

Huawei: lotniskowiec z garażu i nowa metafizyka technologii



AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł stanowi głęboką analizę ewolucji Huawei, postrzeganego nie tylko jako korporacja, ale jako kluczowy element chińskiej strategii suwerenności technologicznej. Autor dekonstruuje retorykę założyciela firmy, ukazując ją jako narzędzie budowania operacyjnej spójności i legitymacji działań o charakterze quasi-państwowym. Tekst szczegółowo omawia rolę infrastruktury 5G jako 'architektury władzy', podważając mit neutralności dostawców technologii. Analizie poddano również systemy Safe City i biometrię w kontekście etyki nadzoru oraz wpływ amerykańskich sankcji na rozwój R&D. Całość dopełnia badanie unikalnej struktury własnościowej i roli partii wewnątrz firmy, co czyni z Huawei technologiczny lotniskowiec w globalnej grze o dominację cyfrową i rentę ekonomiczną.

This article provides an in-depth analysis of Huawei's evolution, viewed not just as a corporation but as a key element of China's strategy of technological sovereignty. The author deconstructs the rhetoric of the company's founder, presenting it as a tool for building operational coherence and legitimizing quasi-state activities. The text discusses in detail the role of 5G infrastructure as a "power architecture," challenging the myth of technology supplier neutrality. Safe City systems and biometrics are also analyzed in the context of surveillance ethics, and the impact of US sanctions on R&D development. The text is complemented by an examination of the unique ownership structure and the role of the party within the company, which makes Huawei a technological aircraft carrier in the global game of digital dominance and economic rent.

Artykuł analizuje fenomen Huawei, dekonstruując go jako przykład współczesnego przedsiębiorstwa funkcjonującego na styku sprzecznych logik: rynkowej, państwowej i militarnej. Autor dowodzi, że sukces firmy nie wynika jedynie z innowacyjności technologicznej, ale przede wszystkim z umiejętnego wykorzystania retoryki założyciela,

Ren Zhengfei, do budowania wewnętrznej spójności i lojalności. Huawei jawi się jako paradoks: prywatna firma działająca jak państwo, komercyjna korporacja przesiąknięta geopolityką, a jej produkty – jak "cyfrowe uzbrojenie" – stają się elementami walki o suwerenność technologiczną. Analiza skupia się na trzech kluczowych pojęciach: infrastrukturze krytycznej, suwerenności technologicznej i metafizyce infrastruktury, by pokazać, że spór o Huawei to w istocie walka o architekturę władzy w globalnych łańcuchach dostaw. Artykuł proponuje program działań dla państw, organizacji społecznych i biznesu, mający na celu projektowanie instytucji zdolnych do funkcjonowania w warunkach trwałej nieufności, bez paraliżu czy paranoi.

SŁOWA KLUCZOWE

suwerenność technologiczna

infrastruktura krytyczna

Safe City

5G

R&D

Entity List

biometria

kultura materaca

hydraulicy danych

standard techniczny

renta ekonomiczna

komitet związkowy

pętla uczenia się

architektura władzy

geopolityka

Retoryka Rena Zhengfei cementuje zgodę operacyjną

Gdy spojrzymy na przedsiębiorstwo nie jako na sumę aktywów, lecz jako na mechanizm koordynacji działań służących wzajemnemu zrozumieniu, retoryka założyciela przestaje być ornamentem. Staje się precyzyjnym narzędziem do budowania operacyjnej zgody: gęstym kodem, który rozdziela role, dyscyplinuje oczekiwania i zamyka spory interpretacyjne. Co więcej, w realiach globalnej wojny technologicznej nadaje ona całemu przedsięwzięciu rangę wspólnoty, pozwalając zwykłej firmie mówić głosem quasi-państwa, a państwu działać niczym jej nieformalny udziałowiec. I to właśnie dlatego Huawei jawi się jako paradoks: prywatny, a zarazem „narodowy”; komercyjny, lecz głęboko geopolityczny; korporacyjny, ale przesiąknięty frontową terminologią. Kluczem do tej zagadki jest fakt, że Ren Zhengfei nie tyle „motywował”, ile konstruował fundamentalne warunki uznania, w ramach których każda strategiczna decyzja musiała uzyskać legitymację jednocześnie w trzech porządkach: prawdziwości propozycjonalnej (czy to działa?), normatywnej słuszności (czy to „służy sprawie”?) oraz autentyczności ekspresji (czy mówimy własnym głosem?).

Huawei: paradoks hybrydy prywatno-narodowej

Celem nie jest tu faktografia godna kronikarza. Rekonstrukcja formalno-pragmatyczna, o którą chodzi, polega na hipotetycznym odtworzeniu ukrytych reguł, dzięki którym Huawei stał się instytucją zdolną do jednoczesnego funkcjonowania w trzech logikach: rynku, państwowego projektu modernizacyjnego oraz organizacji przypominającej — nie bez powodu — oddział sił specjalnych w stanie permanentnej gotowości. Taki model, raz uruchomiony, jest dla biznesu błogosławieństwem i przekleństwem zarazem. Maksymalizuje bowiem tempo adaptacji, ale zatruwa reputację; wytwarza odporność na sankcje, lecz prowokuje ich eskalację; buduje wewnętrzną „zbiorową inteligencję”, ale z zewnątrz wygląda jak czarna skrzynka, skutecznie utrudniając jakąkolwiek zewnętrzną weryfikację.

Kultura materaca: cena i zysk ekstremalnej wydajności

Początek opowieści jest — i w tym punkcie oficjalna narracja ma rację, której nie wolno osłabiać — skrajnie nieheroiczny w sensie materialnym, a właśnie dlatego heroiczny w sensie organizacyjnym. Huawei rodzi się w Shenzhen, w laboratorium chińskiego eksperymentu z kapitalizmem, jako przedsięwzięcie handlowe i drobne, pozbawione własnej technologii, żywiące się montażem, imitacją i improwizacją. Dopiero gdy uruchomione zostają praktyki, które w późniejszej mitologii firmy zyskują miano „kultury materaca”, pojawia się szansa na skrócenie pętli uczenia się do poziomu normalnie dla firm zabójczego. Młode kadry techniczne spalają swój prywatny czas jako paliwo dla działu R&D, a organizacja — niczym system chłodzenia reaktora — odprowadza ludzkie koszty tego przeciążenia, by utrzymać stałą temperaturę wzrostu. I to jest moment, w którym powinniśmy poczuć intelektualny dyskomfort: tak, ten model faktycznie wytwarza przewagę; nie, nie ma w nim nic niewinnego; i owszem, zachodni biznes przez dekady korzystał z bardzo podobnych mechanizmów, tyle że zwykle lepiej je maskował i ubierał w bardziej cywilizowany język.

Cyfrowe uzbrojenie redefiniuje ramy rynkowe

Warto wprowadzić pierwsze pojęcie specjalistyczne, które będzie powracać jak refren. Infrastruktura krytyczna oznacza bowiem te systemy techniczne, których zakłócenie destabilizuje podstawowe funkcje państwa i gospodarki: łączność, energetykę, transport, finanse czy bezpieczeństwo. Gdy Ren mówi o „cyfrowym uzbrojeniu narodu”, nie tworzy metaforycznego fajerwerku, lecz dokonuje performatywnego przestawienia całej ramy. Huawei przestaje być

producentem sprzętu, a staje się dostawcą elementu państwowej odporności; firma prywatna wchodzi w reżim oczekiwań właściwy dla sektora strategicznego. Rynek przestaje być jedynie rynkiem, gdyż staje się teatrem działań, w którym stawką jest suwerenność technologiczna, a więc prawo do decydowania o własnej przyszłości bez cudzego „wyłącznika”. W tej samej mierze, w jakiej to hasło jest fundamentem sukcesu, jest ono źródłem przyszłej katastrofy wizerunkowej. Skoro sam ogłaszasz, że jesteś „uzbrojeniem”, to inni traktują cię jak broń – i nie chodzi tu o złośliwość, lecz o żelazną konsekwencję racjonalności państw, które w warunkach niepewności muszą kalkulować ryzyko systemowe.

Hydraulicy danych: koniec mitu neutralności

Dochodzimy do drugiego hasła, które w tej grze działa jak retoryczny wytrych: „Jesteśmy tylko hydraulikami danych”. Z punktu widzenia strategii komunikacyjnej to posunięcie niemal doskonałe. Po pierwsze, odcina firmę od odpowiedzialności za treść, a więc unieważnia oskarżenia o intencjonalne szpiegostwo. Po drugie, przenosi całą debatę z grząskiego pola polityki na twardy grunt inżynierii, gdzie liczą się tylko „szczelne rury”. Po trzecie, sugeruje, że zarzuty są fundamentalnym błędem kategorialnym – myleniem medium z przekazem.

Lecz właśnie w tym punkcie polemika musi stać się bezkompromisowa. W epoce danych to właśnie „rury” są bowiem epicentrum władzy, gdyż ten, kto projektuje kanał, zyskuje możliwość kontroli przepływu, a z nią zdolność do selekcji, priorytetyzacji, przechwytywania metadanych i modelowania topologii ryzyka. Neutralność infrastruktury jest mitem na miarę mitu neutralności konstytucji: z pozoru jedynie opisuje rzeczywistość, a w istocie ją ustanawia. Dlatego „hydraulik” jest zarazem inżynierem, strażnikiem i potencjalnym szantażystą. Nawet jeśli zarzeka się, że interesuje go wyłącznie ciśnienie w rurach.

Entity List: amerykański oręż w blokadzie rynków

Spór o Huawei, toczony na salonach i w laboratoriach, nie jest wcale dyskusją o moralności, lecz o architekturze władzy ukrytej w globalnych łańcuchach dostaw. I tu trafiamy w sedno: wojna handlowa USA–Chiny przeistoczyła się w wojnę technologiczną, w której kontrola eksportu działa jak zawór tlenu. W języku prawnym „Entity List” to suchy instrument administracyjny, ograniczający transfer technologii objętych amerykańskimi regulacjami. W języku ekonomicznym – narzędzie do przesuwania granic opłacalności, a w języku geopolityki – metoda hodowania chronicznej niepewności u przeciwnika. Formalny próg tej nowej fazy konfliktu wyznaczyło

wpisanie Huawei i spółek zależnych na listę 16 maja 2019 roku. Wielka Brytania, reagując na gwałtowną zmianę parametrów ryzyka, ogłosiła w lipcu 2020 roku zakaz zakupu nowego sprzętu 5G firmy Huawei z końcem roku oraz plan jego usunięcia z sieci do 2027 roku. Te daty to nie są przypisy dla historyków. To twardy dowód, że slogan o „cyfrowym uzbrojeniu” potraktowano z całą dosłownością – zwłaszcza w państwach, które w grze o suwerenność nie mogą sobie pozwolić na luksus wiary w dobre intencje.

Suwerenność technologiczna: model autonomii Huawei

Należy wprowadzić trzecie pojęcie: „suwerenność technologiczną”. Oznacza ona zdolność państwa bądź bloku gospodarczego do utrzymania kluczowych funkcji gospodarki i bezpieczeństwa mimo zakłóceń w dostawach technologii, standardów i wiedzy. W tej definicji kluczowe jest słowo „mimo”, bowiem suwerenność nie oznacza autarkii, czyli samowystarczalnej izolacji, tylko odporność na przymus. Huawei, w swojej strategii, uczyniła z tej idei nie tyle hasło, co program inwestycyjny o niemal wojennej skali: w 2024 roku firma raportowała 862,1 mld CNY przychodów i 179,7 mld CNY wydatków na B+R. Ten współczynnik, sięgający 20,8 % przychodów, jest w biznesie sygnałem skrajnym: dla jednych świadectwem determinacji i zdolności do samoodtworzenia kompetencji; dla innych dowodem, że firma działa w logice „quasi-państwowej”, gdzie rentowność bieżąca jest wtórna wobec długiego marszu po niezależność.

Standardy 5G: walka o globalną rentę ekonomiczną

Jeśli „Safe City” było produktem z pogranicza, łączącym obietnicę porządku z pokusą panowania, to 5G jest polem granicznym w sensie znacznie głębszym. To tutaj bowiem technologia stapia się z ustrojem gospodarczym, a standard techniczny zamienia się w prawo do pobierania renty. Nie chodzi przy tym o potoczną opłatę, lecz o klasyczną rentę ekonomiczną — dochód płynący nie z rynkowej konkurencji, lecz z uprzywilejowanej pozycji, która zamyka drogę innym. W świecie telekomunikacji taką fortecą jest standard: ten, kto zdoła wpisać swoje patenty w jego architekturę, przez lata będzie czerpał zyski z opłat licencyjnych. I nawet jeśli licencje te noszą szlachetną nazwę „uczciwych i niedyskryminacyjnych” (FRAND), w praktyce stają się narzędziem przetłaczającym wartość z całej branży do wąskiej grupy właścicieli praw. Dlatego 5G nie jest po prostu „szybszym internetem”. To mechanizm, który zadecyduje o tym, kto otrzyma prawo do opodatkowania cudzej innowacyjności.

Safe City: systemy nadzoru destabilizują ustrój

Stąd trzeba przejść do „Safe City”, produktu, który w jednym pakiecie skupia wszystko, co w sporze o Huawei jest najostrzejsze: technikę, władzę, prawo, moralność, reputację i geopolitykę. „Safe City” — w korporacyjnym żargonie: zintegrowany system zarządzania bezpieczeństwem publicznym, oparty na sensorach, kamerach i algorytmach — jest jednocześnie obietnicą racjonalizacji państwa i pokusą jego brutalnej efektywności. Sam koncern w raporcie rocznym podawał, że jego rozwiązania służą 800 milionom ludzi w ponad 200 miastach i 80 krajach. Zewnętrzne ośrodki analityczne, jak CSIS, mapując rynek z otwartych źródeł, identyfikowały 73 umowy w 52 państwach. Rozbieżność tych liczb nie jest błędem, lecz symptomem: raport firmy mówi o „zasięgu”, analiza o „umowach”. I tu odsłania się fundamentalna aporia: im większy jest zasięg produktu, tym bardziej staje się on polityczny; im bardziej polityczny, tym mniej przejrzyste stają się informacje, bo rosną bodźce do maskowania, PR-owego kadrowania i dyplomatycznej mgły.

A jednak przez tę mgłę przebija zasadnicza konstrukcja: „Safe City” to próba przełożenia państwa na logikę systemu operacyjnego. W porządku prawnym oznacza to przesunięcie akcentu z procedury i odpowiedzialności na predykcję i zarządzanie ryzykiem. W porządku społecznym pogłębia asymetrię wiedzy między administracją a obywatelem. W porządku ekonomicznym tworzy nowy rynek, na którym sprzedaje się nie tylko sprzęt, ale cały model zarządzania państwem. W tym miejscu metafora „wszechwidzącego oka i mózgu” trafia w sedno. Oko, czyli kamera, nie jest problemem samo w sobie; problemem jest mózg, który działa szybciej niż instytucje kontroli. Władza wykonawcza dostaje narzędzie, którego rozliczalność jest zawsze spóźniona.

Współczesna debata o „Safe City” jest radykalnie spolaryzowana — i tę polaryzację warto pielęgnować jako formę intelektualnej uczciwości. Stanowisko apologetyczne głosi: państwo jest niewydolne, a przestępczość i kryzysy wymagają natychmiastowej reakcji, więc integracja danych i automatyzacja decyzji to cywilizacyjna konieczność. W tym ujęciu „bezpieczne miasto” jest narzędziem modernizacji, a opór wobec niego to sentymentalizm analogowej epoki. Stanowisko krytyczne odpowiada: to eksportowalna infrastruktura autorytaryzmu, która umożliwia masową inwigilację i selektywną represję. W tym ujęciu „bezpieczne miasto” jest miękką wersją obozu, bo zamienia wolność w dane, a dane w profil ryzyka. Pomiedzy tymi skrajnościami rozciąga się strefa hipokryzji, gdzie biznesowi aktorzy mówią o „etyce AI”, po czym sprzedają cokolwiek, byle kontrakt się zgadzał. Etyka technologii w globalnym biznesie bywa często dekoracją konferencyjną, działającą jak zasłona dymna dla decyzji sprzedażowych.

Kontrowersje wokół Huawei stają się najostrzejsze, gdy „Safe City” spotyka się z biometrią i profilowaniem etnicznym. W obiegu publicznym pojawiły się doniesienia o testowaniu rozwiązań do rozpoznawania twarzy, które mogły identyfikować Ujgurów i wysyłać automatyczne alerty, co „Washington Post” opisywał jako „Uighur alarms”. Nie jest moją rolą ferować wyroków o intencjach całej korporacji na podstawie jednego wątku. Jest nią natomiast stwierdzenie faktu: nawet jeśli firma nie „chce” represji, to sprzedając aparat predykcji i identyfikacji, sprzedaje możliwość represji. A możliwość w świecie polityki jest już niem

Struktury partyjne: ukryty mechanizm zarządzania

Aby zrozumieć Huawei, trzeba poruszyć wątek Komunistycznej Partii Chin, bez którego cała dyskusja staje się nieczytelna. Należy przy tym trzymać się faktów z obiegu źródłowego, unikając konfabulacji. W dyskursie zachodnim stałym argumentem jest istnienie struktur partyjnych w firmie oraz ich wpływ na procesy kadrowe i normatywne. Pojawia się twierdzenie, iż w 2007 roku komitet partyjny uzyskał prawo weta w sprawie nominacji na kluczowe stanowiska. Z perspektywy analizy formalnej nie jest istotne, czy weta użyto raz, czy sto razy. Kluczowe jest to, że jego istnienie wprowadza do organizacji drugi, równoległy kanał uzasadniania decyzji: obok racjonalności instrumentalnej, mierzonej wynikiem i efektywnością, pojawia się racjonalność normatywno-polityczna, oparta na lojalności i zgodności z interesem państwa. To właśnie jest „oficer polityczny na okręcie”: nie steruje bezpośrednio, ale ma prawo zakwestionować awans, modelując w ten sposób zachowania całej kadry. Każdy ambitny menedżer uczy się bowiem, że kompetencja nie jest jedyną walutą kariery.

Czy taki system jest z definicji patologiczny? Uczciwa odpowiedź brzmi: to zależy od przyjętego ideału ustroju korporacyjnego. Dla liberalnej teorii przedsiębiorstwa, gdzie prymat mają własność, kontrakt i odpowiedzialność wobec właścicieli, jest to jawna deformacja. Rozmywa ona bowiem klasyczną relację właściciel–zarząd–rynek, wprowadzając aktora, który nie podlega tradycyjnym mechanizmom rozliczalności. Z kolei dla chińskiego modelu rozwoju, który traktuje sektor prywatny jako narzędzie w projekcie modernizacyjnym, jest to pożądanym mechanizm sprzężenia zwrotnego. Państwo minimalizuje w ten sposób ryzyko, że strategiczne firmy „odłączą się” od narodowej strategii. To napięcie nie ma prostego rozwiązania, ponieważ dotyczy dwóch sprzecznych metafizyk politycznych: jednej, w której państwo jest strażnikiem reguł, i drugiej, w której jest inżynierem celów.

Model Huawei: rozdział własności od realnej kontroli

Struktura własnościowa Huawei to majstersztyk strategicznej dwuznaczności, który w publicznym dyskursie działa niczym precyzyjnie skalibrowane, dwoiste urządzenie. Z jednej strony generuje kojącą opowieść o „własności pracowniczej”, z drugiej zaś rodzi uporczywe podejrzenie, że jest jedynie wyrafinowanym obejściem zasad przejrzystości. W literaturze analitycznej często przywołuje się obraz, w którym holding kontrolujący spółkę operacyjną jest w zaledwie 1% własnością założyciela, Rena, a w 99% należy do enigmatycznego bytu prawnego określanego jako „komitet związkowy”. Równolegle istnieją jednak opracowania dowodzące, że mimo tej formalnej rejestracji realna kontrola pozostaje w rękach pracowników dzięki wewnętrznym mechanizmom reprezentacji. To fundamentalne rozdarcie definiuje sposób postrzegania firmy: jedna strona widzi w tym modelu quasi-partyjny system delegatów, druga zaś – unikalny wariant kapitalizmu udziałowego, gdzie dywidenda staje się narzędziem dyscypliny i lojalności.

Jako ekonomista i prawnik muszę jednak wykonać ruch bezlitosny wobec obu tych narracji. Ci, którzy za wszelką cenę chcą udowodnić, że „to na pewno własność państwa”, nagminnie uciekają się do argumentu z niewiedzy: skoro nie znamy procedur, to z pewnością są one złowrogie. To rozumowanie jest logicznie kalekie. Z kolei ci, którzy z entuzjazmem ogłaszają, że „to na pewno własność pracownicza”, mylą udział w zysku z władzą korporacyjną. Można przecież otrzymywać sositą dywidendę, nie mając żadnego realnego wpływu na strategiczny kierunek firmy. W istocie spór nie dotyczy bowiem procentów, lecz fundamentalnego, choć często ignorowanego rozróżnienia między własnością ekonomiczną, czyli prawem do strumienia dochodów, a kontrolą korporacyjną, czyli prawem do obsadzania organów i wytyczania strategii. Dopiero ta perspektywa pozwala czytać Huawei bez naiwności – jako organizację, która opanowała sztukę oddzielania symboli własności od realnych mechanizmów sterowania, by jednocześnie mobilizować załogę, uspokajać regulatorów i zachować żelazną spójność decyzyjną.

Pozwólmy sobie na przypowieść, bez której cała ta struktura może umknąć. Wyobraźmy sobie klasztor, który deklaruje się jako wspólnota formalnie równych braci. Każdy ma udział w chlebie, każdy ma prawo do porannej zupy i każdy składa śluby posłuszeństwa. Kto zatem rządzi? Z pewnością nie „własność”, która jest tu jedynie rytuałem. Rządzi nienaruszalna reguła, a regułą zarządza kapitułarż, w którym zasiadają najbardziej doświadczeni. Wszyscy są więc „współwłaścicielami” zupy, ale nie wszyscy są współautorami reguły. Huawei w wielu aspektach przypomina taki właśnie klasztor nowoczesności: dywidenda jest chlebem, kultura korporacyjna jest regułą, a organ przedstawicielski pełni funkcję kapitułarza. Obraz ten jest trafny, ponieważ demaskuje, że pytanie „kto posiada?” bywa intelektualnym mydleniem oczu, jeśli nie towarzyszy mu znacznie ważniejsze pytanie: „kto kontroluje procedurę?”.

Meng Wanzhou: zakładniczka globalnej wojny technologii

Dopiero na tej podstawie można zrozumieć wątek Meng Wanzhou, której historia nie jest medialną sensacją, lecz dramatem o splocie prawa i symboliki w wojnie technologicznej. Zatrzymana w Vancouver 1 grudnia 2018 roku na wniosek USA, usłyszała zarzuty wprowadzenia w błąd banku HSBC w sprawie relacji Huawei z podmiotem działającym w objętym sankcjami Iranie. W języku polityki nazwano to „dyplomacją zakładników”; dla prawników był to spór o jurysdykcję i oszustwo bankowe; dla świata korporacji stało się to jednak brutalną demonstracją faktu, że działy finansów i compliance są dziś linią frontu równie realną, co laboratoria badawcze. Porozumienie z 2021 roku, które pozwoliło jej wrócić do Chin, zamknęło tylko jeden rozdział.

Aktualizacja tej historii jest bowiem niezwykle wymowna: Sabrina Meng obejmie funkcję rotacyjnej przewodniczącej od 1 października 2025 do 31 marca 2026 roku. To fakt o znaczeniu dalece wykraczającym poza personalia. Huawei zdołał przekuć epizod kryzysowy w element narracji o odporności i ciągłości, a jednocześnie wysłał sygnał, że „korona” w rodzinie i firmie nie jest tematem tabu, lecz instrumentem władzy oswojonym i zrytualizowanym przez procedurę rotacji.

Moment Sputnika: szok dla zachodniej infrastruktury

Pojęcie „momentu Sputnika” wymaga analitycznego doprecyzowania. Nie chodzi tu bowiem o sam szok prestiżowy, lecz o wstrząs instytucjonalny: nagłe uświadomienie sobie, że rynek standardów jest rynkiem władzy. A władza ta jest tym potężniejsza, im bardziej sam standard staje się dla użytkownika niewidzialny. Najbardziej fascynujący w historii 5G jest fakt, że spór o dominację nie toczył się w kampaniach reklamowych, lecz w salach posiedzeń grup standaryzacyjnych. Tam o wyniku decydowała cierpliwość, umiejętność budowania koalicji i zdolność do aranżowania kompromisów, które tylko z pozoru są kompromisami, a w praktyce kodują przyszłą asymetrię sił. Dokumenty opisujące wybór schematów kodowania w 5G New Radio pokazują, że w pracach 3GPP między wiosną a listopadem 2016 roku wyłoniono kody LDPC dla kanałów danych i kody polarne dla kanałów kontrolnych. Ten pozornie techniczny fakt ma ogromną wagę polityczną, dowodzi bowiem, że dyktowanie warunków nie wymaga wygrania wszystkiego. Wystarczy zdobyć przyczółek w architekturze, który gwarantuje trwałe prawa własności intelektualnej i realny wpływ na cały ekosystem.

W tym świetle „hydraulicy danych” okazują się kimś znacznie więcej niż tylko technikami. Stają się notariuszami standardu, a ich praca przypomina wpis do księgi wieczystej przyszłej infrastruktury.

Skoro tak, to staje się zrozumiałe, dlaczego w kręgach biznesu i regulatorów narasta przekonanie, że spór o 5G jest w istocie sporem o „cyfrowy układ nerwowy” państwa. A więc o coś, co w klasycznej teorii polityki podpada pod atrybut suwerenności. Z tego właśnie przekonania rodzi się praktyka wykluczeń i tworzenia „stref zaufania”. W warunkach fundamentalnej niepewności państwa wolą bowiem popełnić błąd typu „fałszywy alarm” niż błąd typu „śmiertelne przeoczenie”. W języku teorii decyzji powiedzielibyśmy, że próg decyzyjny przesunął się w stronę nadwrażliwości na ryzyko. W języku polityki – że logika bezpieczeństwa zdominowała logikę efektywności.

Trzy metafizyki współczesnego kapitalizmu technicznego

Dochodzimy do trzech wielkich metafizyk kapitalizmu technicznego, które — jak sądzę — faktycznie porządkują współczesną debatę, choć rzadko kto ośmiela się nazwać je po imieniu.

Pierwsza to metafizyka rynku. Głosi ona, że innowacja jest funkcją konkurencji, a ta z kolei zależy od swobody wejścia na rynek; kto wygrywa, ten po prostu na to zasłużył. Jej aporia, jej wewnętrzna sprzeczność, ujawnia się w zetknięciu z infrastrukturą krytyczną, której nie da się w pełni urynkować. Generuje ona bowiem zależności o koszcie politycznym, a nie tylko finansowym. Rynek nie posiada narzędzi, by sprawiedliwie i jawnie rozliczać ryzyko geopolityczne; potrafi je jedynie ukryć w cenie albo przerzucić na barki państwa. Wówczas „rynek” przestaje być instytucją rozstrzygania, a staje się jedynie retoryczną zasłoną.

Druga to metafizyka państwa. Jej credo brzmi: bezpieczeństwo jest warunkiem wszelkiej wolności, toteż państwo ma prawo ograniczać technologię, jeśli zagraża ona jego suwerenności. Jej paradoks polega na tym, że państwo, które raz uzna technikę za broń, zaczyna traktować cały handel jak potencjalną wojnę. W długim okresie niszczy to fundamenty dobrobytu, których miało strzec. Państwo, które namiętnie mnoży wyjątki, w końcu samo staje się gospodarką wyjątków. A to prosta droga do trwałej fragmentacji świata.

Trzecia to metafizyka infrastruktury. Mówi ona, że to, co ukryte w „stosie” technicznym, rządzi światem skuteczniej niż ustawy i manifesty. Kto kontroluje standardy, aktualizacje i punkty węzłowe, ten w rzeczywistości kontroluje warunki działania wszystkich innych. Jej słabość polega na tym, że raz zbudowana infrastruktura dąży do autonomii i kolonizacji życia społecznego, ponieważ wygoda i efektywność stają się argumentami absolutnymi. Wtedy „bezpieczeństwo” i „sprawność” służą za usprawiedliwienie dla nadzoru, a „zarządzanie ryzykiem” staje się pretekstem dla państwa predykcyjnego. Spór o monitoring i biometrię w Belgradzie, opisywany w Europie jako

techniczna debata o proporcjonalności masowego nadzoru, jest właśnie lokalnym objawem tej globalnej metafizyki.

Zarządzana bifurkacja: budowa odporności technologicznej

Jeżeli cała dotychczasowa analiza miała sens, to nie dlatego, że pozwala „rozsądzić” spór o Huawei — ten jest bowiem strukturalnie nierozstrzygalny. Jej wartość polega na tym, że zmusza do przejścia od pytań moralnych do pytań projektowych. W świecie, w którym infrastruktura techniczna stała się nośnikiem władzy, a globalizacja utraciła niewinność, nie da się już rządzić ani inwestować na podstawie samych deklaracji. Potrzebne są instytucje zdolne działać w warunkach trwałej nieufności, bez popadania w paraliż czy paranoję. Huawei nie jest tu „problemem”, lecz przypadkiem granicznym, na którym widać, co się dzieje, gdy trzy metafizyki — rynku, państwa i infrastruktury — nachodzą na siebie bez wspólnego języka.

Dlatego finał musi przyjąć formę programu, a nie werdyktu. Programu dla trzech aktorów: państw „spętanych”, organizacji społecznych oraz globalnego biznesu. Każdy z nich stoi dziś przed tą samą aporią, czyli sytuacją pozornie bez wyjścia: musi korzystać z technologii, której nie może w pełni zaufać, a jednocześnie nie może sobie pozwolić na jej odrzucenie.

Państwa spętane — a więc takie, które nie są ani globalnym hegemonem, ani bezwolną peryferią — muszą porzucić złudzenie, że bezpieczeństwo da się „zadekretować” jednym zakazem albo jednym certyfikatem. Zakaz jest instrumentem grubego kalibru; certyfikat bywa instrumentem czysto teatralnym. Racjonalna polityka infrastrukturalna w warunkach rywalizacji bloków wymaga projektowania odwracalności. Odwracalność oznacza zdolność do zmiany dostawcy, architektury lub konfiguracji bez wywołania systemowej katastrofy. To nie jest kwestia geopolitycznych sympatii, lecz twardej inżynierii ryzyka. Państwo, które wybiera rozwiązanie „najtańsze i najszybsze”, a nie projektuje wyjścia awaryjnego, działa jak właściciel elektrowni bez planu ewakuacji: oszczędza na schodach, bo pożar zdarza się rzadko. Huawei jest tu memento: problemem nie jest „czy wolno”, lecz „czy potrafimy się wycofać”.

Drugim elementem programu dla państw jest rozróżnienie segmentów. Nie wszystkie technologie są sobie równe. Infrastruktura rdzeniowa, systemy zarządzania czy warstwy aktualizacji są ustrojowo czymś innym niż sprzęt peryferyjny. Próba jednorodnego traktowania wszystkiego prowadzi albo do nadmiernego wykluczenia i gigantycznych kosztów, albo do nadmiernej ufności i śmiertelnego ryzyka. Rozróżnienie segmentów jest politycznie trudne, bo nie mieści się w logice

chwyтлиwego hasła, ale pozostaje jedyną drogą, by uniknąć zarówno technologicznego wasalstwa, jak i samobójczej autarkii.

Organizacje społeczne stoją przed zadaniem niewdzięcznym, lecz kluczowym: muszą nauczyć się kontrolować nie intencje, lecz procedury. W debacie o systemach „Safe City” spór zbyt często toczy się na poziomie moralnej diagnozy: czy dana firma jest „dobra”, czy „zła”. Tymczasem ustrojowa racjonalność wymaga innego pytania: czy dana technologia ma uprzednią podstawę prawną, jawnie określony cel, proporcjonalność, ograniczenie czasowe, niezależny nadzór oraz realną możliwość zaskarżenia. Bez tych elementów każda technologia nadzoru — niezależnie od dostawcy — staje się narzędziem arbitralnej władzy. Huawei nie jest tu wyjątkiem; jest katalizatorem. Spory o konkretne wdrożenia wywołują w Europie tak silne reakcje nie dlatego, że ktoś nagle odkrył zagrożenia biometrii, lecz dlatego, że technika wyprzedziła prawo, a prawo próbuje teraz dogonić fakt dokonany.

Organizacje społeczne muszą także zrezygnować z łatwego moralizmu. Potępienie technologii bez zrozumienia jej funkcji i architektury prowadzi do utraty wiarygodności. Skuteczna krytyka musi być techniczna i prawna zarazem: musi wiedzieć, gdzie dokładnie leży punkt koncentracji władzy — w algorytmie, w interfejsie, w retencji danych, w integracji systemów — i tam właśnie lokować presję. W przeciwnym razie sprzeciw staje się rytuałem bez sprawczości.

Globalny biznes stoi natomiast wobec najboleśniejszej zmiany: musi przestać traktować zgodność regulacyjną jako koszt administracyjny, a zacząć postrzegać ją jako kompetencję strategiczną. Wojna technologiczna pokazała, że prawo eksportowe, sankcje, jurysdykcje i interpretacje bankowe są dziś równie istotne jak jakość produktu. Przypadek Meng Wanzhou nie był „wypadkiem przy pracy”; był sygnałem, że interpretacja relacji korporacyjnych i ryzyk sankcyjnych stała się polem egzekwowania władzy. Firma, która tego nie rozumie, będzie zawsze reagować spóźniona — i będzie zdziwiona, że prawo działa szybciej niż rynek.

Dla biznesu oznacza to konieczność myślenia wariantowego: produkt musi mieć wersje jurysdykcyjne, łańcuch dostaw musi mieć alternatywy, a architektura danych musi uwzględniać fragmentację. To jest koszt, który obniża krótkoterminową efektywność, ale zwiększa długoterminową zdolność przetrwania. Huawei, przez lata inwestując w „zapasowe koła”, pokazało, że taka strategia jest możliwa, choć okupiona wysoką ceną. Paradoks polega na tym, że firmy zachodnie krytykują ten model jako „quasi-państwowy”, po czym same zaczynają go naśladować pod presją sankcji i ryzyk geopolitycznych.

Wróćmy więc do pytania zasadniczego: czy Huawei jest modelem nowoczesności, czy narzędziem autorytaryzmu? Odpowiedź, która nie ucieka w slogan, brzmi: Huawei jest modelem

nowoczesności w warunkach rywalizacji ustrojowej. To firma, która potrafiła połączyć mobilizację kulturową, inwestycje w standardy, dyscyplinę organizacyjną i wsparcie państwowe w sposób technologicznie skuteczny. Ale właśnie ta skuteczność sprawia, że staje się ona nie do przyjęcia jako neutralny aktor w świecie, który znów myśli kategoriami bloków. Huawei nie eksportuje autorytaryzmu wprost; eksportuje sprawność, która w rękach autorytarnej władzy działa jak akcelerator, a w rękach demokracji kusi pójściem na skróty.

Dochodzimy tu do najważniejszej intelektualnej prowokacji. Autorytaryzm przyszłości nie musi mieć ideologii. Może mieć panel sterowania. Może mieć predykcję. Może mieć „optymalizację”. I właśnie dlatego spór o Huawei jest sporem o granice nowoczesności: o to, czy jesteśmy w stanie zaprojektować technikę, która zwiększa sprawność bez niszczenia wolności proceduralnej. Jeśli nie — jeśli sprawność zawsze wygrywa — to autorytaryzm nie będzie już „chiński” ani „rosyjski”. Będzie po prostu najbardziej wydajną wersją zarządzania.

Z tej perspektywy retoryka Rena Zhengfei okazuje się nie tyle propagandą, ile symptomem epoki. „Cyfrowe uzbrojenie narodu”, „hydraulicy danych”, „zapasowe koła” — to obrazy świata, w którym technika, praca i państwo zlewają się w jedną narrację sensu. Ta narracja jest potężna, bo daje odpowiedź na lęk: przed zależnością, opóźnieniem, marginalizacją. Zachód przez długi czas odpowiadał na te lęki obietnicą rynku i prawa. Dziś widać, że ta odpowiedź jest niewystarczająca, jeśli nie towarzyszy jej projekt instytucjonalny zdolny poradzić sobie z techniką jako władzą.

Jeżeli więc historia Huawei ma być lekcją, to nie taką, że „Chiny są zagrożeniem” albo „Zachód jest hipokrytą” — choć oba zdania zawierają ziarno prawdy. Lekcja jest taka, że nowoczesność technologiczna bez nowoczesnych instytucji kontroli staje się ustrojowo niebezpieczna, niezależnie od flagi. Huawei jest tu soczewką: skupia w jednym punkcie nadzieje modernizacji i lęki suwerenności. Kto chce tylko potępić, niczego się nie nauczy. Kto chce tylko naśladować, powtórzy cudze błędy.

Pozostaje zadanie trudniejsze i mniej efektowne: projektować świat, w którym ani „hydraulik danych”, ani „cyfrowe uzbrojenie” nie są ostatnim słowem. Ostatnim słowem musi być procedura, która potrafi powiedzieć „sprawdzam” — także wtedy, gdy technika działa perfekcyjnie, a rynek bije brawo. Jeśli to się nie uda, przyszła generacja sieci nie będzie już polem wolności ani nawet polem konfliktu. Będzie polem zarządzania, w którym polityka wróci w postaci algorytmu. I wtedy pytanie o Huawei okaże się pytaniem spóźnionym.

Przyszłość nie zależy od tego, kto posiada technologię, lecz kto kontroluje procedury jej użycia. Jeśli zapomnimy o tym, algorytmy przejmą rolę polityki, a pytanie o Huawei

okaże się pytaniem bez odpowiedzi. Czy zatem potrafimy stworzyć system, w którym technologia służy wolności, a nie staje się jej cyfrowym więzieniem?

Inspiracje

[1] "House of Huawei" Eva Dou

2025 | Portfolio / Penguin Publishing Group

Eva Dou jest wielokrotnie nagradzaną dziennikarką piszącą o polityce technologicznej dla „The Washington Post”. Koncentruje się na styku technologii i geopolityki. Jest autorką książki „House of Huawei: The Secret History of China's Most Powerful Company”.

Eva Dou is an award-winning journalist covering technology policy for The Washington Post. She focuses on the intersection of technology and geopolitics. She is the author of 'House of Huawei: The Secret History of China's Most Powerful Company'.

The Washington Post

Literatura uzupełniająca

Książki

Literatura pokrewna (Google Scholar):



[1] "Critical Infrastructure Protection, Risk Management, and Resilience: A Policy Perspective"

2016 | CRC Press | ISBN: 9781315310633



[2] "Homeland Security and Critical Infrastructure Protection"

2018 | Bloomsbury Publishing USA | ISBN: 9798216098744



[3] "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation"

Ted G Lewis

2019 | John Wiley & Sons | ISBN: 9781119614562

Artykuły naukowe

Autorzy przywoływani:

[1] "AI-based threat detection in critical infrastructure: A case study on smart grids"

Muneer et al.

2025 | World Journal of Advanced Research and Reviews

[Google Scholar](#)



Tekst opracowany z udziałem sztucznej inteligencji.

Redakcja i kontrola merytoryczna: Fundacja Dobre Państwo.

APA ONE Publishing System

Fundacja Dobre Państwo © 2026

Article ID: 6fdaad9a-f47a-4d4e-8277-83933c31ec95