# Techplomacja i architektura odpowiedzialności: narzędzia i bronie w geopolityce cyfrowej według Brada Smitha


**AUTOR**

Fundacja Dobre Państwo



## STRESZCZENIE / ABSTRACT

Artykuł analizuje ewolucję roli korporacji technologicznych, które stają się pełnoprawnymi aktorami geopolitycznymi. Autor wprowadza pojęcie funkcjonalnej władzy infrastrukturalnej oraz 'structural power', wskazując, że kontrola nad kodem i chmurą (code Iś law) daje firmom realny wpływ na funkcjonowanie państw, nawet bez formalnej suwerenności. Zjawisko to prowadzi do powstania tzw. władzy węzłowej, gdzie zależności techniczne determinują możliwości polityczne rządów. Przykładem odpowiedzi państw na te zmiany jest Dania, która jako pierwsza powołała ambasadora technologicznego, aby prowadzić bezpośredni dialog z gigantami z Doliny Krzemowej i zarządzać nową dynamiką relacji między sektorem publicznym a prywatnym w przestrzeni cyfrowej.

8. The article analyzes the evolution of the role of technology corporations, which are becoming full-fledged geopolitical actors. The author introduces the concepts of functional infrastructural power and 'structural power,' indicating that control over code and the cloud (code is law) gives companies real influence over the functioning of states, even without formal sovereignty. This phenomenon leads to the emergence of so-called nodal power, where technical dependencies determine the political possibilities of governments. An example of state responses to these changes is Denmark, which was the first to appoint a technology ambassador to conduct direct dialogue with Silicon Valley giants and manage the new dynamics of relations between the public and private sectors in the digital space.

Artykuł analizuje fundamentalną zmianę w strukturze globalnej władzy, w której korporacje technologiczne przestają być jedynie dostawcami usług, a stają się aktorami geopolitycznymi dysponującymi tzw. funkcjonalną władzą infrastrukturalną. Autor stawia tezę, że w świecie, gdzie kod staje się prawem, a kontrola nad chmurą czy AI daje realny wpływ na suwerenność państw, wiara w etykę twórców (tzw. „dobry Big Tech") jest niewystarczająca i ryzykowna. Kluczem do ochrony ludzkiej godności i demokratycznej sprawczości nie jest zatem zakaz innowacji, lecz systemowa konstytucjonalizacja technologii. Oznacza to przejście od modelu zaufania do modelu rozliczalności, opartego na budowie instytucjonalnych bezpieczników: interoperacyjności, publicznym nadzorze i prawie do sprzeciwu (contestability). Tekst rzuca nowe światło na rywalizację USA i Chin, pokazując ją nie jako prosty spór o rynek, lecz jako zderzenie dwóch odmiennych architektur cyfrowego ładu, w których stawką jest to, czy człowiek pozostanie podmiotem, czy stanie się jedynie obiektem algorytmicznej optymalizacji.

**SŁOWA KLUCZOWE**

techplomacja | funkcjonalna władza infrastrukturalna | structural power | władza węzłowa | code is law | suwerenność cyfrowa | multistakeholder governance | norm entrepreneurs | Digital Switzerland | regulatory dependence | problem principal-agent | suwerenność przez opcjonalność | exit option | interoperacyjność danych | augmentacja obywatelska

## Korporacje technologiczne jako nowi aktorzy geopolityczni

Techplomacy. Kiedy przedsiębiorstwo technologiczne zaczyna zachowywać się jak państwo, choć nim nie jest.

Historia polityczna nowoczesności została napisana językiem państw. To państwo dysponowało terytorium, obywatelami, administracją i armią, zarządzało systemem podatkowym oraz posiadało zdolność zawierania traktatów. Przedsiębiorstwo funkcjonowało wewnątrz tego porządku:

produkowało, handlowało, inwestowało i negocjowało warunki podatkowe, próbując wpływać na regulacje. Cyfryzacja komplikuje ten obraz. Najwięksi gracze technologiczni nie kontrolują już jedynie fabryk czy strumieni kapitału; kontrolują infrastrukturę, dzięki której państwa przechowują pamięć, komunikują się, chronią sieci, organizują debatę publiczną i korzystają ze sztucznej inteligencji, realizując w ten sposób część swoich podstawowych funkcji. W tym punkcie klasyczne przeciwstawienie państwa i firmy przestaje wystarczać.

Materiał źródłowy opisuje tę zmianę poprzez pojęcie Techplomacy: przedsiębiorstwa technologiczne stają się partnerami rządów w rozmowach o normach cyberbezpieczeństwa, transgranicznym dostępie do danych, ochronie wyborów czy odpowiedzialnym korzystaniu z infrastruktury. Autorzy źródła idą miejscami bardzo daleko, określając korporacje mianem pełnoprawnych aktorów geopolitycznych. Sformułowanie to trafnie oddaje skalę ich wpływu, lecz wymaga naukowego doprecyzowania.

Korporacja nie jest suwerenem w rozumieniu prawa międzynarodowego. Nie posiada ludności w sensie konstytucyjnym, nie dysponuje demokratyczną legitymacją, nie uchwala powszechnie obowiązującego prawa i co do zasady nie posiada monopolu legalnego przymusu. Posiada jednak coś, co można określić jako funkcjonalną władzę infrastrukturalną. Rozróżnienie to jest kluczowe: suwerenność formalna i realna zdolność oddziaływania nie muszą spoczywać w tych samych rękach. Państwo może formalnie dzierżyć najwyższą władzę prawną na swoim terytorium, a jednocześnie zależeć od zagranicznego dostawcy systemu operacyjnego, usług chmurowych, infrastruktury telekomunikacyjnej, półprzewodników czy zabezpieczeń cybernetycznych. Korporacja nie uchyli ustawy parlamentu, ale decyzja techniczna podjęta w jej centrali może w jednej chwili zmienić dostępność usługi dla milionów obywateli w wielu krajach.

Susan Strange określała podobne zjawiska mianem structural power – władzy polegającej nie tyle na zmuszaniu konkretnego aktora do pojedynczego działania, co na kształtowaniu struktur, w których inni muszą funkcjonować. Władza właściciela infrastruktury ma właśnie taki charakter. Nie musi on wydawać instrukcji każdemu użytkownikowi; zamiast tego definiuje protokoły, dostępność funkcji, warunki bezpieczeństwa, architekturę przechowywania i techniczne możliwości innych podmiotów. To forma władzy subtelniejsza niż rozkaz administracyjny.

## Władza węzłowa i narodziny techplomacji

Kiedy przedsiębiorstwo zmienia standard uwierzytelniania, politykę aktualizacji lub sposób świadczenia usługi chmurowej, tysiące organizacji dostosowują się do tych zmian nie dlatego, że zostały prawnie zobowiązane, lecz dlatego, że funkcjonują wewnątrz stworzonego przez firmę

ekosystemu. Infrastruktura reguluje przez możliwość. Lessigowska formuła code is law nabiera tu wymiaru geopolitycznego. Kod nie zastępuje ustawy, lecz tworzy warunki, w których ta ustawa jest wykonywana. Państwo może gwarantować prawo do prywatności, jednak stopień jego praktycznej realizacji zależy od szyfrowania, logów dostępu, zarządzania kluczami i architektury przechowywania danych. Może nakazać ochronę infrastruktury krytycznej, lecz realna odporność zależy od producentów oprogramowania. Może chronić wybory, ale kampanie polityczne wciąż opierają się na prywatnych systemach pocztowych i usługach cyberbezpieczeństwa.

Powstaje władza węzłowa. Podmiot kontrolujący krytyczny punkt sieci posiada wpływ większy, niż wynikałoby to z jego formalnego statusu. W teorii sieci centralność węzła nie zależy wyłącznie od jego rozmiaru, lecz od liczby kluczowych przepływów, które przez niego przechodzą. W polityce cyfrowej podobny mechanizm dotyczy dostawców chmury, systemów operacyjnych, platform komunikacyjnych, infrastruktury certyfikatów, producentów procesorów czy twórców bazowych modeli AI.

Niewielka liczba firm może uzyskać znaczenie systemowe nawet bez tradycyjnych atrybutów państwowości. Ich władza nie wynika z posiadania terytorium, lecz z zależności innych od infrastruktury, którą kontrolują. Właśnie tę zmianę dostrzegła Dania.

W 2017 roku stała się ona pierwszym państwem, które powołało ambasadora technologicznego, uznając technologię za samoistne zagadnienie polityki zagranicznej i bezpieczeństwa. Urząd duńskiego Tech Ambassadora istnieje do dziś; działa on między Kopenhagą a Doliną Krzemową, prowadząc bezpośredni dialog z globalnymi gigantami technologicznymi oraz współpracując w ramach UE, NATO i ONZ. Duńskie Ministerstwo Spraw Zagranicznych uzasadnia tę strukturę faktem, że największe firmy technologiczne dysponują siłą ekonomiczną i polityczną, która w pewnych wymiarach jest porównywalna ze znaczeniem państw. To symboliczne odwrócenie tradycyjnej dyplomacji. Dawniej ambasador reprezentował jedno państwo wobec drugiego; Dania uznała natomiast, że niektóre relacje z prywatnymi przedsiębiorstwami są na tyle istotne strategicznie, iż wymagają aparatu przypominającego dyplomację. Nie chodzi już o lobbystę odwiedzającego ministerstwo – to państwo wysyła zawodowych dyplomatów w stronę sektora technologicznego.

Pojęcie techplomacji jest czymś więcej niż atrakcyjnym neologizmem. Pokazuje ono zmianę topologii stosunków międzynarodowych. Klasyczny model był przede wszystkim poziomy: państwo–państwo. Współczesny model staje się wielowarstwowy: obejmuje relacje państwo–państwo, państwo–korporacja, korporacja–korporacja, a także interakcje z organizacjami międzynarodowymi oraz wielostronne koalicje łączące rządy, biznes, naukę i społeczeństwo obywatelskie. Robert Keohane i Joseph Nye opisywali już wcześniej świat complex

interdependence, w którym kanały stosunków transnarodowych nie ograniczają się wyłącznie do kontaktów między rządami.

## Korporacje jako operatorzy środowiska politycznego i bezpieczeństwa

Cyfryzacja nadała tej koncepcji materialną infrastrukturę. Przedsiębiorstwo technologiczne przestało być jedynie jednym z aktorów wpływających na politykę; stało się operatorem środowiska, w którym ta polityka jest realizowana. Szczególnie jaskrawym przykładem jest obszar cyberbezpieczeństwa. Materiał źródłowy obrazuje, jak Digital Crimes Unit Microsoftu wykorzystywała instrumenty prawa cywilnego — m.in. ochronę znaków towarowych oraz konstrukcje dotyczące naruszenia własności — do przejmowania infrastruktury używanej przez grupy cyberprzestępcze i aktorów państwowych. Przejęte domeny kierowano do systemów typu sinkhole, co pozwalało skutecznie odciąć napastników od zainfekowanych urządzeń.

Z perspektywy socjologii prawa mamy do czynienia z fascynującą hybrydą. Prywatna firma posługuje się narzędziami prawa cywilnego, by osiągnąć rezultat funkcjonalnie przypominający operację bezpieczeństwa publicznego. Nie jest policją, lecz neutralizuje fragment infrastruktury ataku. Nie jest wywiadem, ale analizuje globalne kampanie. Nie pełni roli ministerstwa spraw zagranicznych, a jednak publicznie przypisuje aktywność grupom powiązanym z państwami i negocjuje normy zachowania z rządami. Można określić to jako prywatyzację fragmentu zdolności bezpieczeństwa, choć termin ten wymaga ostrożności. Firma nie przejmuje bowiem całej funkcji państwa; działa tam, gdzie jej własność, wiedza techniczna, globalny zasięg i szybkość reakcji pozwalają osiągnąć efekty niedostępne dla ociężałego aparatu państwowego. Jest zatem bardziej dodatkiem do suwerenności niż jej formalnym następcą.

Taka komplementarność rodzi jednak problem demokratyczny. Jeśli podmiot prywatny wykonuje funkcje o znaczeniu publicznym, kluczowe staje się pytanie: kto kontroluje jego decyzję o zaniechaniu tych działań? Urzędnika państwowego wiąże ustawa, parlamentarzystę można odsunąć w wyborach, a decyzję administracyjną zaskarżyć. Wobec korporacji mechanizmy odpowiedzialności są zupełnie inne: prawo konkurencji, regulacje sektorowe, kontrakty, rynek, reputacja czy nadzór akcjonariuszy. Choć nie są one pozbawione znaczenia, nie stanowią odpowiednika demokratycznego mandatu. Należy zatem odrzucić romantyczną wizję "dobrego Big Techu", który sprawniej niż państwa rozwiąże globalne problemy. Sprawność nie jest substytutem legitymizacji.

W tym tkwi jedna z największych sprzeczności Techplomacy. Państwa potrzebują firm technologicznych właśnie ze względu na ich wiedzę i infrastrukturę, których brakuje administracji. Jednak im bardziej państwo polega na tych zasobach, tym silniej uzależnia realizację swoich funkcji od podmiotów, których cel korporacyjny nie musi być tożsamy z dobrem publicznym. Ekonomia instytucjonalna określiłaby to mianem problemu principal-agent, z zastrzeżeniem, że relacja ta jest bardziej złożona niż klasyczne zlecenie. Państwo nie zawsze występuje tu w roli zwierzchnika dysponującego pełnią kontroli; często technologiczny agent posiada większą wiedzę niż polityczny principal i to on jest właścicielem infrastruktury. Powstaje tym samym głęboka asymetria informacji i zdolności.

W takich warunkach próby odzyskania kontroli poprzez regulacje napotykają na konieczność współpracy z podmiotem regulowanym. To klasyczny problem regulatory dependence: organ nadzoru kontroluje system, którego technicznego działania nie zna w pełni i musi polegać na dokumentacji dostarczanej przez producenta. Im bardziej złożona technologia, tym większe ryzyko poznawczej zależności urzędu od przedsiębiorstwa. Techplomacy jest więc nie tylko dyplomacją, ale przede wszystkim zarządzaniem asymetrią wiedzy między władzą publiczną a właścicielem technologii.

Korporacyjną odpowiedzią na ten stan rzeczy jest metafora "Digital Switzerland". Microsoft sugeruje w niej, że przedsiębiorstwo technologiczne może być neutralnym obrońcą klientów, zapewniającym cyberochronę niezależnie od narodowości i odmawiającym wspierania ofensywnych operacji państwowych. Idea ta jest normatywnie atrakcyjna, lecz konieczne jest oddzielenie metafory od statusu prawnego. Microsoft nie jest Szwajcarią, a firma nie zyskuje neutralności w rozumieniu prawa międzynarodowego jedynie poprzez deklarację misji. Korporacja posiada państwo siedziby, podlega jego prawom, jej pracownicy podlegają konkretnym jurysdykcjom, a infrastruktura znajduje się na określonych terytoriach. W razie konfliktu prawnego prywatna deklaracja nie uchyla obowiązującego prawa. "Digital Switzerland" należy zatem rozumieć jako doktrynę powiernictwa i strategicznej wiarygodności, a nie jako prywatny odpowiednik neutralności państwowej.

Neutralność ta ma również twarde uzasadnienie biznesowe: globalny dostawca chmury nie może być postrzegany jako nieformalne narzędzie jednego rządu, jeśli chce sprzedawać usługi w jurysdykcjach obcych. Materiał źródłowy wskazuje, że utrata zaufania po ujawnieniach dotyczących amerykańskiego nadzoru bezpośrednio uderzyła w konkurencyjność amerykańskich firm na rynkach takich jak Niemcy.

## Budowanie norm poprzez zaufanie i inicjatywy wielostronne

Etyka i interes handlowy mogą się spotkać, dlatego nie należy automatycznie dyskwalifikować etyki jako formy marketingu. W wielu instytucjach to właśnie perspektywa ekonomicznej nagrody za wiarygodność sprawia, że normy zostają utrwalone. Problem pojawia się jednak wtedy, gdy język dobra publicznego maskuje interes prywatny, zamiast podlegać zewnętrznej kontroli.

Warto w tym miejscu powrócić do pojęcia społecznej licencji na działanie. Firma technologiczna może posiadać formalne zezwolenie prawne na prowadzenie działalności, lecz jej zdolność funkcjonowania w sektorach strategicznych zależy także od społecznego zaufania. Bank przechowujący pieniądze, szpital zarządzający danymi medycznymi czy operator chmury przechowujący cyfrową pamięć instytucji działają na rynkach, gdzie utrata zaufania może być równie dotkliwa co sankcja administracyjna. W tym kontekście techplomacy staje się dyplomacją zaufania. Firma musi przekonać rządy, że nie jest ukrytym instrumentem państwa pochodzenia; państwa muszą uwiarygodnić dostawców, że żądania dotyczące danych będą oparte na prawie, a użytkownicy muszą wierzyć, że ich informacje nie zostaną wykorzystane wbrew przyjętemu celowi.

W jednym ekosystemie splatają się reputacja, prawo, bezpieczeństwo i polityka zagraniczna. Laboratorium tej nowej struktury stanowią inicjatywy wielostronne, w których rządy nie występują samotnie. Cybersecurity Tech Accord, Paris Call for Trust and Security in Cyberspace oraz Christchurch Call obrazują ewolucję w kierunku multistakeholder governance. Są to koalicje przedsiębiorstw, państw i społeczeństwa obywatelskiego, które dążą do wypracowania norm w obszarze cyberbezpieczeństwa, ochrony wyborów i przeciwdziałania najbardziej szkodliwym zastosowaniom technologii. Cybersecurity Tech Accord pozostaje aktywny również w 2026 roku, publikując stanowiska m.in. wobec eskalacji ofensywnych działań cybernetycznych, działalności cybernajemników oraz zagrożeń związanych z agentową AI.

Informacje o przekroczeniu liczby 160 sygnatariuszy świadczą o instytucjonalizacji współpracy branżowej ponad podziałami korporacyjnymi. Znaczenie tych inicjatyw nie polega na tworzeniu traktatów międzynarodowych — one ich nie tworzą. Ich istotą jest produkcji norm przed powstaniem prawa. Aktorzy definiują w ten sposób akceptowalne zachowania, budują język opisu problemu, ustanawiają oczekiwania reputacyjne i przygotowują rozwiązania, które później mogą przeniknąć do regulacji państwowych lub międzynarodowych. Jest to mechanizm dobrze znany w teorii stosunków międzynarodowych; Martha Finnemore i Kathryn Sikkink opisywały norm entrepreneurs jako aktorów próbujących zmienić społeczne rozumienie zachowań dopuszczalnych. W świecie cyfrowym korporacja może stać się takim przedsiębiorcą normatywnym. Proponowana

przez Microsoft Cyfrowa Konwencja Genewska jest właśnie próbą norm entrepreneurship: firma formułuje problem ochrony cywilów w kategoriach zaczerpniętych z prawa konfliktów zbrojnych, mimo że sama nie posiada kompetencji do stworzenia wiążącego traktatu. Podobnie Paris Call, zainicjowany przez Francję w 2018 roku, został zaprojektowany jako wielostronna platforma łącząca państwa, biznes i społeczeństwo obywatelskie.

Jego architektura zakłada m.in. ochronę osób i infrastruktury, bezpieczeństwo produktów, przeciwdziałanie ingerencjom w wybory oraz ograniczanie proliferacji szkodliwych narzędzi cybernetycznych. Kluczowe jest tutaj odejście od przekonania, że normy cyberprzestrzeni może stworzyć jedna kategoria aktorów. Multistakeholderism posiada jednak własny problem legitymizacyjny. Fakt, że przy jednym stole zasiadają państwo, globalna korporacja, organizacja pozarządowa i ekspert, nie oznacza, iż wszystkie te podmioty dysponują równoważnym mandatem. Państwo demokratyczne posiada bowiem procedurę wyborczą i konstytucyjny obowiązek reprezentowania obywateli.

## Kompetencja techniczna nie daje prawa do suwerenności

Korporacja reprezentuje przede wszystkim własną organizację i interesariuszy. Organizacja pozarządowa kieruje się swoją misją i członkami, natomiast ekspert reprezentuje kompetencję, a nie demos. Dlatego „wielostronność" nie może stać się pretekstem do rozmycia odpowiedzialności politycznej. Konsultacje z przedsiębiorstwami są konieczne tam, gdzie dysponują one niezbędną wiedzą techniczną.

Nie oznacza to jednak prawa firm do współdecydowania na równych zasadach o prawach podstawowych obywateli. Można tu sformułować zasadę: kompetencja daje prawo do wysłuchania; nie daje automatycznie prawa do suwerenności. Jest to szczególnie istotne w obszarze moderacji, AI i cyberbezpieczeństwa, gdzie decyzja techniczna bywa przedstawiana jako ekspercka, choć w rzeczywistości kryje w sobie wybór polityczny. Technologiczne pytanie „jak ograniczyć ryzyko?" często maskuje pytanie normatywne: „jakiego ryzyka i dla kogo?". Ekspert potrafi obliczyć prawdopodobieństwo, lecz to społeczeństwo musi określić granice dopuszczalnej ingerencji. Techplomacy nie może zatem oznaczać rządów technokratów; powinna być instytucjonalnym spotkaniem różnych rodzajów wiedzy i legitymizacji.

Drugim problemem jest konflikt interesów. Firma technologiczna może być jednocześnie dostawcą infrastruktury państwa, doradcą przy tworzeniu standardów, uczestnikiem grup eksperckich,

stroną regulowaną i beneficjentem przyjętego rozwiązania. Takie nagromadzenie ról nie musi dowodzić nadużycia, ale bezwzględnie wymaga przejrzystości. W prawie administracyjnym obowiązuje zasada nemo iudex in causa sua: nikt nie może być sędzią we własnej sprawie. Cyfrowy odpowiednik tej intuicji brzmi: firma nie może być jedynym autorem norm, według których sama zostanie uznana za odpowiedzialną. Współczesne prawo technologiczne rozwija zatem obowiązki audytu, dostęp dla badaczy, raportowanie i zewnętrzny nadzór. Techplomacy pozbawiona rozliczalności łatwo mogłaby przeobrazić się w oligarchiczną dyplomację najpotężniejszych przedsiębiorstw.

Trzeci problem stanowi asymetria między samymi firmami. Termin „Big Tech" sugeruje jednolity sektor, podczas gdy kontrola nad infrastrukturą jest rozproszona: chmura, półprzewodniki, telekomunikacja, systemy operacyjne, wyszukiwarki, platformy społecznościowe, modele AI i cyberbezpieczeństwo mają odmienną strukturę konkurencji. Koalicja największych graczy może kreować normy, których koszt jest dla nich akceptowalny, lecz prohibitywny dla mniejszych podmiotów. Prywatna standaryzacja może więc zwiększać bezpieczeństwo, a jednocześnie tworzyć bariery wejścia. To kolejny przykład punktu styku odpowiedzialności normatywnej i ekonomii konkurencji.

Czwarty problem dotyczy państw słabszych technologicznie. Podczas gdy mocarstwo negocjuje z korporacją jak równorzędny partner, małe państwo, zależne od kilku globalnych dostawców, dysponuje ograniczoną siłą przetargową. Powstaje ryzyko technologicznego odpowiednika zależności centrum-peryferia: formalnie suwerenne państwo nie kontroluje kluczowych warstw własnej infrastruktury i nie posiada zasobów, by samodzielnie je odtworzyć.

W tym kontekście pojęcie suwerenności cyfrowej zyskuje sens szerszy niż tylko lokalizacja danych. Suwerenność nie wymaga autarkii – całkowita samowystarczalność technologiczna jest dziś praktycznie niemożliwa. Wymaga jednak zachowania zdolności wyboru, negocjowania i migracji między dostawcami, a także rozumienia zależności i sprawnego działania w sytuacjach kryzysowych. Można to określić jako suwerenność przez opcjonalność. Państwo traci suwerenność nie w momencie korzystania z zagranicznej technologii, lecz wtedy, gdy utraci zdolność powiedzenia dostawcy „nie" bez sparaliżowania własnych podstawowych funkcji. Wówczas interoperacyjność, migracja danych, otwarte standardy i kontrola łańcucha dostaw stają się narzędziami geopolitycznymi. Exit option, analizowana wcześniej przy Data Act, ma kluczowe znaczenie również dla suwerenności państwa.

Władza dostawcy rośnie wraz z kosztem odejścia klienta. Hirschmanowskie exit, voice and loyalty można zatem przenieść na grunt geopolityki technologicznej. Państwo może próbować wpływać na dostawcę poprzez voice lub pozostać przy nim z powodu loyalty, ale pełną zdolność negocjacyjną

odzyskuje dopiero wtedy, gdy posiada realne exit. Bez tego rozmowa dyplomatyczna łatwo zmienia się w zarządzanie zależnością.

Istnieje jednak zależność odwrotna. Globalna firma potrzebuje państwa: prawa własności, sądów, infrastruktury energetycznej, wykształconych kadr, stabilnej waluty, bezpieczeństwa fizycznego i dostępu do rynku. Wielkie korporacje nie istnieją „ponad państwami" w sensie dosłownym; ich globalność opiera się na sieci narodowych porządków prawnych. Państwo i korporacja pozostają zatem w relacji wzajemnej zależności asymetrycznej, a nie prostego podporządkowania jednej strony drugiej.

## Odpowiedzialna Techplomacy jako kompozycja niepełnych kompetencji

W szczególnie drażliwy sposób ujawnia to geopolityka praw człowieka. Human Rights Assessments służą jako instrument oceny, czy lokalizacja infrastruktury w danej jurysdykcji nie stworzy nadmiernego ryzyka wykorzystania technologii do inwigilacji i represji. Pokazuje to, że decyzja o budowie centrum danych może być traktowana jako wybór etyczno-geopolityczny, a nie tylko rachunek kosztów energii i latencji. Tutaj jednak znów pojawia się pytanie o mandat.

Czy prywatna korporacja powinna samodzielnie oceniać, które państwo zasługuje na dostęp do określonej technologii? Jeśli tak, firma staje się prywatnym arbitrem praw człowieka. Jeśli nie, może zostać zmuszona do dostarczania narzędzi represyjnemu systemowi tylko dlatego, że jej działalność pozostaje formalnie legalna. Nie ma prostego rozwiązania.

Najbardziej rozsądny model wymaga synergii prawa państwowego, sankcji międzynarodowych, zasad ONZ dotyczących biznesu i praw człowieka, korporacyjnego due diligence oraz transparentności. Odpowiedzialność nie może być ani całkowicie sprywatyzowana, ani w pełni przerzucona na państwo. To sedno współczesnego corporate governance. Dawny model Miltona Friedmana redukował społeczną rolę przedsiębiorstwa do działania w interesie właścicieli w ramach obowiązującego prawa. W świecie przedsiębiorstw infrastrukturalnych taka odpowiedź staje się trudna do utrzymania, ponieważ firma współtworzy środowisko, dla którego prawo dopiero powstaje. Jeśli przedsiębiorstwo wie wcześniej niż ustawodawca, że dana technologia niesie wielkoskalowe ryzyko, nie może moralnie czekać biernie na pierwszą ustawę. Właśnie taki sens ma maksyma Smitha i Browne: jeśli technologia zmienia świat, jej twórcy ponoszą część odpowiedzialności za problemy świata, który pomogli stworzyć.

Nie oznacza to jednak przyznania korporacjom prawa do samodzielnego definiowania dobra wspólnego. Oznacza obowiązek uczestnictwa w rozwiązywaniu problemów, ale pod warunkiem publicznej rozliczalności. Można tu sformułować trzyczęściową doktrynę odpowiedzialnej Techplomacy. Pierwszym elementem jest kompetencja bez suwerenności: przedsiębiorstwo wnosi wiedzę, infrastrukturę i zdolność działania, ale nie przejmuje demokratycznego mandatu państwa. Drugim jest współpraca bez podporządkowania: państwo korzysta z firmy, lecz zachowuje alternatywy, kontrolę regulacyjną i możliwość odejścia. Trzecim jest normotwórstwo bez samolegitimizacji: sektor prywatny może proponować standardy i budować koalicje, ale normy ingerujące w prawa człowieka wymagają publicznej legitymacji.

Techplomacy przestaje być wtedy niepokojącym obrazem "korporacji większej od państwa". Staje się techniką zarządzania światem, w którym żaden pojedynczy rodzaj instytucji nie posiada już wystarczającej wiedzy i zdolności, aby samodzielnie regulować infrastrukturę cyfrową. Państwo ma legitymację, lecz często brakuje mu technologii. Firma dysponuje technologią, ale nie ma demokratycznego mandatu. Nauka posiada wiedzę, lecz nie władzę wykonawczą. Społeczeństwo obywatelskie reprezentuje prawa i interesy, ale nie dysponuje aparatem przymusu. System międzynarodowy tworzy normy, lecz zwykle działa wolniej niż rynek. Cyfrowe governance jest więc sztuką komponowania niepełnych kompetencji.

## Technologia jako nowa gramatyka potęgi i zderzenie modeli cyfrowego ładu

To właśnie dlatego duński eksperyment dyplomatyczny okazał się czymś więcej niż tylko ciekawostką z 2017 roku. Aktualna strategia Tech Ambassadora wciąż opiera się na bezpośrednich relacjach z globalnymi gigantami technologicznymi, zarządzaniu AI i technologiami kwantowymi, współpracy w obszarze bezpieczeństwa oraz budowaniu globalnych norm. Oficjalny urząd definiuje bowiem technologię nie jako element polityki przemysłowej, lecz jako kwestię geopolityczną, dotyczącą bezpieczeństwa i praw człowieka.

Ambasada przyszłości może zatem posiadać nie tylko wydziały polityczny, handlowy czy wojskowy, ale także kompetencję technologiczną. Współczesny dyplomata musi rozumieć półprzewodniki, chmurę, AI, cyberbezpieczeństwo i standardy danych, podobnie jak jego poprzednicy musieli orientować się w energetyce, szlakach morskich czy broni nuklearnej. Technologia weszła do gramatyki potęgi.

W tym miejscu otwiera się kolejny etap analizy. Korporacje technologiczne stały się pełnoprawnymi uczestnikami geopolityki, jednak nie działają one w próżni. Funkcjonują w świecie coraz ostrzejszej rywalizacji dwóch największych ekosystemów: amerykańskiego i chińskiego. Ich spór nie dotyczy wyłącznie wolumenu sprzedaży urządzeń czy skali modeli AI; dotyczy on fundamentalnie odmiennych relacji między państwem, przedsiębiorstwem, jednostką a przepływem informacji i bezpieczeństwem. W tym kontekście pojawia się prowokacyjna figura: Arystoteles spotyka Konfucjusza.

Nie wolno jednak zamienić jej w cywilizacyjny stereotyp, według którego „Zachód to wolność", a „Chiny to kontrola". Takie uproszczenie byłoby historycznie i naukowo niepoważne. Metafora ta może natomiast otworzyć znacznie ciekawsze pytanie: jak różne tradycje polityczne, modele kapitalizmu, koncepcje bezpieczeństwa i relacje państwo-rynek wpływają na sposób organizacji technologii? Stajemy przed próbą głębszego zderzenia filozofii politycznej: „Arystoteles spotyka Konfucjusza. USA, Chiny i dwie konkurujące architektury cyfrowego ładu". Zamiast prostego katalogu przewag mocarstw, należy zapytać, czym różnią się ich modele innowacji, suwerenności danych, kontroli przedsiębiorstw, bezpieczeństwa narodowego i praw jednostki – oraz dlaczego ta konkurencja może przesądzić nie tylko o rynku technologii, ale o instytucjonalnej architekturze XXI wieku.

Metafora „Arystoteles spotyka Konfucjusza" jest intelektualnie kusząca, lecz bywa również niebezpieczna. Przeciwstawia ona Zachód – kojarzony z logiką, jednostką, liniowym postępem i "wolnościami tygrysa" – Wschodowi, utożsamianemu z relacyjnością, harmonią, cyklicznością i "bezpieczeństwem dżungli". Jako heurystyka pozwala to uchwycić odmienne intuicje dotyczące relacji między jednostką a zbiorowością, jednak jako opis historyczny byłoby zbyt powierzchowne.

Arystoteles nie był filozofem liberalnego indywidualizmu w dzisiejszym rozumieniu, a Konfucjusz nie stworzył doktryny cyfrowego autorytaryzmu. Pierwszy uważał człowieka za zoon politikon – istotę realizującą się we wspólnocie politycznej; drugi budował etykę relacji, rytuału i moralnego samodoskonalenia, a nie teorię totalnej administracyjnej kontroli. Współczesnych Stanów Zjednoczonych nie można więc wyprowadzać prostą linią z Aten, podobnie jak systemu Chińskiej Republiki Ludowej nie można redukować do Konfucjusza. Trafniej jest potraktować obu myślicieli jako symbole dwóch pytań, które każda cywilizacja musi zadać technologii. Pierwsze brzmi: jaką przestrzeń autonomii należy pozostawić jednostce, innowatorowi i przedsiębiorcy? Drugie: jak utrzymać ład zbiorowy, bezpieczeństwo i zdolność do wspólnego działania?

Napięcie między tymi pytaniami nie przebiega dokładnie wzdłuż Pacyfiku – istnieje ono wewnątrz obu systemów. Stany Zjednoczone dysponują rozbudowanym aparatem bezpieczeństwa narodowego, sankcji i kontroli eksportu; Chiny z kolei tworzą rynek, dopuszczają konkurencję

przedsiębiorstw i mechanizmy ochrony danych osobowych. Różnica dotyczy przede wszystkim sposobu hierarchizacji tych wartości oraz instytucji, które mają ostatnie słowo. Obraz "wolności tygrysa" i "bezpieczeństwa dżungli" jest zatem użyteczny tylko wtedy, gdy pozostaje metaforą.

## Różnica w architekturze koordynacji innowacji między USA a Chinami

Amerykański model historycznie opierał się na założeniu, że innowacja rodzi się z rozproszenia eksperymentu. Firma, laboratorium, uniwersytet czy przedsiębiorca dysponują szeroką swobodą poszukiwania rozwiązań, a państwo interweniuje punktowo: poprzez prawo konkurencji, kwestie bezpieczeństwa narodowego, zamówienia publiczne, finansowanie badań federalnych i regulacje sektorowe. Chiny częściej stosują model koordynowany: państwo identyfikuje obszary strategiczne, mobilizuje kapitał, infrastrukturę, administrację i przedsiębiorstwa, dążąc do pełnej zgodności innowacji z szerokim planem rozwoju i bezpieczeństwa. Nie jest to jednak proste przeciwstawienie rynku i państwa. Dolina Krzemowa nie powstała poza państwem.

Internet, półprzewodniki, GPS oraz fundamenty współczesnej informatyki rozwijały się przy ogromnym udziale publicznego finansowania i zamówień obronnych USA. Z drugiej strony chińska gospodarka nie jest wyłącznie administracyjną piramidą: przedsiębiorstwa konkurują, podejmują ryzyko, tworzą globalne produkty, a prywatny kapitał pozostaje istotnym elementem ekosystemu. Prawdziwa różnica leży zatem w architekturze koordynacji.

Amerykański model można interpretować przez pryzmat Hayeka i Schumpetera. Hayek podkreślał rozproszenie wiedzy: żadne centrum nie dysponuje informacjami wystarczającymi do skutecznego planowania całej gospodarki, przez co rynek staje się mechanizmem odkrywania. Schumpeter wprowadził figurę przedsiębiorcy i twórczej destrukcji, w której rozwój dokonuje się poprzez nieustanne burzenie starych układów. W takim świecie technologiczny tygrys powinien mieć miejsce do biegu, ponieważ państwo nie wie z góry, który eksperyment okaże się przełomowy. Chińska praktyka rozwojowa jest bliższa logice państwa rozwojowego, choć to pojęcie nie wyczerpuje jej specyfiki. System ten łączy mechanizmy rynkowe z głęboką zdolnością administracyjnego wyznaczania kierunków strategicznych, finansowania infrastruktury i koordynowania zasobów z celami bezpieczeństwa oraz modernizacji państwa. Nie jest to czysty konfucjanizm. Współczesna chińska architektura instytucjonalna łączy tradycję konfucjańską, legalistyczne myślenie o sprawności aparatu władzy, leninowską organizację partyjną, doświadczenia gospodarki planowej oraz późniejszy pragmatyzm rynkowy. To rozróżnienie ma kluczowe znaczenie dla technologii.

W modelu amerykańskim przedsiębiorstwo może przez długi czas wyprzedzać regulatora. W modelu chińskim firma technologiczna może dynamicznie rosnąć, lecz jej przestrzeń działania pozostaje ostatecznie podporządkowana strategicznym priorytetom państwa i partii. Nie oznacza to, że jeden system jest „innowacyjny", a drugi „kontrolujący". Oba dążą do jednoczesnego osiągnięcia innowacyjności i kontroli, lecz odmiennie rozkładają ryzyko utraty tej ostatniej. Aktualna polityka Stanów Zjednoczonych obrazuje ten dualizm. Administracja prezydenta Donalda Trumpa w styczniu 2025 roku uchyliła poprzednie podejście wykonawcze, deklarując usuwanie barier dla amerykańskiego przywództwa w AI. Następnie America's AI Action Plan z lipca 2025 roku połączył deregulacyjną retorykę przyspieszania innowacji z twardą polityką geostrategiczną w obszarze mocy obliczeniowej, półprzewodników, infrastruktury i kontroli eksportu.

To pozorny paradoks tylko wtedy, gdy bezpieczeństwo i wolny rynek traktujemy jako jedną oś. W rzeczywistości Stany Zjednoczone budują maksymalnie konkurencyjny ekosystem wewnętrzny, jednocześnie ograniczając dostęp strategicznych rywali do kluczowych zasobów. Rynek jest wolniejszy wewnątrz granicy bezpieczeństwa, lecz sama granica bezpieczeństwa może być bardzo twarda. Najlepszym przykładem są półprzewodniki. W ostatnich latach USA konsekwentnie rozbudowywały ograniczenia dotyczące zaawansowanych procesorów, urządzeń produkcyjnych i high-bandwidth memory, argumentując, że technologie te mogą wspierać chińskie zastosowania wojskowe, wywiadowcze oraz rozwój zaawansowanej AI.

## Dynamika zależności i chiński model governance AI

Sytuacja na sierpień 2026 roku nie jest jednak prostą historią coraz szczelniejszej blokady. W styczniu tego samego roku BIS zmienił politykę licencyjną wobec części układów, w tym Nvidia H200 i AMD MI325X, dopuszczając indywidualne rozpatrywanie eksportu do zatwierdzonych odbiorców w Chinach, pod warunkiem zastosowania określonych zabezpieczeń.

Jest to istotna korekta wobec uproszczonego języka "technologicznego decouplingu". Amerykańska strategia okazuje się bardziej dynamiczna: dąży do ograniczenia dostępu do zdolności uznanych za krytyczne, lecz jednocześnie stara się nie oddać całego rynku chińskim konkurentom i nie niszczyć własnej bazy przemysłowej. Kontrola eksportu staje się zatem instrumentem nie tylko bezpieczeństwa, lecz także zarządzania zależnością technologiczną przeciwnika.

Geopolityka AI prowadzi tu do paradoksu przypominającego klasyczną teorię odstraszania. Stany Zjednoczone chcą pozostać źródłem technologii, gdyż zależność innych od amerykańskiego ekosystemu daje realny wpływ. Całkowite odcięcie mogłoby jednak zmusić odbiorcę do przyspieszenia budowy własnego substytutu. Sankcja może zatem jednocześnie ograniczać

możliwości konkurenta w krótkim okresie i zwiększać jego motywację do autonomii w długim. To właśnie ten rodzaj sprzężenia zwrotnego umyka statycznym analizom: broń ekonomiczna zmienia zachowanie systemu, przeciwko któremu jest używana.

Chińska odpowiedź nie ogranicza się wyłącznie do obrony przed restrykcjami. Państwo systematycznie buduje własną infrastrukturę AI – moce obliczeniowe, ekosystem modeli, półprzewodniki, zasoby danych i zastosowania przemysłowe. Oficjalny program "AI Plus" z 2025 roku przedstawia sztuczną inteligencję jako narzędzie transformacji nauki, przemysłu, konsumpcji, usług publicznych, ochrony zdrowia, edukacji, administracji i bezpieczeństwa. Dokument mówi jednocześnie o „bezpieczeństwie i kontrolowalności", regulacjach, klasyfikowaniu ryzyka oraz włączeniu AI w system zarządzania państwem. To charakterystyczny element chińskiej architektury: AI jest jednocześnie technologią produkcji i technologią governance.

Zachodnia dyskusja często rozdziela te sfery, pytając raczej o to, jak regulować prywatne systemy wykorzystywane przez obywateli i przedsiębiorstwa. Chińska strategia znacznie jawniej opisuje AI także jako narzędzie poprawiania zdolności administracji, monitorowania ryzyka, zarządzania miastem czy zasobami państwa.

Nawet w tym kontekście stereotyp mówiący, że „Chiny nie mają prywatności", jest naukowo nie do utrzymania. Chiński system opiera się na Cybersecurity Law, Data Security Law i Personal Information Protection Law; kolejne regulacje wprowadzają obowiązki dotyczące ochrony informacji, bezpieczeństwa danych i odpowiedzialności dostawców systemów AI. W 2026 roku zmienione chińskie prawo cyberbezpieczeństwa jeszcze wyraźniej połączyło rozwój AI z bezpieczeństwem i istniejącą strukturą prawa danych.

Różnica nie polega na prostym przeciwstawieniu: „USA chronią prywatność, Chiny nie". Trafniejsze pytanie brzmi: przed kim i w jakim zakresie prawo chroni jednostkę oraz jakie wyjątki zachowuje państwo w imię bezpieczeństwa i interesu publicznego? Liberalna tradycja prawna silniej koncentruje się na ograniczaniu władzy publicznej wobec jednostki. Chiński system ochrony informacji działa natomiast w architekturze, w której państwo zachowuje znacznie szerszą zdolność do definiowania interesu bezpieczeństwa, porządku publicznego i zgodności treści z wymaganiami politycznymi.

Tutaj metafora Konfucjusza staje się użyteczna, o ile nie zostanie nadużyta. W klasycznym konfucjanizmie jednostka jest rozumiana poprzez relacje: dziecko-rodzic, obywatel-władca, członek wspólnoty-wspólnota. Etyka nie rozpoczyna się od abstrakcyjnej, autonomicznej jednostki w stylu późniejszego liberalizmu, lecz od odpowiedzialności wpisanej w strukturę tych powiązań.

Współczesna technologia państwowa może łatwo wykorzystać taki język do uzasadnienia pierwszeństwa harmonii i bezpieczeństwa zbiorowego.

Historyczna uczciwość wymaga jednak dodania: konfucjańska harmonia nie jest tożsama z techniczną kontrolą zachowania. Konfucjusz kładł ogromny nacisk na moralną jakość rządzącego; władza miała być legitymizowana cnotą, edukacją i przykładem, a nie samą zdolnością do obserwacji.

Redukowanie konfucjanizmu do argumentu za cyfrowym nadzorem byłoby równie absurdalne, co wyprowadzanie współczesnego kapitalizmu inwigilacyjnego bezpośrednio z Arystotelesa. Co więcej, chińska polityka AI roku 2026 nie ogranicza się do kwestii bezpieczeństwa. W lipcu Chiny przedstawiły międzynarodowy plan etycznego governance AI, nawołując do zarządzania ryzykiem w całym cyklu życia, ochrony prywatności, ograniczania biasu, rozwijania wyjaśnialności i uwzględniania potrzeb grup szczególnie wrażliwych. Kilka miesięcy wcześniej regulacja usług antropomorficznych AI wprowadziła obowiązki dotyczące m.in. prywatności, przeciwdziałania manipulacji emocjonalnej, ochrony małoletnich i zapobiegania projektowaniu systemów ukierunkowanych na psychologiczne uzależnianie użytkownika.

## Różna lokalizacja kontroli w modelach USA i Chin

To dowodzi, jak nieaktualny staje się uproszczony podział, według którego Zachód reguluje ryzyko, a Chiny jedynie rozwijają technologię. Oba systemy równolegle i intensywnie kształtują innovation policy oraz risk governance; różnią się jednak konstrukcją instytucjonalną, hierarchią prawa i rolą państwa. Równie błędny byłby obraz USA jako przestrzeni opartej wyłącznie na dobrowolnej samoregulacji. Choć NIST AI Risk Management Framework pozostaje instrumentem dobrowolnym i jest rozwijany także w 2026 roku, amerykańskie państwo stosuje jednocześnie twarde narzędzia wszędzie tam, gdzie AI styka się z bezpieczeństwem narodowym i infrastrukturą krytyczną.

Nie mamy zatem do czynienia z dychotomią "wolność versus kontrola", lecz występuje tu różna lokalizacja kontroli. W języku ekonomii instytucjonalnej można to ująć następująco: system amerykański koncentruje się na kontrolowaniu granic ekosystemu — obejmuje to eksport, dostęp strategicznych podmiotów do technologii, zamówienia publiczne, konkurencję, cyberbezpieczeństwo oraz wybrane zastosowania. Wewnątrz znacznej części rynku pozostawia on przedsiębiorstwom szerokie pole do eksperymentów. System chiński natomiast wbudowuje kontrolę wewnątrz ekosystemu, realizując to poprzez obowiązki platform, rejestrację i ocenę konkretnych systemów, zarządzanie danymi, bezpieczeństwo treści oraz strategiczne kierownictwo rozwoju.

# Rywalizacja mocarstw jako walka o stos technologiczny

Oczywiście to rozróżnienie jest kwestią stopnia, a nie absolutnej różnicy. Rywalizacja obu systemów nie jest przy tym wyłącznie walką o tempo innowacji, lecz starciem o komplementarny stos technologiczny. Najlepszy model AI bez zaawansowanych półprzewodników nie stanowi geopolitycznej potęgi. Półprzewodnik pozbawiony maszyn litograficznych, projektowania układów, pamięci HBM, centrów danych, energii, sieci, oprogramowania i talentu również nią nie jest. Przewaga w obszarze AI jest zatem właściwością systemu, a nie pojedynczego produktu.

Stanford AI Index 2026 obrazuje tę konkurencję w interesujący sposób. Chiny prowadzą pod względem wolumenu publikacji naukowych, cytowań i liczby przyznawanych patentów AI, podczas gdy Stany Zjednoczone zachowują przewagę w tworzeniu najbardziej znaczących modeli: w 2025 roku raport klasyfikuje 50 notable models jako amerykańskie i 30 jako chińskie. Jednocześnie rośnie udział Chin wśród najczęściej cytowanych publikacji. Nie mamy już do czynienia z prostym podziałem na "wynalazcze USA i kopiujące Chiny", który jeszcze kilkanaście lat temu dominował w zachodniej publicystyce. Chiny stały się jednym z centralnych producentów wiedzy, patentów, infrastruktury i modeli. Stany Zjednoczone utrzymują natomiast bardzo silną pozycję frontierową oraz dysponują wyjątkowym ekosystemem kapitału, laboratoriów i przedsiębiorstw zdolnych do przekładania badań na produkty globalne.

W tym kontekście kontrola eksportu zyskuje kluczowe znaczenie. Gdy konkurent posiada własnych naukowców, firmy i dane, najskuteczniejszą barierą staje się próba ograniczania dostępu do wąskich gardeł stosu technologicznego. Półprzewodniki są tu odpowiednikiem cieśnin geograficznych w klasycznej geopolityce.

Kto kontroluje chokepoint, może wpływać na cały system. Jednak każde wąskie gardło rodzi program jego obejścia. Państwo podlegające restrykcjom inwestuje w substytuty, tworzy własnych dostawców, reorganizuje łańcuchy dostaw i buduje alternatywne standardy. Dlatego geopolityka półprzewodników jest jednocześnie geopolityką przyspieszonej autonomizacji.

W ten sposób powstaje najważniejsze niebezpieczeństwo dla globalnego systemu technologicznego: nie wojna handlowa o jeden produkt, lecz rozchodzenie się całych ekosystemów. Materiał źródłowy dostrzega tę możliwość i nazywa ją "Cyfrową Żelazną Kurtyną", przywołując przykład Huawei, Cisco, 5G, podejrzenia dotyczące backdoorów oraz amerykańskie ograniczenia eksportowe. Ta analogia wymaga ostrożności, ale trafnie wskazuje kierunek. Klasyczna żelazna kurtyna oddzielała terytoria; cyfrowa może oddzielać standardy, procesory, modele, chmury, sklepy aplikacji, systemy płatności, protokoły bezpieczeństwa i zasady przepływu danych.

Najbardziej niepokojące jest to, że obie strony mogą interpretować fragmentację jako formę obrony. USA ograniczają transfer technologii w imię bezpieczeństwa narodowego. Chiny odpowiadają, że globalne łańcuchy dostaw są "celowo rozrywane" i ostrzegają przed podziałem cyfrowego świata. W oficjalnym stanowisku z lipca 2026 roku Pekin połączył cyberbezpieczeństwo z suwerennością i krytyką fragmentacji światowej infrastruktury cyfrowej. Każda strona posługuje się własną narracją defensywną.

Dla Waszyngtonu ograniczenie dostępu konkurenta do najbardziej zaawansowanej mocy obliczeniowej jest ochroną bezpieczeństwa. Dla Pekinu budowa technologicznej autonomii to ochrona suwerenności przed uzależnieniem i zewnętrznym przymusem. Powstaje klasyczny security dilemma znany z teorii stosunków międzynarodowych. Działanie, które jedna strona uważa za defensywne, druga może interpretować jako przygotowanie przewagi ofensywnej. USA ograniczają eksport, obawiając się zastosowań wojskowych; Chiny inwestują w samowystarczalność, bojąc się odcięcia. Stany Zjednoczone widzą przyspieszoną chińską autonomię jako dowód rosnącego zagrożenia. Spirala sama się wzmacnia.

Technologia jest szczególnie podatna na ten mechanizm ze względu na podwójne zastosowanie (dual-use). Ten sam zaawansowany procesor może trenować model medyczny lub system wspierający rozpoznanie wojskowe. Ten sam system computer vision może diagnozować nowotwór albo śledzić obywatela. Ta sama chmura może obsługiwać uniwersytet i ministerstwo obrony. Oddzielenie sfery "cywilnej" od "strategicznej" staje się coraz trudniejsze.

W tym miejscu powracamy do tytułowego rozróżnienia tools and weapons. W geopolityce technologicznej narzędzie i broń nie muszą być dwoma różnymi urządzeniami. Czasem są dwiema funkcjami tej samej infrastruktury.

## Zdolność cywilizacyjnego uczenia się jako klucz do przewagi systemowej

Podważa to dawną, liberalną nadzieję, że głęboka współzależność gospodarcza automatycznie zredukuje ryzyko konfliktu. Choć może ona działać stabilizująco, podnosząc koszt zerwania relacji, może stać się również źródłem weaponized interdependence: państwo kontrolujące kluczowe węzły globalnej sieci zyskuje instrument przymusu. Zależność handlowa nie jest więc wyłącznie mostem; jest także potencjalną dźwignią.

Warto w tym miejscu ponownie zestawić Arystotelesa i Konfucjusza. Arystotelesowska phronesis, czyli roztropność praktyczna, zakładała zdolność działania w świecie, którego nie da się sprowadzić

do jednej reguły. Z kolei konfucjański ideał harmonii nie oznaczał braku różnic, lecz właściwe uporządkowanie relacji. Obaj filozofowie przypominają o czymś, co dzisiejsza geopolityka technologiczna często pomija: ład nie wynika z maksymalizacji jednego dobra. Maksymalna wolność przedsiębiorstwa bez odpowiedzialności prowadzi do prywatnej koncentracji władzy. Maksymalne bezpieczeństwo państwa może stworzyć system permanentnego nadzoru. Maksymalna autonomia technologiczna mocarstw grozi zniszczeniem korzyści wspólnego ekosystemu, podczas gdy maksymalna współzależność generuje strategiczne podatności. Prawdziwe zarządzanie technologią jest zatem sztuką proporcji.

Granica między modelem amerykańskim a chińskim nie przebiega tam, gdzie jeden kocha innowację, a drugi kontrolę. Dotyczy ona pytania o to, kto ma prawo wyznaczać proporcję pomiędzy innowacją, bezpieczeństwem, prywatnością, porządkiem i interesem państwa. W Stanach Zjednoczonych odpowiedź ta jest rozproszona między Kongres, prezydenta, sądy, agencje, stany, przedsiębiorstwa i społeczeństwo obywatelskie. W Chinach system jest silniej koordynowany hierarchicznie przez państwo i partię, nawet jeśli wykonanie rozkłada się na administrację, firmy, prowincje i środowiska badawcze. Różnica ta wpływa nie tylko na prawa jednostki, ale i na tempo strategicznego działania. System scentralizowany potrafi szybciej przesunąć zasoby w wybranym kierunku; system pluralistyczny generuje większą różnorodność eksperymentów i lepiej koryguje błędy dzięki konkurencji instytucjonalnej. Każdy z nich niesie własną klasę ryzyka: centralizacja może skalować błąd centrum, decentralizacja zaś prowadzić do chaosu, opóźnień i rozmytej odpowiedzialności. Nie ma zatem naukowych podstaw, by wyłonić zwycięzcę na podstawie samej filozoficznej etykiety.

Historia gospodarcza zna zarówno katastrofy planowania centralnego, jak i nieregulowanego rynku. Zna skuteczne państwa rozwojowe i skostniałe biurokracje; innowacyjne gospodarki liberalne oraz okresy prywatnej koncentracji władzy niszczącej konkurencję. Technologiczny XXI wiek jest eksperymentem, w którym oba mocarstwa szukają własnej kombinacji rynku, państwa, danych, bezpieczeństwa i wolności. Istotą konkurencji nie będzie zatem to, kto pierwszy zbuduje najpotężniejszy model. Długoterminową potęgę uzyska system, który potrafi jednocześnie tworzyć wiedzę, przyciągać talenty, finansować ryzyko, produkować półprzewodniki, zapewniać energię, budować infrastrukturę, chronić bezpieczeństwo, utrzymywać zaufanie społeczne i korygować własne błędy. Można to nazwać zdolnością cywilizacyjnego uczenia się.

Przewagą systemu politycznego nie jest brak błędów – taki system nie istnieje. Jest nią zdolność ich wykrywania, uznawania i korygowania, zanim zostaną zakodowane w infrastrukturze na skalę pokolenia. Ostateczne pytanie nie brzmi więc: Arystoteles czy Konfucjusz? Wolność tygrysa czy bezpieczeństwo dżungli? Stany Zjednoczone czy Chiny? Brzmi ono: który model potrafi stworzyć

technologię o ogromnej mocy, nie tracąc zdolności do politycznego korygowania sposobu, w jaki tej mocy używa?

Odpowiedź pozostaje nieznana, lecz coraz wyraźniej widać cenę niepowodzenia. Jeśli bezpieczeństwo zacznie być utożsamiane z technologiczną samowystarczalnością, a współzależność z podatnością na szantaż, oba mocarstwa będą miały racjonalne powody, by rozdzielać systemy, które przez trzy dekady integrowały świat. Kontrola półprzewodników pociągnie za sobą autonomizację produkcji. Spór o 5G przeniesie się na standardy sieci następnej generacji. Nieufność wobec chmury zwiększy wymagania suwerenności danych, a konkurencja modeli AI stworzy presję na budowę własnych ekosystemów obliczeniowych, regulacyjnych i językowych.

## Od globalnej optymalizacji do odporności strategicznej

Nie będzie to już zwykła wojna handlowa, lecz fragmentacja samej architektury cywilizacji cyfrowej. Cyfrowa żelazna kurtyna. Od półprzewodników po chmurę: czy globalizacja technologiczna rozpada się na konkurujące stosy cywilizacyjne?

Spór Stanów Zjednoczonych i Chin jawi się jako konkurencja dwóch odmiennych architektur koordynowania innowacji, bezpieczeństwa i władzy. Następnym krokiem nie może być jednak proste pytanie o to, które państwo okaże się silniejsze. Znacznie ważniejsze jest pytanie, co ta rywalizacja robi z samą strukturą globalnego systemu technologicznego. Przez trzy dekady dominującą intuicją globalizacji było przekonanie, że specjalizacja, interoperacyjność i transgraniczne łańcuchy wartości tworzą jeden, coraz gęściej połączony ekosystem. Projektor chipów znajdował się w jednym państwie, litografia w drugim, produkcja wafli w trzecim, montaż w czwartym, oprogramowanie w piątym, a użytkownik końcowy w szóstym. Technologia była globalna nie dlatego, że przestała mieć geografię, lecz dlatego, że jej geografia została rozproszona pomiędzy wiele komplementarnych centrów kompetencji. Możliwość odwrócenia tego procesu określono mianem „Cyfrową Żelazną Kurtyną", wiążąc ją z konfliktem wokół Huawei, doświadczeniami wynikającymi z ujawnień Edwarda Snowdena, kontrolą eksportu oraz niebezpieczeństwem powstawania niekompatybilnych ekosystemów technologicznych.

Metafora ta jest sugestywna, lecz wymaga doprecyzowania. Dzisiejsza kurtyna nie przypomina muru berlińskiego; nie istnieje jedna linia geograficzna, po której jednej stronie zaczyna się infrastruktura amerykańska, a po drugiej chińska. Powstaje raczej wielowarstwowa geografia selektywnego rozłączenia: w jednym miejscu współpraca trwa, w drugim wymagana jest licencja, w trzecim pojawia się zakaz, w czwartym budowany jest lokalny odpowiednik, a w piątym państwo żąda interoperacyjności właśnie po to, aby zmniejszyć zależność od konkretnego dostawcy. Nie jest

to jeszcze pełny decoupling. Trafniejszym określeniem jest de-risking przez architekturę. Państwa próbują zachować korzyści globalnej wymiany, a równocześnie usunąć z niej te zależności, które w sytuacji konfliktu mogłyby zostać użyte jako narzędzie presji. W rezultacie globalizacja technologiczna nie tyle znika, ile zmienia logikę: z optymalizacji efektywności przechodzi ku optymalizacji pod warunkiem odporności strategicznej. To zasadnicza zmiana ekonomiczna.

Klasyczna teoria przewagi komparatywnej zachęca do specjalizacji tam, gdzie podmiot posiada względną przewagę produkcyjną. W stabilnym środowisku im głębsza specjalizacja, tym większe korzyści z handlu. Bezpieczeństwo narodowe wprowadza jednak do tego rachunku zmienną, której Ricardo nie traktował jako centralnej: wartość możliwości działania po przerwaniu wymiany. Państwo może zaakceptować droższą lokalną fabrykę półprzewodników, jeśli uzna ją za ubezpieczenie przed geopolitycznym szokiem. Ekonomiczna nieefektywność w okresie pokoju może być ceną strategicznej dostępności w czasie kryzysu.

Półprzewodniki są idealnym laboratorium nowej geopolityki. OECD wskazuje, że ich łańcuch wartości jest jednocześnie silnie rozproszony i skoncentrowany: różne państwa posiadają dominującą pozycję na poszczególnych etapach, co tworzy rozległe współzależności, ale również bardzo konkretne punkty podatności. Zakłócenie w jednym z kluczowych centrów może wywołać niedobory w wielu sektorach niższego szczebla.

## Kontrola wąskich gardeł jako regulator mocy obliczeniowej

Nie istnieje „przemysł chipów” w liczbie pojedynczej. Istnieje ekosystem projektowania architektury układów, oprogramowania EDA, własności intelektualnej, produkcji wafli, maszyn litograficznych, chemikaliów, gazów przemysłowych, substratów, pamięci, zaawansowanego pakowania, testowania i montażu. Do tego dochodzi energia, ultraczysta woda, infrastruktura transportowa i wysoko wyspecjalizowana praca. Fabryka półprzewodników jest mniej autonomiczna, niż sugeruje jej fizyczna monumentalność. Może kosztować dziesiątki miliardów dolarów i nadal pozostawać zależna od zagranicznych narzędzi, materiałów oraz wiedzy. Można powiedzieć, że najważniejszym produktem fabryki chipów nie jest sam chip, lecz skoordynowanie globalnego systemu zdolnego go wyprodukować.

Współczesna polityka technologiczna coraz częściej skupia się na tak zwanych chokepoints. Państwo nie musi kontrolować całego łańcucha, aby posiadać znaczną władzę; wystarczy, że kontroluje komponent trudny do zastąpienia. W teorii sieci ma to charakter podobny do kontroli

mostu pomiędzy dwiema częściami grafu. W geopolityce morskiej odpowiednikiem były cieśniny. W geopolityce obliczeniowej takim wąskim gardłem mogą być określone urządzenia produkcyjne, procesory akceleracyjne, pamięci HBM albo oprogramowanie projektowe. W tej logice amerykańskie kontrole eksportowe stają się czymś więcej niż sankcją handlową.

Są próbą zarządzania tempem rozwoju zdolności technologicznej rywala. Jednocześnie ewolucja tych kontroli pokazuje, że strategia nie polega na prostym odcinaniu Chin od wszystkich zaawansowanych chipów. W styczniu 2026 roku amerykański BIS dopuścił rozpatrywanie licencji na zasadzie case-by-case – dotyczących między innymi Nvidia H200 i AMD MI325X dla zatwierdzonych odbiorców w Chinach – pod warunkiem spełnienia dodatkowych wymogów bezpieczeństwa i kontroli końcowego użytkownika.

Jest to bardzo wymowne. Polityka eksportowa zaczyna przypominać regulator przepływu mocy obliczeniowej, a nie zawór ustawiony tylko w pozycji otwartej lub zamkniętej. Państwo próbuje określić, jaka zdolność obliczeniowa może zostać udostępniona, komu, pod jakimi warunkami i przy jakim stopniu weryfikacji. Taka polityka zawiera wewnętrzne napięcie. Jeśli ograniczenia są zbyt łagodne, mogą nie osiągnąć celu bezpieczeństwa. Jeśli są zbyt silne, zagraniczni klienci otrzymują bodziec do przyspieszenia rozwoju alternatywnych architektur, dostawców i standardów. Instrument zaprojektowany jako sposób zachowania przewagi może więc, po przekroczeniu pewnego progu, zwiększyć determinację konkurenta do stworzenia równoległego ekosystemu. To klasyczny problem endogeniczności sankcji. Sankcja nie oddziałuje na nieruchomy obiekt – zmienia strategię podmiotu objętego ograniczeniem.

Chiny odpowiadają podobną logiką w innych segmentach łańcucha. Prowadzą system kontroli eksportu dóbr i technologii podwójnego zastosowania, obejmujący między innymi określone technologie związane z metalami i materiałami strategicznymi. W 2025 roku Pekin rozszerzył kontrole dotyczące technologii związanych z wydobyciem, separacją i produkcją materiałów ziem rzadkich, a w 2026 roku utrzymuje szczegółowe wymagania licencyjne wobec części produktów i technologii. Powstaje symetria narzędzi przy asymetrii zasobów.

## Weaponizacja współzależności i geopolityka zaufania technologicznego

Stany Zjednoczone dysponują wpływem w określonych segmentach zaawansowanej elektroniki, oprogramowania i architektury obliczeniowej. Chiny z kolei kontrolują znaczącą część zdolności w obszarze materiałów, przetwórstwa i produkcji przemysłowej.

Oba mocarstwa dostrzegają, że globalizacja stworzyła nie tylko wspólne dobro, ale i zestaw potencjalnych punktów nacisku. To mechanizm, który Farrell i Newman określają mianem weaponized interdependence. Sieć powiązań globalnych tworzy centralne węzły; państwo posiadające nad nimi jurysdykcję lub wpływ może wykorzystać je do obserwacji, blokowania bądź warunkowania przepływów. Paradoks polega na tym, że im bardziej efektywna i scentralizowana jest sieć, tym większa staje się strategiczna wartość jej kluczowych punktów. W epoce „niewinnej globalizacji" centralizacja była korzyścią; w dobie rywalizacji mocarstw staje się podatnością.

Stąd powrót polityki przemysłowej. Przez dekady państwa Zachodu akceptowały zasadę, że nie trzeba produkować wszystkiego lokalnie, jeśli produkt można taniej nabyć na rynku światowym. Jednak wstrząsy pandemiczne, agresja Rosji przeciw Ukrainie, kryzysy energetyczne oraz niedobory półprzewodników zmieniły intuicję polityczną. Pytanie „gdzie produkcja jest najtańsza?" zastąpiło pytanie: „czy produkcja pozostanie dostępna w sytuacji kryzysowej?". Tak narodziły się koncepcje friend-shoringu, near-shoringu, strategicznej autonomii i bezpieczeństwa ekonomicznego. Nie oznaczają one końca rynku, lecz włączenie ryzyka geopolitycznego do funkcji kosztu.

Warto posłużyć się tu językiem teorii portfelowej. Firma nie inwestuje całego kapitału w jeden instrument – nawet ten z najwyższą stopą zwrotu – ponieważ dywersyfikacja ogranicza ryzyko katastroficzne. Podobnie zaczyna patrzeć na łańcuch dostaw państwo. Pojedynczy, najtańszy dostawca maksymalizuje efektywność, ale kilku dostawców z różnych regionów zwiększa odporność systemu. Redundancja, dotychczas traktowana jako zasada cyberbezpieczeństwa, powraca jako zasada gospodarki politycznej. Strategiczna redundancja jest kosztownym odpowiednikiem kopii zapasowej.

To jednak dopiero pierwsza warstwa cyfrowej fragmentacji. Druga dotyczy infrastruktury telekomunikacyjnej. Konflikt wokół Huawei był jednym z pierwszych przypadków, w których urządzenie sieciowe przestało być traktowane jedynie jako produkt, a stało się problemem zaufania geopolitycznego. Zestawienie podejrzeń wobec infrastruktury chińskiej z ujawnieniami Snowdena dotyczącymi amerykańskiego wywiadu wskazuje na symetryczną strukturę nieufności: każda strona obawia się, że sprzęt przeciwnika może stać się instrumentem w rękach jego państwa. Nie należy tu tworzyć fałszywej symetrii faktów – konkretne zarzuty i ramy prawne są odmienne. Istotna dla analizy jest natomiast wspólna struktura epistemiczna problemu: w infrastrukturze krytycznej brak możliwości pełnego udowodnienia bezpieczeństwa jest traktowany jako ryzyko samo w sobie.

Sieć telekomunikacyjna stanowi szczególny przypadek, gdyż operator sprzętu zyskuje pozycję niezwykle głęboką. Sieć widzi ruch, autoryzuje urządzenia, aktualizuje oprogramowanie i zarządza zależnościami przez wiele lat. Oceniając dostawcę, państwo nie pyta więc tylko o to, czy produkt

jest dziś bezpieczny, lecz czy może zaufać przyszłym aktualizacjom, strukturze własności, prawu kraju pochodzenia i zachowaniu firmy w czasie kryzysu. Cyberbezpieczeństwo przestaje być wyłącznie testem kodu; staje się oceną instytucjonalnego pochodzenia technologii.

To przesunięcie może mieć długofalowe konsekwencje dla 6G, komunikacji satelitarnej czy infrastruktury kwantowej. Jeśli zaufanie do urządzenia zacznie zależeć od przynależności geopolitycznej producenta, wspólny standard techniczny zostanie zastąpiony standardem koalicyjnym. Państwa będą wybierać nie tylko najlepszą technologię, ale ekosystem polityczny, którego dostawcom są gotowe zaufać.

## Standardy i chmura jako narzędzia geopolitycznej kontroli

Tu pojawia się trzeci poziom fragmentacji: standardy. Standard techniczny z pozoru wygląda neutralnie – określa częstotliwość, protokół, format danych, sposób komunikacji lub interfejs. W rzeczywistości jednak niesie on ze sobą ogromne skutki ekonomiczne. Produkt zgodny z dominującym standardem może funkcjonować na globalnym rynku; ten niezgodny zostaje zamknięty w niszy. Standardy tworzą zatem efekty sieciowe, a wojna o nie może okazać się znacznie bardziej doniosła niż wojna ceł. Cło jedynie podnosi koszt produktu, podczas gdy niekompatybilny standard może całkowicie uniemożliwić jego użycie.

Organizacje normalizacyjne stają się przez to nieoczywistymi arenami geopolityki. Państwa i przedsiębiorstwa walczą w nich nie tylko o patenty, ale przede wszystkim o to, jakie rozwiązania zostaną wpisane w techniczną gramatykę przyszłego systemu. Jeśli dany standard zdominuje rynek, jego twórcy zyskują efekt pierwszeństwa, przewagę patentową, doświadczenie przemysłowe i realny wpływ na cały ekosystem producentów. W cyfrowej żelaznej kurtynie granica nie musi więc przebiegać przez terytorium. Może przebiegać przez API.

Czwarta warstwa dotyczy chmury. Przez lata była ona jednym z najpotężniejszych narzędzi ponownego scalania świata technologicznego: globalne przedsiębiorstwo mogło korzystać z podobnej infrastruktury w wielu państwach, skalować aplikacje i swobodnie przenosić dane. Jednak im bardziej chmura staje się fundamentem administracji, obronności, zdrowia i AI, tym kluczowsze staje się pytanie o suwerenność dostawcy. Europejska reakcja jest w tym kontekście szczególnie interesująca, ponieważ Unia nie dąży do pełnej technologicznej autarkii wobec USA i Chin, lecz próbuje zwiększać kontrolę nad warunkami zależności. Komisja Europejska opracowała

Cloud Sovereignty Framework, w którym suwerenność chmurowa jest oceniana wielowymiarowo, a nie redukowana wyłącznie do fizycznej lokalizacji centrum danych. To istotna ewolucja pojęcia.

Serwer znajdujący się w Europie nie gwarantuje pełnej suwerenności, jeśli kluczowe uprawnienia administracyjne, aktualizacje, szyfrowanie, własność intelektualna czy corporate control pozostają poza europejską jurysdykcją. Z drugiej strony sam fakt europejskiego pochodzenia dostawcy nie czyni go automatycznie bezpiecznym. Suwerenność chmurowa jest zatem kombinacją lokalizacji, kontroli operacyjnej, prawnej i kryptograficznej, a także możliwości audytu i zdolności migracji. Potwierdza to wcześniejszą tezę tego artykułu: lokalizacja danych jest tylko jednym z wymiarów suwerenności. Najważniejsze pytanie często nie brzmi „gdzie leży dysk?", lecz „kto może skutecznie zmienić sposób działania systemu?".

## Fragmentacja AI i wiedzy prowadzi do podziałów epistemicznych

Piąta warstwa fragmentacji koncentruje się na sztucznej inteligencji. Choć modele bazowe wydają się niematerialne, ich rozwój jest ściśle uzależniony od fizycznej infrastruktury: procesorów, pamięci, energii, centrów danych, sieci oraz zbiorów danych. W sytuacji, gdy półprzewodniki i chmura zostaną podzielone geopolitycznie, modele AI mogą zacząć ewoluować w odrębnych ekosystemach technicznych i regulacyjnych. Otwiera to drogę do powstania tzw. AI blocs – grup państw korzystających z modeli, infrastruktury i zasad governance powiązanych z konkretnym ekosystemem. Jeden blok może opierać się głównie na amerykańskich rozwiązaniach; drugi na chińskiej infrastrukturze; trzeci, jak Unia Europejska, dążyć do większej autonomii, podczas gdy inne kraje mogą przyjąć strategię wielowektorową, korzystając z technologii obu stron.

W tym obszarze fragmentacja może okazać się szczególnie głęboka, gdyż modele językowe nie są jedynie narzędziami produkcji, lecz warstwą reprezentacji wiedzy i kultury. Dane treningowe, języki, systemy moderacji, ograniczenia bezpieczeństwa oraz normy kulturowe kształtują sposób, w jaki model komunikuje się z użytkownikiem. Jeśli zatem modele powstają w odmiennych porządkach prawnych, będą nosić ich ślady. Użytkownik nie otrzymuje wtedy tylko innego produktu technologicznego, lecz interfejs do wiedzy zbudowany w odmiennej architekturze normatywnej. Może to oznaczać początek fragmentacji epistemicznej technologii.

Przez dekady Internet opierał się na wspólnej architekturze protokołów, nawet jeśli treści i regulacje różniły się między państwami. Przyszły świat może zachować częściowo wspólne protokoły sieciowe, ale wprowadzić odmienne warstwy dostępu do modeli, danych i platform. Nie

jest to jeszcze „splinternet” w najostrzejszym sensie, lecz raczej Internet warstwowy – taki, w którym fizyczne połączenia pozostają nienaruszone, ale nad nimi wyrastają różne reżimy dopuszczalnych usług i technologii.

Szósta warstwa dotyczy łańcucha dostaw oprogramowania. Nowoczesny kod nie powstaje z próżni; składa się z bibliotek, frameworków, kontenerów i komponentów open source, co czyni oprogramowanie globalnym ekosystemem reużycia wiedzy. Jeśli napięcia geopolityczne przełożą się na zakazy dotyczące repozytoriów lub narzędzi rozwojowych, koszty fragmentacji gwałtownie wzrosną.

Tu pojawia się sprzeczność między logiką bezpieczeństwa narodowego a etosem nauki i open source. Podczas gdy nauka i rozwój kodu opierają się na publikacji oraz wymianie, bezpieczeństwo strategiczne wymaga czasem ograniczenia przepływu wiedzy. Im więcej technologii zostanie uznanych za dual-use, tym trudniej będzie utrzymać granicę między otwartą nauką a kontrolą eksportu. Jeśli ta granica zostanie przesunięta zbyt szeroko, państwo może osłabić własną innowacyjność, gdyż wiedza rodzi się w otwartych sieciach współpracy. Jest to paradoks bezpieczeństwa przez zamknięcie: system może stać się bezpieczniejszy pod kątem transferu technologii, a jednocześnie mniej produktywny poznawczo.

Siódma warstwa fragmentacji dotyczy talentów. Globalny sektor technologiczny rozwijał się dzięki migracji naukowców i inżynierów, co uczyniło laboratoria w USA, Europie czy Azji ośrodkami międzynarodowymi. Znaczenie tej różnorodności dla innowacji jest kluczowe. Jeśli jednak konkurencja strategiczna sprawi, że badacz zostanie uznany za ryzyko transferu wiedzy wyłącznie ze względu na pochodzenie, system wejdzie w niebezpieczną spiralę podejrzliwości. Potrzeba ochrony technologii jest realna, ale równie realne jest ryzyko, że nadmierne ograniczenia odstraszą ludzi niezbędnych do utrzymania przewagi. Potęga technologiczna wynika bowiem nie tylko z ochrony tajemnic, ale przede wszystkim z atrakcyjności ekosystemu dla talentów.

Ósma warstwa dotyczy energii.

## Materialne fundamenty i mechanizm cyfrowej żelaznej kurtyny

Wraz z rozwojem AI moc obliczeniowa przestaje być abstrakcyjnym parametrem informatycznym. Centra danych wymagają energii, sieci przesyłowych, chłodzenia, gruntów i infrastruktury. W geopolityce zaawansowanych modeli państwo posiadające wybitnych naukowców, lecz niewystarczającą wydajność energetyczną, może napotkać fizyczną granicę skalowania. Oznacza to,

że geopolityka AI splata się z energetyką, polityką klimatyczną, dostępem do miedzi i transformatorów, zasobami wody oraz planowaniem przestrzennym. Cyfrowość wraca do materii. To kluczowe spostrzeżenie, gdyż obala mit gospodarki cyfrowej jako sfery pozbawionej zasobów. Cloud ma fundamenty z betonu. Model AI ma elektrownię. Chip ma kopalnię, fabrykę chemiczną i tysiące litrów ultraczystej wody. Digital sovereignty jest więc w równej mierze suwerennością energetyczną, co przemysłową.

W tym kontekście można już dostrzec pełną strukturę cyfrowej żelaznej kurtyny. Nie powstaje ona z jednego zakazu, lecz kumulatywnie. Najpierw państwo ogranicza sprzęt telekomunikacyjny. Później chipy, a następnie technologię ich produkcji. Potem dostęp do chmury, danych, inwestycji lub konkretnego modelu. W odpowiedzi druga strona buduje własne odpowiedniki, standardy i łańcuchy dostaw. Każdy z tych kroków, rozpatrywany indywidualnie, może wydawać się racjonalny, jednak ich suma tworzy nowy system. To klasyczny problem emergencji instytucjonalnej: makrostruktura powstaje bez centralnego planu, poprzez agregację wielu lokalnie racjonalnych decyzji. Żaden minister nie musi ogłaszać budowy dwóch osobnych Internetów. Wystarczy, że setki decyzji w obszarze bezpieczeństwa będą systematycznie premiować lokalizację, narodowych dostawców, zamknięte listy zaufania i ograniczenia transferów transgranicznych. Po dekadzie przedsiębiorca może odkryć, że globalny produkt wymaga dwóch architektur, dwóch chmur, dwóch modeli zgodności, dwóch stosów AI i dwóch łańcuchów dostaw.

Fragmentacja staje się procesem samowzmacniającym, ponieważ koszt ponownej integracji stale rośnie. Ekonomiści opisują to zjawisko przez path dependence. Raz dokonany wybór technologiczny generuje inwestycje, kompetencje i grupę interesariuszy dążących do jego utrzymania. Jeśli państwo zainwestuje setki miliardów w autonomiczny ekosystem półprzewodników, późniejsze odprężenie polityczne nie będzie oznaczać automatycznego powrotu do dawnej globalizacji. Powstały bowiem nowe fabryki, miejsca pracy, systemy subsydiów i strategiczne narracje.

Cyfrowa żelazna kurtyna może więc przetrwać konflikt, który ją stworzył. Co więcej, fragmentacja ma swoich beneficjentów. Lokalni producenci otrzymują ochronę i dotacje, agencje bezpieczeństwa zyskują większą kontrolę nad dostawcami, a politycy mogą wskazywać nowe inwestycje jako dowód suwerenności. Rynek zyskują także przedsiębiorstwa zajmujące się compliance. Nawet jeśli w skali globalnej system staje się mniej efektywny, lokalne koalicje polityczne mogą uznać go za korzystny. Nie oznacza to jednak, że każda polityka autonomii jest błędna. Błędem byłoby jedynie mylenie odporności z autarkią. Odporność to zdolność funkcjonowania mimo zakłóceń; autarkia zaś to próba samodzielnego wytwarzania wszystkiego.

## Suwerenność jako zdolność do negocjowania zależności

Pierwsze podejście może być racjonalne. Drugie zaś, w przypadku technologii o ogromnej specjalizacji, okazuje się ekonomicznie nierealistyczne i poznawczo szkodliwe.

Dojrzała strategia powinna zatem dążyć do współzależności kontrolowanej, a nie do jej całkowitej likwidacji. Państwo musi precyzyjnie wiedzieć, które zależności są krytyczne, gdzie niezbędna jest alternatywa, gdzie wystarczy zapas, gdzie wsparcie sojusznika, a gdzie globalny rynek pozostaje optymalnym rozwiązaniem. Nie każdy chip jest strategiczny, nie każda biblioteka oprogramowania stanowi zagrożenie dla bezpieczeństwa i nie każdy serwer musi być narodowy.

W tym miejscu pomocna staje się teoria opcji realnych. Aby zachować zdolność działania, nie trzeba posiadać w pełni autonomicznej fabryki wszystkiego. Często wystarczy opcja przestawienia produkcji, dostęp do alternatywnego dostawcy, odpowiedni zapas lub umowa sojusznicza. Suwerenność może polegać na posiadaniu możliwości reakcji, a nie na permanentnym duplikowaniu całego świata. Jest to szczególnie istotne dla państw średnich i mniejszych, których nie stać na budowę pełnego, własnego stosu technologicznego. Ich strategią nie powinna być imitacja mocarstw, lecz portfolio zależności: korzystanie z wielu dostawców, udział w kształtowaniu standardów, regionalne sojusze, interoperacyjność, rozwój własnych nisz technologicznych oraz zdolność prawna do wymuszania warunków korzystania z infrastruktury.

Unia Europejska próbuje iść właśnie tą drogą. Choć nie posiada samowystarczalnego ekosystemu odpowiadającego w pełni modelowi amerykańskiemu czy chińskiemu, może wykorzystywać rozmiar rynku, regulacje, standardy, politykę konkurencji, inwestycje przemysłowe oraz wymagania suwerenności chmurowej do budowania autonomii negocjacyjnej zamiast autarkii. Cloud Sovereignty Framework dobrze ilustruje to podejście: suwerenność jest tu oceniana wielowymiarowo, a nie poprzez prosty narodowy paszport dostawcy. Może to być jedna z najcenniejszych lekcji dla świata postglobalnego.

Nie trzeba bowiem posiadać całej technologii, aby posiadać sprawczość wobec niej. Sprawczość wymaga interoperacyjności. Jeśli państwo może zmienić dostawcę, przenieść dane, użyć otwartego standardu, zachować własne klucze kryptograficzne i utrzymać kompetencje techniczne, jego zależność pozostaje negocjowalna. Jeśli jednak zmiana dostawcy wymusza przebudowę całej administracji, zależność staje się quasi-strukturalna.

Odpowiedzią na cyfrową żelazną kurtynę może paradoksalnie być nie zamknięcie własnej części świata, lecz budowanie mostów technicznych odpornych na polityczne pęknięcia: otwartych standardów, możliwości migracji, wspólnych zasad bezpieczeństwa i minimalnych interoperacyjnych fundamentów. Historia Internetu pokazuje, że jego największym wynalazkiem nie była pojedyncza aplikacja, lecz protokół umożliwiający komunikację heterogenicznych sieci. Być może geopolityka XXI wieku potrzebuje analogicznej zasady: interoperacyjności pomiędzy różnymi porządkami politycznymi, bez wymogu ich aksjologicznej identyczności. Oczywiście nie wszystkie systemy mogą zostać połączone bezwarunkowo – granice wyznaczają prawa człowieka, bezpieczeństwo oraz ryzyka wojskowe.

## Interoperacyjność jako alternatywa dla całkowitego rozdzielenia systemów

Jeśli jednak każda różnica wartości zostanie automatycznie przełożona na osobną infrastrukturę techniczną, ludzkość może utracić jeden z największych efektów sieciowych współczesności. Fragmentacja niesie bowiem koszt niewidoczny w budżecie pojedynczego ministerstwa. Dwie fabryki, dwa standardy, dwa ekosystemy chmurowe, dwa modele zgodności i dwa zestawy komponentów oznaczają duplikację kapitału oraz wiedzy.

Z punktu widzenia bezpieczeństwa takie rozwiązanie może być uzasadnione, lecz z perspektywy globalnej produktywności stanowi stratę możliwości. Problem pogłębia się w nauce. Wielkie pytania – dotyczące klimatu, chorób, energetyki czy bezpieczeństwa żywnościowego – wymagają współpracy badaczy oraz wymiany danych i zasobów obliczeniowych ponad granicami mocarstw. Świat całkowicie podzielony technologicznie może być bezpieczniejszy pod kątem transferu technologii militarnych, a jednocześnie mniej zdolny do wspólnego rozwiązywania problemów egzystencjalnych.

Teza, że całkowite rozdzielenie ekosystemów byłoby strategią o sumie ujemnej, zasługuje na zachowanie, choć należy ją traktować jako ocenę normatywną, a nie mechaniczne prawo ekonomii. W określonych dziedzinach separacja może być racjonalną ceną bezpieczeństwa. Jednak bezpieczeństwo wymaga również wiedzy, innowacji i gospodarczej zdolności działania; autarkia chroniąc przed jedną podatnością, może tworzyć inną. Dojrzała strategia technologiczna powinna zatem operować nie pojęciem pełnego decouplingu, lecz selektywnego rozdzielenia przy zachowaniu maksymalnej interoperacyjności tam, gdzie ryzyko jest akceptowalne. Pozwala to sformułować kilka zasad wynikających z analizy – nie jako listę zaleceń administracyjnych, lecz jako spójną doktrynę.

Pierwsza mówi, że zależność nie jest przeciwieństwem suwerenności; przeciwieństwem suwerenności jest zależność bez alternatywy. Druga: redundancja jest kosztem, dopóki nie nastąpi kryzys; wtedy staje się wartością. Trzecia: standard techniczny jest niewidzialną polityką przemysłową. Czwarta: każdy zakaz eksportowy jest równocześnie bodźcem do stworzenia substytutu. Piąta: najbardziej trwałą formą potęgi technologicznej pozostaje ekosystem, do którego inni chcą dobrowolnie dołączyć.

Ta ostatnia zasada może być najważniejsza. Przymusem można ograniczyć przepływ technologii, lecz znacznie trudniej przymusem stworzyć środowisko, w którym najlepsi naukowcy chcą prowadzić badania, przedsiębiorcy zakładają firmy, inwestorzy podejmują ryzyko, a inne państwa dobrowolnie przyjmują standardy. Joseph Nye określiłby część tej zdolności mianem soft power. W technologii istnieje jej specyficzna forma: platform power przez atrakcyjność ekosystemu. Państwo posiada przewagę, jeśli inni chcą używać jego standardów, uczyć się w jego uniwersytetach, budować produkty na jego platformach i lokować kapitał w jego przedsiębiorstwach.

Cyfrowa żelazna kurtyna jest ryzykowna również dla tego, kto ją buduje. Mur chroni, ale jednocześnie zmniejsza atrakcyjność przestrzeni znajdującej się za murem. Powracamy tu do Arystotelesowskiej phronesis. Roztropność nie polega na maksymalizacji jednego kryterium, lecz na właściwym osądzie proporcji w konkretnej sytuacji. Państwo musi wiedzieć, kiedy otwartość jest przewagą, kiedy podatnością, a kiedy warunkiem własnego rozwoju. Podobnie konfucjańska harmonia, odarta z propagandowych uproszczeń, nie oznacza mechanicznej uniformizacji. Harmonia muzyczna powstaje właśnie dlatego, że różne dźwięki pozostają różne, lecz tworzą uporządkowaną całość. Świat technologiczny również nie potrzebuje identyczności systemów politycznych; potrzebuje minimalnego poziomu kompatybilności, która zapobiegnie automatycznemu przejściu różnicy w rozpad współpracy. W przeciwnym razie kurtyna cyfrowa przestanie być jedynie metaforą.

## Konstytucjonalizacja technologii jako jedyny bezpiecznik przed arbitralnością

Najpierw podzielimy chipy, potem chmury, a następnie modele AI. Później przyjdzie kolej na systemy płatnicze, tożsamości cyfrowe, standardy bezpieczeństwa i źródła informacji. W końcu dwa urządzenia wyprodukowane w różnych porządkach politycznych mogą technicznie widzieć tę samą sieć, lecz należeć do tak odmiennych ekosystemów zaufania, prawa i wiedzy, że praktycznie przestaną dzielić wspólną przestrzeń cyfrową. Internet pozostanie fizycznie połączony. Cywilizacja cyfrowa może jednak zostać semantycznie rozłączona.

Historia Tools and Weapons zmierza ku pytaniu znacznie szerszemu niż spór Microsoftu z rządem, kwestie chmury, cyberbezpieczeństwa czy AI. Każdy analizowany wcześniej problem prowadził do tej samej konkluzji: technologia zwiększa skalę ludzkiej sprawczości szybciej, niż instytucje uczą się ją kontrolować. Chmura rozszerzyła skalę pamięci, analityka – wiedzy, platformy – komunikacji, a cyberbroń – destrukcji.

AI zwiększyła skalę automatyzowanego sądu, zaś geopolityka technologiczna – skalę zależności. Fundacja Dobre Państwo musi spróbować odpowiedzieć na pytanie, które przebiegało pod powierzchnią artykułu: jak zachować człowieczeństwo w systemie, w którym nasze narzędzia osiągnęły skalę instytucji i zaczynają kształtować warunki, w których sami rozumiemy świat?

Doktryna odpowiedzialnego narzędzia w cywilizacji technologii większej od jej twórców

Punktem wyjścia analizy była rzecz banalna: narzędzie nie posiada własnej moralności. Miotła może służyć porządkowaniu przestrzeni albo uderzeniu człowieka; brzytwa może golić lub ranić; kod może diagnozować nowotwór, organizować transport czy zabezpieczać wybory, a jednocześnie umożliwiać inwigilację, sabotaż infrastruktury, automatyczną dyskryminację lub manipulację środowiskiem informacyjnym. Konstrukcja Tools and Weapons właśnie w tej ambiwalencji lokuje centralny problem współczesnej technologii: gdy narzędzie osiąga wystarczającą skalę, twórca nie może dłużej ograniczać odpowiedzialności do pytania, czy system poprawnie wykonuje polecenie. Musi pytać, jaki świat powstaje w wyniku działania tego systemu.

Materiał źródłowy streszcza tę zmianę maksymą, że kiedy technologia zmienia świat, jej twórcy ponoszą odpowiedzialność za świat, który pomagają stworzyć. Pojawia się zatem pytanie: nie tylko co komputer może zrobić, lecz co powinien robić. To przesunięcie od możliwości do powinności jest w istocie przejściem od inżynierii do filozofii politycznej. Problem technologiczny staje się problemem ustrojowym, gdy narzędzie zaczyna wpływać na warunki korzystania z wolności, dostęp do wiedzy, rynek pracy, bezpieczeństwo, prywatność i demokratyczną partycypację.

Wówczas pytanie o właściwą architekturę systemu przypomina pytanie konstytucyjne. Konstytucja nie zakłada przecież, że człowiek sprawujący władzę jest z natury zły; zakłada raczej, że możliwość działania na wielką skalę powinna zostać ograniczona kompetencją, procedurą, kontrolą i odpowiedzialnością. Podobnie odpowiedzialna technologia nie może opierać się na przekonaniu, że dobry inżynier, zarząd czy rząd zawsze użyją narzędzia właściwie. Powinna być projektowana tak, aby nawet w warunkach błędu, konfliktu interesów, zmiany władzy, presji ekonomicznej czy działania wrogiego ograniczać przestrzeń katastrofalnego nadużycia.

Dojrzałą odpowiedzią na technologię nie jest kodeks etyczny ani zakaz innowacji, lecz konstytucjonalizacja możliwości technologicznej. Oznacza ona budowanie ograniczeń funkcjonalnie

podobnych do tych, które nowoczesne państwo wprowadziło wobec władzy politycznej: rozdzielanie uprawnień, minimalizowanie koncentracji, tworzenie śladów decyzyjnych, zapewnianie kontroli zewnętrznej, definiowanie procedur odwoławczych oraz ograniczanie celu i możliwość cofnięcia błędnej decyzji. Technologia nie jest wtedy jedynie projektowana pod kątem funkcjonalności, lecz wyposażana w instytucjonalne bezpieczniki.

Można wręcz powiedzieć, że historia cyfryzacji jest historią odkrywania, iż sprawność bez ograniczeń jest inną nazwą arbitralności. Baza danych pozbawiona ograniczeń celu jest niezwykle użyteczna, dopóki nie staje się narzędziem profilowania całego życia człowieka. System rozpoznawania twarzy zyskuje na skuteczności wraz z dostępem do większej liczby kamer, lecz ta sama efektywność może zlikwidować anonimowość przestrzeni publicznej.

## Tarcie systemowe jako gwarant wolności w świecie algorytmów

Algorytm decyzyjny działa szybciej, gdy nie musi czekać na człowieka, lecz to właśnie ta szybkość może odebrać przestrzeń niezbędną dla wątpliwości, sprzeciwu i wyjątku. Platforma zwiększa zaangażowanie, gdy perfekcyjnie przewiduje, co utrzyma uwagę użytkownika, ale jednocześnie ryzykuje przekształcenie obywatela w obiekt nieustannej behawioralnej optymalizacji.

Prawo konstytucyjne od stuleci wie coś, czego kultura technologiczna musi nauczyć się na nowo: pewna ilość tarcia jest ceną wolności. Sąd kontrolujący organ śledczy spowalnia państwo. Procedura odwoławcza hamuje administrację. Wymóg uzasadnienia decyzji zwiększa koszt działania urzędnika, a ochrona prywatności ogranicza zasób informacji dostępnych władzy. Z punktu widzenia czystej efektywności wszystkie te mechanizmy wyglądają jak zbędne opóźnienia. Z perspektywy państwa prawa są one jednak technologiami ochrony człowieka przed wydajną arbitralnością.

Tę samą intuicję należy przenieść do systemów cyfrowych. Nie każdy proces powinien być optymalizowany pod kątem minimalnego czasu odpowiedzi. Nie każda informacja musi być połączona z każdą inną, a nie każdy błąd powinien pozostawać w profilu jednostki przez całe życie. Nie każda korelacja nadaje się na kryterium decyzji i nie każda techniczna zdolność przewidywania zachowania daje moralne prawo do wykorzystania tej predykcji przeciwko człowiekowi.

Prywatność, analizowana wcześniej jako „system rozdzielania uprawnień do wiedzy”, okazuje się zatem czymś znacznie bardziej fundamentalnym niż tylko prawem do ukrywania sekretów. Jest ona odpowiednikiem separation of powers w przestrzeni informacyjnej.

Jeżeli jeden podmiot wie o człowieku wystarczająco dużo, może coraz precyzyjniej przewidywać jego zachowania, klasyfikować ryzyko, różnicować ceny, ograniczać dostęp lub wpływać na wybory. Władza informacyjna przekształca się wówczas w władzę behawioralną. Ochrona danych nie jest więc archaicznym hamulcem analityki, lecz sposobem przeciwdziałania koncentracji epistemicznej przewagi jednej strony nad drugą. Stąd kluczowe znaczenie powiernictwa danych (stewardship). Koncepcja ta przeciwstawia stewardship własności, przedstawiając dostawcę infrastruktury jako podmiot odpowiedzialny za bezpieczeństwo „kontenera", podczas gdy klient zachowuje zasadniczą kontrolę nad treścią i celem wykorzystania danych. Nasza analiza rozszerza tę intuicję: powiernictwo nie może być rozumiane wyłącznie jako korporacyjna obietnica. Powinno oznaczać realne ograniczenie zakresu własnej władzy przez dostawcę, zapewnienie interoperacyjności, możliwości odejścia, przejrzystości podwykonawców oraz minimalizację dostępu w celu zachowania operacyjnej suwerenności klienta.

## Odpowiedzialność ludzka zamiast zaufania do algorytmów

Dobry powiernik nie jest tym, który mówi „zaufaj mi", lecz tym, który buduje system, w którym klient nie musi ufać mu bardziej, niż jest to konieczne. Ta sama zasada dotyczy sztucznej inteligencji. Wiele dyskusji o AI skupia się na pytaniach o to, czy maszyna „myśli", „rozumie" lub „jest świadoma", a także kiedy osiągnie inteligencję przewyższającą człowieka. Są to rozważania filozoficznie interesujące, lecz z punktu widzenia współczesnego ładu instytucjonalnego często mniej pilne niż pytanie bardziej przyziemne: kto może zrobić co komu przy użyciu systemu AI i kto odpowiada za konsekwencje? Nie potrzeba świadomej maszyny, aby człowiek został błędnie zakwalifikowany, pozbawiony świadczenia, nadmiernie nadzorowany lub odrzucony przez system rekrutacyjny. Sprawczość polityczna technologii nie wymaga jej świadomości.

Należy zatem odróżnić inteligencję od odpowiedzialności. Model może wykonywać operacje poznawcze z niezwykłą skutecznością, a jednak nie staje się przez to podmiotem moralnym. Nie doświadcza wstydu, winy ani obowiązku i nie czuje odpowiedzialności za cudze cierpienie. Nie można więc uczynić z niego wygodnego pośrednika, na którego instytucja przeniosłaby ciężar własnego wyboru. Zdanie „algorytm zdecydował" jest zazwyczaj kategoriowym błędem organizacyjnym. Algorytm obliczył wynik, lecz to instytucja wcześniej zdecydowała, że wynik tego rodzaju będzie miał określoną moc.

Odpowiedzialność za AI musi zatem zachować ciągłość ludzkiego przypisania. Ktoś definiuje cel, ktoś wybiera dane, ustawia próg, decyduje o wdrożeniu lub ustala, czy rekomendacja jest wiążąca.

Ktoś także musi mieć możliwość wycofania systemu. Nawet jeśli kolejne ogniwa tego procesu należą do różnych organizacji, architektura governance musi pozwalać na odtworzenie tej sekwencji. Bez tego złożoność technologiczna może stać się nową formą uchylania się od odpowiedzialności: nie ma winnego, ponieważ każdy posiadał jedynie mały fragment systemu. Teoria organizacji od dawna zna problem rozproszonego sprawstwa, jednak technologie wielkoskalowe nadają mu nowy wymiar.

W systemie złożonym szkoda może nie być wynikiem pojedynczego błędu, lecz interakcji wielu poprawnie działających komponentów. Charles Perrow określił podobne zjawiska mianem normal accidents: w systemach ściśle sprzężonych i złożonych nie wszystkie kombinacje awarii można przewidzieć. W świecie AI, chmury, cyberbezpieczeństwa i globalnych platform oznacza to konieczność odejścia od modelu „znajdź winny moduł" na rzecz analizy bezpieczeństwa systemowego.

Odpowiedzialność nie może zaczynać się dopiero po katastrofie. Musi obejmować redundancję, monitoring, procedury wycofania, testowanie scenariuszy brzegowych, ograniczenie skali eksperymentu, segmentację, ocenę zależności oraz projektowanie zdolności powrotu do trybu bezpiecznego. Dojrzały system to nie taki, który nigdy nie popełnia błędu, lecz taki, który potrafi przeżyć własną awarię bez przekształcenia jej w katastrofę społeczną. W tym punkcie cyberbezpieczeństwo spotyka się z filozofią odpowiedzialności.

WannaCry i NotPetya pokazały, że cyfrowy incydent może sparaliżować szpital lub globalną logistykę bez niszczenia fizycznej infrastruktury. Materiał źródłowy wyciąga z tego zasadę, że „nie ma bezpieczeństwa narodowego bez cyberbezpieczeństwa". Nasza analiza rozwija ją do twierdzenia silniejszego: współczesne państwo posiada cyfrowy układ nerwowy, dlatego odporność systemów informacyjnych jest elementem jego zdolności konstytucyjnej do istnienia. W teorii systemów odpowiedzialny układ potrzebuje nie tylko sterowania, lecz również obserwowalności i kontrolowalności. Jeśli operator nie widzi, co dzieje się wewnątrz systemu, nie potrafi rozpoznać odchylenia. Jeżeli zaś widzi problem, ale nie posiada możliwości interwencji, obserwacja pozostaje bezsilna. Te pojęcia teorii sterowania mają zaskakująco trafny odpowiednik w polityce technologicznej. Audytowalność zapewnia obserwowalność instytucjonalną, natomiast możliwość wycofania modelu, cofnięcia aktualizacji, zmiany dostawcy lub zawieszenia procesu zapewnia kontrolowalność. System, którego nie da się ani zrozumieć, ani zatrzymać, jest politycznie niebezpieczny nawet wtedy, gdy statystycznie działa znakomicie. Do tego należy dodać odwracalność – w klasycznej administracji błędna decyzja może zostać uchylona, a w systemie sądowniczym istnieją instancje odwoławcze.

# Odpowiedzialność za nieodwracalność i architekturę wspólnego świata

Technologia często sprzyja nieodwracalności: raz ujawnione dane nie mogą zostać „odzyskane", rozpowszechniony deepfake pozostaje w sieci, a zniszczona reputacja może długo ciążyć człowiekowi. Im mniej odwracalny skutek, tym wyższy powinien być próg odpowiedzialności przed jego wywołaniem. Hans Jonas stworzył etykę odpowiadającą właśnie tej asymetrii.

Im większa skala możliwych i długotrwałych skutków działania technologicznego, tym słabsze jest usprawiedliwienie dla eksperymentowania według zasady „najpierw spróbujemy, później naprawimy". Przedsiębiorcza kultura iteracji świetnie sprawdza się w przypadku produktu, w którym wadliwy przycisk można poprawić następnego dnia. Jest jednak znacznie mniej odpowiednia tam, gdzie „iteracja" dotyczy zdrowia, wolności, reputacji, infrastruktury krytycznej albo integralności procesu wyborczego. Z tego wynika zasada proporcjonalności innowacyjnej: tempo eksperymentu powinno być odwrotnie proporcjonalne do nieodwracalności potencjalnej szkody. Im łatwiej cofnąć konsekwencję, tym większa przestrzeń dla szybkiego testowania. Im bardziej decyzja wpływa na podstawowe prawa lub bezpieczeństwo, tym większa potrzeba walidacji, nadzoru i procedury ex ante. Nie jest to argument przeciw innowacji, lecz przeciw infantylnej definicji innowacji jako szybkości. Technologia dojrzała nie jest tą, która wdraża wszystko natychmiast, ale tą, która wie, kiedy szybkość jest przewagą, a kiedy staje się nierozsądkiem. Ta intuicja przenosi nas w stronę demokracji.

Platformy społecznościowe ujawniły, że problem odpowiedzialności technologicznej nie ogranicza się do danych czy bezpieczeństwa systemów; dotyczy również kształtu środowiska, w którym społeczeństwo poznaje samo siebie. Platforma nie musi tworzyć konkretnej wypowiedzi, aby wpływać na jej zasięg – może projektować widzialność, ranking, rekomendację, intensywność powiadomień i ekonomię uwagi. Oznacza to władzę nie nad treścią w klasycznym sensie cenzury, lecz nad warunkami spotkania człowieka z treścią. Demokracja wymaga czegoś więcej niż wolności emisji; wymaga wspólnego świata wystarczającego do prowadzenia sporu. Arendt przypominała, że polityka rodzi się w przestrzeni pluralności: ludzie nie muszą myśleć jednakowo, lecz muszą pojawiać się wobec siebie jako uczestnicy tej samej rzeczywistości. Algorytmicznie spersonalizowane środowisko może tę wspólność osłabiać bez zakazywania komukolwiek wypowiedzi. Jeżeli każdy otrzymuje osobną hierarchię wydarzeń, inne dowody, innych przeciwników i inne źródła oburzenia, obywatelom coraz trudniej spierać się o ocenę wspólnego przedmiotu, ponieważ przestają uznawać, że przedmiot jest wspólny.

Odpowiedzialność platformy nie powinna być zatem rozumiana jako obowiązek ustanowienia jednej prawdy. Byłoby to zagrożenie równie poważne jak chaos informacyjny. Chodzi raczej o projektowanie odpornej niezgody: środowiska, w którym pluralizm pozostaje możliwy, ale system nie jest ekonomicznie premiowany za maksymalizowanie epistemicznego rozpadu społeczeństwa. Habermasowski ideał sfery publicznej w epoce cyfrowej wymaga zatem aktualizacji.

## Prawo do sprzeciwu i suwerenność poznawcza

Nie wystarczy pytać, kto może mówić. Trzeba zapytać o mechanizmy, które decydują o tym, kto zostaje usłyszany, z jaką częstotliwością i dlaczego. Architektura widzialności jest częścią architektury politycznej. Stąd kolejne kryterium odpowiedzialnego narzędzia: contestability, czyli możliwość zakwestionowania wyniku. Człowiek powinien mieć prawo podważyć decyzję administracyjną, ocenę algorytmiczną, moderację, błędne dane, klasyfikację ryzyka czy przypisaną mu reprezentację. Nie dlatego, że zawsze ma rację, lecz dlatego, że żaden system klasyfikacji nie powinien posiadać nieodwołalnej władzy nad jednostką.

Godność ludzka może być opisana w sposób niezwykle techniczny: oznacza między innymi, że człowiek posiada nadwyżkę nad swoim profilem. Nie jest on tożsamy z rekordem, historią kliknięć, scoringiem, predykcją ani statystycznym podobieństwem do innych. Model może tworzyć użyteczną reprezentację osoby, ale ta reprezentacja nigdy nie wyczerpuje człowieka.

Ta różnica niesie za sobą konkretne konsekwencje prawne i moralne. Jeśli człowiek zostanie całkowicie utożsamiony z profilem, traci prawo do niespodzianki, poprawy, zmiany i drugiej szansy. System predykcyjny może wtedy nie tylko opisywać przyszłość, ale wręcz ją współtworzyć: odmowa kredytu utrudnia budowanie historii kredytowej, uznanie za osobę ryzykową zwiększa nadzór, a gorsza ocena rekrutacyjna ogranicza możliwość zdobycia doświadczenia. Predykcja staje się performative prediction – prognozą, która sama wytwarza warunki własnej trafności.

Sprawiedliwa technologia powinna zatem bronić możliwości człowieka do wyrwania się z własnej statystyki. Problem ten prowadzi bezpośrednio do kwestii edukacji, którą należy rozumieć jako infrastrukturę bezpieczeństwa epistemicznego. Nie jest to figura retoryczna.

Społeczeństwo korzystające z AI, które nie rozumie probabilistycznej natury modeli, nie odróżnia płynności wypowiedzi od jej prawdziwości i nie posiada kompetencji do krytyki źródeł, staje się poznawczo zależne od infrastruktury, której nie potrafi nadzorować. W takim układzie zasada human-in-the-loop zostaje spełniona formalnie, lecz unieważniona realnie. Człowiek siedzi przy

ekranie, ale brakuje mu epistemicznej zdolności sprzeciwu. Jest obecny w pętli jako podpis, a nie jako podmiot sądu.

Edukacja przyszłości musi bronić suwerenności poznawczej, którą należy odróżnić od technologicznej samowystarczalności. Człowiek suwerenny poznawczo nie musi wykonywać wszystkich obliczeń samodzielnie, musi jednak rozumieć granice delegowania zadań. Wie, kiedy warto użyć maszyny, kiedy sprawdzić jej wynik, kiedy poszukać innego źródła i kiedy odmówić działania opartego na niewystarczającym dowodzie.

Ludzką kompetencją nie jest konkurencja z maszyną w szybkości generowania odpowiedzi, lecz zdolność brania za tę odpowiedź odpowiedzialności. Ta sama zasada pozwala inaczej spojrzeć na rynek pracy. Lęk przed automatyzacją często redukuje człowieka do poziomu jednostki produkcyjnej; pytamy wtedy jedynie, czy model wykona jego zadanie taniej, szybciej i dokładniej.

## Skala techniczna jako zmienna moralna wymagająca nowych barier prawnych

Praca posiada jednak również wymiar społeczny, statusowy i egzystencjalny. Dostarcza nie tylko dochodu, ale organizuje czas, relacje, rolę w społeczeństwie, rozwój kompetencji oraz poczucie uczestnictwa we wspólnym przedsięwzięciu. AI zwiększy produktywność, lecz korzyści z tego wzrostu mogą zostać nadmiernie skoncentrowane; technologia może osiągnąć ekonomiczny sukces i społeczną porażkę. Wzrost PKB nie jest zatem wystarczającą miarą odpowiedzialnej transformacji. Należy pytać, czy nowe narzędzia rozszerzają sprawczość pracownika, czy jedynie umożliwiają likwidację jego stanowiska; czy tworzą nowe zadania, czy koncentrują rentę; czy skracają czas rutyny, czy zwiększają intensywność nadzoru. Powraca pytanie o kierunek innowacji.

Technologia nie rozwija się według jednej, nieuchronnej trajektorii. Projekty badawcze, podatki, zamówienia publiczne, prawo pracy, system własności intelektualnej i strategie przedsiębiorstw decydują o tym, czy bardziej opłacalne staje się zastępowanie człowieka, czy jego wzmacnianie. Polityka technologiczna nie może zatem ograniczać się do postulatu „więcej AI”. Musi pytać: AI po co, dla kogo i z jaką strukturą podziału korzyści? Pytanie to łączy ekonomię z Kantowską kategorią człowieka jako celu. Człowiek nie powinien być wyłącznie kosztem optymalizowanym w procesie. Gospodarka istnieje dla ludzkiego dobrobytu, a nie człowiek dla wskaźnika produktywności. To nie jest antyrynkowy slogan, lecz przypomnienie, że produktywność ma wartość tylko dlatego, że pozwala społeczeństwu realizować ludzkie cele.

Podobną korektę należy zastosować wobec państwa. Władza może wykorzystywać technologię do zwiększania bezpieczeństwa, wydajności administracji i jakości usług publicznych. Jednak administracja cyfrowa z łatwością może przeobrazić się z „państwa, które lepiej obsługuje obywatela" w „państwo, które wie o obywatelu wszystko". Wysoka sprawność administracyjna nie jest więc automatycznie dobrem, jeśli nie towarzyszą jej ścisłe ograniczenia prawne.

Historia Stasi stanowi skrajne przypomnienie tej prawdy. Ogrom archiwum i doświadczenie represyjnego systemu służą jako ostrzeżenie przed technologią przekształcającą informację w instrument totalnej kontroli. Cyfrowość nie stworzyła pokusy wszechwiedzy państwa, lecz usunęła bariery techniczne, które dawniej tę pokusę ograniczały. O ile kiedyś totalna inwigilacja wymagała tysięcy funkcjonariuszy, segregatorów i fizycznego śledzenia, o tyle dziś procesy te można zautomatyzować. Skoro bariera techniczna dla nadużycia spada, bariera prawna i instytucjonalna musi rosnąć.

Jest to jedna z uniwersalnych prawidłowości epoki cyfrowej: gdy technologia obniża koszt określonego działania, instytucje powinny ponownie ocenić, czy istniejące normy wystarczają do kontroli nowej skali. Tani monitoring zmienia znaczenie prawa do prywatności. Tania generacja treści zmienia ekonomię dezinformacji. Tania analiza danych zmienia możliwości profilowania. Tania automatyzacja decyzji zmienia skalę błędu. Tania cyberbroń zmienia relację między mocarstwem a niewielkim aktorem. Skala jest zmienną moralną, ponieważ zmienia wielkość możliwej szkody i asymetrię pomiędzy stronami.

## Interoperacyjność i policentryczne zarządzanie jako bezpieczniki władzy

Wszystko to prowadzi nas w stronę geopolityki. W świecie, w którym chipy, chmura, modele AI i infrastruktura komunikacyjna są jednocześnie produktami gospodarczymi i zasobami strategicznymi, polityka technologiczna staje się de facto polityką potęgi. USA i Chiny dążą do ochrony własnych systemów, ograniczania podatności i kontroli nad punktami krytycznymi. Europa z kolei stara się zwiększać swoją autonomię regulacyjną oraz negocjacyjną, podczas gdy inne państwa szukają miejsca pomiędzy tymi wielkimi ekosystemami.

Cyfrowa żelazna kurtyna ujawnia jeszcze jedną cechę odpowiedzialnego narzędzia: interoperacyjność jest wartością polityczną. System zdolny do współpracy z innym systemem obniża koszt zmiany dostawcy, stymuluje konkurencję, ułatwia mobilność danych i redukuje strukturalne uzależnienie. Zamknięty standard może być wygodny handlowo dla jego właściciela,

lecz z perspektywy dobra wspólnego przekształca zależność technologiczną w polityczną. Odpowiedzialna technologia potrzebuje zatem nie tylko bezpieczeństwa i prywatności, ale wyjścia awaryjnego. Użytkownik, przedsiębiorstwo, instytucja czy państwo powinny w rozsądnym zakresie zachowywać możliwość opuszczenia danego ekosystemu. W przeciwnym razie zgoda na korzystanie z usługi staje się pozorna, gdyż koszt rezygnacji jest zbyt wysoki. To rozwiązanie ogranicza również władzę korporacji infrastrukturalnych. Część XV pokazała, że wielkie firmy technologiczne zyskały funkcjonalne znaczenie geopolityczne – nie są państwami, lecz kontrolują zasoby, z których te państwa korzystają.

Z powyższego wynika potrzeba stewardship i odpowiedzialności wykraczającej poza tradycyjną rolę dostawcy kodu. Nie wolno jednak przekształcić tego postulatu w pochwałę prywatnego paternalizmu. Korporacja nie powinna zostać cyfrowym filozofem-królem. Może dysponować kompetencją, infrastrukturą i wiedzą, ale nie posiada konstytucyjnego mandatu do definiowania dobra wspólnego. Dlatego odpowiedzialność korporacyjna musi rosnąć wraz ze skalą wpływu, lecz polityczna legitymizacja musi pozostać domeną publiczną. To rozróżnienie pozwala uniknąć dwóch naiwnych modeli.

Pierwszy zakłada, że przedsiębiorstwo ma wyłącznie maksymalizować zysk, a każda kwestia społeczna należy do państwa. Model ten nie sprawdza się w świecie, w którym firma dostrzega skutki działania własnej technologii szybciej niż regulator i posiada techniczną zdolność powstrzymania szkody. Drugi model sugeruje, że odpowiedzialne firmy technologiczne same stworzą etyczną przyszłość. Jest on równie niebezpieczny, ponieważ oddaje ogromną władzę podmiotom niepodlegającym demokratycznej wymianie władzy.

Dojrzały model wymaga policentrycznego governance: współpracy państw, prawa, nauki, przedsiębiorstw, społeczeństwa obywatelskiego, standardów zawodowych i instytucji międzynarodowych. Żaden z tych podmiotów samodzielnie nie posiada wszystkich niezbędnych kompetencji. Państwo dysponuje mandatem, lecz często brakuje mu wiedzy technicznej. Przedsiębiorstwo ma technologię, ale nie legitymację polityczną. Nauka oferuje metodę krytyki, lecz nie władzę wykonawczą. Społeczeństwo obywatelskie potrafi artykułować prawa i zagrożenia, ale nie zarządza infrastrukturą. Strukturę tę można opisać za pomocą cybernetycznego prawa wymaganej różnorodności Ashby'ego: regulator systemu musi dysponować dostateczną różnorodnością odpowiedzi wobec różnorodności stanów systemu. Technologia, której skutki obejmują prawo, psychologię, ekonomię, bezpieczeństwo, edukację i politykę międzynarodową, nie może być sensownie zarządzana przez jedną specjalność. Monodyscyplinarna regulacja wielowymiarowej technologii jest poznawczo niedostateczna.

Interdyscyplinarność nie jest więc ozdobą naukowego tekstu o technologii, lecz wymogiem adekwatności poznawczej. Informatyk widzi model, statystyk – błąd, prawnik – kompetencję i uprawnienie, psycholog – zachowanie użytkownika, socjolog – zmianę relacji społecznych, ekonomista – bodźce i rozkład rent, politolog – władzę, a filozof – wartość i granicę dopuszczalności. Dopiero złożenie tych perspektyw pozwala dostrzec obiekt, który faktycznie istnieje w świecie społecznym. To największa lekcja Tools and Weapons.

## Systemowa doktryna odpowiedzialnego narzędzia jako fundament demokratycznej kontroli

Technologia przestała być osobnym sektorem; stała się warstwą przekrojową cywilizacji. Nie istnieje już odrębna „polityka technologiczna" w sensie niszowej polityki jednego przemysłu, gdyż technologia przenika prawo rodzinne, medycynę, obronność, edukację, rynek pracy, dyplomację, administrację, kulturę i demokrację.

Zarządzanie (governance) musi zatem obejmować wszystkie te dziedziny. Można w tym kontekście zaproponować syntetyczną doktrynę odpowiedzialnego narzędzia, lecz nie jako katalog technicznych zasad do odhaczenia. Jej pierwszą cechą jest celowość: przed wdrożeniem należy nazwać dobro, któremu system ma służyć, a nie jedynie funkcję, którą wykonuje. Drugą jest proporcjonalność: intensywność ingerencji powinna odpowiadać wadze chronionego celu. Trzecią – minimalizacja władzy: system nie powinien uzyskiwać więcej danych, uprawnień i autonomii, niż jest to niezbędne.

Czwartym filarem jest obserwowalność: działanie musi pozostawiać ślad umożliwiający audyt. Piątym – kontrolowalność, czyli realna możliwość zatrzymania lub zmiany działania. Szóstym – odwracalność, tam gdzie jest ona technicznie i prawnie możliwa. Siódmym – contestability, pozwalająca człowiekowi zakwestionować reprezentację i rezultat. Ósmym – odporność, zakładająca możliwość błędu. Dziewiątym – interoperacyjność oraz prawo do wyjścia (exit), ograniczające zamknięcie w zależności. Dziesiątą zaś jest publiczna rozliczalność, proporcjonalna do publicznego znaczenia technologii.

Kluczowe jest to, że właściwości te tworzą system. Transparentność bez możliwości sprzeciwu jest tylko oglądaniem własnej bezsilności. Human oversight bez kompetencji staje się teatrem kontroli. Prywatność bez cyberbezpieczeństwa nie chroni danych przed kradzieżą, natomiast cyberbezpieczeństwo pozbawione praw człowieka może chronić aparat represji równie skutecznie jak demokrację. Interoperacyjność bez bezpieczeństwa zwiększa powierzchnię ataku, a innowacja

bez edukacji pogłębia nierówności zamiast budować dobrobyt. Odpowiedzialność technologiczna jest problemem kompozycyjnym – nie wystarczy maksymalizować jednej wartości; trzeba budować właściwe proporcje między wartościami pozostającymi w napięciu. To właśnie odróżnia etykę dojrzałą od moralnego sloganu.

Prywatność i bezpieczeństwo mogą wejść w konflikt. Wolność słowa może ścierać się z ochroną przed skoordynowaną manipulacją. Innowacja i ostrożność regulacyjna nie zawsze wskazują ten sam kierunek, a otwarta nauka pozostaje w napięciu z kontrolą technologii podwójnego zastosowania. Globalna interoperacyjność może z kolei konfliktować z odpornością strategiczną. Dojrzałość nie polega na udawaniu, że trade-offy nie istnieją, lecz na instytucjonalizacji sposobu ich rozstrzygania.

Technokracja jest w tym zakresie niewystarczająca. Ekspert może wyliczyć skutki, ale nie może samodzielnie rozstrzygnąć, jaki rozkład ryzyka społeczeństwo uważa za sprawiedliwy. Model może przewidzieć rezultat, lecz nie może z samej predykcji wyprowadzić prawa do działania. Nauka wskazuje prawdopodobne konsekwencje, jednak to polityka i etyka muszą zdecydować, które z nich są dopuszczalne.

Nie oznacza to relatywizmu. Istnieją granice wyznaczane przez godność człowieka, zakaz arbitralnej przemocy, podstawowe prawa i zasadę rządów prawa. Oznacza to natomiast, że poza tym rdzeniem pozostaje obszar rozumnego pluralizmu, w którym społeczeństwa mogą wybierać różne konfiguracje prywatności, bezpieczeństwa, innowacji i odpowiedzialności.

W tym miejscu filozofia spotyka się z demokracją. Demokracja nie gwarantuje, że decyzja technologiczna będzie zawsze najlepsza, zapewnia jednak procedurę, w której osoby dotknięte skutkami mogą uczestniczyć w definiowaniu granic władzy. Jest to kluczowe, ponieważ technologia wykazuje naturalną tendencję do przenoszenia decyzji z przestrzeni widzialnej polityki do niewidzialnej architektury systemu. Kod może depolityzować decyzję, która w istocie pozostaje polityczna.

Gdy algorytm ustala priorytet świadczeń, ranking kandydatów, strukturę informacji, poziom ryzyka albo dostęp do zasobu publicznego, kryteria te nie powinny znikać z demokratycznego pola widzenia tylko dlatego, że zostały zapisane matematycznie. To, co jest normatywne, pozostaje normatywne nawet wtedy, gdy przyjmuje postać funkcji celu.

Przyszłość demokracji może zatem zależeć od zdolności społeczeństwa do repolityzacji ukrytych założeń technicznych: ujawniania, jakie wartości zawiera model, kto ponosi koszt błędu, jakie zachowania są nagradzane i kto posiada możliwość zmiany parametrów. Nie jest to wezwanie do

parlamentarnego głosowania nad każdą linią kodu, lecz do zachowania hierarchii: ekspert wybiera implementację, ale społeczeństwo powinno zachować prawo do określania celu i granicy ingerencji.

## Człowieczeństwo jako podmiotowość przeciw optymalizacji

Z tej perspektywy wezwanie, by "zachować swoje człowieczeństwo", nabiera znacznie głębszego znaczenia niż sentymentalne ostrzeżenie przed maszynami. Materiał źródłowy wiąże tę maksymę z sprzeciwem wobec redukcji człowieka do zestawu danych oraz z pamięcią o systemach wykorzystujących informację do represji. W końcowej części notatki przesłanie to staje się wręcz zasadą: AI powinna wzmacniać ludzki potencjał, a nie przekształcać się w broń wymierzoną w ludzką godność. "Człowieczeństwo" nie oznacza tu jednak przeciwstawienia chłodnej maszyny ciepłemu człowiekowi – przecież ten ostatni bywa okrutny, stronniczy, nieracjonalny i podatny na manipulację.

Chodzi o wymiar bardziej instytucjonalny: zachowanie przestrzeni, w której człowiek pozostaje podmiotem, a nie wyłącznie obiektem optymalizacji. Podmiot posiada prawo do uzasadnienia. Może powiedzieć "nie". Może się odwołać, zmienić zdanie lub rozpocząć od nowa. Może nie odpowiadać statystycznemu profilowi swojej grupy. Może domagać się, aby decyzja o jego wolności lub godności była podjęta w procedurze, a nie tylko wygenerowana przez system. Może oczekiwać, że państwo, korporacja i ekspert będą ograniczeni normami, nawet jeśli mogliby działać szybciej bez tych barier. To właśnie jest polityczna treść człowieczeństwa.

W tym kontekście można wyobrazić sobie co najmniej trzy kierunki rozwoju cywilizacji cyfrowej. Pierwszy to model augmentacji obywatelskiej. AI zwiększa produktywność i dostęp do wiedzy; automatyzacja ogranicza rutynę, podczas gdy społeczeństwo inwestuje w edukację i przekwalifikowanie zawodowe; chmura podnosi efektywność państwa, lecz prywatność i interoperacyjność wyznaczają granice władzy; technologie bezpieczeństwa chronią infrastrukturę, nie tworząc przy tym permanentnego nadzoru. W tym scenariuszu narzędzie zwiększa sprawczość człowieka, a instytucje ewoluują wraz z jego mocą.

Drugi wariant to administracyjny technokratyzm. Systemy działają coraz wydajniej, lecz człowiek stopniowo traci zdolność rozumienia i kwestionowania decyzji. Edukacja uczy obsługi systemów zamiast samodzielnego myślenia, prawo staje się procedurą zatwierdzania wyników modeli, a human oversight pozostaje formalnością. Państwo i korporacje wiedzą o jednostce coraz więcej, podczas gdy ona sama coraz mniej rozumie reguły środowiska, w którym funkcjonuje. Nie jest to

klasyczny totalitaryzm, lecz subtelniejsza postać łagodnej heteronomii, w której większość ograniczeń jest wygodna, spersonalizowana i przedstawiana jako optymalizacja.

Trzeci scenariusz to fragmentacja techno-polityczna. Państwa budują konkurujące stosy technologiczne, ograniczają przepływ danych, talentów i półprzewodników, a modele AI stają się elementem narodowych ekosystemów informacyjnych. Cyberbezpieczeństwo zlewa się z bezpieczeństwem narodowym, a interoperacyjność ustępuje koalicyjnemu zaufaniu. Taki świat może być bardziej odporny na niektóre zależności, ale mniej zdolny do wspólnego rozwiązywania globalnych problemów i bardziej podatny na spirale bezpieczeństwa.

Żaden z tych scenariuszy nie jest nieuchronny. To najważniejszy wniosek.

## Projektowanie możliwości poprawy jako fundament kontroli nad technologią

Determinizm technologiczny jest wygodnym sposobem uchylania się od odpowiedzialności. Twierdzenie, że „technologia i tak to zrobi", stanowi politycznym odpowiednikiem fatalizmu. Maszyny nie ustalają samodzielnie prawa podatkowego, standardów interoperacyjności, zasad dostępu do danych, finansowania edukacji ani zakresu kontroli eksportu. To ludzie budują instytucje kształtujące trajektorię technologii. Przyszłość nie zostanie zatem „przyniesiona przez AI", lecz współwytworzona w interakcji sztucznej inteligencji z prawem, ekonomią, kulturą, instytucjami i ludzkimi decyzjami.

Podstawowym narzędziem kontroli technologii pozostaje zdolność społeczeństwa do samokorekty. Nauka opiera się na replikacji i krytyce; demokracja na wyborach, opozycji i debacie; prawo na apelacji i kontroli sądowej, a rynek na konkurencji i możliwości odejścia.

Dobra inżynieria wykorzystuje testy, monitoring i rollback. Wszystkie te mechanizmy realizują tę samą głęboką ideę: żaden pojedynczy wynik nie powinien być traktowany jako nieomylny. Można tu sformułować być może najważniejszą zasadę odpowiedzialnej cywilizacji technologicznej: projektuj możliwość poprawienia siebie. System, który nie dopuszcza korekty, wymagałby bowiem nieomylnego projektanta, a tacy nie istnieją – dotyczy to zarówno państw i korporacji, jak i modeli AI czy teorii naukowych. Wielkość nowoczesnej cywilizacji nie polega na wyeliminowaniu błędu, lecz na stworzeniu instytucji pozwalających go rozpoznać i naprawić bez całkowitego zniszczenia systemu. Technologia powinna zostać włączona do tej tradycji samokorekty, a nie postawiona ponad nią. Wówczas można na nowo odczytać źródłową formułę: „pierwsza nagroda to zrobić coś wielkiego, druga – naprawić błędy". Nie jest to jedynie korporacyjna pochwała pokory, lecz

fundamentalna zasada epistemologiczna. Organizacja dojrzała nie buduje swojej reputacji na braku błędów, lecz na zdolności ich rozpoznawania, ujawniania i korygowania. W tym sensie Pokora staje się kompetencją technologiczną.

Podobnie zaufanie nie powinno być rozumiane jako przeciwieństwo kontroli. Najbardziej dojrzałe zaufanie jest produktem systemu, który pozwala weryfikować obietnicę. Materiał źródłowy wiąże wiarygodność z gotowością do ponoszenia kosztów za dochowanie zobowiązań oraz z powiernictwem globalnego zaufania. Z perspektywy instytucjonalnej można powiedzieć mocniej: zaufanie jest stabilne wtedy, gdy nie zależy wyłącznie od charakteru człowieka sprawującego władzę, lecz od struktury ograniczającej jego arbitralność.

Dojrzała cywilizacja nie potrzebuje zatem „dobrego algorytmu" bardziej niż potrzebowała „dobrego króla". Potrzebuje dobrych procedur, ograniczeń, kompetencji i możliwości sprzeciwu. Technologia większa od jej twórców nie musi więc oznaczać technologii poza kontrolą. Fakt, że jest „większa", może oznaczać jedynie, iż przekroczyła zdolność pojedynczego człowieka lub organizacji do ogarnięcia wszystkich konsekwencji. Odpowiedzią na to nie jest heroiczny geniusz, lecz instytucja zbiorowego rozumu. Nauka, demokratyczne prawo, profesjonalny etos, audyt, techniczne zabezpieczenia, konkurencja, interoperacyjność, edukacja i dyplomacja są różnymi postaciami tego samego mechanizmu: rozkładają władzę poznawczą i wykonawczą pomiędzy wielu aktorów, aby zminimalizować ryzyko, że pojedynczy błąd stanie się losem wszystkich.

W tym miejscu pojawia się najgłębsze znaczenie Dobra Wspólnego w epoce technologicznej.

## Technologia bezpieczna bez konieczności ufania twórcom

Nie jest nim jedna wspólna odpowiedź ani zatrzymanie różnic. Dobro Wspólne polega na zachowaniu warunków, dzięki którym różni ludzie mogą nadal wspólnie korygować świat, który tworzą. Jeśli technologia pozbawi społeczeństwo tej zdolności — poprzez nieprzejrzystość, nieodwracalność, monopol, manipulację, automatyczne profilowanie albo epistemiczną fragmentację — może działać znakomicie jako produkt i jednocześnie niszczyć podstawę politycznej wspólnoty. Jeśli natomiast zwiększy dostęp do wiedzy, zdolność współpracy, odporność instytucji, kompetencje człowieka i możliwość pokojowego kwestionowania władzy, stanie się jednym z najpotężniejszych narzędzi emancypacyjnych w historii.

Ostateczny podział nie przebiega między technofilami a technosceptykami. Przebiega między tymi, którzy wierzą, że moc wystarcza, a tymi, którzy rozumieją, że moc wymaga ustroju. Materiały

źródłowe Tools and Weapons wracają w końcu do obrazu człowieka stojącego przed własnym wynalazkiem i słyszącego wezwanie: "zachowaj swoje człowieczeństwo".

Po przejściu przez chmurę, prywatność, analitykę, cyberwojnę, demokrację, sztuczną inteligencję, pracę, edukację i geopolitykę można już precyzyjniej określić, co to wezwanie oznacza. Oznacza projektowanie technologii, której można odmówić. Technologii, której wynik można zakwestionować. Technologii, której władza jest proporcjonalna do celu. Technologii pozostawiającej człowiekowi możliwość zmiany, błędu i drugiej szansy. Technologii, która dokumentuje swoje działanie, ale nie dokumentuje człowieka ponad konieczność. Technologii, której dostawca nie przekształca zależności użytkownika w polityczny monopol. Technologii, która w warunkach kryzysu degraduje się bezpiecznie zamiast ciągnąć cały system za sobą. Technologii, której twórca potrafi powiedzieć nie tylko "działa", lecz również "wiemy, dlaczego powinna działać właśnie w ten sposób i kto może nas zatrzymać, gdy się mylimy".

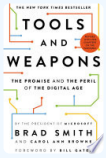
Narzędzie pozostaje narzędziem nawet wtedy, gdy posiada ogromną moc. Brak tych warunków nie musi od razu przekształcić go w broń. Może jednak stworzyć broń oczekującą jedynie na zmianę operatora, modelu biznesowego, prawa albo politycznego reżimu.

I to jest najtrwalsza lekcja historii cyfrowej transformacji: nie projektujemy technologii tylko dla ludzi, którym dzisiaj ufamy. Projektujemy ją również dla świata, w którym władza, interes i intencje mogą się zmienić.

Najlepsza technologia nie jest tą, której twórcy obiecują, że nigdy nie nadużyją własnej potęgi. Najlepsza jest ta, która nie wymaga od społeczeństwa takiej wiary.

> Ostatecznie najwyższą formą dojrzałości technologicznej nie jest stworzenie systemu nieomylnego, lecz takiego, który projektuje możliwość własnej korekty. Prawdziwie bezpieczna technologia to nie ta, której twórcy obiecują, że nigdy nie nadużyją swojej potęgi, ale ta, która w swojej architekturze nie wymaga od społeczeństwa takiej wiary. Czy jesteśmy zatem gotowi zaakceptować systemowe 'tarcie' i spowolnienie w imię wolności, czy pozwolimy, by wydajność stała się nową formą arbitralnej władzy?

## Inspiracje

[1] 


**"Tools and Weapons"** Brad Smith

*2019 | Penguin Press | ISBN: 978-1984877710*

Bradford Lee Smith (ur. 17 stycznia 1959 r.) to amerykański prawnik i dyrektor zarządzający, pełniący funkcję prezesa i wiceprezesa Microsoftu. Dołączył do firmy w 1993 roku i odegrał kluczową rolę w jej sprawach prawnych i korporacyjnych, w szczególności prowadząc do rozwiązania poważnych sporów antymonopolowych. Smith jest powszechnie uznawany za swoją pracę na styku technologii i społeczeństwa, koncentrując się na takich kwestiach jak cyberbezpieczeństwo, sztuczna inteligencja, prywatność, prawa człowieka i zrównoważony rozwój środowiska. Jest absolwentem Uniwersytetu Princeton i Columbia Law School, a wcześniej praktykował prawo w kancelarii Covington & Burling. Jako prominentny przedstawiciel branży technologicznej, opowiada się za społeczną odpowiedzialnością biznesu i zacieśnioną współpracą między sektorem technologicznym a rządami w celu sprostania złożonym wyzwaniom ery cyfrowej.

*Bradford Lee Smith (born January 17, 1959) is an American attorney and business executive serving as the president and vice chair of Microsoft. He joined the company in 1993 and has played a pivotal role in its legal and corporate affairs, notably leading the resolution of major antitrust controversies. Smith is widely recognized for his work at the intersection of technology and society, focusing on issues such as cybersecurity, artificial intelligence, privacy, human rights, and environmental sustainability. He is a graduate of Princeton University and Columbia Law School, and he previously practiced law at the firm Covington & Burling. As a prominent voice in the technology industry, he advocates for corporate responsibility and increased collaboration between the tech sector and governments to address the complex challenges of the digital age.*

*Microsoft*

## Literatura uzupełniająca

### Książki

## Autorzy przywoływani w artykule:


**[1] "All Hat"**

Brad Smith

2013 | Henry Holt and Company | ISBN: 9781466855557


**[2] "Shoot the Dog"**

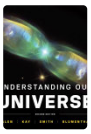
Brad Smith

2013 | Simon and Schuster | ISBN: 9781439197493


**[3] "Crow's Landing"**

Brad Smith

2012 | Simon and Schuster | ISBN: 9781439197530



**[4] "Understanding Our Universe"**

Stacy Palen, Laura Kay, Brad Smith, George Ray Blumenthal

2015 | W. W. Norton | ISBN: 9780393936315


**[5] "Copperhead Road"**

Brad Smith

2022 | At Bay Press | ISBN: 9781988168708


**[6] "The Return of Kid Cooper"**

Brad Smith

2018 | Simon and Schuster | ISBN: 9781628728729

## Literatura pokrewna (Google Scholar):


**[7] "After Hegemony"**

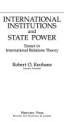
Robert Keohane

2005 | Princeton University Press | ISBN: 9781400820269


**[8] "Power and Interdependence"**

Robert Owen Keohane, Joseph S. Nye

1977 | Addison-Wesley Educational Publishers




**[9] "International Institutions And State Power"**

Robert O Keohane

1989 | Westview Press

[10] **"Still holding its own"**

Joseph Nye

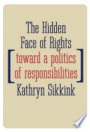
[11] **"Soft Power: The Means To Success In World Politics"**

Joseph Nye

Hachette UK | ISBN: 9780786738960

[12] **"Joseph Nye: Global power shifts"**

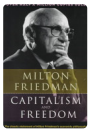
Joseph Nye



[13] **"The Hidden Face of Rights"**

Kathryn Sikkink

2020 | Yale University Press | ISBN: 9780300233292



[14] **"Capitalism and Freedom"**

Milton Friedman

1962 | Chicago : University of Chicago Press | ISBN: 9780226264011

[15] **"The Great Contraction, 1929-1933"**

Milton Friedman, Anna Jacobson Schwartz, National Bureau of Economic Research

2008 | Princeton University Press | ISBN: 9780691137940

[16] **"The Analects of Confucius"**

Konfucjusz

[17] **"Great Learning"**

Konfucjusz

[18] **"Translation: Analects of Confucius"**

Konfucjusz

[19] **"A free-market monetary system"**

Friedrich August Von Hayek

Ludwig von Mises Institute | ISBN: 9781610164450

[20] **"A free-market monetary system (2008)"**

Friedrich August Von Hayek

Ludwig von Mises Institute | ISBN: 9781610164450

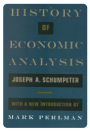
[21] **"Individualism and Economic Order"**

Friedrich August Von Hayek

ISBN: 9780226320892

[22] **"Capitalism, Socialism and Democracy"**

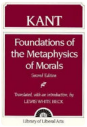
Joseph Schumpeter




[23] **"History of Economic Analysis"**

Joseph Schumpeter

Oxford University Press, USA | ISBN: 9780195105599




[24] **"Foundations of the Metaphysics of Morals And, What is Enlightenment"**

Immanuel Kant

1990 | Prentice Hall

[25] **"History of Economic Analysis (Oxford Press, 1955)"**

Joseph Schumpeter

Taylor & Francis | ISBN: 9781134838714

[26] **"covfefe"**

Donald Trump

ISBN: 9781521582510

[27] **"Despite the constant negative press covfefe"**

Donald Trump

[28] **"Trump on China: Putting America First"**

Donald Trump

[29] **"Weaponized interdependence"**

Abraham Newman


[30] **"Normal accidents : living with high-risk technologies : with a new afterword and a postscript on the Y2K problem"**

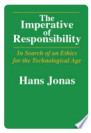
Charles Perrow

Princeton University Press | ISBN: 9780691004129


**[31] "Normal Accidents"**

Charles Perrow

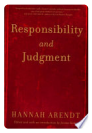
Princeton University Press | ISBN: 9780691004129




**[32] "The Imperative of Responsibility"**

Hans Jonas

2025 | University of Chicago Press | ISBN: 9780226850337




**[33] "Responsibility and Judgment"**

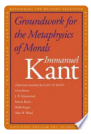
Hannah Arendt

Schocken | ISBN: 9780307544056


**[34] "Knowledge and Human Interests"**

Jürgen Habermas

John Wiley & Sons | ISBN: 9780745694177




**[35] "Groundwork for the Metaphysics of Morals"**

Immanuel Kant, Jerome B. Schneewind

2002 | Yale University Press | ISBN: 9780300094862


**[36] "Design for a brain"**

W. Ross Ashby

ISBN: 9781614277569


**[37] "Design for a brain; the origin of adaptive behavior"**

W. Ross Ashby

ISBN: 9781614277569


**[38] "An introduction to cybernetics"**

W. Ross Ashby


**[39] "Deconstructing Digital Capitalism and the Smart Society"**

Mel van Elteren

2025 | McFarland | ISBN: 9781476696096


**[40] "De Gruyter Handbook of Digital Cultures"**

Grant Bollmer, Katherine Guinness, Yiğit Soncul

2025 | Walter de Gruyter GmbH & Co KG | ISBN: 9783111317267


**[41] "The Human Paradox"**

Frank Gaffikin

2023 | Taylor & Francis | ISBN: 9781000893366


**[42] "Global Financial Media and China's Greater Bay Area"**

Vincent P. Wong, Anilesh Kumar

2026 | Taylor & Francis | ISBN: 9781040872130

**[43] "Proceedings of the American Power Conference"**

1999


**[44] "Economic and Political Weekly"**

2000

## Artykuły naukowe

### Autorzy przywoływani:

**[1] "Power and Interdependence"**

Robert O. Keohane, Joseph S. Nye

2013 | International Organization | DOI: 10.1057/9781137356734.0006

Google Scholar

**[2] "Soft Power: The Means to Success in World Politics"**

G. John Ikenberry, Joseph S. Nye

2004 | Foreign Affairs | DOI: 10.2307/20033985

Google Scholar

**[3] "Soft Power"**

Joseph S. Nye

1990 | Foreign Policy | DOI: 10.2307/1148580

Google Scholar

**[4] "International Norm Dynamics and Political Change"**

Martha Finnemore, Kathryn Sikkink

1998 | International Organization | DOI: 10.1162/002081898550789

Google Scholar

[5] **"Designing Social Inquiry"**

Gary King, Robert O. Keohane, Sidney Verba

1994 | Princeton University Press eBooks | DOI: 10.1515/9781400821211

Google Scholar

[6] **"After Hegemony: Cooperation and Discord in the World Political Economy"**

William Diebold, Robert O. Keohane

1984 | Foreign Affairs | DOI: 10.2307/20042201

Google Scholar

[7] **"Power and Interdependence: World Politics In Transition"**

Robert O. Keohane, Joseph S. Nye

2017 | The SHAFR Guide Online | DOI: 10.1163/2468-1733_shafr_sim280020670

Google Scholar

[8] **"The Politics, Power, and Pathologies of International Organizations"**

Michael Barnett, Martha Finnemore

1999 | International Organization | DOI: 10.1162/002081899551048

Google Scholar

[9] **"Norms, culture, and world politics: insights from sociology's institutionalism"**

Martha Finnemore

1996 | International Organization | DOI: 10.1017/s0020818300028587

Google Scholar

[10] **"Rules for the World"**

Michael Barnett, Martha Finnemore

2019 | Cornell University Press eBooks | DOI: 10.7591/9780801465161

Google Scholar

[11] **"The socialization of international human rights norms into domestic practices: introduction"**

Thomas Risse, Kathryn Sikkink

1999 | Cambridge University Press eBooks | DOI: 10.1017/cbo9780511598777.002

Google Scholar

[12] **"Human rights, principled issue-networks, and sovereignty in Latin America"**

Kathryn Sikkink

1993 | International Organization | DOI: 10.1017/s0020818300028010

Google Scholar

[13] **"Restructuring World Politics: Transnational Social Movements, Networks, and Norms"**

Sanjeev Khagram, James V. Riker, Kathryn Sikkink

2002 | Project Muse (Johns Hopkins University)

Google Scholar

[14] **"The X Club: Power and Authority in Victorian Science by Ruth Barton (review)"**

J. Browne

2020

Google Scholar

[15] **"The Pretence of Knowledge"**

Friedrich von Hayek

1975 | Ekonomisk Tidskrift | DOI: 10.2307/3439337

Google Scholar

[16] **"The Transmission of the Ideals of Economic Freedom"**

Friedrich von Hayek

2012 | Econ journal watch

Google Scholar

[17] **"The Market and Other Orders"**

Friedrich von Hayek

2014 | RePEc: Research Papers in Economics

Google Scholar

[18] **"The Sensory Order and Other Writings on the Foundations of Theoretical Psychology"**

Friedrich von Hayek

2017 | RePEc: Research Papers in Economics

Google Scholar

[19] **"Executive Order 13914: Encouraging International Support for the Recovery and Use of Space Resources"**

Donald J. Trump

2020

Google Scholar

[20] **"Executive Order 13944: Combating Public Health Emergencies and Strengthening National Security by Ensuring Essential Medicines, Medical Countermeasures, and Critical Inputs Are Made in the United States"**

Donald J. Trump

2020

Google Scholar

[21] **"Executive Order 13935: White House Hispanic Prosperity Initiative"**

Donald J. Trump

2020

Google Scholar

[22] **"Local flux of hydrogen from magnesium alloy corrosion investigated by scanning electrochemical microscopy"**

Ushula M. Tefashe, Michael E. Snowden, Philippe Dauphin-Ducharme, Mohsen Danaie, Gianluigi A. Botton

2014 | Journal of Electroanalytical Chemistry | DOI: 10.1016/j.jelechem.2014.03.002

Google Scholar

[23] **"Intrinsic Kinetics of Gypsum and Calcium Sulfate Anhydrite Dissolution: Surface Selective Studies under Hydrodynamic Control and the Effect of Additives"**

Michael M. Mbogoro, Michael E. Snowden, Martin A. Edwards, Massimo Peruffo, Patrick R. Unwin

2011 | The Journal of Physical Chemistry C | DOI: 10.1021/jp201718b

Google Scholar

[24] **"Measurement on isolated lithium iron phosphate particles reveals heterogeneity in material properties distribution"**

Michael E. Snowden, Malak Dayeh, Nicholas A. Payne, Simon Gervais, Janine Mauzeroll

2016 | Journal of Power Sources | DOI: 10.1016/j.jpowsour.2016.06.081

Google Scholar

**[25] "Localized Investigations of the Electrochemical Properties of Lithium Battery Materials Using Micro-Pipets"**

Michael E. Snowden, J. Mauzeroll, S. Schougaard

2015 | DOI: 10.1149/ma2015-01/30/1723

Google Scholar

**[26] "Impact of choral singing on the formation of responsibility value in students"**

Arién, Rodríguez-Juan, Sandra Yanet Ricardo-Rodríguez, Arlena Osa-Ricardo, Elisneisis Jones-Sánchez

2022 | Revista de Educación Básica | DOI: 10.35429/jbe.2022.15.6.1.8

Google Scholar

**[27] "Weaponized Interdependence: How Global Economic Networks Shape State Coercion"**

Henry Farrell, Abraham L. Newman

2019 | International Security | DOI: 10.1162/isec_a_00351

Google Scholar

**[28] "The power and politics of blogs"**

Henry Farrell, Daniel W. Drezner

2007 | Public Choice | DOI: 10.1007/s11127-007-9198-1

Google Scholar

**[29] "Breaking the Path of Institutional Development? Alternatives to the New Determinism"**

Colin Crouch, Henry Farrell

2004 | Rationality and Society | DOI: 10.1177/1043463104039874

Google Scholar

**[30] "Formal and Informal Institutions Under Codecision: Continuous Constitution-Building in Europe"**

Henry Farrell, Adrienne Héritier

2003 | Governance | DOI: 10.1111/1468-0491.00229

Google Scholar

**[31] "Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union"**

Burkard Eberlein, Abraham L. Newman

2008 | Governance | DOI: 10.1111/j.1468-0491.2007.00384.x

Google Scholar

**[32] "The European regulatory state and global public policy: micro-institutions, macro-influence"**

David Bach, Abraham L. Newman

2007 | Journal of European Public Policy | DOI: 10.1080/13501760701497659

Google Scholar

**[33] "Making global markets: Historical institutionalism in international political economy"**

Henry Farrell, Abraham L. Newman

2010 | Review of International Political Economy | DOI: 10.1080/09692291003723672

Google Scholar

**[34] "The Modern Corporation Statement on Management"**

H. Willmott, M. Djelic, A. Spicer, Martin Parker, C. Perrow

2016 | DOI: 10.2139/ssrn.2863077

Google Scholar

**[35] "Responsibility Today: The Ethics of an Endangered Future 1"**

Hans Jonas

2017 | Global Ethics and Moral Responsibility | DOI: 10.4324/9781315584829-2

Google Scholar

**[36] "Technology and Responsibility: Reflections on the New Tasks of Ethics"**

Hans Jonas

2014 | Ethics and Emerging Technologies | DOI: 10.1057/9781137349088_3

Google Scholar

**[37] "The Human Condition"**

Hannah Arendt, Margaret Canovan, Danielle Allen

1998 | DOI: 10.7208/chicago/9780226586748.001.0001

Google Scholar

[38] **"Between past and future eight exercises in political thought"**

Hannah Arendt

1987

Google Scholar

[39] **"Lectures on Kant's Political Philosophy"**

Hannah Arendt, Ronald Beiner

1982 | DOI: 10.7208/chicago/9780226231785.001.0001

Google Scholar

[40] **"Between Past and Future."**

Judith N. Shklar, Hannah Arendt

1963 | History and Theory | DOI: 10.2307/2504107

Google Scholar

[41] **"Critique of the Power of Judgment"**

Immanuel Kant

2000 | Cambridge University Press eBooks | DOI: 10.1017/cbo9780511804656

Google Scholar

[42] **"Groundwork of The Metaphysic of Morals"**

Immanuel Kant

2020 | DOI: 10.4324/9780203714805-2

Google Scholar

[43] **"Grounding for the Metaphysics of Morals"**

Immanuel Kant, James W. Ellington

2020 | Medical Entomology and Zoology

Google Scholar

[44] **"Kant: The Metaphysics of Morals"**

Immanuel Kant, Roger J. Sullivan

1996 | Cambridge University Press eBooks | DOI: 10.1017/cbo9780511809644

Google Scholar

[45] **"Every good regulator of a system must be a model of that system †"**

Roger C. Conant, W. Ross Ashby

1970 | International Journal of Systems Science | DOI: 10.1080/00207727008920220

Google Scholar

[46] **"Requisite Variety and Its Implications for the Control of Complex Systems"**

W. Ross Ashby

1991 | Facets of Systems Science | DOI: 10.1007/978-1-4899-0718-9_28

Google Scholar

[47] **"Every Good Regulator of a System Must Be a Model of That System"**

Roger C. Conant, W. Ross Ashby

1991 | Facets of Systems Science | DOI: 10.1007/978-1-4899-0718-9_37

Google Scholar

[48] **"Principles of the Self-Organizing Dynamic System"**

W. Ross Ashby

1947 | The Journal of General Psychology | DOI: 10.1080/00221309.1947.9918144

Google Scholar

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System

Article ID: 034689f5-b32b-4984-9b11-7286c756c3d7