**Polska Agenda Odporności Cyfrowej 2040**
model strategicznego przygotowania
na antynomie cyfryzacji.

# Scenariusz:
# W stronę zintegrowanej infrastruktury cyfrowo-biologicznej

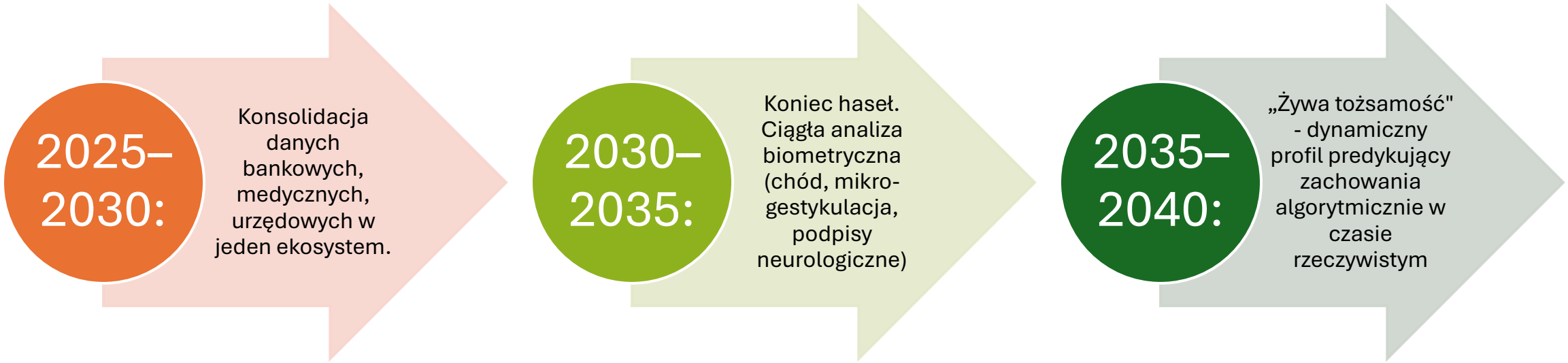
## obszar strategiczny: Internet i IT

Kod DNA i kod binarny — dwa kompatybilne języki programowania rzeczywistości.

# Zmiana paradygmatu: technologia jako środowisko biologiczne

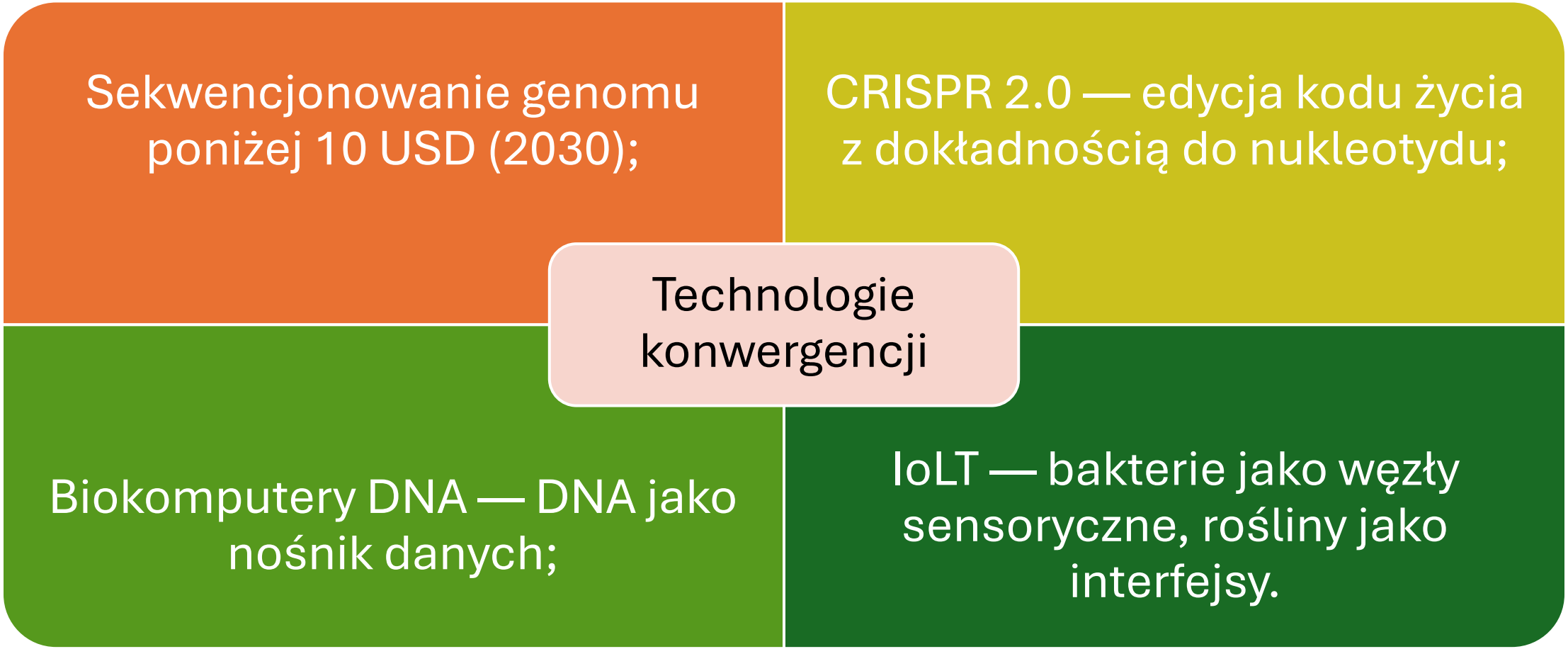
# Wątek I: Internet Tożsamości (2025–2040)

Trzy fazy ewolucji tożsamości:



# Wątek II: Biologia jako infrastruktura cyfrowa

Zmiana epoki: od odczytywania biologii do jej pisania.



# Medycyna proaktywna

Nowe zjawiska na styku IT i medycyny

## Diagnozomaty

- rozproszone węzły globalnej sieci monitoringu biomedycznego. 85% diagnoz wstępnych automatycznych.

## Paszport zdrowia

- terabajty danych, profil genetyczny, modele predykcyjne.

## Gamifikacja zdrowia

- dane z diagnozomatów wpływają na awatara w metawersum.

## Zmiana paradygmatu

- medycyna reaktywna (leczenie) na medycyna proaktywna (prewencja na podstawie danych).

# Interfejsy mózg-komputer (BCI) i Smart Cities 3.0

## BCI:

- od urządzeń inwazyjnych do konsumenckich gadżetów
- komunikacja mózg-mózg
- współdzielenie emocji
- „umysły kolektywne"
- nowa ontologia rzeczywistości.

## Smart Cities 3.0:

- miasta jako żywe superorganizmy
- budynki metabolizują odpady
- parki zintegrowane z wentylacją miejską
- IoLT jako tkanka sensoryczna.

# Wątek III: Supremacja kwantowa i kryzys kryptograficzny

**2027–2028:**

- komputery kwantowe osiągają supremację kryptanalityczną — RSA-2048 złamany (algorytm Shora).

**Skutek:**

- całe dotychczasowe szyfrowanie bankowe, rządowe, militarne staje się transparentne.

**2–3 biliony USD (2028–2032)**

- Koszt globalnej migracji do kryptografii postkwantowej.

**Okno decyzyjne:**

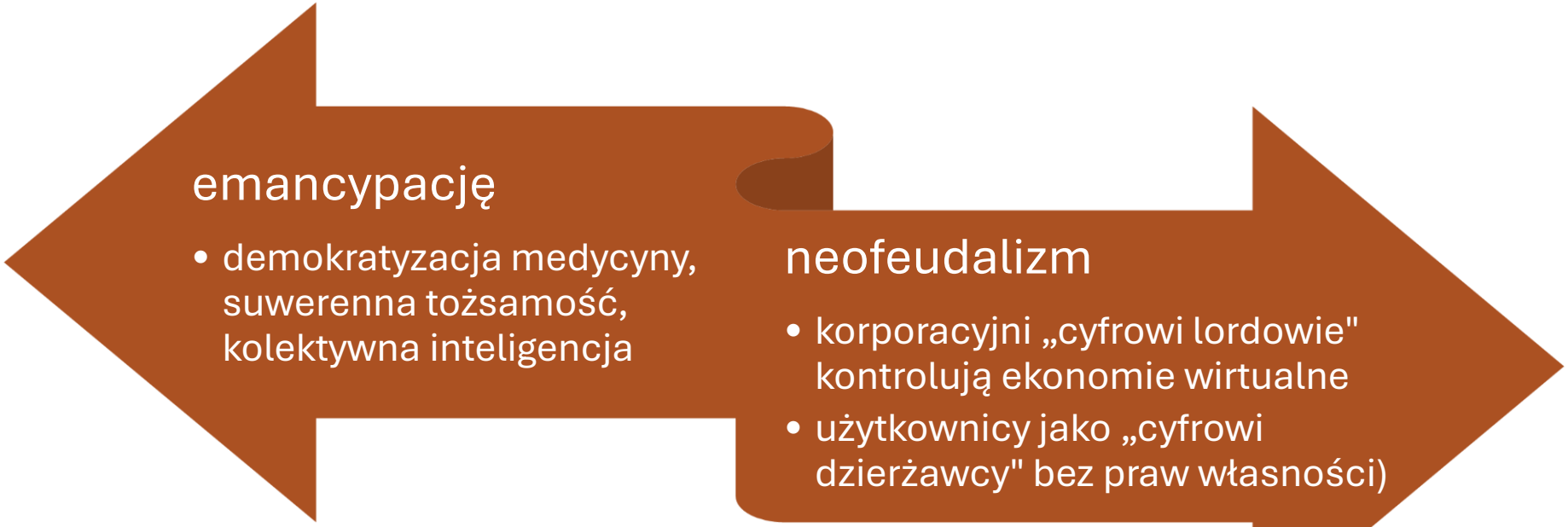
- do 2027 r.

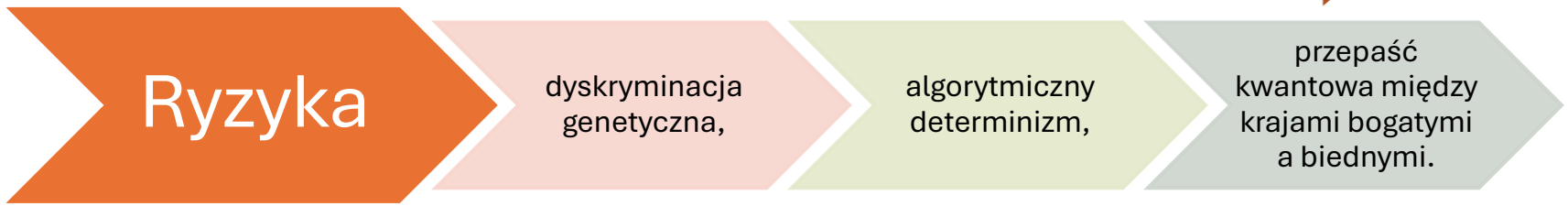
**Analogia:**

- atak NotPetya kosztował 10 mld USD — to był wstęp.

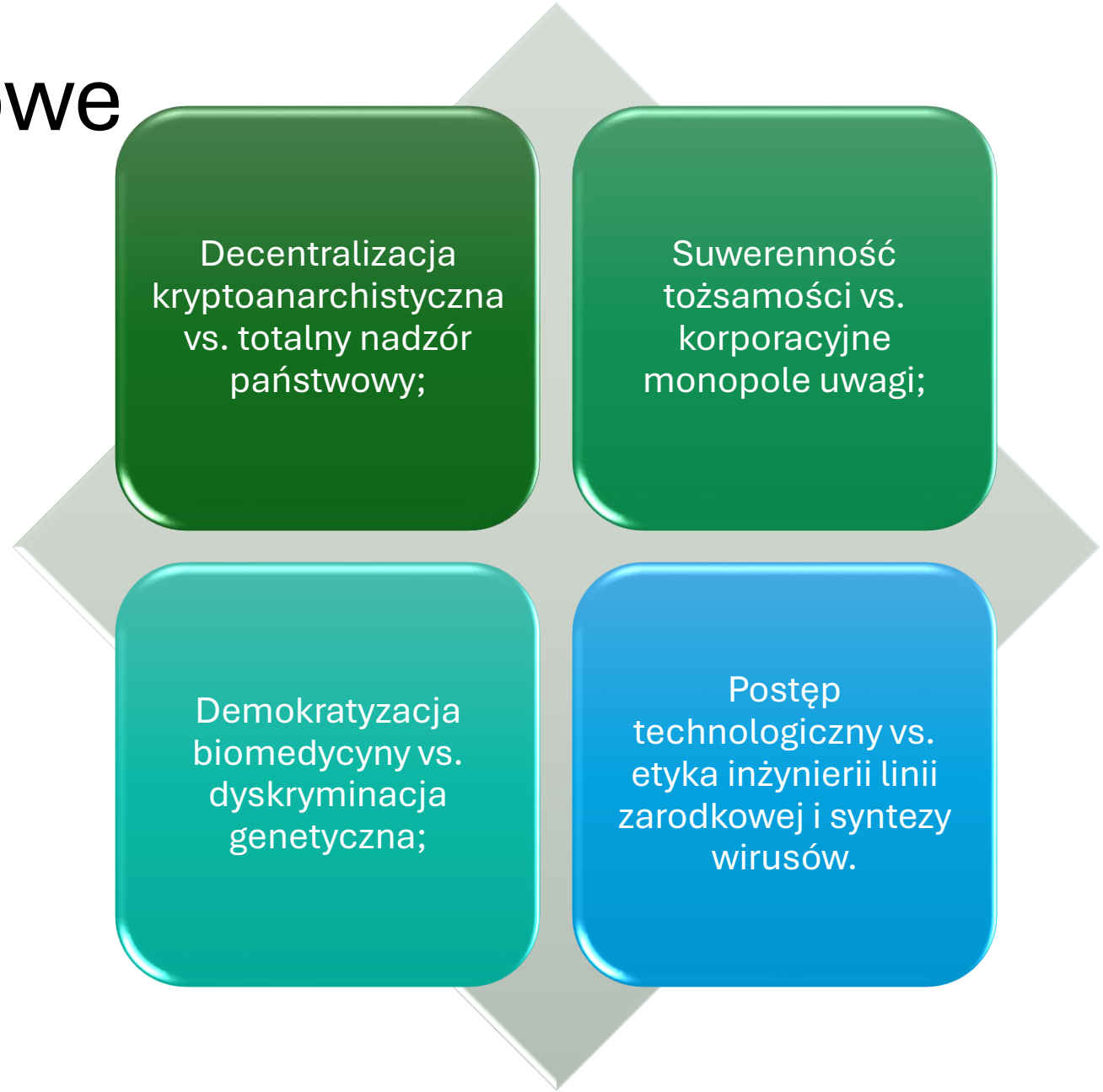
# Cyfrowy feudalizm: paradoks emancypacji

Ta sama technologia tworzy dwa światy równolegle:



# Napięcia systemowe



# Implikacje dla Polski: co zrobić przed 2027 r.?

**Trzy priorytety strategiczne:**

- **Migracja postkwantowa** — bankowość i administracja przed 2027 r. (w scenariuszu „Polski Paradoks" wspominał ten sam deadline);
- **Budowa cyberodporności biologicznej** — SOC nowej generacji, 50 tys. specjalistów;
- **Regulacja danych biologicznych** — ochrona genomu obywateli przed „cyfrowymi lordami", zakaz dyskryminacji genetycznej.

# Konkluzja

*Czy do 2040 r. Polska będzie podmiotem, czy przedmiotem* w cywilizacji cyfrowo-biologicznej?

Trzy wymiary podmiotowości:

- własna kryptografia postkwantowa,
- własne standardy danych biologicznych,
- własna architektura tożsamości cyfrowej niepodporządkowana „cyfrowym lordom".

---

Okno decyzyjne:
**2027 r.** — po tym terminie bez podjęcia działań suwerenność kryptograficzna staje się nieodwracalnie utracona.

*„Obserwujemy narodziny cywilizacji, w której kod DNA i kod binarny stają się wzajemnie kompatybilnymi językami programowania rzeczywistości."*

Ministerstwo Nauki i Szkolnictwa Wyższego
NAUKA DLA SPOŁECZEŃSTWA
Polskie Towarzystwo Cyfrowe
http://cyfryzacja.org
Projekt finansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Nauka dla Społeczeństwa II".
Dofinansowanie: 1 467 000 zł, Całkowita wartość: 1 467 000 zł

# Postscriptum: scenariusz na jedną stronę

Scenariusz ogłasza **koniec epoki technologii jako narzędzia** — i narodziny ery, w której technologia staje się **integralnym środowiskiem biologicznym człowieka**. Teza jest radykalna i precyzyjna zarazem: kod DNA i kod binarny stają się wzajemnie kompatybilnymi językami programowania rzeczywistości. To nie kontynuacja dotychczasowego postępu — to **zmiana paradygmatu cywilizacyjnego** porównywalna z rewolucją przemysłową.

Narracja prowadzi przez trzy splecione ze sobą wątki, które razem tworzą obraz 2040 roku.

**Wątek pierwszy: tożsamość.** Państwo przestaje być instytucją *potwierdzającą* tożsamość obywatela — staje się instytucją, która tę tożsamość *aktywnie konstytuuje i zarządza nią w czasie rzeczywistym*. System Identity Directory Services (IDS) weryfikuje uprawnienia w czasie poniżej 100 ms, integrując dane bankowe, medyczne i urzędowe w jeden ekosystem blockchain. Do 2030–2035 r. hasła zanikają — zastępuje je ciągła analiza wzorców behawioralnych: chód, mikro-gestykulacja, podpisy neurologiczne. Do 2035–2040 r. tożsamość staje się **„żywa"** — dynamiczny profil aktualizowany w czasie rzeczywistym, predykujący zachowania algorytmicznie.

**Wątek drugi: biologia jako infrastruktura.** Do 2030 r. pełne sekwencjonowanie genomu kosztuje **10 USD** — i wchodzi do powszechnego użytku. CRISPR 2.0 pozwala edytować kod życia z dokładnością do pojedynczego nukleotydu. Przechodzimy od *odczytywania* biologii do jej *pisania*. Diagnozomaty — rozproszone węzły globalnej sieci monitoringu biomedycznego — generują **85% diagnoz wstępnych** automatycznie, przekształcając medycynę z reaktywnej w proaktywną. Internet Rzeczy ewoluuje w **Internet Żyjących Rzeczy (IoLT)**: bakterie stają się węzłami sensorycznymi, rośliny interfejsami środowiskowymi, a miasta funkcjonują jako żywe superorganizmy (Smart Cities 3.0). Interfejsy mózg-komputer (BCI) ewoluują od inwazyjnych urządzeń do konsumenckich gadżetów, umożliwiając komunikację mózg-mózg i współdzielenie emocji — rodzą się **„umysły kolektywne"**.

**Wątek trzeci: cyberbezpieczeństwo jako nowy filar suwerenności państwowej.** W latach 2027–2028 komputery kwantowe osiągają supremację kryptanalityczną — RSA-2048 przestaje być bezpieczny. Migracja do kryptografii postkwantowej kosztuje globalnie **2–3 biliony USD** i musi zostać przeprowadzona do 2028–2032 r. Nakłady na cyberbezpieczeństwo rosną z obecnych ~2% PKB (NATO) do **4–6% PKB** w państwach rozwiniętych. Przyszłe konflikty to **„flash wars"** — starcia algorytmów AI vs. AI eskalujące w ułamkach sekund, wobec których ludzka reakcja jest bezradna. Nowy paradygmat obronny: **cyberodporność biologiczna** — system immunologiczny jako model architektury bezpieczeństwa.

**Centralny paradoks** scenariusza: ta sama technologia, która obiecuje emancypację (demokratyzacja medycyny, tożsamość suwerenna, kolektywna inteligencja), równocześnie tworzy **„cyfrowy feudalizm"** — korporacyjni „cyfrowi lordowie" kontrolują ekonomie wirtualne, a użytkownicy stają się „cyfrowymi dzierżawcami" bez realnych praw własności, poddanymi monopolom uwagi i algorytmicznemu determinizmowi. Ryzyko dyskryminacji genetycznej, inżynierii linii zarodkowej i przepaści kwantowej między krajami bogatymi a biednymi dopełniają obraz układu napięć.