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

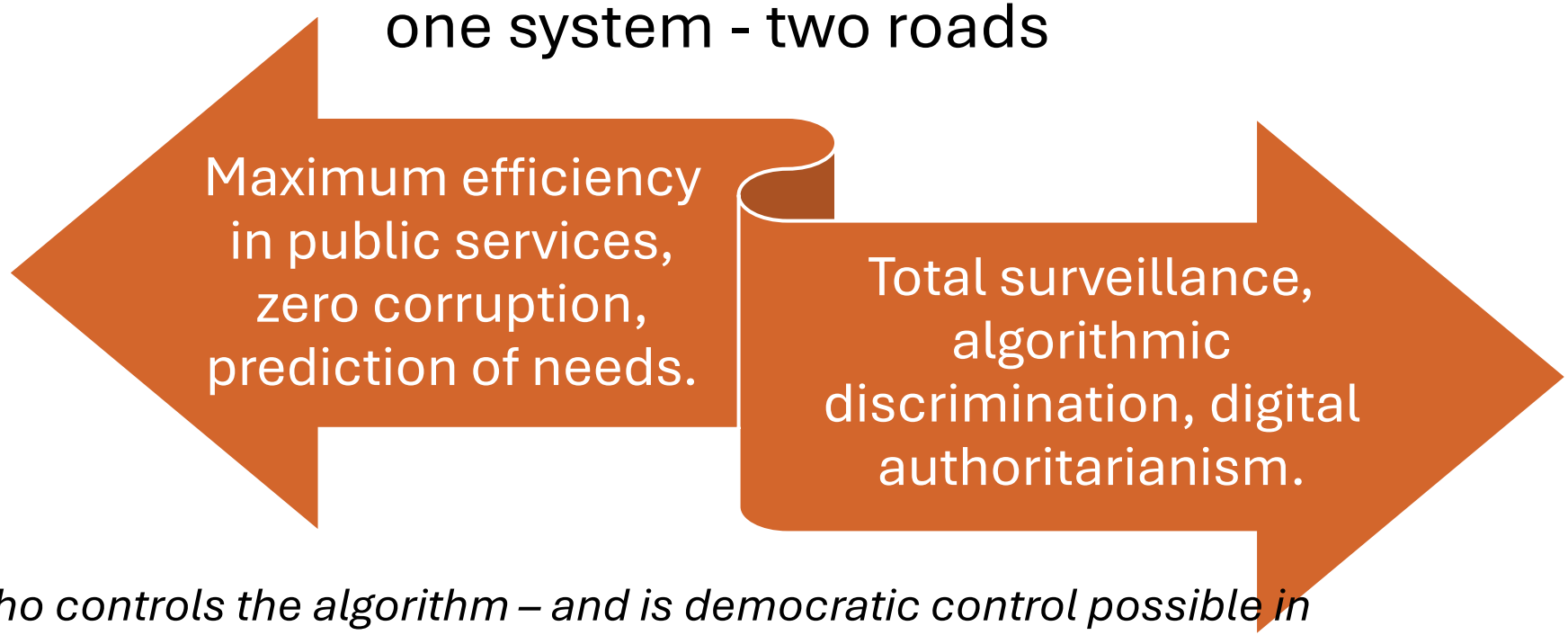
Scenario: CyberTransformation

strategic area: Internet and IT

The state as a digital nervous system - utopia, panopticon or fragmentation?

Paradox: efficiency vs. freedom

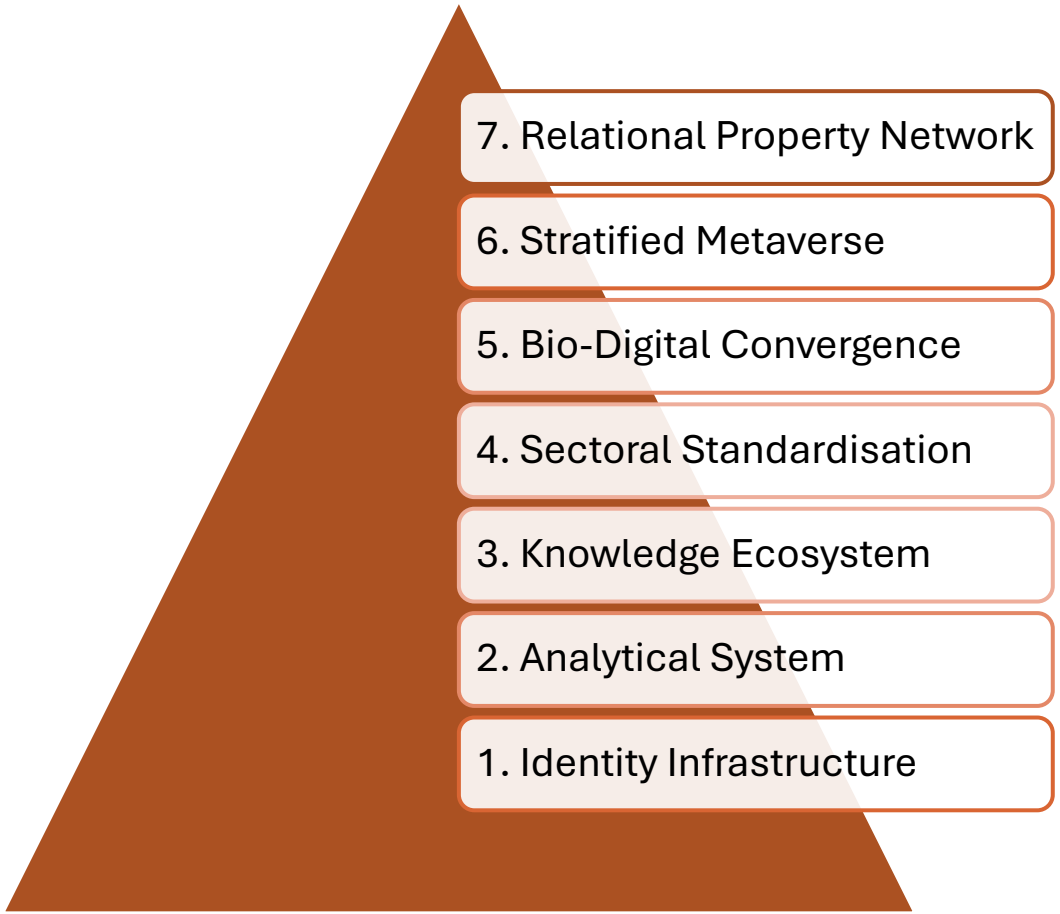
one system - two roads



Who controls the algorithm – and is democratic control possible in machine time?

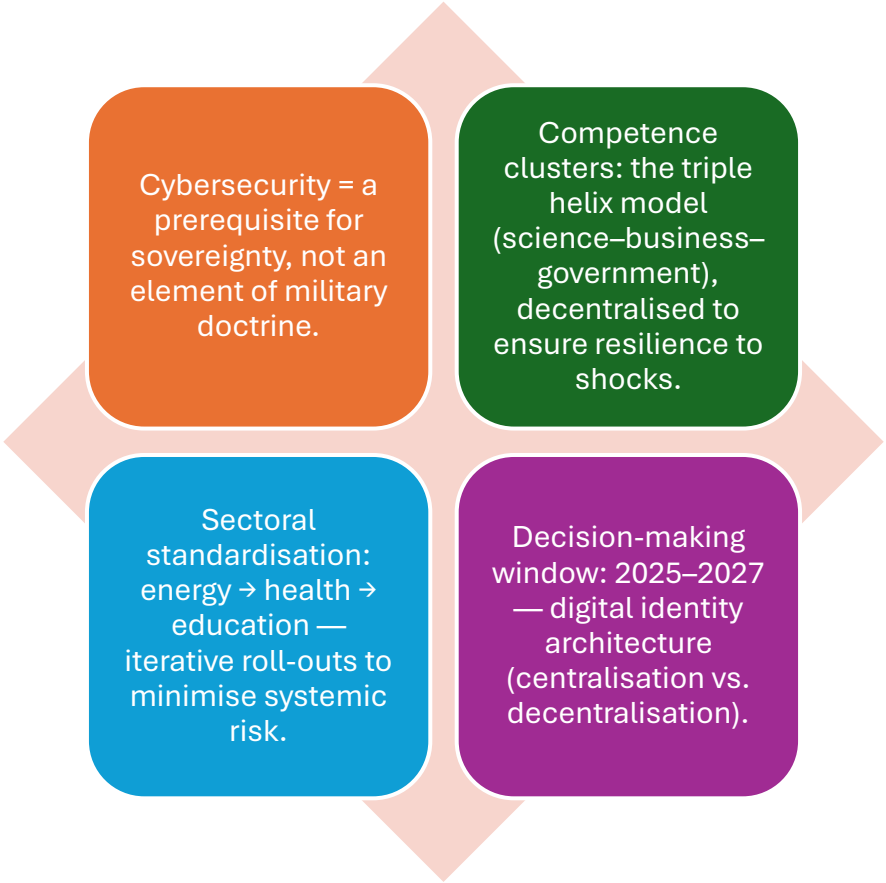
There is no technologically safe path - only a political choice.

Seven-layer architecture

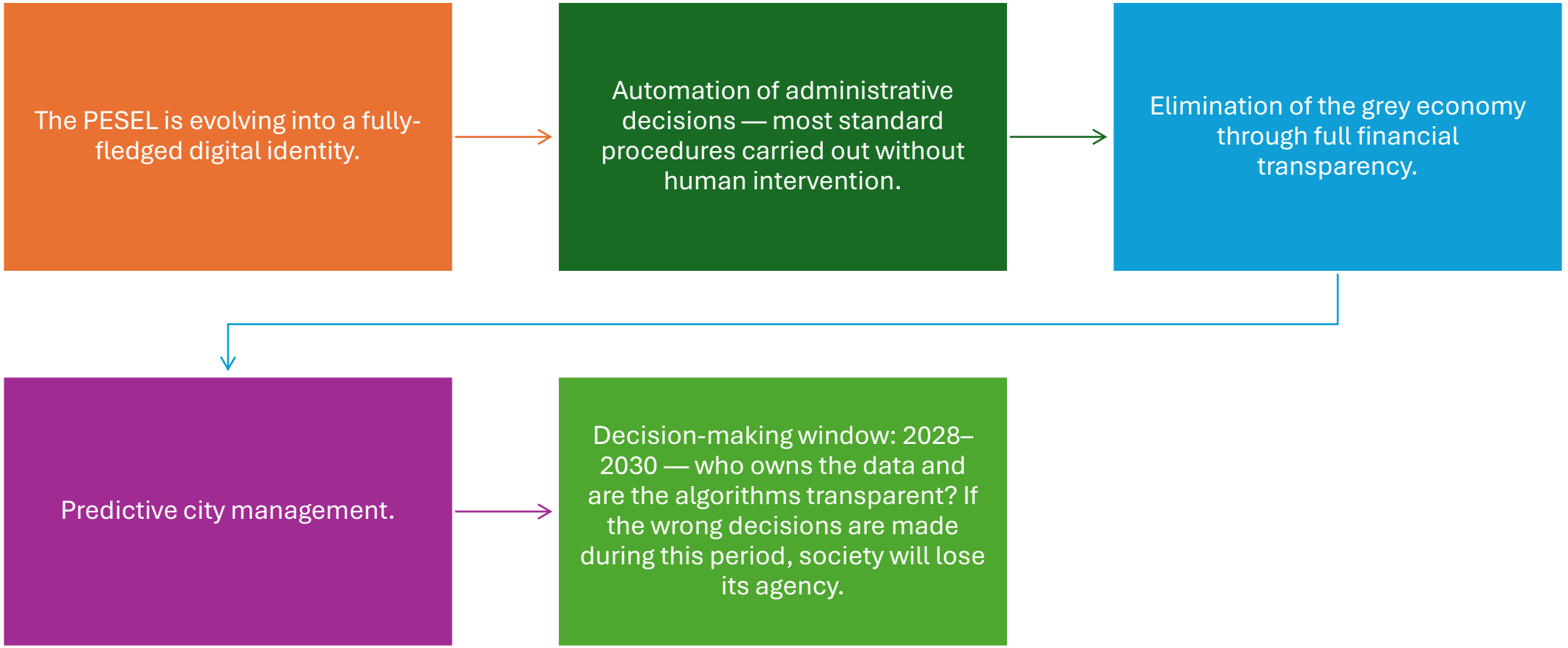


A single point of failure at the layer level paralyzes everything above it.
Each layer accumulates dependencies and values – and risks.

Phase I (2025–2030): Origin - building foundations



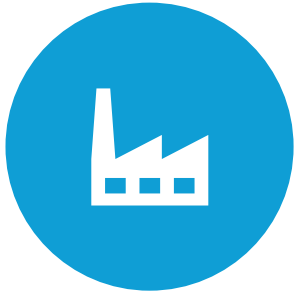
Phase II (2030–2035): Integration - the algorithmic state



Phase III (2035–2040): Convergence and bifurcation

Crossing the bio-digital boundary: BCIs, neural interfaces, the Metaverse as an alternative reality.

Digital stratification: elites with access to the full-resolution Metaverse vs. the lower classes in ‘limited versions of reality’.



Bifurcation: the same technologies, the same investments — leading to four completely different worlds depending on regulatory choices.

Decision window: 2032–2035 — ethical standards for neural interfaces.

Phase IV (2040+): Hyperconnection and relational ownership

The ubiquity of the IoT: every physical object has a digital twin.

The shift from exclusive ownership to relational ownership: you don’t own a car — you have the right to use it within the ecosystem.

A new ontology of reality: the boundary between the physical and the digital is becoming indistinguishable.

Decision-making window: 2037–2040: principles of jurisdiction and governance in the Metaverse.

Four subscenarios for 2040

Subscenario	Probability	Description
A: Digital utopia	10%	Democratic control of algorithms, universal prosperity, protected individual rights
B: Digital panopticon	30%	Total control of the state or corporation, elimination of opposition
C: Digital fragmentation	40%	Balkanization of the Internet, incompatible blocks, Poland between hegemons
D: Hybrid reality	20%	Persistent centralization-decentralization tension, different regimes for different groups

Systemic threats

Five categories of risk:

Single points of failure — the centralisation of identity and payments as a target for hybrid attacks;

Algorithmic bias — the automation of discrimination on a massive scale;

Technological dependency — society held hostage by infrastructure;

Digital authoritarianism — surveillance infrastructure in the hands of authoritarian regimes;

Corporate dominance — global oligopolies taking regulatory power away from states.

Poland's technological sovereignty: opportunities and threats

Opportunities:

triple-helix clusters build resilience through decentralisation;
iterative sector-specific roll-outs minimise risk;
Poland as a hub between blocks

Threats:

lack of proprietary platforms and chipsets;
risk of internet fragmentation;
“digital authoritarianism” possible if poor political choices are made between 2025 and 2027.

Strategic recommendations

Law must stay ahead of technology — a proactive regulatory framework for AI and digital identity before implementation, not after

Algorithmic literacy — universal digital education as a prerequisite for democratic control

Institutional oversight of algorithms — independent bodies to audit decision-making algorithms against constitutional values

The right to be offline — legally designated surveillance-free zones as sanctuaries of privacy

Digital redistribution — a robotisation tax or digital dividend, so that the profits from automation do not go solely to the elite

Conclusion

Timeline of four irreversible milestones:

2025–2027 (identity architecture — centralised vs. decentralised),

2028–2030 (data ownership and algorithm transparency),

2032–2035 (ethics of BCI and neural interfaces), 2037–2040 (Metaverse jurisdiction).

Any window closed without the right decision leads to Sub-scenario B or C. C is the most likely (40%)

Poland may become digitally trapped between the blocs of the hegemons if it does not decide on its own identity architecture within the next two years.

“The paradox of efficiency and total surveillance: the unprecedented convenience of public services is inextricably linked to the loss of privacy. There is no technologically safe path - only a political choice."

Ministerstwo Nauki i Szkolnictwa Wyższego

Polish Digital Society
http://cyfryzacja.org

The project is financed from state budget funds allocated by the Minister of Education and Science under the "Science for Society II" Program._x000B_Funding: PLN 1,467,000, Total value: PLN 1,467,000

Postscript: one-page script

The scenario describes the most profound transformation possible: the state becomes a digital nervous system. Technology ceases to be a management tool - it becomes the very fabric from which the state is built. This is not the digitalisation of offices or e-services - it is a change in the ontology of what power, property and reality are.

The central thesis is provocative: optimally designed cybersecurity and digitalisation can make the state dramatically more efficient — but the same system, in different hands or with different regulatory choices, becomes a perfect tool for total control. The scenario therefore poses a paradox of efficiency and total monitoring: the unprecedented convenience of public services is inextricably linked to the loss of privacy and the submission of every aspect of life to algorithmic analysis. There is no technologically "safe" path - only the choice of who controls the algorithm.

The narrative progresses through four phases with increasing depth of transformation. Phase I (2025-2030) - Origin: building foundations - cybersecurity as a condition of sovereignty, competence clusters in the triple helix model (science-business-administration), sector standardization in energy, health and education. Phase II (2030–2035) — Integration: evolution of PESEL into a full digital identity, algorithmization of administrative decisions, elimination of the gray zone, predictive systems in city management. Phase III (2035-2040) - Convergence and Bifurcation: Crossing bio-digital boundaries (BCI, neural interfaces), the triumph of the Metaverse, and the key bifurcation point - the same technologies lead to radically different worlds depending on political choices. Phase IV (2040+) - Hyperconnection: Internet of Things at a total scale, moving from "exclusive ownership" to "relational ownership" - you don't own the thing, but the rights to use it in the ecosystem.

The architecture of the entire system is based on seven layers: identity infrastructure → analytical system → knowledge ecosystem → sector standardization → bio-digital convergence → Stratified metaverse → relational property network. Each layer builds on the previous one, creating cumulative dependency - but also cumulative risk: a failure at the identity infrastructure level paralyzes all layers above (single point of failure).

The key narrative drama is revealed in Phase III: same infrastructure, same code - in Subscenario A it creates a digital utopia (democratic control of algorithms, universal prosperity), in Subscenario B a digital panopticon (total state or corporate control), and in Subscenario C - a collapse into incompatible geopolitical blocs (Splinternet). The most likely scenario is Subscenario C (fragmentation, 40%), not D or A. Poland may find itself in the least favorable global situation - digitally isolated between the blocs.