, local autonomy	Service reliability, safety
Explainability	Regulatory compliance, stakeholder trust	Accountability, transparency	Trust, informed participation
Cognitive Resilience	System stability, risk mitigation	Crisis management, continuity	Safety, protection
Digital Sovereignty	Strategic control, vendor independence	National security, policy autonomy	Data protection, rights preservation

Table 2: Physical Internet Principles and Stakeholder Value

Table 2 illustrates how the core principles of the Physical Internet generate differentiated value across stakeholder groups. Interoperability delivers operational efficiencies for utilities, coordination benefits for public administrators and service accessibility for citizens. Distributed intelligence enhances resilience for infrastructure operators while improving emergency response capabilities and service reliability. Explainability strengthens regulatory compliance and stakeholder trust for utilities, enables democratic accountability for public administrators and builds citizen confidence in digital systems. Cognitive resilience supports system stability for operators, crisis management for governments and safety for citizens. Digital sovereignty provides strategic control for utilities, policy autonomy for governments and data protection for citizens. These value propositions demonstrate that the Human-centric Physical Internet addresses not only technical challenges but also governance, trust and societal legitimacy concerns across multiple stakeholder dimensions.

4. Conceptual Roadmap

The following conceptual roadmap illustrates the progressive evolution from traditional automation toward human-centric cognitive infrastructures. This visualization represents a strategic pathway rather than a prescriptive timeline, as different sectors and organizations will advance at different paces depending on their starting positions, resources and regulatory contexts. The roadmap emphasizes that technical sophistication alone is insufficient; socio-technical and institutional alignment is required to ensure long-term sustainability, especially within critical infrastructures subject to public accountability and regulatory oversight.

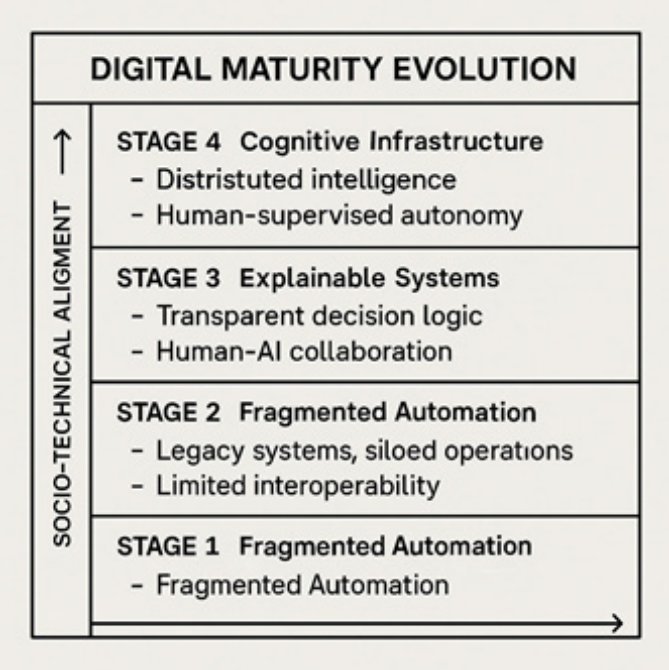

Figure 1: Evolution Roadmap – From Automation to Cognitive Infrastructure

The roadmap demonstrates that the evolution toward cognitive infrastructures requires simultaneous advancement across technical, organizational and governance dimensions. Organizations cannot simply upgrade technology and expect to achieve cognitive maturity; they must also develop new competencies, redesign governance structures and establish trust-building mechanisms that enable human-AI collaboration. The vertical axis represents increasing socio-technical alignment with human-centric values such as transparency, accountability and ethical oversight. Organizations at Stage 1 exhibit low alignment despite potentially sophisticated automation, while organizations at Stage 4 demonstrate high alignment through explicit human-AI collaboration mechanisms, explainable decision processes and embedded digital sovereignty principles. The transition from Stage 1 to Stage 4 typically requires multi-year transformation initiatives spanning technology deployment, organizational change management and stakeholder engagement.

5. Managerial and Societal Implications

5.1 Implications for Utilities and Energy Operators

Utilities and energy system operators sit at the centre of European digital transformation strategies. Over the last decade, smart grid programs, distributed generation and renewable integration have compelled operators to shift from centralized control to distributed coordination. The Human-centric Physical Internet reinforces this evolution by demanding interoperable infrastructures, transparent decision paths and cognitive resilience. Utilities must therefore adopt governance models capable of accommodating distributed intelligence, ensuring that human operators maintain supervisory authority even when automated balancing, load prediction or grid segmentation operate autonomously.

This has direct implications for workforce competencies, requiring operators to combine engineering expertise with cognitive analytics skills and regulatory knowledge. It also reshapes operational risk profiles as resilience is no longer about mechanical redundancy but about the capacity to reason across distributed digital layers under uncertainty. In this sense, explainability becomes a structural requirement for regulatory alignment, particularly in Europe where grid transparency and data traceability are increasingly mandated by institutional frameworks. Utilities that successfully integrate human-centric principles into their digital strategies will gain competitive advantages through enhanced regulatory compliance, improved stakeholder trust and superior operational resilience.

5.2 Implications for Healthcare Systems

Healthcare systems represent one of the most sensitive domains for human-AI collaboration. Digital transformation in hospitals, clinics and national health infrastructures remains uneven, constrained by data privacy, ethical considerations and institutional fragmentation. The Human-centric Physical Internet enables a gradual transition toward interoperable digital health ecosystems, where diagnostic platforms, clinical systems and public health infrastructures can exchange information through explainable and distributed cognitive mechanisms.

However, the implications are profound. Human-in-the-loop becomes essential as clinicians must retain authority over diagnostic and therapeutic decisions even as predictive analytics and cognitive triage systems become ubiquitous. Explainability is not merely a regulatory requirement but a professional necessity, enabling clinicians to understand the rationale behind AI-generated insights and integrate them into medical judgment. Governance must therefore incorporate ethical, clinical and cognitive considerations, not just technical ones. The ultimate implication is an evolution toward cognitive healthcare systems where patient safety, transparency and human authority remain structurally embedded.

5.3 Implications for Citizens and Society

The Human-centric Physical Internet ultimately impacts citizens as final recipients of digital services and as sources of data within distributed systems. Citizens benefit from reliable infrastructures, more resilient services and transparent decision paths. However, trust becomes a central issue as citizens must trust that cognitive infrastructures operate under clear ethical rules, protect privacy and maintain human oversight. This implies that societal expectations must be integrated into digital governance frameworks. Cognitive infrastructures must demonstrate fairness, transparency and public accountability. Citizen trust becomes an operational parameter, not only a political expectation. Digital sovereignty, data ethics and explainability thus emerge as societal necessities rather than abstract regulatory concepts [24]. Organizations that prioritize these dimensions will be better positioned to maintain social license to operate and achieve long-term sustainability.

6. Consulting Pill and Executive Takeaways

Organizations operating critical infrastructures must recognize that the Human-centric Physical Internet demands a structural shift toward interoperable and explainable architectures. This shift cannot be reduced to incremental technology upgrades; it requires strategic redesign, cognitive governance and human-AI integration embedded in every operational layer. Executives should treat this transformation as a multi-year strategic initiative rather than a short-term technology project, allocating resources not only to technical implementation but also to organizational change management, competency development and stakeholder engagement.

Explainability becomes a managerial asset rather than a technical detail. Executives must treat transparent decision-making as a mechanism to secure regulatory alignment, societal trust and organizational resilience. Without explainability, distributed intelligence cannot scale safely across sectors. Organizations should invest in explainability frameworks, natural-language explanation systems and audit mechanisms that enable human operators and external stakeholders to understand algorithmic decision processes. This investment pays dividends through improved regulatory compliance, enhanced stakeholder trust and reduced operational risk.

Human-AI collaboration should be reframed as a shared cognitive

process rather than a supervision task [25]. Human-in-the-loop is not simply a safety requirement but a source of contextual intelligence, ethical interpretation and adaptive reasoning that AI alone cannot provide. Organizations should design workflows that position human expertise at strategic intervention points, enabling operators to provide contextual judgment while leveraging AI computational power. This approach maximizes the complementary strengths of human and artificial intelligence.

Organizations must develop cognitive competencies capable of interpreting algorithmic outputs, redesigning workflows and governing distributed infrastructures. Skills in digital ethics, AI auditing, cyber-physical risk and cross-sector integration become essential managerial capabilities. Human resource strategies should prioritize recruitment and training programs that build these competencies across technical, operational and executive levels. Organizations that successfully develop cognitive capabilities will gain competitive advantages through superior decision quality, faster adaptation and better risk management.

Digital sovereignty must be strategically embedded into infrastructure planning. As infrastructures become increasingly interconnected, organizations must ensure control over data, algorithms and governance processes to mitigate systemic risks and maintain public legitimacy. This requires careful vendor management, strategic technology choices and governance frameworks that preserve organizational autonomy while enabling beneficial collaboration with external partners.

The adoption of cognitive infrastructures should be accompanied by cross-sector governance agreements that ensure coherent standards, interoperable platforms and shared ethical baselines. Without such alignment, cognitive infrastructures may fragment into incompatible islands, undermining resilience and societal benefits. Industry associations, regulatory bodies and standards organizations should collaborate to establish governance frameworks that enable interoperability while respecting organizational autonomy and competitive dynamics.

Executives should interpret the Human-centric Physical Internet as a long-term organizational transformation, where trust, systemic resilience and socio-technical coherence become the strategic metrics of digital maturity. Traditional metrics focused on automation levels, cost reduction and efficiency gains remain relevant but must be complemented by measures of explainability, human-AI collaboration effectiveness and stakeholder trust. Organizations that adopt this broader view of digital maturity will be better positioned to navigate the increasingly complex landscape of critical infrastructure management in the cognitive era.

7. Conclusions and Future Directions

The Human-centric Physical Internet represents an evolutionary step in the digital transformation of critical infrastructures. It shifts attention from automation to cognitive collaboration, from digitalization to explainability, and from efficiency to societal resilience. Organizations adopting this paradigm must integrate human-in-the-loop mechanisms, transparent governance frameworks and distributed decision-making capabilities into their operational models. This transformation is not merely technological but fundamentally organizational and cultural, requiring changes in mindset, processes and power structures across multiple organizational levels.

Future trajectories indicate an increasing convergence between cognitive infrastructures and sustainable societal priorities. As energy systems become more dynamic, healthcare systems more data-driven, logistics more interoperable and public administrations more connected, the need for transparent cognitive decision processes becomes even more urgent. The Physical Internet provides a structural foundation for this convergence by enabling transparent and interoperable interactions across domains. Organizations that recognize this trajectory and position themselves accordingly will gain first-mover advantages in what promises to be a fundamental reshaping of critical infrastructure management.

Explainability will continue to evolve as the most critical requirement for AI deployment in critical infrastructures. In the future, organizations will adopt advanced cognitive dashboards, natural-language explanations and automated audits that help translate algorithmic reasoning into human-interpretable narratives. Digital sovereignty will also become central, ensuring that infrastructures remain aligned with national and European strategic interests. The convergence of explainability and sovereignty creates a new foundation for trustworthy digital transformation that respects both technical efficiency and democratic values [26,27].

Over the next decade, the expansion of cognitive infrastructures will likely progress through three directions: the institutionalization of explainability frameworks within regulated sectors; the emergence of distributed cognitive grids supported by edge intelligence; and the convergence of human-AI decision models that balance efficiency with societal responsibility. As these transformations unfold, organizations capable of integrating cognitive governance with strategic foresight will be best positioned to navigate the new digital landscape. The Human-centric Physical Internet thus represents not an endpoint but a conceptual framework for ongoing evolution, providing a strategic lens through which organizations can interpret emerging technologies, anticipate regulatory developments and design transformation initiatives that balance technological advancement with human-centric values and societal legitimacy.

References

1. Benelli, F., Maciariello, F., & Salvadori, C. (2024). The influence of technologies on organizational culture in innovative SMEs.
2. European Commission. (2023). Digitalisation of critical infrastructures: Policy framework and strategic directions.
3. Platform, E. E. T. (2022). European network of transmission system operators for electricity.
4. McKinsey & Company. (2023). AI in critical infrastructure:

Strategic implications for utilities and public systems.
5. International Energy Agency. (2024). Digitalization and energy: Technology report 2024.
6. World Health Organization. (2025). Global Strategy on Digital Health 2020-2027. World Health Organization.
7. European Union Agency for Cybersecurity. (2023). Cybersecurity challenges in critical energy infrastructure.
8. European Commission, Joint Research Centre. (2024). Data governance for energy systems: Technical assessment.
9. Organisation for Economic Co-operation and Development. (2023). Artificial intelligence in society: Foresight report.
10. IEEE. (2023). Standards for ethical AI systems in critical domains (IEEE Standard 7000).
11. Energy, A. W. (2024). Edge driven Digital Twins in distributed energy systems.
12. Boston Consulting Group. (2023). Distributed digital systems: The next wave of infrastructure innovation.
13. World Economic Forum. (2024). Trustworthy AI for public systems: Framework and guidelines.
14. Gartner. (2024). Explainable AI: Market forecast and technology assessment 2024–2028.
15. Accenture. (2023). Cognitive infrastructure study: Organizational transformation in the digital age.
16. Deloitte. (2024). AI governance for societal systems: Best practices and case studies.
17. Capgemini Research Institute. (2024). Data-driven public services: European benchmarking study.
18. IBM Institute for Business Value. (2023). Cognitive enterprises and operational models: Industry survey.
19. Benelli, F., Këlliçi, E., Maciariello, F., & Stile, V. (2025). Artificial Intelligence for Decentralized Orchestration in the Physical Internet: Opportunities, Business Trade-offs, and Risks in Road Freight Logistics. In Conference Book of Abstract of the 4th International Conference Creativity And Innovation In Digital Economy (CIDE 2025).
20. Maciariello, F., Benelli, F., Sangiuolo, G., Lorenzi, E., Caponio, C., & Salvadori, C. (2025, September). TrackOne: Smart Logistics for a Sustainable and Interoperable Agricultural Supply Chain in the Era of Digitization. In 2025 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-7). IEEE.
21. Benelli, F., Maciariello, F., Marku, R., & Stile, V. (2025). Towards an Energy Physical Internet: Open Business Models and Platforms for Electricity Distribution Enabled by IoT, Blockchain, and Conditional Payments. In Conference Book of Abstracts of the 4th International Conference Creativity and Innovation In Digital Economy (CIDE 2025). Universitatea Petrol-Gaze (UPG).
22. European Commission, Directorate-General for Communications Networks, Content and Technology. (2024). Digital sovereignty in the EU: Policy framework.
23. European AI Observatory. (2024). Explainable intelligence framework: Technical guidelines and best practices.
24. Benelli, F., Këlliçi, E., Maciariello, F., Salvadori, C., & Stile, V. (2025). Enhance Student Well being and Digital Literacy with Machine Learning and Spatial Analysis. In The 2nd Workshop on Education for Artificial Intelligence (EDU4AI 2025).
25. Benelli, F., Maciariello, F., Salvadori, C., Kelliçi, E., & Stile, V. (2025). Human-AI Collaboration in SMEs: A Role-Sensitive Framework for Cognitive Enterprise Hubs. In Proceedings of the 22nd Conference of the Italian Chapter of the Association for Information Systems (ITAIS 2025).
26. Benelli, F., Caronna, M., Këlliçi, E., & Maciariello, F. (2025). Leveraging the urban physical internet for sustainable heritage management: Edge AI, federated learning, and digital twins. In HERITAGE CAPITALISATION AND DEVELOPMENT-IDENTITY, INNOVATION, DIGITALISATION, ENVIRONMENT, AWARENESS AND SECURITY" HERITAGE–IIDEAS.
27. MIT Technology Review Insights. (2024). Human-AI interaction research digest: Current state and future directions.

List of Acronyms

Copyright: *©2025 Franco Maciariello, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*