Digitalisation scenarios and automation for IT sector

Polish Digital Resilience Agenda 2040 - a model of strategic preparedness for the antinomies of digitalisation.

Visions of the future 2025–2040: From biological integration to systemic reconfiguration

Date
February 2025

Scope
Global / IT

Scenarios
4 Models

Agenda

01

Foundations

Common elements of the scenarios

Analysis of technological foundations, common time phases (2025-2040) and universal challenges and paradoxes of transformation.

02

Comparison

Comparative matrix

A detailed summary of four scenarios in key dimensions: the role of the state, corporations, corporations, property, identity and economics. economics.

03

Details

Scenario characteristics

An in-depth analysis of each of the 4 models: from techno-optimistic integration to dystopian reconfiguration.

04

Synthesis

Conclusions and implications for IT

Summary of key findings and practical strategic recommendations for the IT sector and technology leaders.

Technological foundations

Underlying technologies (appear in all scenarios)

Digital identity
Based on blockchain and biometrics, the foundation of digital trust.

Health diagnostics
Biosensors and AI monitoring 200+ biomarkers in real time.

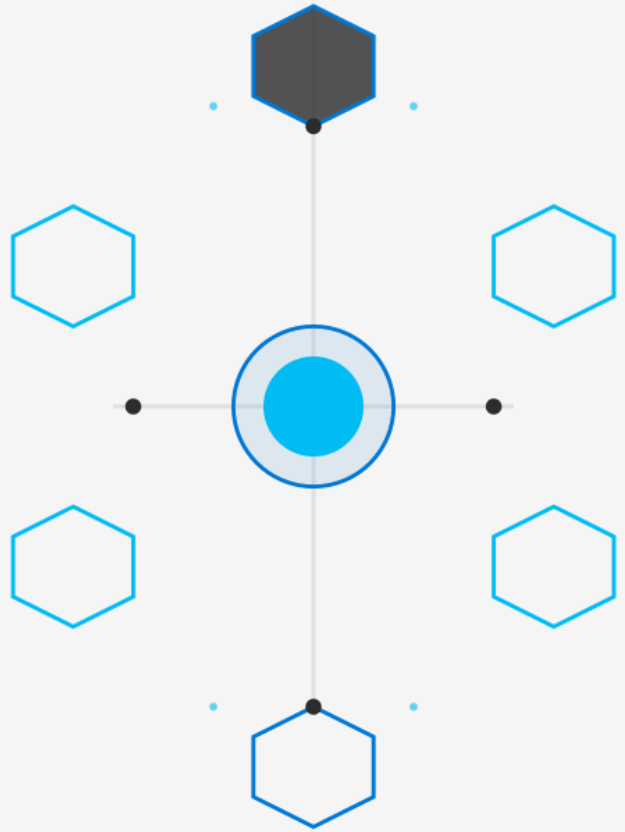
Post-quantum cryptography
Security resistant to future quantum computer attacks.

Brain-computer interfaces (BCI)
Direct communication and cognitive augmentation (expanding the capabilities of the mind).

Metaverse
A socio-economic space integrating physical and virtual worlds.

Artificial intelligence
Advanced predictive analytics and decision automation.

Internet of Things (IoT)
Ubiquitous sensors and digital twins of physical objects.



Common time phases 2025–2040

2025 – 2030

Phase I

Foundations and genesis of transformation

- Technology pilots and early implementations
- Creating interoperability standards
- Building the base infrastructure (Web (Web 4.0)
- The beginnings of digital identity

2030 – 2035

Phase II

Integration and consolidation of power

- Full system interoperability
- Scaling solutions to a global level
- Crystallization of the regulatory framework
- Mass adaptation of BCI interfaces

2035 – 2040

Phase III

Systemic maturity and the new order

- The emergence of a new social order
- Stabilization of value models (post-capitalism)
- Full bio-digital fusion
- Autonomous system management

Common challenges (2025–2040)

Paradox: privacy vs. security

The fundamental tension between the individual's right to anonymity and the security requirements of critical systems. Is blockchain identity protection or ultimate surveillance?

Digital inequality

Social stratification related not only to access to technology, but also to the competences to use it. The risk of creating a "digitally excluded" caste in the bio-tech world.

Biological-digital convergence

Blurring the boundaries between body and technology. Ethical challenges of BCI implants, biosensors and gene editing. Defining humanity in the era of cognitive augmentation.

Work transformation

Mass automation of cognitive processes by AI. by AI. Redefining the concept of "work", the the need for constant reskilling and the debate debate on the Guaranteed Income (UBI).

Comparison matrix (part 1)

Dimensions/Scenarios	SC1: Integration Digital-Biological	SC2: Convergence Seven Vectors	SC3: Cyber Transformation Sectoral	SC4: Reconfiguration DYSTOPIA
Dimension I The role of the state	Centralized superstate Controls identity and constitutes the subjectivity of citizens.	Emergent State Coordinator/"gardener". Defines standards, does not control directly.	Predictive state Algorithmic management. Proactive action based on analytics.	Eroded state Loss of regulatory capacity. Subordination to corporations.
Dimension II The role of corporations	Cyber-states They manage the metaverse, but cooperate closely with public administration.	Ecosystem creators Market competition within imposed public standards.	Surveillance Capitalists Domination through control of technical standards and data.	Digital Lords Total domination. Taking over traditional state functions.
Dimension III Ownership model	Digital Feudalism Ownership of digital assets, heavily regulated by the state.	Sharing economy Fractional ownership, NFT 2.0, product passports (DPP).	Relational property Temporal and contextual, allocated algorithmically.	Corporate neo-feudalism Subscription model ("everything as a service"). Zero real ownership.
Dimension IV Identity	Centralization + Web 4.0 National identity, decentralized transactions.	Self-Sovereign (SSI) Entity controls the disclosure of attributes.	State blockchain Central control and total monitoring of the citizen.	Privacy 2.0 Paradox: surveillance defined as a "new form of privacy".

Comparison matrix (part 2)

Dimensions/Scenarios	SC1: Integration Digital-Biological	SC2: Convergence Seven Vectors	SC3: CyberTransf. Sectoral	SC4: Reconfiguration DYSTOPIA
Dimension V **Vision of society**	**Functional stratification** Division into elites, middle class (owners of NFT assets) and the digital precariat. Stability at the price of hierarchy.	**Hybrid society** The tension between the "hyperconnected" and the "selectively present." An attempt to maintain the work-life-tech balance.	**Bifurcation of reality** Physical separation: elites in premium "offline" spaces, masses in the Metaverse.	**Total dystopia** Biomedical apartheid. Hyperalienation of individuals. UBI as a means of social pacification.
Dimension VI **Data control**	**Duality of control** The state strictly controls the citizen's identity, and corporations have access to transaction data.	**Differential privacy** Federated learning (locally trained AI). Data remains decentralized and under user control.	**Selective monitoring** The state monitors areas critical to infrastructure security, the rest in the commercial sphere.	**Total extraction** Data-for-services model. No privacy. Biometric and behavioral data are currency.
Dimension VII **Economy**	**Bio-digital fusion** 40% of GDP from bio-based manufacturing and digital services. "Attention-Free" commerce (shopping via AI, zero-UI commerce).	**Origin value** An economy based on Digital Product Passports, subscriptions and certified authenticity.	**Economics of access** Dematerialization of capital. Surveillance capitalism. You pay for access, you own nothing.	**Neofeudal exploitation** Attention tax. Gamification of work (gig economy). Cognitive exploitation in exchange for survival.

Scenario 1: Digital-biological integration

SCENARIUSZ 1

Digital-biological integration

The nature of the scenario

"A techno-optimistic vision of the future in which technological progress combines with state centralization to maximize prosperity."

Domination

Freedom

Key elements and differentiators

Internet of Identity (IDS)

A superlayer on top of the current Internet. Internet. Identity is key to every digital interaction.

Bioproduction on demand

30-40% of the chemical industry is switching to biological production in local hubs.

Digital feudalism

Clear division of roles: the state regulates, corporations provide services within strict frameworks.

Living identity

Citizen profile dynamically updated by biomarkers in real time.

Attention-Free Economics

Automation of negotiations and purchases through personal AI (algorithmic agency). No more fighting for user's attention in favor of fighting for algorithms.

A key paradox

Maximum system efficiency is achieved only with maximum centralization and privacy restrictions.

Scenario 2: Convergence of seven vectors

SCENARIUSZ 2

Convergence of seven vectors

The nature of the scenario

"The most balanced scenario - an attempt to reconcile technological efficiency with democratic values and individual autonomy."

Cooperation

Autonomy

Key elements and differentiators

The emergent state

The state as a "gardener" (complex systems systems theory) - defines standards, does not does not directly control.

Self Sovereign Identity (SSI)

The entity has full, cryptographic control over the data and decides to whom it discloses the attributes.

Three identity players

The EU, USA and Asia as digital superstates competing with regulatory models.

Federated learning

Train AI models on local devices without having to centralize sensitive data.

Relationship restoration movement

A strong social trend: active resistance to hyperconnection, a renaissance of physical contacts.

Protocol-based Social Networks

Separation of the data hosting layer from algorithms. The user chooses the algorithm, not the platform.

A key paradox

How to maintain decentralization and individual freedom in the face of increasing pressure on centralization for security?

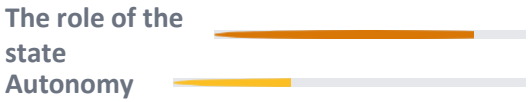
Scenario 3: CyberTransformation

SCENARIUSZ 3

CyberTransformation

The nature of the scenario

"Sectoral transformation with a strong role of the predictive state, based on the triple helix model (science-business-state)."



Key elements and differentiators

Competence clustering

Triple helix model – close cooperation of of science, business and the state in creating creating innovations.

7-layer architecture

Hierarchical social structure, from identity infrastructure to relational ownership.

Bifurcation of reality

Conscious separation of the virtual and physical worlds; elites in premium spaces.

Process ontology

Identity defined as a continuous process of change, not a fixed essence.

Digital unconscious

A new layer of the human psyche. The predictive state manages algorithmically, using analytics to act proactively.

Key Paradox

Efficiency of the predictive state vs. individual autonomy.

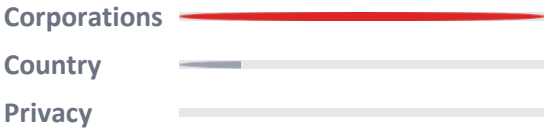
Scenario 4: Reconfiguration (DYSTOPIA)

SCENARIUSZ 4

Reconfiguration (Dystopia)

The nature of the scenario

"Warning - conscious extrapolation of negative trends. Erosion of the state and total corporate domination in a world of deep inequality."



Key elements and threats

Erosion of the state
Complete loss of regulatory capacity to transnational corporations.

Privacy 2.0
Paradoxical redefinition: total monitoring as a new security standard.

Biomedical apartheid
Dramatic stratification: elites with improvements vs. masses excluded.

Hyperalienation
The paradox of being "always connected" leading to deep social isolation.

Patent Trolling 2.0
Aggressive privatization of public research blocking social innovation.

Attention tax
Value extraction from attention time. Friendship-as-a-Service.

Key Paradox

The normalization of total surveillance and loss of agency is sold and accepted as "comfort".

Comparison of the roles of the state

Scenario 1

Centralized superstate

The state has a monopoly on identity and constitutes the subjectivity of citizens. A central decision-making center manages access to digital and biological services.

Control — Regulation

Scenario 2

The emergent state

The "gardener" model inspired by the theory of complex systems. The state defines standards and frameworks (interoperability), but does not directly control how citizens interact.

Control — Coordination

Scenario 3

The predictive state

Algorithmic management. The state uses advanced analytics and AI to act proactively, anticipating needs and threats before they occur.

Control — Automation

Scenario 4

An eroded state

Loss of regulatory capacity. The state is becoming a façade, subordinated to the interests of global digital corporations ("Digital Lords").

Control — Dependence

Comparing corporate roles

Scenario 1

Cyber-states (Partners)

Corporations manage metaverses and infrastructure, but under a strict legal regime imposed by the state. They operate as licensed public utility service providers.

Cooperation with the government	95%	Decision-making autonomy	30%

Scenario 2

Ecosystem creators

Companies compete on innovations under open, public standards. No corporation can monopolize the market through forced interoperability.

Competitiveness	90%	Monopolization	15%

Scenario 3

Surveillance capitalists

Market domination achieved through the control of closed standards (proprietary). Corporations are more powerful than weakening states thanks to their information advantage.

Data extraction	95%	Impact on standards	85%

Scenario 4

Digital lords

Total domination. Corporations take over traditional state functions (security, currency, law). The citizen becomes a user subject to the regulations.

Absolute power	98%	Social responsibility	5%

Digital identity models

Scenario 1

Centralized + Web 4.0

The state issues and guarantees digital identity, but transactions take place in a decentralized Web 4.0 architecture. A hybrid of institutional trust and blockchain technology.

Data Centralization	High	Verifiability	Full

Scenario 2

Self-sovereign (SSI)

Digital wallet model (Wallet). An entity is the sole owner of its identity attributes. Using Zero-Knowledge Proofs to confirm age/authorities without disclosing data.

User Control	100%	Privacy	Maximum

Scenario 3

State Blockchain

Total data integration in one national distributed register. Identity is not a property, but a service provided by the state in exchange for citizen transparency.

Anonymity	Lack	Service integration	Full

Scenario 4

Privacy 2.0

A paradoxical redefinition: being monitored is proof that "you have nothing to hide." Behavioral identity created by corporate algorithms based on continuous observation.

Real privacy	0%	Profiling	Totally

Visions of society

Scenario 1

Functional stratification

A society divided by function and access to resources. Stable, but strongly hierarchical. A middle class defined by digital asset ownership (NFT).

Class structure

Scenario 2

Hybrid society

Balanced tension between two attitudes. It is not the wealth hierarchy, but the choice of lifestyle (online vs. offline) that defines social divisions.

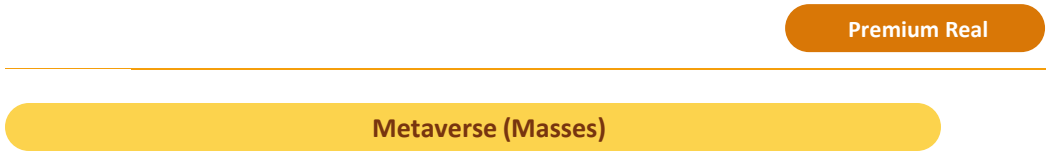
Social poles

Scenario 3

Bifurcation of reality

Fork of worlds. The elites live in "premium spaces" (physical, ecological), while ecological), while the masses meet their life needs mainly in the Metaverse. Metaverse.

Division of reality

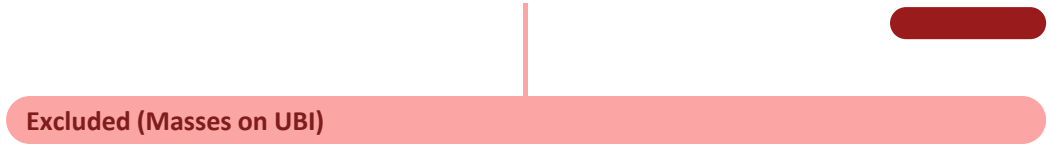


Scenario 4

Total dystopia

Biomedical apartheid. A deep gap between the genetically/technologically genetically/technologically enhanced elites and the "redundant" rest, kept in kept in check by an existential UBI.

Systemic Exclusion



Key conclusions

A profound transformation

All scenarios predict a fundamental change in IT operating models by 2040. Maintaining the status quo is impossible. An era is coming in which biology and digitalisation form an inextricable intertwine, redefining the concept of infrastructure.

01

Tension: efficiency vs. freedom

The main dilemma of the future is the tragic conflict between systemic systemic efficiency (provided by centralization and AI) and individual individual autonomy. Every increase in security and convenience comes at a comes at a cost in the form of loss of some privacy.

02

Common technology, different governance governance

The technology stack (Blockchain, BCI, AI, PQC) is almost identical in all all scenarios. It is not technology that differentiates the future, but the the Governance model - who owns the data, who controls the algorithms and algorithms and how value is distributed.

03

Political decision

The choice of scenario does not depend on engineers, but on social and and political decisions. Whether data will be a commodity (Dystopia), a public (Dystopia), a public good (Integration) or personal property (Convergence) - it (Convergence) - it is a matter of legislation, not code.

04

Implications for IT

Scenario architecture

- Moving away from monoliths in favor of microservices ready for quick reconfiguration.
- Interoperability as a priority (readiness for SSI and Web 4.0 standards).
- Modularity allows you to "plug in" regulatory components.

API-FIRST MODULARITY

Ethics & Governance

- Implementation of "Privacy-by-design" as a standard, not an add-on.
- Preparing for algorithmic audits and AI Act regulations.
- Cryptographic compliance (migration to Post-Quantum Cryptography).

PQC AI ETHICS

The new role of specialists

- Evolution from "code providers" to "trust architects".
- Data Stewardship – responsible management of the data life cycle.
- Co-creating open standards (preventing vendor lock-in).

STEWARDSHIP SOFT SKILLS

Flexible strategies

- **Multi-cloud & Hybrid: Avoiding dependence on a single supplier (risk of (risk of "Digital Lords").**
- **LLMOps: Implementation of processes for operationalizing large language models while maintaining control over the data.**
- **Observability: Full visibility into the operation of complex systems and AI.**

The project is financed from state budget funds allocated by the Minister of Education and Science under the "Science for Society II" Program.
Funding: PLN 1,467,000, Total value: PLN 1,467,000

Early signals radar

- Monitoring of legislation (centralization vs decentralization index).
- Analysis of the adoption of identity standards (SSI vs GovID).
- Tracking progress in BCI and biotechnology interfaces (integration phase phase 2030+).