Architektura odporności: decyzje w obliczu ewakuacji i kaskadowych awarii infrastruktury w świetle The Emergency Playbook Amy Edelman



AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje proces ewakuacji jako złożoną dynamiczną optymalizację ryzyka, a nie zwykłe przemieszczenie osób. Autor podkreśla, że kluczowym wyzwaniem jest rozpoznanie momentu, w którym ryzyko pozostania w miejscu zagrożenia przewyższa ryzyko ucieczki. Tekst wyjaśnia różnicę między ewakuacją a strategią shelter-in-place, wskazując, że wybór zależy od rodzaju zagrożenia (np. tsunami kontra skażenie radiologiczne). Omówiono asymetrię kosztów decyzji: podczas gdy fałszywy alarm generuje jedynie niedogodności, zignorowanie realnego niebezpieczeństwa prowadzi do tragedii. Wskazano również na problem habituacji w systemach ostrzegania oraz konieczność redukcji niepewności decyzyjnej poprzez precyzyjne instrukcje, co pozwala uniknąć paraliżu poznawczego w sytuacjach kryzysowych.

The article analyzes the evacuation process as a complex dynamic risk optimization rather than a simple movement of people. The author emphasizes that the key challenge is recognizing the moment when the risk of staying in the danger zone outweighs the risk of fleeing. The text explains the difference between evacuation and the shelter-in-place strategy, noting that the choice depends on the type of threat (e.g., tsunami versus radiological contamination). It discusses the asymmetry of decision costs: while a false alarm generates only inconvenience, ignoring real danger leads to tragedy. It also points to the problem of habituation in warning systems and the need to reduce decision uncertainty through precise instructions, which helps avoid cognitive paralysis in crisis situations.

Artykuł analizuje współczesną odporność kryzysową jako złożony system zależności między jednostką, infrastrukturą a państwem. Autor odrzuca wizję całkowitej samowystarczalności na rzecz budowania wielopoziomowej architektury zabezpieczeń, w której indywidualne przygotowanie (Positive Prepping) nie jest jedynie aktem prywatnego przetrwania, lecz strategicznym buforem dla systemów publicznych. Tekst szczegółowo omawia dynamikę decyzji o ewakuacji jako proces optymalizacji ryzyka oraz analizuje zjawisko kaskadowych awarii infrastrukturalnych (np. blackoutów), w których współzależność sieci energetycznych, wodociągowych i komunikacyjnych sprawia, że lokalny błąd może doprowadzić do systemowego paraliżu. Główna teza zakłada, że prawdziwa odporność nie polega na unikaniu awarii, lecz na zdolności do 'kontrolowanej degradacji' funkcji życiowych i sprawnym powrocie do normalności. W tym ujęciu domowe zapasy i plany rodzinne pełnią funkcję makroekonomiczną: redukują gwałtowny wzrost popytu na pomoc w pierwszej fazie kryzysu, pozwalając służbom ratunkowym skupić się na grupach najbardziej bezbronnych.

SŁOWA KLUCZOWE

architektura odporności | dynamiczna optymalizacja ryzyka | Protective Action Decision Model | normalcy bias | place attachment | redundancja modalna | shadow evacuation | efficiency-resilience trade-off | graceful degradation | cognitive offloading | Positive Prepping | distributed cognition | capacity management | single point of cognitive failure

Ewakuacja to dynamiczna optymalizacja ryzyka

Ewakuacja jako problem decyzji pod niepewnością: kiedy dom przestaje chronić, a droga zaczyna zagrażać

Najtrudniejszą decyzją kryzysową wcale nie musi być wybór sposobu działania po wystąpieniu katastrofy. Często wcześniejszym i poznawczo bardziej wymagającym problemem jest rozpoznanie momentu, w którym należy przestać zachowywać się tak, jakby otoczenie nadal było normalne. To tutaj spotykają się fizyka zagrożenia, psychologia decyzji, socjologia zaufania, teoria informacji, ekonomika behawioralna i inżynieria transportu. Ewakuacja nie jest bowiem zwykłym przemieszczeniem człowieka z punktu A do punktu B, lecz procesem decyzyjnym podejmowanym

pod presją czasu, przy niepełnej informacji, zmiennym ryzyku i ograniczonej zdolności do przewidywania zachowań innych ludzi.

Decyzja ta może być kosztowna niezależnie od wybranego wariantu. Wyjazd może okazać się zbędny, uciążliwy i niebezpieczny; pozostanie zaś może zakończyć się śmiercią. Dlatego dojrzała teoria przygotowania nie może sprowadzać problemu do prostej formuły „uciekaj wcześniej". Musi najpierw odpowiedzieć na pytanie, **jak człowiek rozpoznaje, że nadszedł moment, w którym niebezpieczeństwo opuszczenia bezpiecznego dotąd miejsca stało się mniejsze niż niebezpieczeństwo pozostania w nim**. Autor książki intuicyjnie ujmuje tę asymetrię.

W przypadku powodzi wskazuje on na konieczność opuszczania stref zalewowych i odradza forsowanie zalanych dróg; przy huraganie akcentuje podporządkowanie się nakazom ewakuacji; w obliczu pożaru zaleca natychmiastowe opuszczenie zagrożonego obszaru, natomiast przy złej jakości powietrza dopuszcza pozostanie wewnątrz budynku z odpowiednią filtracją.

Już ten zestaw pokazuje, że nie istnieje uniwersalna przewaga ruchu nad schronieniem. Strategia zależy od rodzaju zagrożenia, dynamiki jego propagacji, jakości budynku, dostępności drogi ewakuacyjnej, odległości do bezpiecznej strefy, stanu zdrowia mieszkańców i wiarygodności informacji. Przy tsunami wywołanym silnym wstrząsem na wybrzeżu opóźnianie ucieczki może być fatalne, dlatego autor zaleca natychmiastową relokację na wyżej położony teren. W przypadku zagrożenia radiologicznego sytuacja bywa odwrotna: pierwszym działaniem jest często pozostanie wewnątrz solidnego budynku, ograniczenie ekspozycji i oczekiwanie na wiarygodne instrukcje. Ta pozorna sprzeczność stanowi fundament nauki o ochronie ludności. **Ewakuacja i shelter-in-place nie są konkurencyjnymi ideologiami, lecz alternatywnymi interwencjami ochronnymi**, których skuteczność zależy od scenariusza.

Polski **Poradnik bezpieczeństwa** zachowuje tę samą logikę. Z jednej strony stwierdza, że przy bezpośrednim zagrożeniu życia lub zdrowia nie należy zwlekać z ewakuacją, a po wydaniu decyzji przez służby trzeba się jej podporządkować; wskazuje również na konieczność pomocy sąsiadom, wykorzystania transportu zorganizowanego lub poruszania się pieszo i niedopuszczania do blokowania dróg. Z drugiej strony rządowe materiały podkreślają, że w niektórych scenariuszach właściwą odpowiedzią jest szukanie schronienia w budynku, jego centralnych częściach albo przestrzeniach zapewniających osłonę.

Nie jest to niekonsekwencja, lecz przyznanie, że decyzja ochronna wymaga rozpoznania mechanizmu zagrożenia. W teorii decyzji problem ten można przedstawić jako dynamiczną optymalizację ryzyka. Człowiek porównuje dwie wartości oczekiwane, choć oczywiście nie dokonuje

formalnych obliczeń. Pozostanie w domu wiąże się z pewnym prawdopodobieństwem szkody i określoną skalą konsekwencji; podobnie ewakuacja. Wraz z rozwojem pożaru, powodzi czy skażenia wartości te ulegają zmianie. Co szczególnie ważne, **koszt błędnej decyzji jest asymetryczny**. Fałszywy alarm może oznaczać kilka godzin w korkach, stracony dzień pracy, koszty hotelu i irytację. Zignorowanie prawdziwego alarmu może oznaczać utratę życia. Teoria detekcji sygnału opisuje podobną strukturę problemu poprzez cztery możliwe rezultaty: trafne wykrycie zagrożenia, trafne odrzucenie fałszywego alarmu, alarm fałszywy i przeoczenie rzeczywistego niebezpieczeństwa. Racjonalny próg reakcji powinien zależeć nie tylko od prawdopodobieństwa zdarzenia, lecz także od względnego kosztu obu typów pomyłki. Z tego wynika istotna konsekwencja polityczna.

Skuteczny alarm to instrukcja redukująca niepewność decyzyjną

Społeczeństwo domagające się od systemu alarmowego zerowej liczby fałszywych ostrzeżeń może nieświadomie wymuszać ustawienie progu tak wysoko, że wzrośnie liczba przeoczonych zagrożeń. Z kolei administracja alarmująca zbyt często ryzykuje wywołaniem efektu habituacji – przyzwyczajenia do sygnałów i spadku ich znaczenia behawioralnego. Popularna metafora „chłopca wołającego wilka” nie oddaje w pełni tego mechanizmu, gdyż reakcja na ostrzeżenie zależy również od reputacji nadawcy, dotychczasowej precyzji komunikatów, spójności informacji w różnych kanałach oraz doświadczenia odbiorcy. Wysokiej jakości system ostrzegania musi zatem zarządzać nie tylko samą informacją, lecz także kapitałem wiarygodności, który jest zasobem wyczerpywalnym.

W tym kontekście szczególnego znaczenia nabiera Protective Action Decision Model Michaela Lindella i Ronalda Perry'ego. Model ten odrzuca założenie, że człowiek po prostu „otrzymuje alarm i działa”. Decyzji poprzedzają co najmniej trzy procesy: odebranie informacji, zwrócenie na nią uwagi oraz jej zrozumienie. Dopiero później kształtują się oceny samego zagrożenia, możliwych działań ochronnych i wiarygodności podmiotów przekazujących dane, a ostateczną reakcję modyfikują dodatkowo bariery i ułatwienia sytuacyjne. Takie ujęcie jest niezwykle użyteczne, ponieważ usuwa ze słownika zarządzania kryzysowego wygodne, ale intelektualnie leniwe zdanie: „ludzie nie posłuchali ostrzeżenia”. Zanim sformułujemy taki wniosek, należy ustalić, czy ostrzeżenie rzeczywiście dotarło do odbiorcy, czy było zrozumiałe i wiarygodne, czy osoba ta rozpoznała siebie jako zagrożoną oraz czy znała i miała materialną możliwość wykonania konkretnego działania ochronnego.

Różnica pomiędzy reception, attention a comprehension jest kluczowa w erze komunikacji wielokanałowej. Wiadomość może dotrzeć technicznie do telefonu, lecz nie zostać zauważona. Może zostać dostrzeżona, ale niezrozumiana z powodu bariery językowej, niepełnosprawności, stresu, niejasnej terminologii lub braku kontekstu. Z kolei komunikat zrozumiany semantycznie może nie przełożyć się na działanie, jeśli informuje jedynie o „istnieniu zagrożenia", nie odpowiadając na praktyczne pytania: gdzie dokładnie, od kiedy, dla kogo, jak długo i co należy zrobić. Skuteczny komunikat kryzysowy nie powinien więc ograniczać się do przekazania prawdy o zagrożeniu; musi być skonstruowany jako instrukcja redukująca przestrzeń niepewności decyzyjnej. Polski system formalnie zmierza właśnie w tym kierunku.

Oficjalne kanały obejmują syreny, megafony, radio, telewizję, Internet, Regionalny System Ostrzegania, Alert RCB oraz kontakt bezpośredni, a współczesne materiały edukacyjne dążą do ograniczenia liczby kodów, które obywatel musi rozpoznawać. Jest to racjonalne z perspektywy cognitive load theory: system alarmowy powinien być skuteczny także wobec człowieka niewyspanego, przestraszonego i nieznającego specjalistycznej terminologii, który podejmuje decyzję w hałasie informacyjnym. Każda dodatkowa kategoria sygnału zwiększa rozdzielczość systemu, lecz jednocześnie podnosi wymagania poznawcze wobec odbiorcy. Wyrafinowany system kodów, których nikt nie pamięta, może okazać się mniej użyteczny niż prostszy system stosowany konsekwentnie. Odbiorca alarmu nie jest jednak biernym terminalem.

Psychologia i bariery decyzji o ewakuacji

Badania nad ewakuacją pokazują, że ludzie konfrontują oficjalne komunikaty z tzw. environmental cues i social cues – czyli tym, co widzą, słyszą i obserwują u innych. Jeśli telefon ostrzega o pożarze, a na horyzoncie widać dym, zgodność sygnałów zwiększa subiektywną wiarygodność zagrożenia. Jeżeli natomiast komunikat jest alarmujący, lecz otoczenie pozostaje pozornie spokojne, część osób będzie szukała dodatkowego potwierdzenia. Proces ten nazywany jest w socjologii katastrof millingiem: ludzie kontaktują się z rodziną, sąsiadami, mediami i instytucjami, aby wspólnie nadać znaczenie niejednoznacznej sytuacji.

Z zewnątrz może to wyglądać jak irracjonalna zwłoka, lecz w rzeczywistości bywa próbą redukcji niepewności. Tu właśnie pojawia się krytyczny czynnik czasu. Poszukiwanie potwierdzenia jest adaptacyjne dopóki środowisko pozwala czekać; jednak przy szybko przemieszczającym się pożarze, gwałtownej powodzi czy tsunami każda kolejna minuta może ograniczać dostępność bezpiecznych dróg. Badania nad ewakuacją podczas pożarów terenów dzikich wskazują na istnienie znaczącej grupy osób przyjmujących strategię wait and see: nie decydują z góry ani o wyjeździe, ani

o pozostaniu, lecz obserwują rozwój sytuacji. Problem polega na tym, że późna decyzja o ucieczce może zostać podjęta dokładnie wtedy, gdy warunki drogowe stają się najgorsze. To przykład dynamic inconsistency: strategia, która wydawała się rozsądna piętnaście minut wcześniej, przestaje być bezpieczna, lecz człowiek nadal mentalnie ocenia sytuację według wcześniejszego obrazu ryzyka.

Potoczne pojęcie normalcy bias opisuje część tego zjawiska, jednak warto posługiwać się nim ostrożniej niż czynią to poradniki survivalowe. Nie każda zwłoka jest skutkiem "wyparcia rzeczywistości". Czasem człowiek dysponuje sprzecznymi informacjami, opiekuje się osobą zależną, nie posiada samochodu, obawia się utraty dobytku, pamięta wcześniejsze fałszywe alarmy lub interpretuje zachowanie sąsiadów jako sygnał, że zagrożenie nie jest jeszcze poważne. Przyczyna behawioralna może zatem leżeć nie w pojedynczym błędzie poznawczym, lecz w konstelacji percepcji ryzyka, ograniczeń zasobowych, norm społecznych i doświadczenia.

Do tego dochodzi place attachment, czyli przywiązanie do miejsca. Dom nie jest wyłącznie punktem w przestrzeni geograficznej; stanowi nośnik własności, tożsamości, wspomnień, statusu, prywatności, bezpieczeństwa ontologicznego i relacji społecznych. Literatura poświęcona katastrofom wskazuje, że przywiązanie do domu, sąsiedztwa i miejscowości jest zjawiskiem wielowymiarowym, powiązanym z czynnikami demograficznymi, społeczno-ekonomicznymi, przestrzennymi i psychospołecznymi. Ewakuacja nie oznacza więc dla człowieka tylko fizycznego oddalenia od zagrożenia, lecz chwilowe, a czasem trwałe zerwanie relacji ze środowiskiem, w którym zorganizował własne życie. W ekonomii behawioralnej można to zestawić z loss aversion oraz efektem posiadania: potencjalna utrata domu, zwierząt, dokumentów czy warsztatu pracy może psychologicznie ważyć więcej niż abstrakcyjna korzyść w postaci zwiększonego bezpieczeństwa.

Nie należy jednak pochopnie interpretować każdej odmowy ewakuacji jako irracjonalności. Czasami decyzja jest wynikiem realnych kosztów: człowiek nie ma dokąd jechać, brakuje mu środków na hotel, obawia się utraty pracy lub opiekuje się zwierzętami gospodarskimi, osobą z niepełnosprawnością bądź sprzętem medycznym trudnym do transportu. To rozróżnienie jest zasadnicze: behavioural bias i structural constraint mogą prowadzić do identycznego zachowania, ale wymagają całkowicie różnych interwencji publicznych. Jeśli problemem jest błędna ocena ryzyka, niezbędna jest edukacja i lepszy komunikat.

Jeśli jednak problemem jest brak samochodu, sama informacja nie stworzy pojazdu. Gdy osoba na wózku mieszka w budynku bez windy awaryjnej, apel o szybką ewakuację nie zniesie bariery architektonicznej. Jeśli senior nie może samodzielnie zabrać koncentratora tlenu, powtarzanie mu, że "powinien być przygotowany", może jedynie moralizować strukturalną bezradność. Dlatego we

współczesnej polityce ochrony ludności coraz większego znaczenia nabiera pojęcie functional needs. Odchodzi ono od mechanicznego katalogowania "grup szczególnych" na rzecz pytania o to, jakiej konkretnej funkcji człowiek nie jest w stanie wykonać samodzielnie: przemieszczenia, komunikacji, utrzymania terapii, orientacji, pozyskania informacji czy dostępu do transportu.

Krzywa wykonalności i pułapka indywidualnej racjonalności w ewakuacji

Równie istotny jest wymiar temporalny, gdyż ewakuacja posiada swoją krzywą wykonalności. W początkowej fazie zagrożenia dostępnych jest wiele potencjalnych tras i niewiele osób na drogach, jednak subiektywna pewność co do niebezpieczeństwa pozostaje niska. W miarę narastania kryzysu pewność rośnie, lecz maleje swoboda działania: zwiększa się liczba ewakuujących, część dróg zostaje zamknięta, stacje paliw ulegają przeciążeniu, a pogarsza się widoczność lub pogoda. W pewnym momencie napływ nowych informacji przestaje poprawiać jakość decyzji, ponieważ opcja działania zanika szybciej, niż rośnie pewność. Z punktu widzenia teorii real options ma to szczególne znaczenie: możliwość ewakuacji jest opcją o określonej wartości czasowej, która może wygasnąć.

Właśnie dlatego przygotowanie tras alternatywnych ma znaczenie wykraczające poza samą kartografię. Autor książki zaleca wcześniejsze ustalenie dróg zapasowych i uwzględnienie ryzyka paraliżu szlaków samochodowych, co wymusza przejście na rowery lub ruch pieszy. Nie należy jednak bezkrytycznie kopiować amerykańskich rozwiązań technicznych do warunków polskich; kluczowy jest sam mechanizm: mobilność kryzysowa musi mieć redundancję modalną, ponieważ ten sam kryzys, który wymusza przemieszczenie, może jednocześnie niszczyć infrastrukturę je nach umożliwiającą. Transport ujawnia tu charakterystyczny problem dóbr wspólnych. Samochód zwiększa autonomię jednostki, lecz jeśli każda rodzina wyjeżdża kilkoma pojazdami, suma indywidualnie racjonalnych decyzji pogarsza sytuację wszystkich. Federal Highway Administration odnotowała po ewakuacji przed huraganem Rita w 2005 roku, że część gospodarstw zabierała więcej niż jeden samochód – m.in. by chronić mienie pozostawione w strefie zagrożenia – co drastycznie zwiększyło zatłoczenie dróg. To klasyczny konflikt między micro-rationality i macro-efficiency: działanie rozsądne z perspektywy jednego gospodarstwa staje się dysfunkcjonalne systemowo, gdy zostanie powielone przez setki tysięcy innych osób.

W tym miejscu inżynieria ewakuacji spotyka się z teorią przepustowości sieci. Sieć drogowa ma ograniczoną zdolność przenoszenia strumienia pojazdów. Po przekroczeniu określonej gęstości ruchu wzrost liczby samochodów nie zwiększa już liczby osób opuszczających obszar w jednostce

czasu, lecz obniża prędkość całego systemu. Zjawisko to jest nieliniowe: niewielki przyrost obciążenia może doprowadzić do przejścia z płynnego ruchu w stan zakleszczenia. Ewakuacja masowa jest zatem problemem network flow, przy czym sieć transportowa różni się od rurociągu tym, że każdy jej element podejmuje własne decyzje: zmienia trasę, zatrzymuje się, poszukuje paliwa i reaguje na zachowanie innych. Pojęcie shadow evacuation opisuje dodatkową trudność – z obszaru wyjeżdżają również osoby, którym formalnie nie nakazano ewakuacji. Z indywidualnego punktu widzenia jest to przejaw ostrożności; dla planisty oznacza jednak ruch spoza modelowanej populacji. Problem rozszerza pojęcie evacuation convergence, odnoszące się do osób zmierzających w kierunku strefy kryzysowej: krewnych, mediów, wolontariuszy czy ciekawskich. System transportowy w chwili katastrofy nie przenosi więc jednego uporządkowanego strumienia „na zewnątrz", lecz jest obciążony wieloma nakładającymi się mobilnościami.

Huragan Rita dostarczył również znacznie ponurejszej lekcji o ewakuacji jako źródle ryzyka. 23 września 2005 roku, podczas transportu mieszkańców placówki opiekuńczej, autokar przewożący 44 osoby oraz personel zapalił się na autostradzie Interstate 45. Zginęło dwudziestu trzech pasażerów.

Ewakuacja jako proces generujący ryzyka wtórne

NTSB ustaliła, że bezpośrednią przyczyną był problem techniczny związany z niedostatecznym smarowaniem zespołu łożyska koła. Wskazała jednak również na braki w utrzymaniu pojazdu, nieskuteczny nadzór regulacyjny, właściwości materiałów oraz ograniczoną zdolność osób ze szczególnymi potrzebami do szybkiego opuszczenia autobusu. Przypadek ten jest wyjątkowo istotny, ponieważ burzy intuicyjny podział na "niebezpieczną strefę" i "bezpieczną ewakuację". Działanie ochronne może generować własne ryzyko wtórne.

Ewakuacja osoby zdrowej prywatnym samochodem a transport czterdziestu osób zależnych medycznie to dwa zupełnie różne procesy; ich funkcje ryzyka różnią się radykalnie. W przypadku osób starszych, hospitalizowanych czy wymagających aparatury medycznej każda godzina podróży niesie dodatkowe zagrożenia: przerwanie opieki, zmianę mikroklimatu, brak dostępu do leków, dezorientację, urazy podczas transferu czy trudności z opuszczeniem pojazdu. Dlatego postulat „wcześniejszej ewakuacji" nie może być abstrakcyjnym nakazem, lecz musi uwzględniać jakość transportu, miejsce docelowe i ciągłość opieki. Na poziomie państwowym oznacza to konieczność przejścia od evacuation planning do evacuation system design – samo wyznaczenie drogi jest niewystarczające.

Konieczne jest precyzyjne określenie populacji objętej ewakuacją, jej rozmieszczenia, dostępności pojazdów i przepustowości sieci, a także zaplanowanie punktów medycznych, zapotrzebowania na paliwo, transportu zwierząt oraz procedur dla szkół i domów opieki, włącznie z zasadami ponownego wejścia do strefy. Doświadczenia po huraganach Katrina i Rita skłoniły amerykańskich analityków transportowych właśnie do podkreślenia potrzeby koordynacji dowodzenia, komunikacji, ruchu, paliwa oraz ewakuacji osób ze szczególnymi potrzebami.

Współczesny polski model w coraz większym stopniu dostrzega tę złożoność. Poradnik bezpieczeństwa zaleca m.in., aby dzieci posiadały dane kontaktowe opiekunów i informacje medyczne, a mieszkańcy wspierali sąsiadów ze szczególnymi potrzebami oraz dbali o to, by nie blokować dróg prywatnymi samochodami. W październiku 2026 r. opublikowano wzorcowe procedury reagowania dla szkół i przedszkoli po komunikacie o zagrożeniu z powietrza, zakładając jednocześnie, że każda placówka musi dostosować je do własnych warunków. To drobny, ale poznawczo ważny sygnał zmiany paradygmatu: procedura centralna ma być szablonem adaptowanym lokalnie, a nie instrukcją zakładającą identyczność wszystkich miejsc.

W tym kontekście zasadne jest wprowadzenie koncepcji distributed cognition. Wiedza niezbędna podczas ewakuacji nie znajduje się wyłącznie w głowie jednej osoby; jest ona rozproszona między mapą, telefonem, oznakowaniem, rodziną, sąsiadami, dyspozytorem, kierowcą autobusu, służbą meteorologiczną, systemem alarmowym a pamięcią lokalną.

Budowanie redundancji poznawczej i komunikacyjnej w planowaniu rodzinnym

Bezpieczeństwo zależy od tego, czy poszczególne elementy systemu potrafią skutecznie wymieniać informacje. Listy kontaktów, papierowa mapa czy wcześniej ustalone punkty spotkania nie są zatem nostalgicznym powrotem do epoki analogowej, lecz przykładami **cognitive offloading** – przeniesienia części obciążenia pamięci i orientacji z człowieka na zewnętrzne artefakty. Cyfrowa nawigacja fundamentalnie zmieniła relację między kompetencją a narzędziem: smartfon zapewnia znakomitą orientację przestrzenną, dopóki działają bateria, GPS, mapy, transmisja danych i samo urządzenie. Problemem nie jest jednak samo uzależnienie od technologii.

Byłoby intelektualnie jałowe nawoływać do powrotu do kompasu jako symbolu rzekomej dawnej zaradności. Kluczowym zagrożeniem jest **single point of cognitive failure**: sytuacja, w której jedna awaria pozbawia człowieka nie tylko konkretnej usługi, lecz całej zdolności zastępczej.

Racjonalny model nie odrzuca aplikacji nawigacyjnej, lecz zachowuje minimalną alternatywę – mapę offline, zapisany adres, fizyczny punkt spotkania czy orientację w układzie głównych dróg.

Analogicznie należy myśleć o komunikacji rodzinnej. Wspólny plan powinien redukować konieczność wzajemnego poszukiwania się właśnie wtedy, gdy infrastruktura jest przeciążona. Rodzina, która wcześniej ustaliła dwa miejsca spotkania – lokalne i oddalone – posiada prosty **protocol for degraded communications**. Jeśli telefon działa, członkowie komunikują się normalnie; jeśli sieć zawodzi, wiedzą, gdzie próbować się odnaleźć. W przypadku niedostępności punktu lokalnego, wchodzi w życie reguła przejścia do punktu dalszego. Istotą nie jest sam adres, lecz ustalona wcześniej logika przełączania między stanami systemu. Prowadzi to do zagadnienia **common operating picture**, czyli wspólnego obrazu sytuacyjnego. W organizacjach ratowniczych pojęcie to oznacza współdzieloną reprezentację zdarzeń: wiedzę o tym, co się dzieje, gdzie znajdują się zasoby, jakie są zagrożenia i jakie działania podejmują poszczególne jednostki. Analogiczna potrzeba istnieje również w gospodarstwie domowym.

Jeżeli jedna osoba uważa, że należy natychmiast wyjechać, druga chce czekać na kolejny komunikat, a trzecia jedzie po dziecko do szkoły bez powiadomienia pozostałych, nawet dobrze wyposażona rodzina może zostać sparaliżowana przez **coordination failure**. Plan rodzinny redukuje nie tyle brak wiedzy, co ryzyko powstania kilku sprzecznych wersji działania. Nie można jednak przeciwstawiać racjonalnego planowania emocjom, jakby najlepiej ewakuował się człowiek pozbawiony uczuć. Strach pełni funkcję adaptacyjną: zwiększa czujność, przyspiesza mobilizację zasobów i skłania do unikania zagrożenia. Problem pojawia się przy zbyt niskim lub zbyt wysokim pobudzeniu. Zbyt niskie może utrzymać zachowania rutynowe mimo zmiany warunków; nadmierne zaś zawęża uwagę i redukuje elastyczność. Badania nad percepcją ryzyka podczas ewakuacji przeciwpożarowych podkreślają złożony związek między emocjami, oceną ryzyka, situational awareness a działaniem ochronnym. Zamiast więc przeciwstawiać „zimną głowę" emocjom, trafniej mówić o **regulacji pobudzenia pozwalającej utrzymać funkcje wykonawcze**. Jeszcze subtelniejszym problemem jest zaufanie: człowiek nie jest w stanie samodzielnie mierzyć stężenia wszystkich substancji, prognozować trajektorii powodzi ani modelować rozwoju pożaru.

Odporność informacyjna i decyzyjna jako fundament działania

Człowiek musi delegować część oceny na ekspertów i instytucje, co prowadzi do powstania tzw. epistemic dependence. Nie jest ona wadą, lecz warunkiem funkcjonowania złożonego

społeczeństwa; problemem staje się dopiero zależność pozbawiona procedury korekty. Fałszywy alarm balistyczny na Hawajach pokazał, że system może niezwykle sprawnie przekazać błędną informację.

Katastrofy infrastrukturalne pokazują z kolei, że instytucje eksperckie mogą opóźnić reakcję. Nie wynika z tego jednak racjonalność całkowitej nieufności, lecz potrzeba calibrated trust – zaufania proporcjonalnego do kompetencji, wiarygodności i kontekstu źródła. Taka kalibracja jest szczególnie trudna w środowisku mediów społecznościowych. W sytuacji kryzysowej informacja konkurencyjna wobec komunikatu oficjalnego może pochodzić od naocznego świadka, eksperta, lokalnego mieszkańca, konta propagandowego lub osoby zwyczajnie powtarzającej plotkę. Prędkość transmisji wzrosła szybciej niż zdolność społeczeństwa do walidacji źródeł. W rezultacie powstaje information overload, którego skutkiem nie musi być brak informacji, lecz utrata zdolności ustalenia, która z nich zasługuje na działanie. Odporność informacyjna jest więc kompetencją równie praktyczną jak filtracja wody: chodzi o oddzielenie użytecznego sygnału od zanieczyszczenia.

Ewakuacja staje się testem wszystkich warstw odporności jednocześnie. Wymaga wcześniejszego planu, materialnego wyposażenia, wiarygodnej informacji, transportu, sprawności fizycznej, regulacji emocji, zaufania do instytucji, współpracy rodzinnej i zdolności rezygnacji z dóbr materialnych. Nie jest jednym zachowaniem, lecz skomprymowanym sprawdzianem systemu społeczno-technicznego.

Positive Prepping odsłania w tym miejscu swoją największą przewagę nad kulturą doomsdayową. Doomsday prepper przygotowuje się przede wszystkim na świat po upadku instytucji. Positive prepper uwzględnia również znacznie bardziej prawdopodobny scenariusz: świat, w którym instytucje istnieją, lecz przez pewien czas działają gorzej, częściowo, nierówno albo wymagają współdziałania przygotowanych obywateli. W pierwszym modelu ewakuacja może przybrać postać samotnej ucieczki do schronu; w drugim jest elementem koordynacji między gospodarstwem, sąsiadami, transportem publicznym, szkołą, samorządem i służbami.

Najważniejsza różnica nie przebiega więc pomiędzy decyzją o tym, czy „zostać”, czy „uciec”. Przebiega ona pomiędzy działaniem reaktywnym a antycypacyjnym. Człowiek reaktywny zaczyna organizować ewakuację w chwili, gdy musi wyjść. Człowiek przygotowany podjął część decyzji wcześniej: wie, co zabiera, czego nie będzie ratował, dokąd jedzie, jak skontaktuje się z rodziną, kto pomoże osobie zależnej i jaką informację uzna za wystarczający sygnał do uruchomienia planu. I właśnie ten ostatni element jest być może najważniejszy.

Dobrze przygotowany człowiek nie posiada tylko plecaka ewakuacyjnego – posiada wcześniej określone kryteria zmiany decyzji. Nie negocjuje z pożarem, czy może jeszcze zaczekać godzinę. Nie testuje głębokości rwącej wody przednim kołem samochodu. Nie potrzebuje stuprocentowej pewności, gdy koszt błędu wynikającego ze zwłoki jest nieporównywalnie większy niż koszt wcześniejszego wyjazdu. Przygotowanie okazuje się więc nie tyle magazynem rzeczy, co sztuką wcześniejszego ustalania warunków, po których spełnieniu człowiek przestaje improwizować i zaczyna wykonywać ustalony plan.

Dalsza analiza musi jednak zejść głębiej. Nawet najlepsza decyzja jednostki może okazać się niewystarczająca, gdy przestają działać energetyka, telekomunikacja, płatności, logistyka i administracja. Następny poziom stanowi zatem blackout oraz kaskadowa awaria infrastruktury – sytuacja szczególnie interesująca, ponieważ nie niszczy jednego urządzenia, lecz równocześnie odbiera współczesnemu człowiekowi dostęp do całych wiązek funkcji, których istnienia na co dzień niemal nie zauważa. Blackout jako laboratorium kruchości cywilizacji pozwala dostrzec awarie kaskadowe i pozorną autonomię nowoczesnego człowieka w obliczu współzależnych systemów.

Blackout jest jednym z najbardziej pouczających scenariuszy kryzysowych, ponieważ odróżnia awarię pojedynczego urządzenia od awarii funkcji społecznych. Brak energii elektrycznej sam w sobie jest tylko zmianą stanu fizycznego sieci. Jego znaczenie cywilizacyjne wynika z tego, że elektryczność stała się infrastrukturą infrastruktury: zasila systemy wodne, telekomunikację, chłodnictwo, część ogrzewania, sterowanie ruchem, logistykę, handel, bankowość, stacje paliw, windy, urządzenia medyczne, serwerownie oraz liczne elementy administracji publicznej.

Współzależność systemów jako źródło kaskadowych awarii

Autor książki trafnie zwraca uwagę na asymetrię podatności między mieszkańcem wysokiego budynku miejskiego, który wraz z zanikiem zasilania stopniowo traci dostęp do wody z pomp, wind, chłodzenia żywności czy ogrzewania, a gospodarstwem dysponującym bardziej autonomicznymi źródłami ciepła i wody. Nie chodzi tu jednak o romantyczne przeciwstawienie „odpornej wsi” „kruchemu miastu”.

Znacznie istotniejszym problemem badawczym jest stopień zależności funkcjonalnej od sieci oraz liczba alternatywnych ścieżek podtrzymywania podstawowych funkcji. Blackout pozwala dostrzec mechanizm, który pozostaje niewidoczny podczas normalnej eksploatacji infrastruktury: współczesny człowiek jest znacznie mniej samodzielny, niż sugeruje jego prywatna własność. Może

posiadać mieszkanie, samochód, pieniądze czy zapasy, ale korzystanie z tych aktywów zależy od warstw infrastrukturalnych pozostających poza jego kontrolą. Samochód wymaga paliwa; stacja paliw – energii do pomp i systemów płatności; systemy płatnicze – telekomunikacji i infrastruktury bankowej; telekomunikacja – zasilania; serwery – chłodzenia i sieci transmisyjnych, a wodociągi – pomp, uzdatniania, automatyki i dostaw chemikaliów.

Autonomia jednostki okazuje się zatem w dużej mierze autonomią pożyczoną od sprawnie działających systemów zbiorowych. Prowadzi to do kluczowego pojęcia we współczesnych badaniach nad bezpieczeństwem infrastrukturalnym: interdependence, czyli współzależności. Klasyczna praca Stevena Rinaldiego, Jamesa Peerenbooma i Terrence'a Kelly'ego już na początku XXI wieku dowodziła, że infrastruktury krytyczne nie powinny być analizowane jako oddzielne sektory, gdyż są one powiązane fizycznie, informacyjnie, przestrzennie i funkcjonalnie. Awaria jednej z nich może przenosić się na drugą nie dlatego, że oba systemy uległy uszkodzeniu w wyniku tego samego zdarzenia, lecz dlatego, że produkt jednego systemu jest warunkiem działania drugiego.

Woda wymaga energii, energia potrzebuje telekomunikacji i systemów sterowania, telekomunikacja zależy od energii, a energetyka od transportu, paliw i pracy ludzi. Prosty łańcuch przyczynowy znika, ustępując miejsca pętlom sprzężeń zwrotnych. Dlatego współczesną katastrofę należy modelować nie jako przewrócenie szeregu kostek domina, lecz jako awarię sieci sieci. Model domina sugeruje sekwencję liniową: A powoduje B, a B wywołuje C.

W systemach infrastrukturalnych zależności bywają jednak zwrotne. Awaria energetyki może ograniczać przesył gazu, podczas gdy energetyka gazowa potrzebuje tego paliwa do przywrócenia generacji prądu. Utrata telekomunikacji utrudnia koordynację napraw energetycznych, a brak energii skraca czas funkcjonowania węzłów telekomunikacyjnych. Uszkodzenie transportu blokuje dowóz ekip naprawczych i paliwa do generatorów, co wydłuża awarię pierwotną. Autor książki prawidłowo wskazuje na ten kaskadowy charakter współczesnych zakłóceń, w których uszkodzenie jednego elementu technicznego lub środowiskowego przenosi się na kolejne systemy społeczne.

Przełomowym wkładem teorii sieci było wykazanie, że współzależność może zmieniać samą naturę odporności. Sergey Buldyrev, Shlomo Havlin i współautorzy w pracy z 2010 roku udowodnili, że sieci wzajemnie zależne zachowują się inaczej niż izolowane: awaria w jednej uruchamia uszkodzenia w drugiej, które następnie wracają do pierwszej, generując kaskadę. Szczególna niewygoda tego wniosku polega na tym, że cechy zwiększające odporność pojedynczej sieci nie muszą przekładać się na odporność całego układu. Można doskonalić sektor energetyczny, telekomunikacyjny i transportowy oddzielnie, a mimo to pozostawić między nimi połączenia będące kanałami propagacji kryzysu.

Tutaj teoria sieci spotyka się z koncepcją normal accidents Charlesa Perrowa. W systemach jednocześnie złożonych i ściśle sprzężonych niebezpieczeństwo nie wynika wyłącznie z niskiej jakości komponentów czy niedbalstwa operatora, lecz z samej struktury systemu. Wielość wzajemnych interakcji sprawia, że nie wszystkie sekwencje zdarzeń są przewidywalne, a silne sprzężenie powoduje, że gdy nieoczekiwany proces już się rozpocznie, operator ma zbyt mało czasu na jego zrozumienie i zatrzymanie. Katastrofa systemowa może więc powstać nie dlatego, że jeden element był wadliwy, lecz dlatego, że kilka pozornie niewielkich odchyleń weszło ze sobą w relację, której wcześniej nie przewidziano.

Paradoks kaskady i różnica między triggerem a przyczyną systemową

Elektroenergetyka stanowi modelowy przykład takiego systemu. Energia elektryczna nie jest bowiem magazynowana w sieci w sposób analogiczny do wody w zbiorniku; w każdej chwili system musi utrzymywać dynamiczną równowagę między wytwarzaniem a poborem, dbając o odpowiednie parametry częstotliwości i napięcia. W Europie kontynentalnej częstotliwość nominalna wynosi 50 Hz, a jej odchylenia sygnalizują nierównowagę mocy czynnej. Napięcie z kolei wiąże się przede wszystkim z lokalnym bilansem mocy biernej oraz zdolnością systemu do jego regulacji. System elektroenergetyczny jest zatem jednocześnie systemem transportowym i sterowania, w którym fizyka narzuca ograniczenia szybciej, niż procedura administracyjna może zebrać się na naradę.

Współczesna energetyka opiera się na zasadach takich jak kryterium N-1: system powinien w określonym zakresie wytrzymać utratę pojedynczego istotnego elementu – linii, transformatora czy jednostki wytwórczej – bez ryzyka rozległej awarii. Problem pojawia się jednak wtedy, gdy kolejne elementy wypadają szybciej, niż system jest w stanie się ustabilizować, lub gdy pierwotne zdarzenie zmienia przepływy tak drastycznie, że pozostałe komponenty zostają przeciążone i ich zabezpieczenia również zaczynają działać. Zabezpieczenie, które lokalnie funkcjonuje prawidłowo, odłączając zagrożony element, z perspektywy całości może stać się zapalnikiem kolejnego etapu kaskady. Ochrona części może zatem pogarszać stan całości – to jeden z klasycznych paradoksów złożonych systemów technicznych.

Blackout północnoamerykański z 14 sierpnia 2003 roku pozostaje podręcznikową ilustracją tego mechanizmu. Początkowe problemy w Ohio obejmowały m.in. wyłączenia linii wskutek kontaktu przewodów z drzewami, jednak katastrofa nie była prostym skutkiem „jednego drzewa”. Dołożyły do niej błędy organizacyjne, niedostateczna świadomość sytuacyjna oraz awarie narzędzi monitorujących i komunikacji; po przekroczeniu punktu krytycznego system wszedł w szybką fazę

kaskady. Oficjalna analiza wykazała, że po określonej sekwencji wyłączeń w ciągu zaledwie kilku minut awaria objęła rozległe obszary Stanów Zjednoczonych i Kanady, pozbawiając energii około 50 mln ludzi. Wspólna komisja USA i Kanady uznała, że blackout był w znacznej mierze możliwy do uniknięcia, co doprowadziło do wprowadzenia obowiązkowych standardów niezawodności.

Wydarzenie z 2003 roku pozwala rozróżnić trigger od root causes. Zdarzenie inicjujące może być banalne, lecz rzeczywiste przyczyny katastrofy tkwią w sposobie organizacji systemu. Gałąź drzewa nie jest w stanie "wyłączyć cywilizacji" bez infrastruktury i organizacji, w których lokalne uszkodzenie może zostać przekształcone w systemową kaskadę. W analizie powypadkowej pytanie „co się zepsuło?" jest więc często mniej użyteczne niż „dlaczego system pozwolił, aby to uszkodzenie rozprzestrzeniło się tak daleko?". Ta różnica oddziela myślenie inżynieryjne od poszukiwania kozła ofiarnego.

Jeszcze bardziej aktualnym laboratorium stał się blackout Hiszpanii i Portugalii z 28 kwietnia 2025 roku. Było to najpoważniejsze zdarzenie w europejskim systemie elektroenergetycznym od ponad dwóch dekad, obejmujące praktycznie całe kontynentalne systemy obu państw. Po wielomiesięcznym badaniu panel ENTSO-E opublikował w marcu 2026 roku raport końcowy.

Złożoność awarii i pułapka jednoczynnikowych wyjaśnień

Ustalenia autora są poznawczo istotne właśnie dlatego, że nie dają się zamknąć w politycznie atrakcyjnej, jednoczynnikowej formule. Panel wskazał na splot oscylacji, niedostatków regulacji napięcia i mocy biernej, różnic w praktykach regulacyjnych, gwałtownych redukcji mocy i odłączeń generatorów oraz nierównomiernych zdolności stabilizacyjnych. To doprowadziło do szybkiego wzrostu napięcia i kaskadowych odłączeń generacji.

Jest to niemal modelowa lekcja przeciwko **monocausal storytelling**, czyli potrzebie odnalezienia jednego winnego złożonej awarii. W pierwszych godzinach po blackoutcie w przestrzeni publicznej zwykle pojawia się popyt na prostą odpowiedź: cyberatak, odnawialne źródła energii, operator, błąd człowieka, sabotaż albo niewłaściwa polityka energetyczna. Tymczasem system złożony może doznać katastrofy dlatego, że kilka zjawisk, z których żadne oddzielnie nie musiało być krytyczne, stworzyło wspólnie niebezpieczną konfigurację. Właśnie takie przypadki uzasadniają metodologiczne rozróżnienie między **proximate cause**, przyczyną bezpośrednią, a **systemic causation**, przyczynowością rozproszoną pomiędzy konstrukcję, regulację, parametry techniczne, zachowanie operatorów i wcześniejsze decyzje instytucjonalne.

Iberyjski blackout ujawnił jeszcze jeden kłopotliwy wymiar bezpieczeństwa: sam proces rekonstrukcji katastrofy wymaga dostępu do danych należących do wielu podmiotów. ENTSO-E informowała latem 2025 r. o trudnościach w pozyskiwaniu kompletnych i wysokiej jakości danych od części operatorów dystrybucyjnych i przedsiębiorstw wytwórczych w Hiszpanii, co wpłynęło na harmonogram badania. To nie jest anegdota administracyjna.

W świecie infrastruktury cyfrowej **data availability staje się składnikiem safety**: jeśli instytucje nie potrafią szybko odtworzyć sekwencji zdarzeń, trudniej jest wyciągać wnioski, poprawiać modele i rozpoznawać podatności przed kolejną awarią. Blackout teksański podczas mrozów w lutym 2021 r. dostarcza z kolei wyjątkowo wyraźnego przykładu **feedback failure** między dwoma sektorami.

ERCOT musiał nakazać około 20 GW kontrolowanego odciążenia systemu, aby uniknąć jeszcze głębszego rozpadu sieci. FERC i NERC wykazały, że awarie dotyczyły różnych technologii wytwórczych; ogromne znaczenie miało zarówno zamarzanie urządzeń, jak i problemy z dostawami gazu. Szczególnie pouczające jest to, że część spadku produkcji gazu wiązała się z utratą zasilania infrastruktury wydobywczej i przesyłowej – a zatem blackout osłabiał system gazowy, od którego zależała energetyka potrzebna do zakończenia blackoutu. Co istotne, 81% odnotowanych wyłączeń jednostek związanych z zamarzaniem nastąpiło przy temperaturach wyższych niż deklarowane przez te jednostki temperatury projektowe.

To spostrzeżenie brzmi niemal jak oskarżenie wobec powierzchownego rozumienia "ekstremalnego zdarzenia". Skoro awaria następuje w warunkach, które urządzenie według deklaracji miało wytrzymywać, problem nie leży wyłącznie w ekstremum meteorologicznym. Pojawia się **performance gap** między projektem, deklarowaną zdolnością a realną operacyjnością systemu.

Skandalicznego posmaku przypadkowi teksańskiemu dodaje fakt, że podobny alarm wygenerowały już silne mrozy w 2011 r. Po tamtym dochodzeniu sformułowano zalecenia dotyczące przygotowania infrastruktury do warunków zimowych, lecz po wydarzeniach z 2021 r. przewodniczący FERC musiał przypominać, że poprzednie rekomendacje nie zostały właściwie zrealizowane.

Odporność to zdolność działania, a nie dokumentacja

To klasyczna ilustracja omawianego wcześniej zjawiska organizational forgetting oraz jeszcze bardziej cynicznej odmiany patologii instytucjonalnej: organizacja może doskonale wiedzieć, co powinna zrobić, a mimo to przez lata nie przekształcić tej wiedzy w realną zdolność. Blackout

pozwala zatem odróżnić resilience as documentation od resilience as performance. System może dysponować planami awaryjnymi, instrukcjami, standardami czy generatorami, a jednak pozostać niezdolnym do adaptacyjnego działania. Erik Hollnagel proponuje, aby odporność oceniać poprzez cztery potencjały: zdolność reagowania na bieżące zdarzenia, monitorowania elementów krytycznych, uczenia się z doświadczeń oraz antycypowania przyszłych zmian.

Taka definicja jest znacznie bardziej wymagająca niż samo posiadanie zapasów. Wymaga od organizacji nie tylko posiadania urządzeń awaryjnych, ale przede wszystkim wiedzy, kiedy je uruchomić, stałej obserwacji ich stanu, wyciągania wniosków z wcześniejszych prób i przewidywania scenariuszy, w których obecne rozwiązania przestaną wystarczać. W energetyce kluczowym przykładem takiej zdolności jest black start – możliwość uruchomienia fragmentów systemu bez zewnętrznego zasilania z sieci. Po totalnym blackoutcie nie można bowiem po prostu "włączyć elektrowni i światła". Duże jednostki same potrzebują energii do uruchomienia pomp, sterowania, wzbudzenia oraz systemów pomocniczych i chłodzenia. Odbudowa sieci wymaga zatem źródeł zdolnych do autonomicznego startu, tworzenia niewielkich wysp energetycznych, stopniowego przyłączania kolejnych odbiorów i synchronizowania rekonstruowanych obszarów. Iberyjski system w 2025 roku był przywracany m.in. dzięki zasobom hydroenergetycznym oraz połączeniom z Francją i Marokiem.

Jest to techniczny odpowiednik zasady Positive Prepping: system przetrwa nie dlatego, że nigdy nie upadnie, lecz dlatego, że zachował zdolność samodzielnego rozpoczęcia odbudowy. Na poziomie gospodarstwa domowego odpowiednikiem black start nie jest oczywiście prywatna elektrownia, lecz możliwość zachowania minimalnych funkcji w momencie odłączenia od infrastruktury zewnętrznej. Należy przy tym odróżnić backup power od energy resilience.

Powerbank podtrzyma telefon, ale nie lodówkę. Mały UPS pozwoli bezpiecznie wygasić komputer, lecz nie ogrzeje mieszkania. Generator zapewni znaczną moc, ale wymaga paliwa, właściwej wentylacji i konserwacji. Instalacja fotowoltaiczna nie zawsze automatycznie zasila dom podczas blackoutu; typowy system sieciowy może odłączyć się ze względów bezpieczeństwa, jeśli nie wyposażono go w magazyn energii i funkcję pracy wyspowej. Odporność energetyczna zaczyna się więc od hierarchizacji obciążeń, a nie od maksymalizacji produkcji: trzeba wiedzieć, które funkcje są niezbędne, które mogą działać okresowo, a z których można całkowicie zrezygnować. To mikroekonomiczny odpowiednik load shedding stosowanego przez operatorów sieci. Gdy nie da się podtrzymać wszystkiego, system powinien degradować się selektywnie. Krytyczne urządzenie medyczne ma pierwszeństwo przed telewizorem, komunikacja przed ozdobnym oświetleniem, a chłodzenie leków przed komfortem termicznym części pomieszczeń. Takie podejście można nazwać functional triage.

Nie pyta ono: "ile energii mamy?", lecz: "jakie funkcje społeczne i biologiczne musimy utrzymać przy dostępnej energii?". Tę samą logikę stosuje państwo, gdy przy ograniczonych zasobach priorytetyzuje szpitale, wodociągi, służby ratownicze i infrastrukturę łączności. Kryzys energetyczny bowiem łatwo przekształca się w kryzys wodny.

Odporność to dywersyfikacja modalna i kapitał społeczny

Nowoczesne wodociągi nie są grawitacyjnym cudem; pompowanie, uzdatnianie, dozowanie chemikaliów, kontrola ciśnienia i kanalizacja opierają się na energii oraz automatyce. W wysokich budynkach nawet sprawna sieć miejska nie gwarantuje dopływu wody na wyższe kondygnacje, jeśli zawiedzie lokalny system podnoszenia ciśnienia. Opozycja między wieżowcem a domem ze studnią ma tu wartość heurystyczną, choć wymaga subtelności: studnia również może wymagać pompy elektrycznej, a nowoczesny budynek może dysponować zasilaniem awaryjnym. Realną zmienną nie jest zatem romantycznie pojmowany typ miejsca zamieszkania, lecz **functional dependency profile** gospodarstwa.

Podobnie rzecz ma się z telekomunikacją. Sieć mobilna może funkcjonować przez pewien czas dzięki bateriom i generatorom, jednak jej autonomia energetyczna jest ograniczona, a jednocześnie ruch gwałtownie rośnie, gdy miliony użytkowników próbują skontaktować się z bliskimi. W efekcie komunikacja może zawieść z dwóch odmiennych powodów: fizycznego braku zasilania infrastruktury albo **congestion failure**, czyli przeciążenia wciąż działającego systemu. Dla obywatela rezultat jest identyczny – telefon „nie działa” – lecz z punktu widzenia projektowania odporności są to różne mechanizmy, wymagające odmiennych zabezpieczeń.

Analogiczny błąd pojawia się w myśleniu o pieniądzu. Autor książki formułuje mocną tezę, że w pierwszej fazie zakłócenia gotówka staje się podstawowym płynnym środkiem wymiany, gdyż transakcje bezgotówkowe zależą od infrastruktury cyfrowej. Sens tej intuicji jest słuszny, choć jej absolutna forma wymaga korekty.

Nie każdy blackout automatycznie wyłącza wszystkie płatności elektroniczne; część infrastruktury posiada rezerwy, a niektóre rozwiązania pozwalają na ograniczoną pracę offline. Z drugiej strony Europejski Bank Centralny podkreśla, że gotówka pełni funkcję **resilience layer**, ponieważ jej użycie nie wymaga Internetu ani elektryczności. Banki centralne utrzymują odpowiednie rezerwy właśnie z myślą o zakłóceniach w elektronicznych systemach płatniczych, co ECB potwierdzał

również w 2026 r., wskazując na gotówkę jako instrument odporności w obliczu awarii zasilania, sieci czy cyberincydentów.

Gotówka nie jest jednak magicznym narzędziem autonomii. Bankomat potrzebuje prądu i łączności, transport pieniędzy – logistyki, a sklep – personelu i możliwości otwarcia placówki. Jeśli gospodarstwo posiada środki wyłącznie na rachunku, staje się silnie zależne od infrastruktury cyfrowej; jeśli zaś trzyma wszystkie oszczędności w domu, naraża się na kradzież, pożar, inflację czy utratę płynności w codziennym życiu. Odporność finansowa jest zatem kwestią **dywersyfikacji modalnej**, a nie wyboru jednej „prawdziwej" formy pieniądza.

Należy zachować szczególną ostrożność wobec wizji barteru obecnej w książce. W przypadku długotrwałej dezintegracji systemu monetarnego wymiana bezpośrednia może powracać lokalnie, ale rozwinięte gospodarki nie przeskakują automatycznie z płatności kartą do powszechnego handlu puszki fasoli za filtr do wody. Barter obarczony jest klasycznym problemem **double coincidence of wants**: aby doszło do transakcji, obie strony muszą posiadać dokładnie to, czego pragnie druga.

Pieniądz powstał m.in. po to, by radykalnie zredukować koszty takiej koordynacji. Użyteczniejszy od fantazji o postapokaliptycznym rynku jest wniosek, że w kryzysie wzrasta znaczenie **płynności wielokanałowej**: gotówki, sprawnych płatności cyfrowych, kredytu społecznego, wzajemnej pomocy i wymiany usług. W tym miejscu kluczowy staje się kapitał społeczny.

Hydraulik może pomóc sąsiadowi nie dlatego, że wcześniej ustalili kurs wymiany godziny pracy na kilogram ryżu, lecz dlatego, że łączy ich relacja wzajemności. Ekonomiczna antropologia kryzysu podpowiada, że obok rynku i barteru istnieje trzecia kategoria – **reciprocity**. Wspólnoty przetrwania nie są miniaturowymi giełdami towarowymi; to układy, w których dzisiejsza pomoc może zostać odpłacona jutro inną przysługą, bez natychmiastowej kalkulacji równowartości. To kolejny powód, dla którego Positive Prepping różni się od modelu doomsdayowego: w pierwszym sąsiad jest magazynem kompetencji i partnerem wzajemności, w drugim – potencjalnym konkurentem o zapasy.

Blackout ujawnia również zależność systemu miejskiego od **just-in-time logistics**. Supermarket nie jest magazynem żywności dla miasta, lecz końcowym punktem strumienia logistycznego. Stacja paliw nie produkuje paliwa, apteka nie wytwarza leków, a placówka medyczna polega na ciągłych dostawach materiałów, produktów farmaceutycznych, tlenu, usług pralniczych i żywienia oraz odbiorze odpadów.

Indywidualne zapasy jako bufor systemowy

Efektywność gospodarcza ostatnich dekad została osiągnięta w dużej mierze dzięki redukcji zapasów i zwiększeniu częstotliwości dostaw. Jest to racjonalne podejście w stabilnym świecie, lecz drastycznie zmniejsza tzw. slack – margines zasobowy pozwalający systemowi przetrwać zakłócenie. Z perspektywy ekonomii przedsiębiorstwa niewykorzystany magazyn jest kosztem.

Z punktu widzenia resilience engineering ten sam magazyn stanowi option value – opcję nabywaną na wypadek przyszłego kryzysu. W tym miejscu bezpieczeństwo wchodzi w bezpośredni konflikt z efektywnością, gdyż maksymalne wykorzystanie zasobów zazwyczaj oznacza minimalny bufor. System pracujący stale na granicy przepustowości może być ekonomicznie atrakcyjny w czasie normalności i niebezpiecznie kruchy w ekstremum. Ten konflikt opisuje pojęcie efficiency-resilience trade-off. Nie należy go absolutyzować – nowoczesne technologie czasem pozwalają zwiększać oba parametry jednocześnie – jednak nie można udawać, że każda redukcja „marnotrawstwa" jest neutralna dla odporności. To właśnie na tym poziomie Positive Prepping zyskuje znaczenie makroekonomiczne.

Domowy zapas wody, żywności, leków, baterii, gotówki czy alternatywnej łączności to prywatny bufor, którego efekt jest jednak społeczny. Jeśli milion gospodarstw potrafi funkcjonować przez kilkadziesiąt godzin bez natychmiastowej pomocy, służby publiczne mogą skoncentrować ograniczone zasoby na szpitalach, osobach zależnych, domach opieki i miejscach katastrofy. Gdy ten sam milion rodzin nie posiada żadnych zapasów, nawet krótkotrwała awaria infrastruktury może w ciągu kilku godzin wygenerować gigantyczny popyt na wodę, paliwo, informację i transport. Mechanizm ten opisuje pojęcie demand surge: katastrofa drastycznie ogranicza podaż dokładnie wtedy, gdy gwałtownie rośnie popyt. Stacja paliw ma problemy z dostawą, a tysiące kierowców jednocześnie chcą zatankować; sieć komórkowa traci przepustowość w momencie, gdy wszyscy próbują dzwonić; sklepy mierzą się z przerwą w logistyce, podczas gdy ludzie podejmują paniczne zakupy. Służby medyczne mają ograniczoną mobilność, a jednocześnie rośnie liczba urazów i zaostrzeń chorób przewlekłych.

Przygotowanie domowe działa więc nie tylko po stronie podaży bezpieczeństwa, lecz przede wszystkim poprzez spłaszczenie szczytu popytu kryzysowego. Analogia do zarządzania epidemią jest tu kluczowa: celem nie zawsze jest całkowita eliminacja zdarzenia, lecz niedopuszczenie do sytuacji, w której tempo narastania potrzeb przekroczy zdolność systemu do ich obsługi. Odporność społeczna jest zatem częściowo problemem capacity management. Nawet najlepiej wyposażona straż pożarna, pogotowie czy administracja nie są w stanie pomóc wszystkim mieszkańcom dużego miasta w tej samej minucie. Autonomiczność gospodarstwa w pierwszej fazie kryzysu staje się więc

formą solidarności z tymi, którzy autonomiczni być nie mogą. Jednocześnie nie wolno przekształcać tej argumentacji w wygodne alibi dla państwa.

Odporność jako wielopoziomowa architektura kontrolowanej degradacji

Apel do społeczeństwa, by gromadzić zapasy na 72 godziny, jest racjonalny tylko wtedy, gdy stanowi element warstwowej architektury odporności, a nie substytut inwestycji w sieci, ochronę infrastruktury, systemy black-start, rezerwy, łączność czy profesjonalne służby. Gdy państwo przenosi odpowiedzialność za zawodność infrastruktury na obywatela, Positive Prepping może zostać ideologicznie wypaczony w kierunku prywatyzacji ryzyka: dostawca oszczędza na redundancji, regulator toleruje kruchość, a człowiek ma po prostu kupić agregat i beczkę wody.

Odpowiedzialność powinna być zatem wielopoziomowa. Jednostka odpowiada za rozsądne przygotowanie w miarę własnych możliwości. Wspólnota lokalna – za zdolność do wzajemnej pomocy. Samorząd – za organizację ochrony ludności, dostęp do wody, ewakuację, schronienie i komunikację. Operator infrastruktury – za niezawodność, redundancję i procedury odbudowy. Państwo – za normy, strategiczną koordynację, rezerwy oraz bezpieczeństwo systemowe. Z kolei Unia Europejska i systemy transgraniczne powinny odpowiadać za koordynację infrastruktury, która nie kończy się na granicy administracyjnej. Blackout iberyjski pokazał niemal laboratoryjnie, że awaria lokalnych mechanizmów może mieć konsekwencje systemowe, a jej wyjaśnienie wymaga skoordynowania danych, operatorów i regulatorów na poziomie ponadpaństwowym.

Najbardziej dojrzałym pojęciem dla takiej konstrukcji nie jest samowystarczalność, lecz graceful degradation połączona z graceful recovery. System powinien tracić funkcje w sposób uporządkowany i odzyskiwać je według hierarchii ważności. Miasto może utracić iluminacje reklamowe, część handlu czy komfort usług, ale musi zachować wodę, ratownictwo, podstawową łączność i opiekę medyczną. Gospodarstwo może stracić Internet i pełny komfort termiczny, lecz nie powinno z tego powodu natychmiast tracić dostępu do informacji, wody i leków. Odporność nie jest zatem zdolnością do zachowania normalności w każdych warunkach, lecz umiejętnością kontrolowanego przejścia z normalności do trybu ograniczonego, a następnie sprawnego powrotu.

W tym miejscu można precyzyjnie określić relację między robustnością, redundancją a resilience. Robustness pozwala elementowi wytrzymać uderzenie. Redundancy zapewnia alternatywę w razie awarii elementu. Resilience pozwala całemu systemowi dostosować sposób działania, gdy zarówno podstawowy komponent, jak i jego zabezpieczenia okazują się niewystarczające. Jeszcze dalej

znajduje się to, co David Woods określa jako graceful extensibility – zdolność systemu do tworzenia nowych możliwości w sytuacjach przekraczających założenia projektowe. Prepper z precyzyjnym, trzydniowym planem jest przygotowany na znane. Społeczność posiadająca kompetencje, zaufanie i zdolność improwizacji potrafi reagować także na wydarzenia, których scenariusza nikt nie napisał. Blackout przestaje wówczas być opowieścią o świeczkach. Staje się eksperymentem odsłaniającym rzeczywistą architekturę nowoczesności.

Pokazuje on, które funkcje uzależniliśmy od wspólnych punktów awarii, gdzie efektywność wypchnęła redundancję, technologia zastąpiła kompetencję, a prywatna wygoda opiera się na niewidzialnej pracy tysięcy ludzi i urządzeń. Uczy również, że najbardziej niebezpieczny system wcale nie musi być zacofany. Przeciwnie – może być niezwykle nowoczesny, wydajny i zautomatyzowany, a zarazem tak ściśle sprzężony, że małe zaburzenie swobodnie przenika przez jego kolejne warstwy. Właściwym przeciwieństwem blackoutu nie jest światło, lecz zdolność zachowania funkcji mimo jego utraty.

Ta perspektywa otwiera kolejny, trudniejszy poziom analizy. W energetyce można obliczać przepływy, częstotliwość i napięcie. W kryzysie społecznym zawodzi jednak nie tylko technika, lecz także zaufanie, ceny, reguły wymiany, autorytet instytucji i wspólny obraz rzeczywistości. Następnym krokiem powinno być zatem przejście od blackoutu technicznego do blackoutu społecznego: pandemii, niedoborów, inflacji, paniki zakupowej czy dezinformacji – sytuacji, w których krytycznym zasobem przestaje być kilowatogodzina, a staje się nim zdolność zbiorowości do utrzymania koordynacji mimo narastającej nieufności.

> Właściwym przeciwieństwem blackoutu nie jest samo przywrócenie prądu, lecz zdolność zachowania kluczowych funkcji cywilizacyjnych w momencie jego utraty. Prawdziwym wyzwaniem pozostaje jednak pytanie, czy potrafimy zbudować odporność społeczną równie trwałą jak ta techniczna. Czy w obliczu systemowej awarii, gdy zgasną ekrany, będziemy w stanie utrzymać koordynację i zaufanie, zanim zapadnie ostateczny blackout społeczny?

Inspiracje

[1] 

"The Emergency Playbook" Amy Edelman

Ten Speed Press | ISBN: 9780593837658

Amy Holman Edelman (ur. 1 listopada 1958 r.) jest amerykańską autorką, dziennikarką i specjalistką ds. public relations. Pracowała w korporacyjnych działach public relations i marketingu dla dużych marek lifestylowych i detalicznych, zanim w 2009 roku założyła IndieReader. Jako założycielka i prezes IndieReader, Edelman stworzyła znaną platformę recenzji i serwis informacyjny, poświęcony ocenie i promocji niezależnej i samodzielnie publikowanej literatury. Jako pisarka i powieściopisarka non-fiction, do jej najważniejszych dzieł należą „Mała czarna sukienka" (1997), kulturowo-wizualna historia zgłębiająca wpływ kultowego elementu garderoby na modę i media, oraz „Manless in Montclair" (2007), częściowo autobiograficzna powieść o żałobie, wdowieństwie i randkowaniu na przedmieściach. Jej teksty i wystąpienia medialne były prezentowane w takich mediach jak „The New York Times", „USA Today" i programie „Today" stacji NBC.

Amy Holman Edelman (born November 1, 1958) is an American author, journalist, and public relations professional. She worked in corporate public relations and marketing for major lifestyle and retail brands before founding IndieReader in 2009. As founder and president of IndieReader, Edelman created a prominent review platform and discovery service dedicated to assessing and promoting independently and self-published literature. As a non-fiction writer and novelist, her notable works include 'The Little Black Dress' (1997), a cultural and visual history exploring the influence of the iconic wardrobe staple in fashion and media, and 'Manless in Montclair' (2007), a semi-autobiographical novel examining grief, widowhood, and suburban dating. Her writings and media appearances have been featured in outlets including The New York Times, USA Today, and NBC's Today show.

IndieReader

Literatura uzupełniająca

Książki

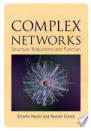
Książki autorów przywoływanych i literatura pokrewna:



[1] "The Social Psychology of Civil Defense"

Ronald W. Perry

1982 | Lexington Books



[2] "Complex Networks"

Shlomo Havlin

Cambridge University Press | ISBN: 9781139489270



[3] "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



[4] "Normal Accidents"

Charles Perrow

Princeton University Press | ISBN: 9780691004129



[5] "Family Tsunami Preparedness: The Ultimate Home Safety Checklist"

Jade Summers

Jade Summers

Artykuły naukowe

Prace autorów przywoływanych w tekście:

[1] "The Protective Action Decision Model: Theoretical Modifications and Additional Evidence"

Michael K. Lindell, Ronald W. Perry

2011 | Risk Analysis | DOI: 10.1111/j.1539-6924.2011.01647.x

Źródło

[2] "Households' Perceived Personal Risk and Responses in a Multihazard Environment"

Michael K. Lindell, Seong Nam Hwang

2008 | Risk Analysis | DOI: 10.1111/j.1539-6924.2008.01032.x

Źródło

[3] "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process"

Ronald W. Perry, Michael K. Lindell

2003 | Disasters | DOI: 10.1111/j.0361-3666.2003.00237.x

Źródło

[4] "Communicating Environmental Risk in Multiethnic Communities"

Michael K. Lindell, Ronald W. Perry

2004 | Sage eBooks | DOI: 10.4135/9781452229188

Źródło

[5] "Attutude-action consistency and social policy related to nuclear technology"

M.K. Lindell, R.W. Perry, M. Greene

1980 | DOI: 10.2172/7041007

Źródło

[6] "Volcanic Risk Perception and Adjustment in a Multi-Hazard Environment"

Ronald W. Perry, Michael K. Lindell

2013 | DOI: 10.2139/ssrn.2282183

Źródło

[7] "The Effects of Ethnicity on Evacuation Decision-Making"

Ronald W. Perry, Michael K. Lindell

1991 | International Journal of Mass Emergencies & Disasters | DOI: 10.1177/028072709100900103

Źródło

[8] "EBP Is Just the Beginning: Defining a National School Social Work Practice and Research Agenda"

Michael S. Kelly

2008 | The Domains and Demands of School Social Work Practice | DOI: 10.1093/acprof:oso/9780195343304.003.0008

Źródło

[9] "Introduction: School Social Work in the 21st Century—Making Evidence-Based Practice (EBP) Work in School Social Work Practice"

Michael S. Kelly

2008 | The Domains and Demands of School Social Work Practice | DOI: 10.1093/acprof:oso/9780195343304.003.0001

Źródło

[10] "Catastrophic cascade of failures in interdependent networks"

Sergey V. Buldyrev, Roni Parshani, Gerald Paul, Eugene Stanley, Shlomo Havlin

2010 | Nature | DOI: 10.1038/nature08932

Źródło

[11] "Cascading failures in networks of networks linked by directional and bidirectional hyperlinks."

David S. Roth, Bo Tong, A. Bashan, S. Buldyrev

2025 | Physical Review E | DOI: 10.1103/physreve.111.014315

Źródło

[12] "Cascading failures in bipartite networks with directional support links."

Bo Tong, David S. Roth, S. Buldyrev

2024 | Physical Review E | DOI: 10.1103/physreve.109.064307

Źródło

[13] "Resilience of the Internet to Random Breakdowns"

Reuven Cohen C, Keren Erez, Daniel ben-Avraham, Shlomo Havlin

2000 | Physical Review Letters | DOI: 10.1103/physrevlett.85.4626

Źródło

[14] "Dynamics of cascades in spatial interdependent networks."

B. Gross, I. Bonamassa, S. Havlin

2023 | Chaos | DOI: 10.1063/5.0165796

Źródło

[15] "Normal Accidents: Living with High-Risk Technologies."

Larry L. Cummings, Charles B. Perrow

1984 | Administrative Science Quarterly | DOI: 10.2307/2392945

Źródło

[16] "THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS. By Mancur Olson, Jr. Rev. ed. New York: Schocken Books, 1971. 184 pp. $2.45"

Charles B. Perrow, Mancur Olson

1973 | Social Forces | DOI: 10.1093/sf/52.1.123

Źródło

[17] "The Significance of Perrow's Normal Accidents: Living with High-Risk Technologies"

Karlene H. Roberts, Charles Perrow

1989 | The Academy of Management Review | DOI: 10.2307/258423

Źródło

[18] "Barriers and Accident Prevention"

Erik Hollnagel

2016 | Routledge eBooks | DOI: 10.4324/9781315261737

Źródło

[19] "Joint Cognitive Systems: Foundations of Cognitive Systems Engineering"

Erik Hollnagel, David D. Woods

2005 | Thammasat University Digital Collections

Źródło

[20] "Joint Cognitive Systems"

Erik Hollnagel, David D. Woods

2005 | CRC Press eBooks | DOI: 10.1201/9781420038194

Źródło

[21] "Resilience Engineering in Practice a Guidebook"

Erik Hollnagel, Jean Pariès, Woods David, D., John Wreathall

2010 | HAL

Źródło

[22] "Four concepts for resilience and the implications for the future of resilience engineering"

David D. Woods

2015 | Reliability Engineering & System Safety | DOI: 10.1016/j.ress.2015.03.018

Źródło

[23] "How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control"

Nadine B. Sarter, David D. Woods

1995 | Human Factors The Journal of the Human Factors and Ergonomics Society | DOI: 10.1518/001872095779049516

Źródło

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System
Fundacja Dobre Państwo © 2026
Article ID: 40e15aaa-b180-4059-b76d-4ede3cfefa3f