

Obszar strategiczny

Internet i IT

Streszczenie scenariusza

### **Konwergencja siedmiu wektorów**

\*\*\*

#### **Wprowadzenie**

Współczesna cywilizacja stoi u progu fundamentalnej reorganizacji relacji między technologią cyfrową, strukturami państwowymi a jednostką ludzką. Zjawisko to nie stanowi linearnej kontynuacji dotychczasowych procesów cyfryzacji, lecz reprezentuje przejście fazowe w kierunku jakościowo nowego układu społeczno-technicznego, w którym granice między sferą cyfrową a fizyczną ulegają progresywnemu rozmyciu.

Analiza siedmiu zidentyfikowanych wektorów transformacyjnych ujawnia spójną narrację przyszłości, w której automatyzacja i cyfryzacja prowadzą do powstania hybrydowego ekosystemu techno-społecznego. Proces ten charakteryzuje się trzema głównymi fazami rozwoju:

- **Faza I: Decentralizacja odpowiedzialności (2025–2030)** – okres dekompozycji tradycyjnych struktur usługowych i przenoszenia ciężaru decyzji na algorytmy brzegowe.
- **Faza II: Reintegracja cyfrowo-fizyczna (2030–2035)** – moment fuzji tożsamości biologicznej z cyfrową oraz materializacji cyfrowych atrybutów w świecie fizycznym.
- **Faza III: Emergencja nowego porządku instytucjonalnego (2035–2040)** – krystalizacja nowych form zarządzania opartych na adaptacji i koordynacji, a nie centralnym planowaniu.

Kluczowym mechanizmem integrującym wszystkie zidentyfikowane trendy jest zjawisko koewolucji technologii i instytucji. Rozwój nowych możliwości technicznych wymusza adaptację struktur zarządzania, a te z kolei kształtują kierunki dalszego rozwoju technologicznego w sprzężeniu zwrotnym o charakterze nieliniowym. Nie mamy tu do czynienia z prostym determinizmem technologicznym, lecz ze złożoną grą sił, w której decyzje regulacyjne, presja rynkowa i innowacje inżynierskie wzajemnie się napędzają, tworząc emergentne, często nieprzewidywalne rezultaty.

## **2. Faza I: Decentralizacja odpowiedzialności i dematerializacja usług (2025–2030)**

### **2.1. Diagnozomaty zdrowotne jako katalizator transformacji**

Wprowadzenie diagnostomatów zdrowotnych stanowi kluczowy punkt zwrotny w dekompozycji tradycyjnych struktur opieki zdrowotnej, inicjując proces określany jako „rozdzielenie funkcji opieki zdrowotnej”. Jest to rozdzielenie zintegrowanych dotąd funkcji diagnostyki, leczenia i monitorowania na autonomiczne moduły technologiczne. Urządzenia te, wykorzystujące zaawansowane biosensory, spektroskopię nieinwazyjną oraz algorytmy uczenia maszynowego, umożliwiają przeniesienie **60–70%** podstawowych procedur diagnostycznych z placówek medycznych do środowiska domowego. Stanowi to największą reorganizację przestrzenną usług zdrowotnych od czasów powstania nowoczesnych szpitali w XIX wieku.

Zmiana ta jest istotna nie tylko z perspektywy logistycznej, lecz przede wszystkim epistemologicznej – przekazanie diagnostyki do domu przekształca relację pacjent-lekarz z modelu hierarchicznego (lekarz jako wyłączny posiadacz wiedzy diagnostycznej) w model partnerski oparty na współinterpretacji danych generowanych przez urządzenia należące do pacjenta.

**Mechanizm technologiczny.** Integracja diagnostomatów z elektroniczną dokumentacją medyczną (EDM) tworzy ciągły strumień danych biomedycznych, gdzie analiza parametrów zdrowotnych przebiega w czasie rzeczywistym poprzez systemy przetwarzania strumieniowego wykorzystujące architektury przetwarzania brzegowego (edge computing). Obliczenia wykonywane są lokalnie na urządzeniu, co minimalizuje opóźnienia i redukuje objętość przesyłanych danych wrażliwych. Algorytmy sztucznej inteligencji, trenowane na rozległych zbiorach danych populacyjnych liczących miliardy punktów pomiarowych, osiągają czułość diagnostyczną i specyficzność porównywalną z lekarzami pierwszego kontaktu w wykrywaniu stanów przedchorobowych, a w niektórych domenach (np. dermatologia, okulistyka) przewyższają zdolności przeciętnego specjalisty.

Kluczowym wyzwaniem technicznym pozostaje problem wyjaśnianej sztucznej inteligencji (Explainable AI). Algorytmy typu „czarna skrzynka”, choć dokładne statystycznie, napotykają opór regulacyjny i społeczny ze względu na brak możliwości śledzenia procesu wnioskowania diagnostycznego. Prowadzi to do rozwoju hybrydowych architektur łączących sieci neuronowe z symbolicznym rozumowaniem medycznym opartym na ontologiach klinicznych typu SNOMED CT.

### **Implikacje społeczno-ekonomiczne**

Redukcja kosztów opieki zdrowotnej o **25–35%** poprzez wczesną detekcję i prewencję wynika z fundamentalnego przesunięcia modelu ekonomicznego od reaktywnego leczenia chorób zaawansowanych w stronę proaktywnego zarządzania zdrowiem. Wykrywanie aberracji biomarkerów w fazie przedklinicznej umożliwia interwencje o rzędy wielkości tańsze (modyfikacja stylu życia, farmakoterapia ambulatoryjna zamiast chirurgii). Oszczędności te nie rozkładają się jednak równomiernie – najwięcej zyskują systemy publiczne zdolne do długoterminowych inwestycji, podczas gdy systemy oparte na modelu *fee-for-service* tracą źródła przychodów, co wymusza radykalne przeprojektowanie modeli finansowania ochrony zdrowia.

Kolejnym aspektem jest demokratyzacja dostępu do diagnostyki w obszarach o niskiej gęstości zaludnienia. W regionach peryferyjnych, gdzie stosunek lekarzy do populacji może być 10-krotnie niższy niż w metropoliach, telediagnostyka wspomagana sztuczną inteligencją umożliwia wyrównanie nierówności zdrowotnych. Jednakże materializacja tego potencjału niesie ryzyko paradoksalne: bez odpowiedniej infrastruktury (szerokopasmowy internet) elity miejskie

zmaksymalizują korzyści z diagnostomatów, podczas gdy populacje ruralne pozostaną wykluczone, pogłębiając cyfrową przepaść zdrowotną.

Na rynku pracy powstaje nowa klasa zawodowa: **interpreterzy medyczni AI**. Są to specjaliści weryfikujący wyniki algorytmów, pełniący funkcję warstwy weryfikacji między algorytmiczną hipotezą a decyzją kliniczną. Są odpowiedzialni za interpretację przypadków granicznych oraz komunikację z pacjentem wymagającą empatii. Jeden interpreter może nadzorować diagnostykę setek pacjentów dziennie, co prowadzi do **10–20-krotnej** poprawy produktywności przy zachowaniu jakości opieki, choć rodzi też uzasadnione obawy o dehumanizację medycyny i potencjalną alienację pacjentów od procesu diagnostycznego.

## 2.2. Cyberbezpieczeństwo jako zadanie publiczne

Masowa cyfryzacja usług zdrowotnych eksponuje fundamentalną lukę w architekturze bezpieczeństwa współczesnych państw, ujawniając, że dotychczasowy model cyberbezpieczeństwa jako odpowiedzialności prywatnej jest nieadekwatny w kontekście systemów o znaczeniu krytycznym dla życia. Dane biometryczne z diagnostomatów, stanowiące najbardziej intymną kategorię informacji, wymagają nowego paradygmatu ochrony. Ich kompromitacja grozi nie tylko naruszeniem prywatności, ale może być wykorzystana do ukierunkowanych ataków biologicznych, dyskryminacji ubezpieczeniowej czy szantażu. Agregacja danych zdrowotnych w skali populacyjnej staje się tym samym zasobem bezpieczeństwa narodowego.

Państwa rozwijają koncepcję **modelu „państwa opiekuńczego w zakresie cyberbezpieczeństwa”**. Stanowi to ideologiczne przesunięcie od neoliberalnej koncepcji cyberbezpieczeństwa jako dobra rynkowego w stronę egalitarnej wizji odporności cyfrowej jako odpowiedzialności zbiorowej. Prognozowane inwestycje w ochronę cyfrową szacuje się na **2–3% PKB** krajów rozwiniętych do 2035 roku, co plasuje je na poziomie wydatków na obronność.

Model ten obejmuje trzy kluczowe filary:

1. **Powszechna kryptografia kwantowo-odporna:** Jest absolutnym priorytetem z powodu zagrożenia „zbieraj teraz, odszyfruj później”. Przeciwnicy gromadzą obecnie zaszyfrowane dane, czekając na komputery kwantowe (przewidywane na lata 2030–2035), które złamią obecne algorytmy. Konieczna jest natychmiastowa migracja na standardy takie jak CRYSTALS-Kyber i CRYSTALS-Dilithium zatwierdzone przez NIST. Jest to operacja logistyczna o skali porównywalnej do przejścia z IPv4 na IPv6, wymagająca dekady i koordynacji międzynarodowej.
2. **Publiczne Centra Operacji Bezpieczeństwa (SOC):** Funkcjonują jako cyfrowe odpowiedniki służb ochrony zdrowia publicznego, zapewniając całodobowy monitoring zagrożeń dla całego ekosystemu medycznego. Wyzwanie stanowi równowaga między nadzorem a prywatnością – rozwiązaniem jest zastosowanie technik prywatności różnicowej, umożliwiających wykrywanie zagrożeń na zagregowanych danych bez dostępu do pojedynczych rekordów.
3. **Obowiązkowa certyfikacja bezpieczeństwa IoT:** Wprowadzenie standardów takich jak IEC 62443-4-2 Medical Extension dla diagnostomatów. Wysoki koszt certyfikacji (500 tys. – 2 mln USD na typ urządzenia) tworzy barierę wejścia, prowadząc do konsolidacji rynku i dylematu: bezpieczeństwo kontra innowacyjność.

Rodzi to **paradoks prywatności**: zapewnienie bezpieczeństwa wymaga centralizacji monitoringu, co stoi w sprzeczności z zasadami prywatności typu RODO. Rozwiązanie techniczne

leży w zastosowaniu przetwarzania poufnego oraz uczenia federacyjnego. Te technologie umożliwiają stan, w którym dane pozostają zdecentralizowane i zaszyfrowane, ale modele uczą się globalnie, tworząc architekturę „nadzoru bez widoczności”.

### 3. Faza II: Reintegracja cyfrowo-fizyczna i fuzja tożsamości (2030–2035)

#### 3.1. Cyfrowa tożsamość jako supranarodowy priorytet

Do 2030 roku chaos w zarządzaniu tożsamością cyfrową osiąga punkt krytyczny, określane jako „kryzys tożsamości ery cyfrowej”. Przeciętny użytkownik posiada ponad 90 cyfrowych kont rozproszonych po niezależnych silosach, co prowadzi do niemożności efektywnego zarządzania danymi, rosnących kosztów tarcia w transakcjach oraz masowych naruszeń bezpieczeństwa. Międzynarodowy konsensus uznaje, że fragmentacja tożsamości stanowi systemowe zagrożenie dla gospodarki cyfrowej.

Odpowiedzią jest konwergencja wokół koncepcji **tożsamości samosuverennej (Self-Sovereign Identity - SSI)**. Jednostki odzyskują pełną kontrolę nad swoimi danymi identyfikacyjnymi, decydując komu i w jakim zakresie je ujawniają. Jest to fundamentalna renegotjacja umowy społecznej – władza nad tożsamością przechodzi od instytucji do jednostek, co ma głębokie implikacje dla kapitalizmu nadzoru.

#### Architektura rozwiązania

- **Warstwowa tożsamość:** Rozwiązuje napięcie między potrzebą uniwersalnego identyfikatora a ochroną prywatności poprzez separację na rdzeń kryptograficzny (pary kluczy) oraz kontekstualne atrybuty weryfikowalne (certyfikaty wydawane przez zaufanych wystawców). Umożliwia to „paradoks prywatności przez ujawnianie” – im więcej wystawców potwierdza atrybuty, tym wyższe zaufanie, przy zachowaniu kontroli użytkownika nad szczegółowością danych.
- **Protokół Zdecentralizowanych Identyfikatorów (DID):** Globalny standard W3C stanowiący techniczną fundację SSI. Umożliwia tworzenie identyfikatorów bez centralnego rejestru. Kluczową innowacją jest separacja identyfikatora od mechanizmu jego rozwiązywania, co zapewnia neutralność technologiczną.
- **Interoperacyjność międzynarodowa:** Geopolityczne wyzwanie polegające na stworzeniu systemu wzajemnego uznawania certyfikatów (np. dyplomów czy ubezpieczeń) ponad granicami. Model inspirowany bezpieczeństwem lotniczym sugeruje potrzebę ponadnarodowej „Organizacji Standardów Cyfrowej Tożsamości”, która pełniłaby rolę neutralnego arbitra.

#### 3.2. Formowanie „superpaństw cyfrowych”

Unia Europejska, konsorcjum azjatyckie oraz inicjatywa amerykańska tworzą trzy główne bloki zarządzania tożsamością cyfrową, funkcjonujące jak federacje z częściową cesją suwerenności członków. Państwa delegują uprawnienia w zakresie standardów tożsamości do poziomu supranarodowego w zamian za dostęp do zunifikowanego rynku. Jest to proces formowania się „imperiiw regulacyjnych”, które nie mają monopolu na przemoc, lecz kontrolują infrastrukturę cyfrową.

Prowadzi to do napięć geopolitycznych i zjawiska „fragmentaryzacji internetu 2.0”. Niezgodność standardów kryptograficznych między blokami sprawia, że poświadczenia z jednej jurysdykcji mogą być nieweryfikowalne w innej, tworząc równoległe cyfrowe wszechświaty. Korporacje i startupy muszą utrzymywać wielokrotne reżimy zgodności, co generuje ogromne

koszty i tarcie w transakcjach transgranicznych. Jest to cena płacona za suwerenność cyfrową i bezpieczeństwo kosztem globalnej efektywności.

### 3.3. Fuzja produktów fizycznych z tożsamością cyfrową

Równolegle do unifikacji ludzkiej tożsamości rozwija się koncepcja **cyfrowych paszportów produktów (DPP)**. Każdy przedmiot fizyczny o znaczącej wartości (np. samochód, elektronika, meble) otrzymuje niezbywalną tożsamość cyfrową w formie NFT drugiej generacji. Jest to fundamentalne przewartościowanie własności i zarządzania cyklem życia produktów.

Mechanizm działania opiera się na czterech filarach:

1. **Zdarzenie początkowe:** Produkt otrzymuje unikalny identyfikator („akt urodzenia”) w momencie produkcji, powiązany z fizycznym obiektem poprzez bezpieczne elementy sprzętowe lub biometryczny odcisk palca produktu (PUF).
2. **Śledzenie cyklu życia:** Blockchain rejestruje kompletną historię produktu (serwis, naprawy, zmiany właściciela) w sposób niezmienny. Automatyzacja poprzez IoT jest kluczowa dla eliminacji tarcia.
3. **Rozszerzenie o metawersum:** Cyfrowy bliźniak produktu istnieje jako interaktywna reprezentacja 3D, otwierając nowe strumienie wartości dla marek (cyfrowe akcesoria, społeczności).
4. **Rynki wtórne:** Inteligentne kontrakty automatyzują odsprzedaż i podział zysków (tantiemy dla producentów).

Ekonomiczne implikacje są znaczące: produkty z weryfikowalnym pochodzeniem i historią osiągają premię **30–60%** na rynkach wtórnych dzięki eliminacji asymetrii informacji. Przykładem jest samochód elektryczny z rocznika 2035, którego cyfrowy bliźniak zawiera każdy przejechany kilometr i cykl ładowania, co pozwala na konserwację predykcijną (wydłużenie żywotności o 20–30%) i eliminuje oszustwa na rynku wtórnym.

## 4. Faza III: Emergencja nowego porządku instytucjonalnego (2035–2040)

### 4.1. Państwo emergentne

W trzeciej fazie następuje fundamentalna transformacja roli państwa od centralnego planisty do **koordynatora adaptacyjnego**. Tradycyjne narzędzia zarządzania okazują się nieadekwatne dla hybrydowych ekosystemów o nieliniowej dynamice. Państwo emergentne nie zarządza bezpośrednio, lecz ustanawia standardy interoperacyjności i projektuje mechanizmy bodźców, czerpiąc z teorii złożoności.

Doskonałym przykładem jest **Protokół Inteligentnej Sieci 3.0**. Zamiast centralnie planować produkcję energii, państwo definiuje protokół umożliwiający autonomicznym aktorom (panelom słonecznym, bateriom domowym, pojazdom EV) handel energią w czasie rzeczywistym i samobilansowanie sieci. Rezultatem jest redukcja szczytowych obciążeń sieci o **40%** oraz system znacznie bardziej odporny na awarie. Rola państwa ogranicza się do bycia arbitrem ostatniej instancji i gwarantem interoperacyjności. Filozofią jest zarządzanie poprzez architekturę możliwości, a nie dyrektywy.

### 4.2. Konwergencja cyfrowo-biologiczna

Granice między sferą cyfrową a biologią ulegają rozmyciu poprzez trzy wektory:

- **Spersonalizowane farmaceutyki:** Druk 3D leków na żądanie, dostosowanych do profilu genetycznego i metabolicznego pacjenta. Eliminuje to działania niepożądane

i optymalizuje dawkowanie, ale wymaga nowego paradygmatu regulacyjnego (zatwierdzanie algorytmów, nie molekuł).

- **Platformy wzmacniania poznawczego:** Urządzenia EEG i neurofeedback umożliwiają użytkownikom modulowanie własnych stanów mózgowych (koncentracja, relaksacja) w czasie rzeczywistym. Rodzi to pytania etyczne o „neuro-doping” w edukacji i pracy.
- **Coaching epigenetyczny:** Interwencje behawioralne modyfikujące ekspresję genów, oparte na skanowaniu metylacyjnym określającym wiek biologiczny. Sektor wellness transformuje się w precyzyjną inżynierię długowieczności, co niesie ryzyko pogłębienia nierówności biologicznych.

#### 4.3. Restauracja relacji społecznych

Równoległe do akceleracji technologicznej rozwija się potężny ruch społeczny odrzucający algorytmiczną eksploatację uwagi. „Ekonomia uwagi” z lat 2010–2020, prowadząca do epidemii problemów psychicznych i polaryzacji, zostaje zastąpiona przez ruch „Restauracji Relacji”. Promuje on selektywną obecność (prawo do bycia offline) oraz sieci oparte na protokołach (jak ActivityPub), a nie scentralizowanych platformach.

Do 2040 roku przewiduje się spadek czasu spędzanego na algorytmicznych mediach społecznościowych o **65%** (ze 145 minut dziennie w 2025 do 50 minut). Skutkuje to poprawą samopoczucia psychicznego młodych dorosłych o 35% oraz wzrostem zaufania społecznego o 40%. Transformacja ta jest wynikiem świadomych wyborów politycznych (regulacje antymonopolowe, edukacja cyfrowa) i rynkowych.

#### 5. Trzy subscenariusze przyszłości 2040

Analiza probabilistyczna identyfikuje trzy główne trajektorie rozwoju, zależne od decyzji podjętych w latach 2025–2030:

##### **Subscenariusz A: Techno-federalizm dystrybutywny (prawdopodobieństwo: 45%)**

Scenariusz sukcesu koordynacji międzynarodowej. Główne bloki geopolityczne osiągają konsensus w zakresie interoperacyjności, tworząc mostki między ekosystemami. Gospodarka oparta na DPP osiąga masowe przyjęcie.

##### **Kluczowe wskaźniki (vs 2025):**

- Koszty opieki zdrowotnej: **-30%**
- Skuteczne cyberataki na infrastrukturę krytyczną: **-80%**
- Zaufanie społeczne: **+40%**
- Nierówności cyfrowe: **-50%**

Jest to wariant najbardziej korzystny społecznie, wymagający wczesnego przyjęcia standardów (DID) i masowych inwestycji w cyberbezpieczeństwo publiczne.

##### **Subscenariusz B: Fragmentacja i wojny kryptograficzne (prawdopodobieństwo: 35%)**

Scenariusz niepowodzenia koordynacji, prowadzący do „bałkanizacji” Internetu. Niezgodne standardy uniemożliwiają weryfikację międzyblokową. Ofensywne użycie cyberbroni staje się normą.

##### **Kluczowe wskaźniki (w porównaniu do 2025 r.):**

- Skuteczne cyberataki na infrastrukturę: **+200%**
- Koszty administracyjne dla firm: **+150%**

- Masowe wycieki danych medycznych dotykające ponad 40% populacji.

Prowadzi to do pogłębienia cyfrowej przepaści, cyfrowego uchodźstwa i zapaści zaufania międzynarodowego.

### Subscenariusz C: Hybrydowa rekalkibracja (prawdopodobieństwo: 20%)

Scenariusz selektywnego przyjęcia, charakteryzujący się silnym oporem społecznym wobec tożsamości cyfrowej. Powstają systemy patchworkowe i „dwutorowe społeczeństwo” (cyfrowi maksymaliści vs minimaliści).

#### Kluczowe wskaźniki (w porównaniu do 2025 r.):

- Adopcja tożsamości cyfrowej: tylko 60% populacji.
- Cyberataki: **-40%** (poprawa, ale niższa niż w Scenariuszu A).
- Polaryzacja cyfrowa: **+25%**.

Scenariusz ten cechuje się wysokimi kosztami utrzymania podwójnych systemów i nierównością dostępu.

## 6. Filary strategiczne i wnioski

Materializacja najbardziej korzystnego Scenariusza A wymaga świadomych inwestycji strategicznych w trzech kluczowych domenach, które stanowią dźwignie transformacji:

### 6.1. Energetyka cyfrowa

Konieczna jest integracja inteligentnej infrastruktury energetycznej z systemami cyfrowymi. Rozproszona produkcja i handel energią peer-to-peer, wspierane przez inteligentne zarządzanie popytem, mogą zredukować szczytowe obciążenia sieci o **40%** i obniżyć koszty dla konsumentów o 25%. Wymaga to inwestycji rzędu 1,5–2% PKB rocznie.

### 6.2. Ochrona zdrowia predykcyjna

Transformacja w kierunku modelu proaktywnego wymaga narodowych baz genomicznych (z uczeniem federacyjnym) oraz diagnostyki AI jako usługi publicznej. Powszechne diagnostyki domowe i nowa kadra interpreterów AI mogą obniżyć koszty systemu o **30%** i wydłużyć życie w zdrowiu o 5–7 lat. Inwestycje powinny wynosić 0,8–1,2% PKB rocznie.

### 6.3. Edukacja adaptacyjna

Personalizacja procesów uczenia się z wykorzystaniem AI („efekt Blooma”) może poprawić wyniki nauczania o **2 odchylenia standardowe** i skrócić czas nabywania kompetencji o 40%. Mikrocertyfikaty na blockchainie i uczenie się przez całe życie muszą stać się normą, aby zapewnić mobilność zawodową w erze automatyzacji.