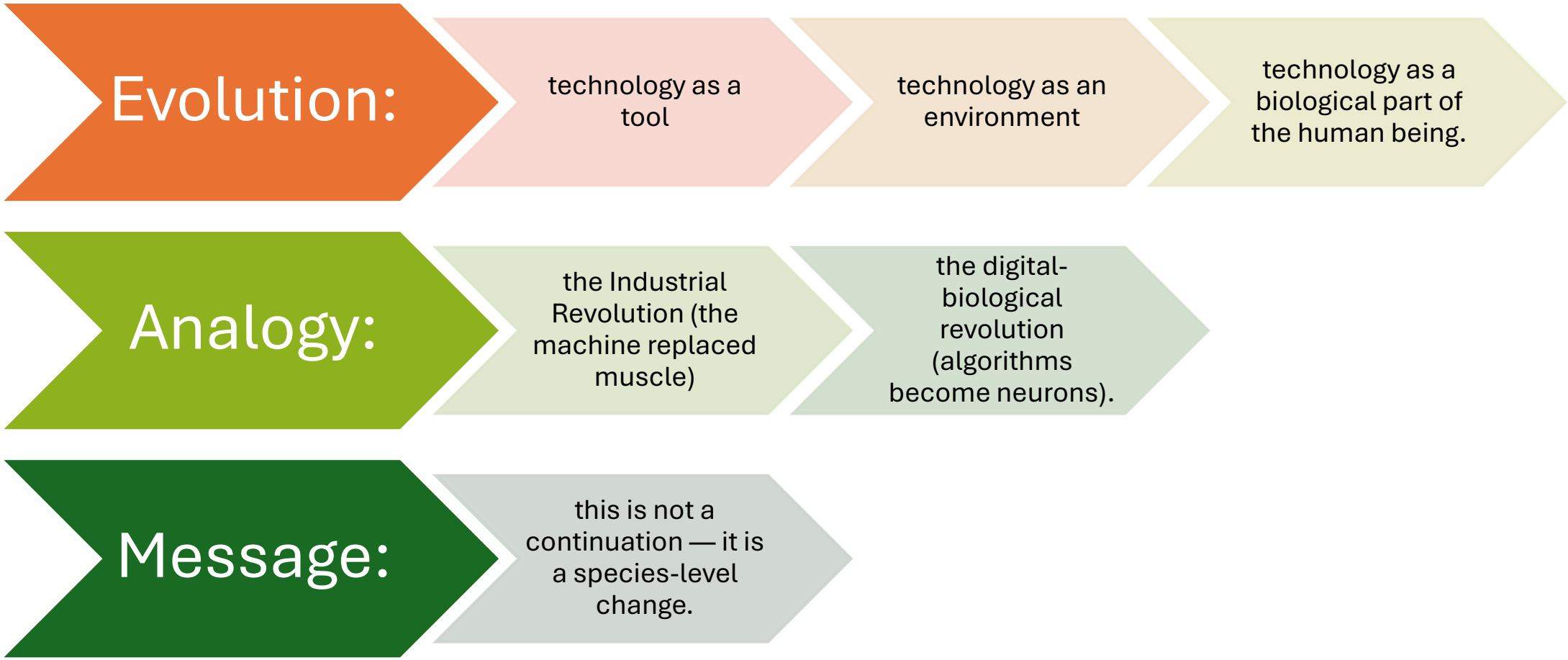
Polish Digital Resilience Agenda 2040
a model of strategic preparedness
for the antinomies of digitalisation.

Scenario: Towards an integrated digital-biological infrastructure

strategic area: Internet and IT

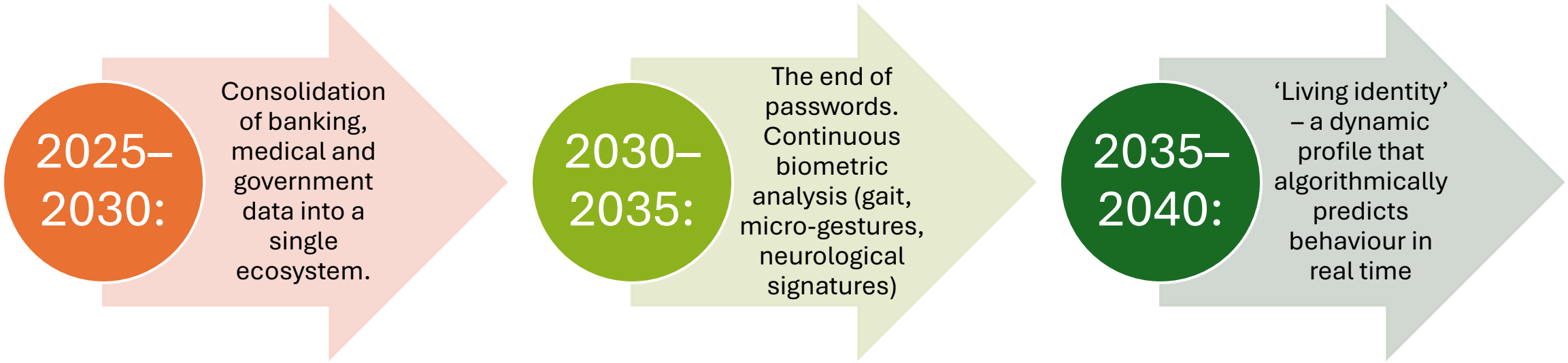
DNA code and binary code - two compatible reality programming languages.

Paradigm shift: technology as a biological environment



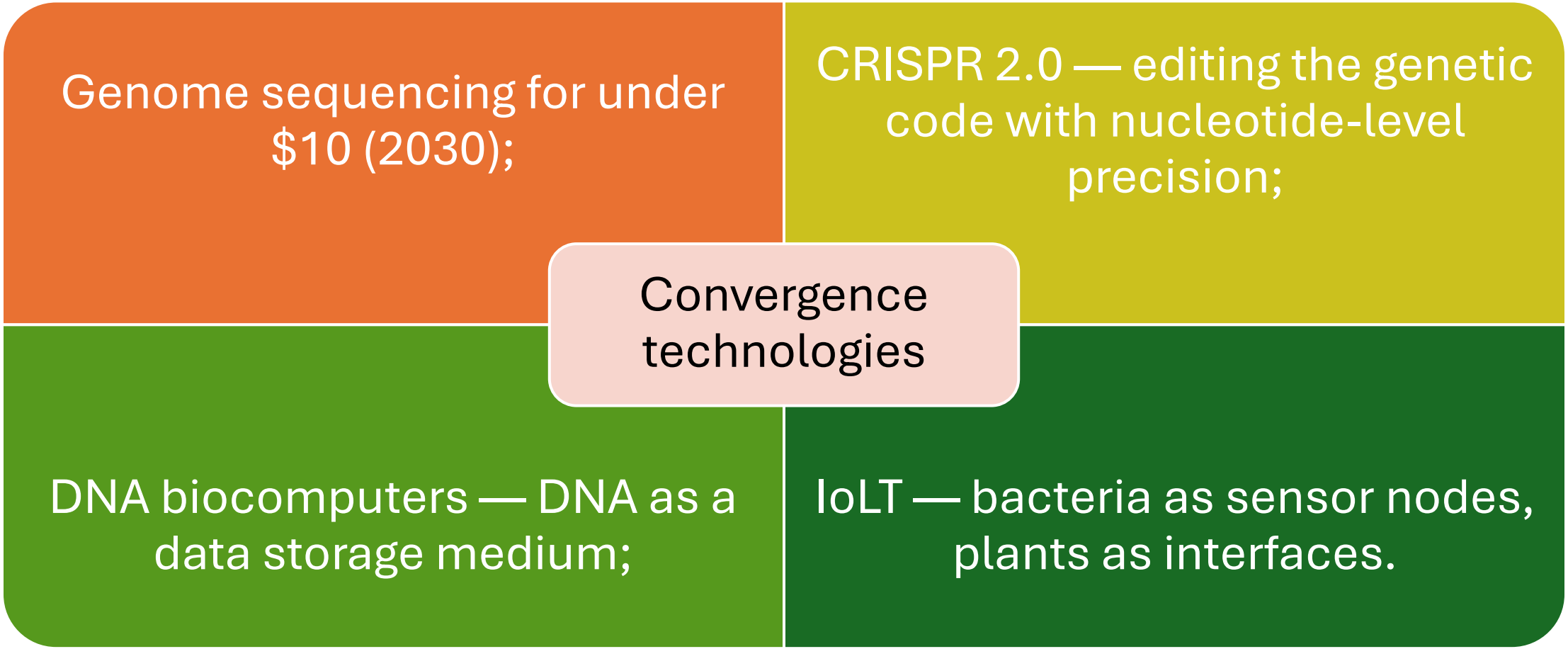
Plot I: Internet of Identities (2025–2040)

Three phases of identity evolution:



Thread II: Biology as digital infrastructure

A change of era: from reading biology to writing it.



Proactive medicine

New phenomena at the intersection of IT and medicine

Diagnostic machines

distributed nodes of a global biomedical monitoring network. 85% of initial diagnoses are automated.

Health passport

terabytes of data, genetic profile, predictive models.

Health gamification

data from diagnostic machines influences an avatar in the metaverse.

Paradigm shift

from reactive medicine (treatment) to proactive medicine (data-driven prevention).

Brain-computer interfaces (BCI) and Smart Cities 3.0

BCI:

- from invasive devices to consumer gadgets
- brain-to-brain communication
- sharing emotions
- “collective minds”
- a new ontology of reality.

Smart Cities 3.0:

- cities as living superorganisms
- buildings metabolising waste
- parks integrated with urban ventilation
- IoLT as a sensory fabric.

Thread III: Quantum supremacy and the crypto crisis

2027–2028:

- quantum computers achieve cryptanalytic supremacy — RSA-2048 is broken (Shor's algorithm).
- Consequence:
  - all existing banking, government and military encryption becomes transparent.

$2–3 trillion (2028–2032)

The cost of global migration to post-quantum cryptography.

Decision window:

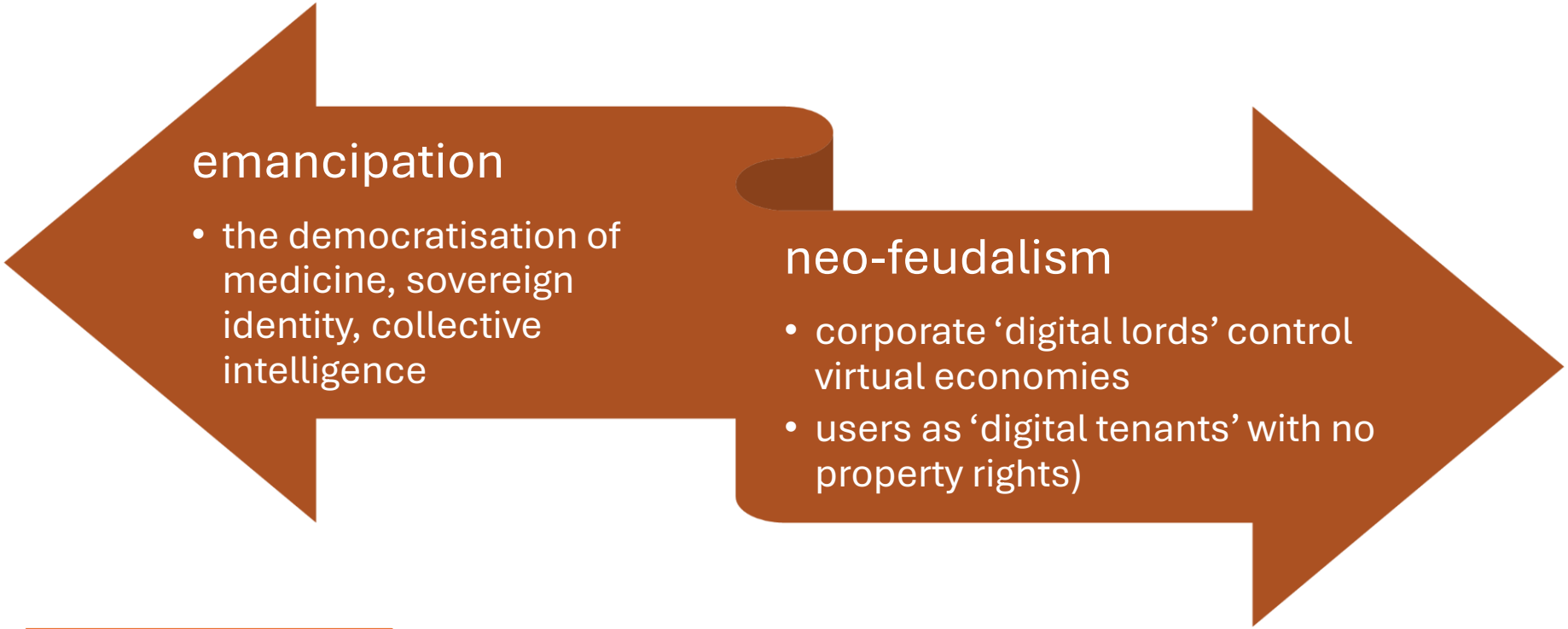
by 2027

Analogy:

the NotPetya attack cost $10 billion — that was just the beginning.

Digital feudalism: the paradox of emancipation

The same technology creates two worlds in parallel:



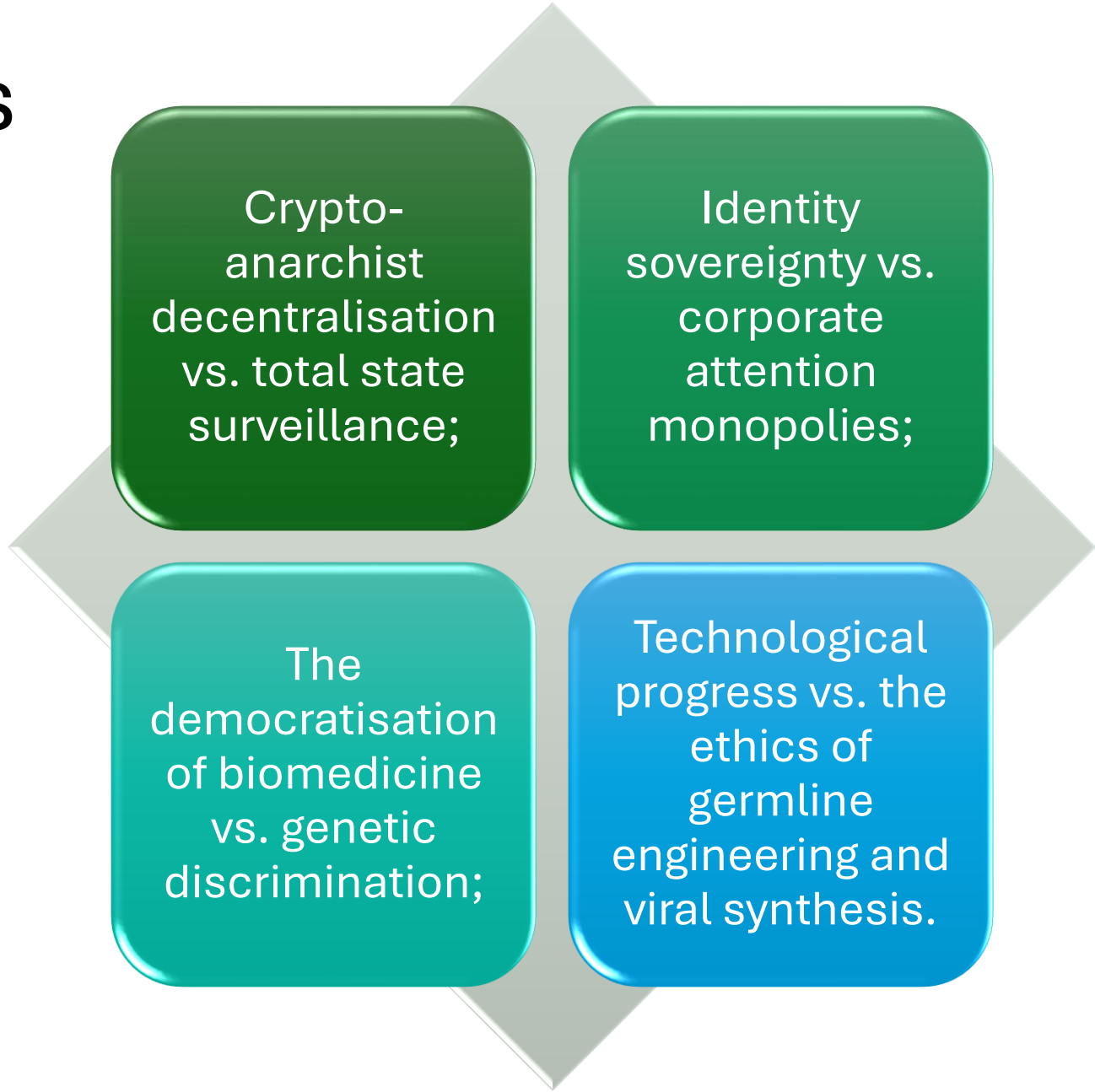
Risks

genetic discrimination,

algorithmic determinism,

the quantum divide between rich and poor countries.

Systemic tensions



Implications for Poland: what to do before 2027?

Three strategic priorities:

- Post-quantum migration — banking and public administration by 2027 (the ‘Polish Paradox’ scenario mentioned the same deadline);
- Building cyber resilience — next-generation SOC, 50,000 specialists;
- Regulation of biological data — protecting citizens’ genomes from “digital lords”, a ban on genetic discrimination.

Conclusion

Will Poland be a subject or an object in the digital-biological civilization by 2040?

Three dimensions of subjectivity:

- own post-quantum cryptography,
- own biological data standards,
- own digital identity architecture not subordinated to "digital lords".

Decision window:
2027 - After this date, without action, cryptographic sovereignty becomes irreversibly lost.

"We are observing the birth of a civilization in which DNA code and binary code become mutually compatible reality programming languages."

Ministerstwo Nauki i Szkolnictwa Wyższego
NAUKA DLA SPOŁECZEŃSTWA
PTC
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 announces the end of the era of technology as a tool — and the birth of an era in which technology becomes an integral human biological environment. The thesis is radical and precise at the same time: DNA code and binary code become mutually compatible reality programming languages. This is not a continuation of previous progress - it is a civilizational paradigm shift comparable to the industrial revolution.

The narrative leads through three interwoven threads that together create the image of 2040.

Thread one: identity. The state is no longer an institution that confirms a citizen's identity - it becomes an institution that actively constitutes and manages this identity in real time. The Identity Directory Services (IDS) system verifies authorizations in less than 100 ms, integrating banking, medical and official data into one blockchain ecosystem. By 2030–2035, passwords will disappear - they will be replaced by continuous analysis of behavioral patterns: gait, micro-gestures, neurological signatures. By 2035-2040, identity becomes "living" - a dynamic profile updated in real time, predicting behavior algorithmically.

The second thread: biology as infrastructure. By 2030, full genome sequencing costs $10 — and comes into widespread use. CRISPR 2.0 allows you to edit the code of life down to a single nucleotide. We move from reading biology to writing it. Diagnozomats – distributed nodes of the global biomedical monitoring network – generate 85% of initial diagnoses automatically, transforming medicine from reactive to proactive. The Internet of Things is evolving into the Internet of Living Things (IoLT): bacteria become sensory nodes, plants become environmental interfaces, and cities function as living superorganisms (Smart Cities 3.0). Brain-computer interfaces (BCIs) are evolving from invasive devices to consumer gadgets, enabling brain-to-brain communication and shared emotions - "collective minds" are being born.

Thread three: cybersecurity as a new pillar of state sovereignty. In 2027–2028, quantum computers achieve cryptanalytic supremacy - RSA-2048 will no longer be secure. Migration to post-quantum cryptography costs USD 2-3 trillion globally and must be completed by 2028-2032. Cybersecurity spending is increasing from the current ~2% of GDP (NATO) to 4-6% of GDP in developed countries. Future conflicts are "flash wars" - AI vs. AI escalating in fractions of seconds, against which human reaction is helpless. A new defense paradigm: biological cyber-immunity – the immune system as a model of security architecture.

The central paradox of the scenario: the same technology that promises emancipation (democratization of medicine, sovereign identity, collective intelligence) also creates "digital feudalism" - corporate "digital lords" control virtual economies, and users become "digital tenants" without real property rights, subject to attention monopolies and algorithmic determinism. The risk of genetic discrimination, germline engineering and the quantum divide between rich and poor countries complete the picture of tensions.