# Suwerenność proceduralna i przyszłość tożsamości cyfrowej

**AUTOR**

Fundacja Dobre Państwo

**STRESZCZENIE / ABSTRACT**

Tekst podejmuje temat transformacji suwerenności państwowej, która w dobie cyfrowej ewoluuje z formy terytorialnej w proceduralną. Na przykładzie paraliżu infrastruktury fizycznej podczas katastrof, autor wykazuje, że to cyfrowe sieci komunikacyjne stają się nowym kręgosłupem koordynacji społecznej i politycznej. Analiza obejmuje reorganizację władzy epistemicznej, gdzie kluczowe stają się mechanizmy weryfikacji tożsamości, cyfrowe znaki wodne oraz audyt infrastrukturalny. Artykuł rzuca światło na wyzwania związane z bałkanizacją sieci i atakami hybrydowymi, postulując nową epistemologię bezpieczeństwa opartą na technicznej weryfikowalności genealogii danych i cyfrowym upodmiotowieniu jednostki.

This article explores the transformation of state sovereignty, which in the digital age is evolving from a territorial form to a procedural one. Using the example of the paralysis of physical infrastructure during disasters, the author demonstrates that digital communication networks are becoming the new backbone of social and political coordination. The analysis encompasses the reorganization of epistemic power, where identity verification mechanisms, digital watermarks, and infrastructural auditing become crucial. The article sheds light on the challenges posed by network balkanization and hybrid attacks, postulating a new security epistemology based on the technical verifiability of data genealogy and the digital empowerment of individuals.

Artykuł analizuje transformację władzy epistemicznej w epoce cyfrowej, gdzie tradycyjne hierarchie ustępują miejsca rozproszonym sieciom komunikacji i weryfikacji. Autor argumentuje, że zaufanie, zarówno do państwa, jak i do sieci, jest warunkowane istnieniem audytowalnego śladu, umożliwiającego procedurę uzasadniania. Przykładem tego jest eksperyment na Haiti po trzęsieniu ziemi, gdzie spontaniczna agregacja informacji

telefonicznych przekształciła się w operacyjną inteligencję. Autor podkreśla, że cyfryzacja obniża barierę wejścia do sfery publicznej, ale jednocześnie stawia nowe wyzwania związane z weryfikacją informacji, ochroną prywatności i utrzymaniem suwerenności w przestrzeni cyfrowej. Kluczowym elementem jest proceduralna jedność uzasadniania, wymagająca precyzyjnych standardów weryfikacji i algorytmicznej przejrzystości. Artykuł proponuje koncepcję cyfrowej suwerenności opartej na zdolności do szyfrowania, weryfikacji, rekonfiguracji, rozliczania i tworzenia wirtualnych instytucji.

**SŁOWA KLUCZOWE**

suwerenność proceduralna | tożsamość cyfrowa | władza epistemiczna | mapowanie kryzysowe | cyfrowe znaki wodne | audyt infrastrukturalny | bałkanizacja sieci | system M-Paisa | hybrydowe ataki | permanentna pamięć cyfrowa | reorganizacja zaufania | epistemologia bezpieczeństwa | ius in bello | cyfrowe upodmiotowienie | weryfikowalność genealogii

## Haiti: sieci komunikacyjne fundamentem ratownictwa

Rozważmy anegdotę, której dydaktyczny sens odsłania się dopiero po uchwyceniu napięcia między światem przeżywanym a sferą technicznej organizacji. Gdy w pewnym mieście trzęsienie ziemi zniszczyło zasilanie, wodę i transport, nie zamilkły jednak telefony. To, co w klasycznej teorii państwa uchodziło za rdzeń jego trwałości – ratusz, koszary, urzędy – rozpadło się na oczach mieszkańców. Ocalała jednak sieć komunikacji. Dopiero wtedy strażacy i lekarze pojęli, że nowym archiwum zbiorowej koordynacji nie są już gmachy władzy, lecz cyfrowa mapa, która scalając setki mikrorelacji, tworzyła makroskop do obserwacji cierpienia i nadziei. Ten obraz nie jest metaforą. W Port-au-Prince po 2010 roku zadziałał eksperyment społeczny, w którym telefoniczna koordynacja przeszła drogę od spontanicznej agregacji do operacyjnej inteligencji, a platforma Ushahidi z doraźnego narzędzia stała się elementem nowej epistemologii bezpieczeństwa, przenosząc ciężar uzasadniania decyzji z biurokratycznych formularzy na wiarygodne sygnały płynące z peryferii. Tę transformację potwierdzają analizy mapowania kryzysowego na Haiti, wskazujące, że napływ wiadomości i ich geolokalizacja tworzyły realny zasób wiedzy operacyjnej dla ratowników oraz instytucji międzynarodowych.

## Schmidt i Cohen: nowa racjonalność świata połączonego

Dostrzegamy tu embrionalną formę procedury zbiorowego rozumienia, u której źródeł leży fundamentalne przestawienie wektora racjonalności. Następuje zwrot od paradygmatu samotnej refleksji ku praktyce uzgadniania, bezpośrednio nastawionej na wzajemne zrozumienie. Tę zmianę syntetycznie ujęli Eric Schmidt i Jared Cohen w stwierdzeniu, które wyznacza ramę sporu o nową epokę. Internet, jak piszą, „jest jedną z niewielu rzeczy, które ludzie zbudowali, a których naprawdę nie rozumieją". Z narzędzia transmisji stał się bowiem ośrodkiem ekspresji i sprawczości, który powiększając się co sekundę, wymyka się prostej ontologii. To nie jest jedynie zgrabna obserwacja językowa, lecz teza o reorganizacji władzy epistemicznej. W nowym układzie nie wypływa ona z odgórnego centrum, lecz rodzi się z proceduralnej jedności rozproszonego uzasadniania.

## Trwałość danych: cyfrowy ślad definiuje tożsamość

Nasze przyszłe ja przestaje być wyłącznie narracją biograficzną, a staje się efektem technicznego utrwalenia śladów, które nadają naszym ekspresjom podwójny status: zarazem prywatny i publiczny. Toteż jakakolwiek debata o tożsamości i prywatności nie może już pomijać kwestii permanentnego charakteru danych. Trwałość ta znosi bowiem dawne mechanizmy zapominania, zastępując je cyfrowym archiwum, w którym weryfikowalność naszych wypowiedzi i nawyków konsumpcyjnych staje się bezwzględnym filtrem, decydującym o dostępie do ról zawodowych, wiarygodności kredytowej czy reputacji. Ten kierunek zmian trafnie diagnozują Schmidt i Cohen, wskazując, że cyfrowe upodmiotowienie dla wielu okaże się pierwszym realnym doświadczeniem sprawczości, ponieważ mieści się w kieszeni, a koszt wejścia w sferę publiczną obniża się do ceny aplikacji. „Cyfrowe upodmiotowienie będzie dla niektórych pierwszym doświadczeniem sprawczości, pozwalającym być słyszanym, liczonym i traktowanym poważnie, wszystko dzięki niedrogiemu urządzeniu w kieszeni". Taki rodzaj sprawczości włącza miliony w grę o społeczne uznanie, lecz jednocześnie wystawia je na bezwzględny rygor permanentnej pamięci.

## Metadane: nowy fundament weryfikacji dziennikarskiej

Aby jednak nie poprzestać na ogólnikach, wątek procedur weryfikacji domaga się konkretyzacji. W warunkach informacyjnego potopu jedyną drogą do odbudowy zaufania nie jest bowiem cenzura, lecz standaryzacja dowodzenia prawdy poprzez wbudowywanie metadanych w samą strukturę treści. Proponowana w literaturze koncepcja cyfrowych znaków wodnych, sprzężonych z odciskami

biometrycznymi i danymi geoprzestrzennymi, wyznacza praktyczny horyzont dla zawodu reportera. Przestawia bowiem punkt ciężkości z perswazyjnej retoryki na techniczną weryfikowalność. Uzasadnienie nie płynie już z autorytetu nadawcy, lecz z weryfikowalnej genealogii samego materiału, co stanowi w istocie fundamentalną reorganizację władzy epistemicznej. Jest to systemowa odpowiedź na marketingowe wojny narracyjne, które w epoce hiperłączności rozciągają pole konfliktu na całą przestrzeń symboliczną. W tych warunkach tradycyjne redakcje zostają sprowadzone do roli kustoszy i architektów zaufania, których zadaniem staje się filtrowanie potoku informacji w rytm globalnych zdarzeń. Tę właśnie transformację opisują autorzy „Nowej ery cyfrowej", akcentując przesunięcie z ekskluzywnego pozyskiwania wiadomości na rzecz kuratorstwa, agregacji i profesjonalnej weryfikacji.

## Egipt 2011: porażka cyfrowej blokady państwa

Dla państw rodzi to konieczność prowadzenia polityki dwutorowej, opartej na logicznym rozdziale między normami rządzącymi porządkiem terytorialnym a tymi, które operują w przestrzeni pozbawionej granic. Takie praktyki jak filtrowanie treści, głęboka inspekcja pakietów czy bałkanizacja sieci nie są zatem doraźnymi technikami obronnymi. Stanowią raczej fundamentalną próbę przywrócenia skuteczności władzy, która z natury pozostaje terytorialna, podczas gdy sfera publicznego dyskursu kształtuje się dziś w globalnej przestrzeni cyfrowych platform.

Przypadek Egiptu z 2011 roku, gdzie władza podjęła próbę całkowitego wyłączenia infrastruktury sieciowej, pozostaje tu przypowieścią o kluczowym znaczeniu. Ujawnił on bowiem nie tylko techniczną możliwość wykonania tak gwałtownego cięcia, lecz przede wszystkim jego polityczną bezsilność i olbrzymie koszty gospodarcze. Szczegółowe analizy dowodzą, że choć odcięcie trwało zaledwie kilka dni, ponowne włączenie sieci nie przywróciło dawnego paradygmatu kontroli. Wręcz przeciwnie, obnażyło przepaść między logiką infrastrukturalnej przemocy a dynamiką tłumu, który zdążył już opanować sztukę koordynacji z pominięciem oficjalnych węzłów komunikacyjnych.

W tej samej mierze, w jakiej reżim w Kairze sięgnął po ostateczny wyłącznik, reszta świata zrozumiała fundamentalną prawdę: centralizacja węzłów kontrolnych oznacza zarazem centralizację odpowiedzialności i ryzyka wizerunkowego. Toteż zrekonstruowany przebieg zdarzeń, zarówno techniczny, jak i czasowy, jedynie potwierdza tezę o nieuchronnej dwupoziomowości, która zdefiniuje politykę państw w nowej epoce.

## Suwerenność proceduralna wypiera granice terytorialne

Suwerenność państwa przestaje być prostym korelatem terytorium, tracąc przy tym monopol na przemoc informacyjną. Państwo, które nie opanuje sztuki tego, co można nazwać suwerennością proceduralną, będzie

skazane na bierny import kryteriów z zewnątrz. W praktyce oznacza to konieczność budowania warstw bezpieczeństwa dla infrastruktury komunikacyjnej, której fundamentalną regułą jest rozdział między kontrolą a audytem. Kontrola pozbawiona audytu nieuchronnie degeneruje się w opresję, podczas gdy audyt pozbawiony realnej kontroli staje się synonimem paraliżu.

Nowoczesna suwerenność cyfrowa opiera się zatem na współistnieniu pięciu fundamentalnych zdolności. Po pierwsze, na zdolności do szyfrowania, które chroni obywatela, nie stając się jednocześnie tarczą dla bezkarności przestępczej. Po drugie, na zdolności do weryfikacji, wzmacniającej siłę dowodu bez naruszania sfery prywatności. Po trzecie, na zdolności do rekonfiguracji, pozwalającej omijać uszkodzone węzły sieci i podtrzymywać ciągłość życia zbiorowego. Po czwarte, na zdolności do rozliczania administracji z każdego użycia danych, aby uniknąć urzeczowienia obywatela, czyli sprowadzenia go do roli obiektu w systemie. I wreszcie, na zdolności do tworzenia wirtualnych instytucji, zdolnych przechować kluczowe rejestry czy listy płac, gdy fizyczna struktura państwa ulega destrukcji.

## Technologie mobilne: cyfrowy oręż przeciw korupcji

Na tym tle inicjatywy mobilnej dystrybucji pensji w sektorach tak wrażliwych, jak policja czy wojsko, odsłaniają swój głęboki, proceduralny sens. Roshan w Afganistanie, wdrażając system M-Paisa, zademonstrował, jak można przeciąć ścieżki korupcji poprzez zmianę architektury przepływu środków. Odłączenie wypłaty od fizycznych pośredników i wpięcie jej w sieć, która pozostawia ślad audytowy, niwelowały opresję anonimowej gotówki. Raporty Banku Światowego dokumentujące pilotaże z lat 2009 i 2011 potwierdziły ten mechanizm: pensje funkcjonariuszy zaczęły płynąć wprost do ich portfeli mobilnych. Państwo odzyskiwało w ten sposób normatywną wiarygodność bez spektakularnych czystek, wzmacniając swoje roszczenie do słuszności poprzez samą przejrzystość transakcji.

## Rewolucje cyfrowe: pułapka łatwej mobilizacji

Podchodząc do zjawiska rewolucji, należy porzucić wszelką euforię. Technologia cyfrowa istotnie obniża barierę wejścia, lecz nie oferuje żadnych skrótów na drodze do cnoty mężów stanu. Zgromadzenie tłumu w symbolicznej przestrzeni sieci nie jest jeszcze miarą sukcesu; prawdziwa sztuka zaczyna się, gdy epifania zwycięstwa musi ustąpić miejsca żmudnej pracy nad instytucjami. Ten krytyczny moment trafnie diagnozują autorzy „Nowej ery cyfrowej”, ostrzegając, że cyfrowe przyspieszenie pozbawia ruchy społeczne bezcennego doświadczenia administracyjnego, co w praktyce ubezwłasnowolnia ich liderów na poziomie pojęciowym.

W procesie dziedziczenia władzy po dawnych rewolucjach nie istnieją bowiem żadne drogi na skróty. Skrupulatne procedury stanowienia prawa, delikatna materia umów społecznych czy twarde realia budżetowe nie poddają się logice marketingu wirusowego. Stąd płynie wniosek tyleż trzeźwy, co surowy: rewolucje stają się łatwiejsze do zainicjowania, lecz zarazem nieporównywalnie trudniejsze do pomyślnego zakończenia. Brak przećwiczonych ról, deficyt odpowiedzialności fiskalnej i nieobecność kompetencji legislacyjnych sprawiają, że cała dynamika społecznego gniewu rozbija się o twardy mur instytucjonalnej inercji.

Taka typologia rewolucyjnego procesu pozwala z kolei zrozumieć, dlaczego współczesne państwa coraz częściej sięgają po strategie subtelnej infiltracji, a nie po spektakularne akty cenzury. Analiza przypadku egipskiego, wraz z dokumentacją precyzyjnych ingerencji w sieci komórkowe, dowodzi, jak dalece bardziej ergonomiczną dla władzy taktyką staje się podszywanie pod uczestników debaty i strategiczne pozycjonowanie własnych przekazów, aniżeli prosta, brutalna cisza informacyjna.

## Powszechna łączność: nowa arena walki z terroryzmem

Terroryzm nie jest tu postrzegany jako osobny, patologiczny wymiar rzeczywistości, lecz jako funkcja tej samej infrastruktury, z której wszyscy korzystamy. Gdy narzędzia komunikacji stają się symetrycznie dostępne, rośnie również potencjał tych aktorów, którzy pragną je wykorzystać wbrew przyjętym normom. Kultura majsterkowiczów, rosnące kompetencje techniczne i tani dron z marketu składają się na nową kategorię zagrożeń, która wymaga nie histerii, lecz systemowej odpowiedzi. Hybrydowe ataki, charakteryzujące się niskim progiem wejścia i wysoką widowiskowością, zyskują na atrakcyjności, lecz jednocześnie każda cyfrowa interakcja zasila olbrzymią kopalnię metadanych, która z kolei wzmacnia zdolności kontrterrorystyczne.

Nie ma w tym żadnej sprzeczności. Tożsamość cyfrowa, nawet gdy usiłuje pozostać niewidzialna, nieuchronnie pozostawia ślady, które w warunkach procesowych stają się czytelnym zapisem. W tym sensie sama weryfikacja tożsamości przekształca się w broń, gdyż poziom dowodowy wymusza przewidywalność i dotrzymywanie gróźb. Z tej racji można zasadnie przewidywać, że grupy ekstremistyczne będą zmuszone do tworzenia własnych, równoległych systemów identyfikacji i dystrybucji treści. Czyniąc to, ryzykują jednak przejęcie kluczowych węzłów swojej sieci i wykorzystanie ich do działań odwróconych. Te właśnie intuicje powracają w analizach nowej ery cyfrowej jako fundamentalny wątek: logika walki ulega przemianie, stając się przede wszystkim wojną o dowody, a nie o samą głośność przekazu.

## Automatyzacja wojny: kryzys odpowiedzialności prawnej

Zarówno konflikt, jak i interwencja podlegają dziś temu samemu prawu proceduralizacji. Gdy automatyzacja powiększa dystans między decyzją a jej śmiertelnym skutkiem, dylematy odpowiedzialności rosną w postępie geometrycznym. Bezzałogowe platformy, operujące z bezpiecznej odległości, być może redukują koszt polityczny interwencji, lecz bynajmniej nie znoszą problemu imputacji winy. Jeśli bowiem autonomiczny system popełnia błąd, spór o sprawstwo rozszczepia się niczym pryzmat, wskazując jednocześnie na projektanta, operatora, dostawcę logistycznego, a nawet na zawodną infrastrukturę łączności. Nie jest to jałowa sofistyka, lecz fundamentalny problem dla ustawodawstwa.

Problem ten nie znajdzie rozwiązania bez dwóch fundamentalnych kroków: ujednolicenia definicji winy w systemach sojuszniczych oraz uczynienia cyberbezpieczeństwa sprzętu wojskowego integralnym elementem ius in bello, czyli prawa regulującego sposób prowadzenia walki. Równolegle do tych dylematów cyberwojna stała się już permanentnym konfliktem o niskiej intensywności, w którym spektakularne operacje w rodzaju Stuxnetu są raczej wyjątkiem niż regułą. Z tego powodu nie wyznaczają one standardu eskalacji, lecz raczej rysują granicę odstraszania w warstwie infrastrukturalnej. I tu odsłania się chłodna logika ryzyka: w tej samej mierze, w jakiej totalne uderzenie cyfrowe stworzyłoby precedens dla symetrycznej odpowiedzi, racjonalny aktor będzie wolał pozostać w szarej strefie szpiegostwa i sabotażu o trudnej do udowodnienia atrybucji. Ta właśnie kalkulacja stanowi integralną część scenariuszy analizowanych przez Schmidta i Cohena.

## Communications-first: priorytet łączności po katastrofie

Odbudowa po katastrofie staje się ostatecznym sprawdzianem dla całej tej koncepcji. Jeśli zasada „łączność przede wszystkim” ma porzucić status chwytliwego hasła na rzecz normy operacyjnej, jej obrona musi oprzeć się nie na retoryce, lecz na chłodnym wyliczeniu konsekwencji. Ośrodki ratownicze działają sprawniej, gdy sieć telekomunikacyjna funkcjonuje. Aparat państwa zachowuje ciągłość, wypłacając wynagrodzenia za pośrednictwem portfeli mobilnych, gdy tradycyjna bankowość leży w gruzach. Diaspora zyskuje realny wpływ, ponieważ wirtualne instytucje przenoszą dane państwowe do chmury, tworząc rządowe interfejsy zdolne do działania w stanie geograficznego rozproszenia. Doświadczenia z Haiti i Afganistanu dowodzą, że w momentach krytycznych to właśnie łączność tworzy przestrzeń, w której decyzje władzy mogą zostać uznane przez obywateli za słuszne. Co więcej, sektor telekomunikacyjny wnosi do tego układu własną motywację inwestycyjną. Potrafi on bowiem zinternalizować, czyli wchłonąć, część kosztów chaosu, gdyż jego infrastruktura generuje przychód nawet w warunkach podwyższonego ryzyka. Na tym

polega deflacyjna elegancja tego pomysłu. Odpowiedzialność za słuszność decyzji przestaje opierać się wyłącznie na moralnych deklaracjach, a zaczyna wynikać z twardego rachunku przepływów: informacji, pieniędzy i władzy.

## Kultura danych: regionalne modele ochrony prywatności

Aby nadać tej analizie rygor porównawczy, musimy rozróżnić kulturowe matryce, w których cyfrowa rewolucja zapuszcza korzenie. Azja Wschodnia, ukształtowana przez doświadczenie państwa inżynieryjnego i konfucjańską aksjologię harmonii, postrzega sferę cyfrową jako naturalne rozszerzenie porządku, nie zaś jego antytezę. Akceptacja dla filtrowania treści czy zarządzania reputacją nie jest tam kapitulacją przed autorytaryzmem, lecz konsekwencją przekonania, że w porządku racji ład wspólnoty ma pierwszeństwo przed wolnością ekspresji jednostki. Afryka, zmagająca się z deficytem infrastruktury i słabością instytucji, odnajduje w telefonii mobilnej swoistą protezę państwa, która generuje codzienną racjonalność wymiany handlowej, transferów finansowych i systemów wczesnego ostrzegania.

Z kolei Ameryka, zbudowana na micie wolnej ekspansji i prymacie prywatnej innowacji, instynktownie powierza procedury weryfikacji i audytu mechanizmom rynkowym oraz ich agencjom reputacyjnym, w efekcie czego dziennikarstwo przesuwa się w stronę platform i weryfikacyjnych start-upów. Europa natomiast, wierna swojemu normatywnemu projektowi opartemu na prawach podstawowych, negocjuje cyfrową tożsamość pod sztandarem ochrony danych, a z prawa do bycia zapomnianym czyni narzędzie łagodzenia cyfrowego absolutyzmu pamięci. Tym samym to, co w Azji jawi się jako porządek, w Ameryce jest przedsiębiorczością, w Afryce praktycznością, a w Europie – proceduralnym legalizmem. Taki czteropolowy model nie unieważnia jednak pojęcia prawdy; pozwala raczej na kalibrację instrumentów władzy i uznania, dostosowując je do odmiennych zasobów świata przeżywanego.

## Ekonomia wstydu: koszt absolutnej pamięci sieci

Nadszedł zatem moment, by oddać głos myślicielom, których diagnoza stanowi oś tej rekonstrukcji. Eric Schmidt i Jared Cohen postrzegają naszą przyszłość jako efekt nałożenia się na siebie dwóch cywilizacji: tej fizycznej, liczącej tysiąclecia, oraz tej wirtualnej, która dopiero nabiera kształtów. Przesunięcie koncentracji władzy ku jednostkom jest już faktem, niemniej stawia nas ono przed fundamentalnym dylematem. Czy wzmocniona sprawczość, sprzężona z absolutną, nieusuwalną pamięcią cyfrową, nie tworzy aby nowej, bezlitosnej ekonomii wstydu i wykluczenia? Odpowiedź, jakiej udzielają, nie jest prostym odrzuceniem technologii; jest postulatem rygoru.

Jedynym kryterium legitymizacji staje się tu bowiem proceduralna jedność uzasadniania. Postulat ten domaga się precyzyjnych standardów weryfikacji, algorytmicznej przejrzystości, interoperacyjnych rejestrów metadanych oraz pełnej możliwości audytu całych łańcuchów publikacji. Nieprzypadkowo to właśnie oni sugerują szereg konkretnych rozwiązań instytucjonalnych, mających na celu weryfikację cyfrową i przeciwdziałanie dezinformacji. Wśród nich znajduje się koncepcja monitorów weryfikacji, pełniących funkcję analogiczną do neutralnych inspektorów, którzy dostarczaliby mediom certyfikowane materiały ze stref konfliktu. Ich tezy nie noszą znamion ideologicznego dekretu. Przeciwnie, wyrastają z chłodnej diagnozy istniejących struktur i rządzących nimi sprzężeń zwrotnych.

## Wirtualne instytucje gwarantują ciągłość państwa

Skoro państwo przestaje być wyłącznie suwerenem terytorialnym, a staje się również operatorem sfery cyfrowej, to w sposób nieunikniony wzrasta ranga bytów takich jak rządy na uchodźstwie, wirtualne instytucje czy chmurowe archiwa. Ich zadaniem jest podtrzymanie ciągłości państwa – od świadczeń po listy płac – gdy fizyczna administracja ulega załamaniu. Ta koncepcja, wysoce prawdopodobna w naszej cyfrowej epoce, stanowi w istocie przeniesienie zasobów ze świata przeżywanego wprost do domeny, gdzie fundamentalne reguły prawomocności można weryfikować i restytuować na żądanie. Dopiero w tym świetle inicjatywy takie jak mobilna dystrybucja pensji dla sektorów kluczowych – policji czy wojska – odsłaniają swój prawdziwy, strategiczny wymiar.

## Audytowalny ślad: technologiczny fundament zaufania

Opuśćmy na chwilę poziom moralnych intuicji, by ująć problem w rygorze formalnej łamigłówki, przenosząc ciężar argumentu na twardy grunt rachunku zdań. Niech P symbolizuje tezę, że państwo jest źródłem zaufania, Q – że jest nim sieć, a R – że istnieje weryfikowalny, audytowalny ślad działania. Przyjmijmy zatem następujące przesłanki: zarówno P, jak i Q implikują R, a negacja R pociąga za sobą negację P oraz Q. Który z tych układów pozostaje spójny z doświadczeniami zebranymi po haitańskim eksperymencie i afgańskim pilotażu? Jeżeli jedynym spójnym modelem okazuje się ten, w którym zaufanie do państwa i sieci jest warunkowane istnieniem śladu, to postulat komunikacji przestaje być ideologiczną preferencją. Staje się logicznym wnioskiem. Zaufanie bowiem odradza się wyłącznie tam, gdzie audytowalny ślad umożliwia procedurę uzasadniania, a jego brak unieważnia zarówno majestat państwa, jak i cyfrowe obietnice platform.

> W świecie, gdzie prawda staje się towarem deficytowym, a informacja walutą, kluczowe staje się pytanie, czy potrafimy odróżnić echo od autentycznego głosu. Czy w pogoni za cyfrową

sprawczością nie zatracimy zdolności do krytycznej refleksji? A może w końcu okaże się, że największym wyzwaniem epoki cyfrowej jest nie technologia, lecz etyka?

## Inspiracje

**[1]** **"The new digital age"** Eric Schmidt, Jared Cohen

*2013 | RNDMHSE, Vintage, John Murray*

Amerykański biznesmen i były inżynier komputerowy. Prezes Google (2001-2011), prezes Alphabet Inc. (2015-2017). Wcześniej prezes Novell, dyrektor techniczny Sun Microsystems. Obecnie prezes Relativity Space.

*American businessman and former computer engineer. CEO of Google (2001-2011), Executive Chairman of Alphabet Inc. (2015-2017). Previously CEO of Novell, CTO at Sun Microsystems. Currently CEO of Relativity Space.*

*Relativity Space*

---

Amerykański biznesmen, historyk prezydentów i ekspert ds. polityki zagranicznej. Prezes ds. globalnych i współprzewodniczący Goldman Sachs Global Institute. Były prezes Jigsaw (Google Ideas). Doradca Condoleezzy Rice i Hillary Clinton. Autor wielu książek.

*American businessman, presidential historian, and foreign policy expert. President of Global Affairs and co-head of the Goldman Sachs Global Institute. Formerly CEO of Jigsaw (Google Ideas). Advisor to Condoleezza Rice and Hillary Clinton. Author of multiple books.*

*Goldman Sachs, Council on Foreign Relations*

## Literatura uzupełniająca

### Książki

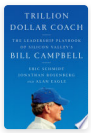
**Autorzy przywoływani w artykule:**


**[1]** **"How Google Works"**

Eric Schmidt, Jonathan Rosenberg, Alan Eagle

2014 | Grand Central Publishing | ISBN: 9781455582334

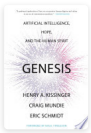
Google Scholar




**[2] "Trillion Dollar Coach: The Leadership Playbook of Silicon Valley's Bill Campbell"**

Eric Schmidt, Jonathan Rosenberg, Alan Eagle

2019 | HarperCollins | ISBN: 9780062839251

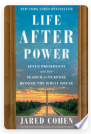



**[3] "Genesis: Artificial Intelligence, Hope, and the Human Spirit"**

Eric Schmidt, Henry Kissinger, Daniel Huttenlocher, Craig Mundie

2024 | Little, Brown | ISBN: 9780316581325

Google Scholar




**[4] "Life After Power: Seven Presidents and Their Search for Purpose Beyond the White House"**

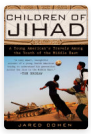
Jared Cohen

2024 | Simon and Schuster | ISBN: 9781982154547


**[5] "Accidental Presidents: Eight Men Who Changed America"**

Jared Cohen

2019 | Simon and Schuster | ISBN: 9781501109843




**[6] "Children of Jihad: A Young American's Travels Among the Youth of the Middle East"**

Jared Cohen

2008 | National Geographic Books | ISBN: 9781592403998

### Literatura pokrewna (Google Scholar):


**[7] "Sovereignty in Post-Sovereign Society"**

Jiří Přibáň

2016 | Routledge | ISBN: 9781317052098

Google Scholar

**[8] "Sovereignty: An Inquiry into the Political Good"**

Bertrand de Jouvenel

1957 | CUP Archive

Google Scholar

## Artykuły naukowe

### Autorzy przywoływani:

[1] **"Making It Possible for the Auditing of AI: A Systematic Review of AI Audits and AI Auditability"**

Yueqi Li, Sanjay Goel

2025 | Information Systems Frontiers

Google Scholar

**Artykuły pokrewne (Google Scholar):**

[2] **"The Central Paradox of the New Digital Age"**

ERIC SCHMIDT, Jared Cohen

2013 | New Perspectives Quarterly

[3] **"Collage of Comment"**

ERIC SCHMIDT, Jared Cohen, Hillary Clinton, [...] , Julian Assange

2011 | New Perspectives Quarterly

APA ONE Publishing System

Fundacja Dobre Państwo © 2026

Article ID: 024d7b03-20db-49fc-a57b-360097735928