Architektura katastrofy: Teoria Normalnych Wypadków Charlesa Perrowa

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje Teorię Normalnych Wypadków (NAT) autorstwa Charlesa Perłowa, która zakłada, że w systemach o wysokiej złożoności interakcyjnej i ścisłym sprzężeniu katastrofy są nieuniknione. Autor argumentuje, że wypadki nie są wynikiem pojedynczych błędów ludzkich, lecz produktem struktury systemu, w której drobne awarie nakładają się na siebie w nieprzewidywalny sposób. Tekst podważa tradycyjne podejście do zarządzania ryzykiem, które często szuka kozła ofiarnego w operatorze, ignorując błędy projektowe i organizacyjne. Persów ostrzega, że nadmierne mnożenie zabezpieczeń może paradoksalnie zwiększyć komplikację systemu, tworząc nowe ścieżki potencjalnych awarii, co czyni katastrofę immanentną cechą architektury nowoczesnych technologii.

The article analyzes the Normal Accident Theory (NAT) by Charles Perrow, which posits that in systems with high interactive complexity and tight coupling, disasters are inevitable. The author argues that accidents are not the result of single human errors, but a product of the system's structure, where minor failures overlap in unpredictable ways. The text challenges the traditional approach to risk management, which often seeks a scapegoat in the operator while ignoring design and organizational flaws. Perrow warns that excessively multiplying safeguards can paradoxically increase system complication, creating new paths for potential failure, making disaster an inherent feature of the architecture of modern technologies.

Czy katastrofy są jedynie wynikiem nieszczęśliwego zbiegu okoliczności lub ludzkiej niekompetencji? Niniejszy artykuł analizuje Teorię Normalnych Wypadków (NAT) Charlesa Perrowa, stawiając prowokacyjną tezę: w określonych typach systemów katastrofa jest immanentną cechą ich architektury. Autor dowodzi, że gdy złożoność interakcyjna (nieprzewidywalne relacje między elementami) spotyka się ze ścisłym

sprzężeniem (brak czasu i buforów na reakcję), system staje się pułapką, w której drobne, nieistotne awarie splotą się w nieliniową konfigurację prowadzącą do nieuchronnego kolapsu. Tekst dekonstruuje mit „błędu ludzkiego", wykazując, że operator jest często jedynie pierwszym świadkiem niewydolności projektu, a tradycyjne metody zarządzania ryzykiem – takie jak mnożenie procedur czy redundancja zabezpieczeń – mogą paradoksalnie zwiększać złożoność i generować nowe ścieżki awarii. To studium nad pychą nowoczesnej technologii i organizacji, które w imię efektywności usuwają „luz" systemowy, zamieniając odporność na kruchą sprawność, która rozpada się gwałtownie w stanach granicznych.

SŁOWA KLUCZOWE

Teoria Normalnych Wypadków | Charles Perrow | NAT - Normal Accident Theory | złożoność interakcyjna | ścisłe sprzężenie | model DEPOSE | architektura systemu | błąd operatora | wypadek systemowy | redundancja papierowa | analiza powypadkowa | interakcje nieliniowe | bezpieczeństwo systemów złożonych | zarządzanie ryzykiem

Katastrofa jako immanentna cecha architektury systemu

Są katastrofy, które zaczynają się od huku, płomieni i głośnych nagłówków. Są też takie, które biorą początek w rzeczach śmiesznie małych: pękniętym dzbanku do kawy, zatrzaśniętych kluczach, zepsutym samochodzie sąsiada, strajku autobusów czy mieście, w którym nagle nie ma ani jednej wolnej taksówki. Nie ma tu jeszcze tragedii – jest tylko poranek człowieka, który chciał zdążyć na ważną rozmowę. Dzbanek pęka: drobiazg. Człowiek się spieszy: normalne. Klucze zostają w mieszkaniu: kłopot, ale przecież istnieje zapasowy komplet. Tyle że ten komplet jest u znajomego. Sąsiad mógłby pomóc, ale akurat zepsuł mu się samochód.

Autobus nie jedzie przez strajk. Taksówka pozostaje nieosiągalna, bo wszyscy inni właśnie próbują ratować swój poranek. Żaden z tych elementów z osobna nie stanowi katastrofy; razem tworzą pułapkę. W tej drobnej anegdocie ukryta jest cała powaga teorii Charlesa Perrowa. Normalny wypadek nie musi wynikać z wielkiego błędu. Może zacząć się od małej awarii, która spotyka drugą małą awarię, trzecią presję, czwartą zależność i piątą iluzję, że „przecież mamy zabezpieczenia".

Wtedy system pęka nie dlatego, że jeden element był wadliwy, lecz dlatego, że elementy zaczynają oddziaływać na siebie w sposób, którego nikt nie przewidział.

To jest istota Teorii Normalnych Wypadków (NAT – Normal Accident Theory). Perrow nie twierdzi, że katastrofy są codzienne czy moralnie dopuszczalne. Słowo „normalny" oznacza tu coś bardziej niepokojącego: w pewnych typach systemów wypadek jest normalny, ponieważ wynika z ich struktury. Jest konsekwencją architektury, a nie wyłącznie skutkiem czyjejś nieuwagi. W systemie prostym awaria ma adres – można wskazać konkretną śrubę, zawór, człowieka lub procedurę.

W systemie złożonym awaria ma biografię zbiorową. Rodzi się z interakcji; nie jest pojedynczym zdarzeniem, lecz splotem. To nie jeden klocek domina przewraca następny w eleganckiej kolejności, lecz raczej sieć, w której kilka pozornie odległych punktów nagle zaczyna drgać jednocześnie. Perrow opiera swoją teorię na dwóch pojęciach: złożoności interakcyjnej i ścisłym sprzężeniu. Pierwsze oznacza, że elementy systemu mogą wchodzić w nieoczekiwane, ukryte i nieliniowe relacje. Drugie zaś, że system nie daje czasu ani przestrzeni na spokojne opanowanie problemu. Gdy te dwa warunki wystąpią razem, katastrofa przestaje być czymś zewnętrznym – staje się jedną z możliwych form działania systemu.

Choć brzmi to jak ponura filozofia technologii, w rzeczywistości jest to praktyczna socjologia organizacji. Perrow sugeruje: przestańmy traktować każdą katastrofę jak moralitet o jednym nieostrożnym człowieku przy pulpicie. Czasem operator nie jest sprawcą. Jest pierwszym świadkiem nieczytelności systemu. Nie „zawiódł systemu" – to system dostarczył mu fałszywy obraz świata i wymusił natychmiastowe działanie.

Tu zaczyna się zasadniczy spór Perrowa z klasycznym językiem zarządzania ryzykiem. Organizacje kochają kategorię "błędu ludzkiego", bo jest wygodna. Ma twarz, nazwisko i stanowisko służbowe; można ją po prostu wpisać do raportu. Błąd człowieka przynosi ulgę: winny został znaleziony, procedurę poprawiono, szkolenie przeprowadzono, a zarząd mógł odetchnąć. System może działać dalej – najlepiej szybciej, taniej i z większą wydajnością.

Katastrofa jako produkt architektury systemu, a nie błąd człowieka

Perrow stawia jednak niewygodne pytanie: a jeśli to nie człowiek był głównym problemem? A jeśli „błąd operatora" jest tylko wygodnym sposobem na ukrycie błędu projektu, organizacji, presji ekonomicznej czy nadmiernej złożoności? Co jeśli katastrofa nie była odstępstwem od normy, lecz

właśnie produktem normalnego działania systemu? NAT jest zatem teorią antykozła ofiarnego. Odbiera ona komfort prostego oskarżenia i nie pozwala zamknąć analizy stwierdzeniem: „ktoś nie dopilnował". Owszem, ktoś mógł nie dopilnować, ale głębsze pytanie brzmi: dlaczego system zaprojektowano tak, że jedno przeoczenie mogło zbiegnąć się w czasie z innym niedopatrzeniem, fałszywym wskaźnikiem, presją czasu, brakiem bufora, wadliwą procedurą i ukrytym sprzężeniem? Normalny wypadek staje się więc lekcją pokory.

Pokazuje on, że nowoczesne systemy mogą przekraczać zdolność rozumienia osób, które je obsługują, regulują i nadzorują. Nie wynika to z ludzkiej głupoty, lecz z faktu, że system jest zbyt gęsty, szybki, powiązany i nieprzejrzysty. To labirynt, który sam sobie dobudowuje korytarze. Stąd prosty, choć trudny do zaakceptowania wniosek Perrowa: nie wystarczy wzmacniać dyscypliny, mnożyć procedur czy dokładać zabezpieczeń. W niektórych systemach każde nowe zabezpieczenie staje się kolejnym elementem struktury, a tym samym nowym potencjalnym miejscem awarii i ścieżką nieprzewidzianych interakcji. Redundancja może ratować, ale może też komplikować. A komplikacja w połączeniu z presją czasu lubi udawać bezpieczeństwo aż do momentu, gdy przestaje nim być. Tematem artykułu nie jest więc pytanie: „dlaczego ludzie popełniają błędy?", lecz: dlaczego pewne systemy produkują sytuacje, w których błąd staje się nieuchronny, niewidoczny albo niemożliwy do naprawienia na czas?

Pytanie to dotyczy elektrowni jądrowych, zakładów chemicznych, lotnictwa, transportu morskiego i misji kosmicznych. Odnosi się jednak również do państwa, administracji, ochrony zdrowia, systemów cyfrowych, rynku finansowego, energetyki, partii politycznych czy samorządów – każdej instytucji dostatecznie złożonej, by nikt nie ogarniał jej w całości, i dostatecznie ciasno sprzężonej, by jedna decyzja natychmiast wywoływała konsekwencje w kilku innych miejscach. Normalne wypadki nie są bowiem tylko teorią o maszynach; są teorią o naszej pysze wobec systemów, które sami zbudowaliśmy. Jeśli pierwsza lekcja Charlesa Perrowa brzmi: nie szukaj zbyt szybko jednego winnego, to druga mówi: rozłóż system na warstwy, zanim zaczniesz wydawać wyroki. Katastrofa systemowa rzadko przychodzi jednymi drzwiami. Zwykle wchodzi kilkoma naraz – czasem nie pukając, czasem udając drobny kłopot techniczny, a czasem przebierając się za procedurę bezpieczeństwa. Dlatego w analizie normalnych wypadków pomocny jest model DEPOSE. To akronim obejmujący sześć składników systemu: Design, Equipment, Procedures, Operators, Supplies, Environment – czyli projekt, sprzęt, procedury, operatorów, zaopatrzenie i środowisko.

W każdym z tych obszarów może pojawić się usterka. Sens teorii Perrowa polega jednak na tym, że żadna z nich nie musi być sama w sobie wystarczająca do wywołania katastrofy. Dopiero ich splot tworzy sytuację, której system nie potrafi już opanować. Pierwszym elementem jest projekt. To architektura systemu: rozmieszczenie wskaźników, logika pulpitów, układ pomieszczeń, schematy

przepływu informacji, zależności między podsystemami, reguły działania automatyki i konstrukcja zabezpieczeń.

Projekt bywa niewinny tylko na papierze. W praktyce może zawierać błędy, które latami śpią spokojnie, by obudzić się w sytuacji kryzysowej. Źle rozmieszczony wskaźnik, nielogiczny pulpit czy zbyt podobne sygnały alarmowe same w sobie nie są katastrofą. Jednak gdy operator w ciągu kilkunastu sekund musi odczytać stan instalacji, odróżnić alarm rzeczywisty od wtórnego, zrozumieć zachowanie automatyki i podjąć decyzję – wtedy projekt przestaje być tłem i staje się współuczestnikiem zdarzenia. To on decyduje o tym, co operator może zobaczyć, jak szybko to zrozumie i czy ma szansę odróżnić przyczynę od skutku. W systemach wysokiego ryzyka nie jest to kwestia estetyki ergonomii, lecz życia, śmierci i odpowiedzialności. Dlatego Perrow uczy sceptycyzmu wobec późniejszego moralizowania. Jeśli system przekazał operatorowi fałszywy obraz, nie wystarczy zapytać, dlaczego ten źle zareagował; trzeba zapytać, dlaczego system zaprojektowano tak, że w chwili kryzysu mówił półprawdami. W zwykłej organizacji analogia jest prosta: projekt to nie tylko technologia, ale także statut, regulamin, struktura kompetencji, obieg dokumentów, system raportowania i hierarchia decyzji. Źle zaprojektowana organizacja potrafi wyprodukować chaos nawet wtedy, gdy każdy pracownik jest rozsądny, punktualny i pełen dobrej woli. Dobra wola w złym projekcie jest jak elegancki parasol w huraganie: miło, że jest, ale dachów nie zatrzyma.

Sprzęt i procedury jako elementy sieci interakcji

Drugim składnikiem jest sprzęt. Tutaj intuicja podpowiada najszybciej, bo sprzęt po prostu ulega awariom: zawory się zacinają, pompy przestają działać, generatory zawodzą, wskaźniki kłamią, uszczelki puszczają, przewody przeciekają, a układy zasilania tracą stabilność. Klasyczne myślenie o awarii często zaczyna się i kończy właśnie w tym punkcie: coś się zepsuło. Perrow idzie jednak dalej. Pojedyncza usterka sprzętowa rzadko tłumaczy katastrofę systemową; jest ona dopiero początkiem pytania. Należy zapytać: z czym ta usterka weszła w interakcję?

Czy uruchomiła fałszywy alarm? Czy wyłączyła zabezpieczenie, czy może zamaskowała inny problem? Czy zmusiła operatora do działania na podstawie błędnych danych lub uderzyła jednocześnie w kilka funkcji poprzez wspólny tryb awarii? W systemie liniowym awaria sprzętu jest przejrzysta: maszyna staje, produkcja zamiera i wiadomo, gdzie leży źródło problemu. W systemie interakcyjnie złożonym usterka może ukryć się za inną awarią, wywołać skutki w odległym podsystemie lub udawać zupełnie inny typ błędu. Sprzęt nie jest więc tylko przedmiotem – jest uczestnikiem sieci. A element sieci rzadko psuje się w izolacji.

Trzecim składnikiem są procedury. W języku organizacyjnym procedura otoczona jest aurą bezpieczeństwa: porządkuje, ujednolica i chroni przed improwizacją. Ma być dowodem na to, że ktoś „zarządza ryzykiem". Perrow nie neguje potrzeby procedur, lecz obnaża ich ciemną stronę.

Procedura może być błędna, nieaktualna, zbyt ogólna, nadmiernie szczegółowa lub sprzeczna z inną instrukcją. Może działać bez zarzutu w sytuacjach typowych, by zawieść w momencie, dla którego nie została napisana. Najgroźniejszy bywa jednak nie brak procedur, lecz ich nadmiar – stan, w którym organizacja produkuje tak wiele wytycznych, że w sytuacji kryzysowej człowiek nie wie już, której ma słuchać. Procedura jest wartościowa, gdy redukuje niepewność; staje się groźna, gdy redukuje myślenie.

W systemach ściśle sprzężonych operator często nie ma czasu na studiowanie instrukcji – musi działać szybko. Jednak w systemach złożonych sytuacja może wymagać interpretacji, a nie automatycznego wykonania. Tu pojawia się paradoks: sprzężenie wymusza posłuszeństwo, podczas gdy złożoność wymaga rozumienia. Procedura może zatem postawić człowieka w tragicznej pozycji: jeśli jej przestrzega, pogarsza sytuację; jeśli ją łamie, bierze na siebie pełną odpowiedzialność bez gwarancji sukcesu.

W życiu instytucjonalnym przejawia się to codziennie. Organizacja może posiadać segregatory ryzyka, które w praktyce funkcjonują jako dekoracja bezpieczeństwa – ładna i ciężka, lecz zupełnie niepotrzebna w momencie, gdy system zaczyna płonąć. Wniosek jest brutalny, ale użyteczny: procedura nie jest mądrością, a jedynie pamięcią organizacji. A pamięć bez rozumu potrafi recytować błędy z imponującą pewnością siebie.

Operatorzy, zaopatrzenie i środowisko jako elementy architektury

Czwartym elementem są operatorzy. To ludzie na pierwszej linii: piloci, dyspozytorzy, pracownicy elektrowni, załogi statków, technicy, lekarze, urzędnicy obsługujący krytyczne procesy, dyżurni, analitycy czy koordynatorzy. W raportach powypadkowych operatorzy często pojawiają się jako winni. „Nie zauważyli". „Źle zinterpretowali". „Nie wykonali procedury". „Zareagowali za późno". Taka narracja jest kusząca, ponieważ upraszcza świat; wskazuje bohatera negatywnego i pozwala szybko zamknąć analizę. Wina zostaje zlokalizowana w człowieku, a system odzyskuje niewinność.

Perrow uważa to za jedno z najpoważniejszych zafałszowań. Nie twierdzi, że ludzie są nieomylni – oczywiście popełniają błędy. Jednak w systemach normalnych wypadków wiele z nich jest wymuszonych przez samą sytuację: fałszywe wskaźniki, presję czasu, sprzeczne alarmy, brak

pełnego obrazu, wadliwe procedury, naciski produkcyjne, zmęczenie, hierarchię czy strach przed zatrzymaniem procesu. Operator nie działa w podręczniku. Operator działa w mgławicy sygnałów.

Dlatego należy odróżnić błąd jako fakt od winy jako interpretacji. Człowiek mógł nacisnąć niewłaściwy przycisk, ale dlaczego ten przycisk znajdował się właśnie tam? Dlaczego system nie potwierdził realnego stanu? Dlaczego alarmy były sprzeczne, a czas reakcji tak krótki? Dlaczego organizacja wcześniej zignorowała podobne sygnały ostrzegawcze i dlaczego presja wydajności przeważyła nad ostrożnością? Jeżeli po katastrofie wszystko da się wyjaśnić jednym zdaniem: „operator popełnił błąd", to najpewniej nie wykonano analizy, tylko odprawiono rytuał. W administracji publicznej operatorem bywa urzędnik przy okienku, lekarz na dyżurze, nauczyciel, policjant w terenie, pracownik socjalny, sędzia referent czy informatyk utrzymujący system – także samorządowiec podejmujący decyzje pod presją sprzecznych przepisów. To oni najczęściej wystawieni są na gniew obywateli, mediów i polityków, choć nie zawsze są źródłem awarii. Często są jedynie miejscem, w którym awaria staje się widoczna. System lubi obwiniać najniższy poziom, bo najwyższy poziom pisze raporty.

Piątym elementem jest zaopatrzenie. W technologii to paliwo, chłodziwo, części zamienne czy stabilne źródło energii. W organizacji społecznej: kadry, fundusze, dane, czas, kompetencje, dostęp do informacji oraz zaplecze prawne. Zaopatrzenie pozostaje niewidzialne, dopóki działa – nikt nie chwali wody chłodzącej za to, że płynie.

Nikt nie dostrzega rezerw kadrowych, dopóki nie wybuchnie epidemia, kryzys lub wojna. Nikt nie myśli o jakości danych, dopóki błędny rejestr nie wygeneruje złej decyzji. A jednak brak zasobu może uruchomić lawinę. W systemach ściśle sprzężonych nie ma czasu na oczekiwanie na dostawę; bez części zamiennej brakuje obejścia. Gdy brakuje personelu, człowiek pracuje dłużej i bardziej nerwowo. Brak danych zmusza do decyzji opartych na domysłach, a brak pieniędzy przesuwa konserwację „na później". To „później" bywa elegancką nazwą dla przyszłej katastrofy. W tym punkcie Perrow dotyka polityki ekonomicznej organizacji.

Wypadki systemowe nie są wyłącznie techniczne; wynikają z decyzji o oszczędzaniu, przyspieszaniu prac, redukcji obsady czy ignorowaniu ostrzeżeń. Braki w zaopatrzeniu rzadko są neutralne – zwykle ktoś wcześniej uznał rezerwę za koszt, a nie warunek przetrwania. W języku zarządu brzmi to niewinnie: optymalizacja. W języku NAT oznacza to usuwanie luzu z systemu. System bez luzu działa szybciej i taniej, aż do chwili, gdy potrzebuje właśnie tego marginesu, który wcześniej uznano za marnotrawstwo.

Szóstym składnikiem jest środowisko. To wszystko poza formalną granicą systemu: pogoda, strajki, naciski polityczne, media, kryzysy gospodarcze czy zmiany prawne. Środowisko obala złudzenie, że

system można analizować jak zamkniętą maszynę. W rzeczywistości systemy są zanurzone w innych strukturach: elektrownia działa w gospodarce, gospodarce towarzyszy polityka, polityce media, mediom emocje społeczne, a tym wszystkim – kalendarz wyborczy i brak cierpliwości. W anegdocie Perrowa środowiskiem jest strajk autobusów i brak taksówek. Dla bohatera to okoliczność zewnętrzna, lecz w krytycznym momencie staje się ona częścią systemu awarii. Środowisko nie musi powodować katastrofy bezpośrednio; wystarczy, że domknie pułapkę.

W państwie środowisko jest jeszcze bardziej nieprzewidywalne. Reforma może wyglądać dobrze na slajdzie, dopóki nie zderzy się z niedoborem kadr, oporem zawodowym, histerią medialną czy obywatelami, którzy – zupełnie bezczelnie – mają własne życie i nie zachowują się jak punkty w prezentacji. Systemy publiczne zawodzą często nie dlatego, że zabrakło planu, ale dlatego, że był on napisany dla świata spokojniejszego niż rzeczywisty.

Model DEPOSE nie jest zwykłą checklistą; jego wartość polega na wymuszeniu wielowarstwowego spojrzenia. Awaria rzadko jest wyłącznie „techniczna", „ludzka" czy „środowiskowa". W normalnym wypadku te kategorie się przenikają: projekt wprowadza błąd informacyjny, sprzęt generuje mylący sygnał, procedura wymusza złą reakcję, a operator działa racjonalnie w granicach fałszywego obrazu. Zaopatrzenie nie daje rezerwy, a środowisko skraca czas i zwiększa presję.

Katastrofa jako konfiguracja relacji między elementami

Wtedy pytanie „co było przyczyną?" staje się zbyt prymitywne. Lepsze brzmi: jakie relacje między elementami sprawiły, że problem przestał być lokalny i stał się systemowy? Ma to kluczowe znaczenie także dla analizy instytucji. Gdy zawodzi państwo, organizacja albo urząd, najczęściej słyszymy sześć osobnych opowieści: o źle napisanym prawie, słabej technologii, wadliwych procedurach, niekompetentnych ludziach, braku środków i presji zewnętrznej. Perrow kazałby powiedzieć: nie rozdzielajcie tego za szybko. Sprawdźcie, jak te elementy się połączyły. Bo katastrofa może nie mieszkać w żadnym z nich osobno. Może mieszkać między nimi. To „między" jest najgroźniejszym miejscem w nowoczesnym świecie.

Zwykły wypadek nie jest sumą błędów, lecz konfiguracją. To dlatego organizacje tak często wyciągają błędne wnioski. Po katastrofie naprawiają jeden element: wymieniają zawór, poprawiają formularz, szkolą operatora, dopisują procedurę, kupują nowy system lub zmieniają kierownika. Każda z tych reakcji może być potrzebna, ale żadna nie wystarczy, jeśli nie zmieni się architektura relacji. Bo jeśli system nadal jest nieprzejrzysty, szybki, ciasno sprzężony, niedofinansowany i pełen ukrytych zależności, to nowa procedura może być tylko świeżą farbą na pękającej ścianie.

DEPOSE uczy więc dojrzałej nieufności. Nieufności wobec prostych winnych, magicznych zabezpieczeń i organizacyjnych rytuałów po awarii. Nieufności wobec raportów, które już po trzech stronach stwierdzają, że „zawiódł człowiek". W rzeczywistości często zawodzi konfiguracja człowieka, maszyny, procedury, zasobu, projektu i środowiska. Człowiek bywa ostatnim ogniwem, ale ostatnie ogniwo nie zawsze jest przyczyną łańcucha. Model DEPOSE pokazuje, z czego zbudowany jest system i którędy może wejść awaria, lecz nie wyjaśnia jeszcze, dlaczego w jednych systemach usterki pozostają lokalne, a w innych rozlewają się jak atrament w wodzie.

Do tego potrzebne są dwa centralne pojęcia Perrowa: złożoność interakcyjna i ścisłe sprzężenie. W następnej części przejdę do pierwszego z nich. Pokażę, czym różni się system liniowy od systemu interakcyjnie złożonego, dlaczego „ukryte ścieżki" są groźniejsze niż widoczne usterki oraz czemu dodatkowe zabezpieczenia czasem przypominają dokładanie korytarzy do labiryntu. Nie chodzi tu po prostu o to, że system jest „skomplikowany" – to słowo bywa mylące.

Złożoność interakcyjna jako bariera poznawcza

Skomplikowany może być zegarek mechaniczny, kodeks podatkowy, silnik samochodu czy struktura dużego urzędu. Jednak samo skomplikowanie nie oznacza jeszcze najgroźniejszego typu ryzyka. Dla Perrowa kluczowe jest to, czy elementy systemu mogą wejść ze sobą w nieoczekiwane, nieliniowe i trudne do zinterpretowania interakcje. To właśnie definiuje złożoność interakcyjną.

System niebezpieczny nie jest po prostu duży – on jest nieprzejrzysty. Zagrożenie zaczyna się tam, gdzie części systemu „rozmawiają" kanałami niewidocznymi dla operatorów, projektantów czy kadry zarządzającej podczas normalnej pracy. Najłatwiej zrozumieć tę naturę poprzez kontrast z systemem liniowym. W takim układzie zdarzenia następują w przewidywalnej kolejności, a proces ma przejrzysty przebieg: element A wpływa na B, B na C, a C na D. Gdy coś zawodzi, skutki są zazwyczaj zrozumiałe i łatwe do zlokalizowania. Typowym przykładem jest linia montażowa – jeśli jedna stacja przestaje działać, półprodukty piętrzą się przed nią, a kolejne stanowiska czekają na dostawę. Widać dokładnie, gdzie powstał korek i co należy naprawić; można zatrzymać fragment procesu, wymienić część lub przesunąć ludzi.

System liniowy również może być groźny – kopalnia może zabijać, tama pęknąć, a fabryka eksplodować. Jednak sama struktura liniowa sprawia, że awaria częściej przypomina błąd konkretnego komponentu niż wypadek systemowy. Jest dramatyczna, lecz zasadniczo zrozumiała. Można wskazać słaby materiał, błąd konstrukcyjny, zaniechanie kontroli lub przeciążenie. W systemie liniowym katastrofa ma biografię prostszą. Nie zawsze jest ona łatwa czy banalna, ale bywa mniej tajemnicza; jej mechanizm częściej przypomina pęknięcie łańcucha niż samorzutne

splątanie sieci. Dzięki temu organizacja zyskuje coś niezwykle cennego: widzialność przyczyn, a ta daje szansę na naukę. Jeśli wiemy, co zawiodło i widzimy przebieg awarii, możemy go odtworzyć i poprawić błędy. System dający czas i obraz pozwala stać się mądrzejszym po porażce.

W systemie interakcyjnie złożonym jest inaczej. Awaria nie idzie prostym korytarzem. Ona przeskakuje. Czasem zaczyna się w jednym miejscu, by objawić się gdzie indziej; jedna usterka może maskować drugą, a dwie niegroźne awarie razem stworzyć zjawisko jakościowo nowe. System potrafi pokazać operatorowi skutek jako przyczynę, ukrywając tę właściwą pod warstwą fałszywych sygnałów. Tutaj intuicja typu „znajdź zepsuty element" zawodzi, bo uszkodzony komponent może być zaledwie początkiem. Prawdziwy problem polega na tym, że wszedł on w relację z innym elementem, procedurą, wskaźnikiem, automatem, presją środowiskową lub błędną interpretacją człowieka.

W systemie złożonym awaria nie tyle się rozprzestrzenia, co przeobraża. To zasadnicza różnica: o ile w układzie liniowym awaria pompy po prostu zatrzymuje przepływ, o tyle w systemie złożonym może ona zmienić odczyty, uruchomić zabezpieczenia i wpłynąć na ciśnienie, co wywoła reakcję automatyki i skłoni operatora do korekty – a ta z kolei pogorszy stan zupełnie innego podsystemu.

Wtedy przyczyna i skutek zaczynają tańczyć menueta w ciemnym pokoju – a potem komisja śledcza dziwi się, że operator nie znał choreografii. Złożoność interakcyjna jest zatem problemem poznawczym. System generuje sytuacje, których nie da się natychmiast rozpoznać. Operator nie widzi „rzeczy samej", lecz wskaźniki, alarmy i komunikaty – często sprzeczne, opóźnione lub pośrednie. Musi budować model rzeczywistości na podstawie danych, które same mogą być już skutkiem awarii. To jedna z najważniejszych lekcji Perrowa: w kryzysie system złożony nie tylko zawodzi technicznie; on zawodzi poznawczo.

Fizyczna i strukturalna bliskość generuje nieprzewidziane interakcje

Nie daje to ludziom pewnego obrazu samego siebie. Jednym ze źródeł złożoności interakcyjnej jest bliskość fizyczna. Elementy systemu mogą znajdować się obok siebie, choć w założeniach projektowych nie są traktowane jako powiązane funkcjonalnie. Ich sąsiedztwo wydaje się nieistotne – do czasu. W analizach Perrowa pojawiają się przykłady, w których sama bliskość instalacji, przewodów, zbiorników czy pomieszczeń stwarza możliwość nieprzewidzianych interakcji. Coś przecieka tam, gdzie nie powinno. Ciepło oddziałuje na substancję, która miała być odizolowana.

Pożar przenosi się nie przez logiczną sekwencję produkcyjną, lecz przez fizyczne sąsiedztwo. System pokazuje wtedy swą drugą mapę: nie tę z instrukcji operacyjnej, lecz tę z realnej przestrzeni.

Projektanci często myślą kategoriami funkcji: ten układ służy temu, tamten tamtemu. Jednak awaria nie musi szanować podziału funkcjonalnego. Awaria szanuje fizykę, ciśnienie, temperaturę, przepływ, grawitację, przewodnictwo czy wilgoć – po prostu wybiera drogę najmniejszego oporu. Świat materialny nie czyta schematów organizacyjnych.

To samo dotyczy instytucji. Dwa departamenty mogą być formalnie niezależne, ale jeśli korzystają z tej samej bazy danych, budżetu, osoby decyzyjnej lub kanału politycznego, w razie kryzysu ta niezależność znika. Ich realna bliskość nie jest przestrzenna, lecz informacyjna, finansowa albo kompetencyjna. W organizacjach wiele katastrof zaczyna się od zdania: „to nie powinno mieć ze sobą związku". Być może i nie powinno. Ale ma.

Drugim mechanizmem jest common-mode failure, czyli wspólny tryb awarii. Chodzi o sytuację, w której jeden element obsługuje kilka funkcji lub kilka formalnie niezależnych podsystemów. Kiedy zawodzi, nie powoduje pojedynczej usterki, lecz szereg równoczesnych zakłóceń. Jest to szczególnie groźne, ponieważ system może sprawiać wrażenie zabezpieczonego przez redundancję, podczas gdy w rzeczywistości kilka „niezależnych" ścieżek zależy od tego samego ukrytego węzła. Organizacja wierzy, że ma trzy drogi ratunku; awaria pokazuje, że wszystkie przechodziły przez jeden most.

Wspólny tryb awarii jest zabójczy dla diagnozy. Operator widzi wiele problemów naraz, nie dostrzegając wspólnego źródła. Może uznać, że ma do czynienia z kilkoma niezależnymi anomaliami i próbować naprawiać skutki po kolei, uruchamiając procedury zakładające sprawność innych części systemu. Tymczasem właśnie one zostały dotknięte tym samym ukrytym uszkodzeniem. W świecie instytucjonalnym wspólnym trybem awarii może być centralny system informatyczny, jedna interpretacja prawna, wąski kanał decyzyjny, dominujący dostawca, jeden budżet czy wspólna narracja polityczna.

Dopóki taki układ działa, daje poczucie sprawności. Gdy zawodzi – paraliżuje wiele obszarów jednocześnie. Dlatego dojrzała analiza bezpieczeństwa nie pyta tylko o liczbę zabezpieczeń, ale przede wszystkim: czy są one naprawdę niezależne? Bo trzy gaśnice zamknięte w tym samym płonącym magazynie to nie redundancja. To dekoracja przeciwpożarowa.

Trzecim źródłem złożoności są niezamierzone pętle sprzężenia zwrotnego. W systemach technicznych i organizacyjnych działania naprawcze mogą zmieniać warunki, które następnie wpływają na kolejne decyzje. System reaguje na własne reakcje. Brzmi to abstrakcyjnie, ale ma wymiar bardzo praktyczny.

Operator nie zarządza rzeczywistością, lecz jej wadliwym modelem

Operator obserwuje wskaźnik i podejmuje działanie, które zmienia stan systemu, lecz sam wskaźnik może nadal przekazywać obraz niepełny, opóźniony lub mylący. Automatyka może uruchomić zabezpieczenie modyfikujące ciśnienie, temperaturę bądź przepływ, co z kolei wywoła nowy alarm. Procedura awaryjna często zakłada jeden scenariusz, podczas gdy system znajduje się już w innym, ponieważ wcześniejsze interwencje przekształciły konfigurację awarii. W takim momencie organizacja nie walczy już z pierwotnym problemem, lecz z kryzysem, który częściowo sama wykreowała w trakcie próby ratowania sytuacji.

Analogicznie przebiega to w polityce publicznej. Państwo reaguje na kryzys regulacją, która wywołuje zachowania adaptacyjne. Te z kolei tworzą nowy problem, uruchamiający kolejną regulację. Po kilku takich cyklach trudno rozstrzygnąć, czy system leczy pierwotną chorobę, czy jedynie skutki własnych leków. Biurokracja ma w tym zakresie talent alchemika: potrafi z prostego problemu wytworzyć złoto proceduralnej nieczytelności, tyle że jest to złoto z ołowiu.

Pętle zwrotne są szczególnie groźne, gdy pozostają ukryte. Jeśli organizacja ma świadomość, że działanie A wywołuje efekt B, może go uwzględnić w planowaniu. Problem pojawia się wtedy, gdy efekt B wraca do systemu jako rzekomo niezależny sygnał C. Wówczas decyzje zapadają na podstawie zniekształconego obrazu skutków wcześniejszych działań. W systemach liniowych człowiek często obserwuje proces bezpośrednio: widzi stojącą taśmę, piętrzący się materiał lub przeciekającą rurę. W systemach interakcyjnie złożonych procesy są ukryte – zachodzą wewnątrz reaktora, instalacji chemicznej, systemu informatycznego, sieci finansowej czy infrastruktury administracyjnej.

Operator nie widzi procesu, lecz jego reprezentację. Ta pozornie drobna różnica w sytuacji kryzysowej staje się fundamentalna. Reprezentacja może kłamać lub być opóźniona. Może pokazywać stan pojedynczego elementu zamiast całego procesu; sygnalizować położenie przełącznika, a nie realny stan zaworu; wskazywać formalne wykonanie procedury, pomijając jej materialny skutek. Może dostarczać odczyt poprawny technicznie, lecz mylący interpretacyjnie. W takim układzie człowiek podejmuje decyzje nie w oparciu o rzeczywistość, lecz o model rzeczywistości generowany przez system. Jeśli ten model jest wadliwy, racjonalne działanie może prowadzić do katastrofy – co stanowi jeden z kluczowych argumentów w obronie operatorów w teorii Perrowa.

Po fakcie wiemy więcej. Widzimy pełną sekwencję i możemy odtworzyć prawdziwy stan rzeczy. Jednak operator w chwili kryzysu działał w świecie wskaźników, a nie pełnej wiedzy. Zarzut, że „powinien był wiedzieć", jest często nadużyciem wiedzy po fakcie. Po katastrofie nawet laik dostrzega ścieżkę awarii; w trakcie jej trwania ekspert widzi jedynie mgłę, alarmy i tykający zegar.

Iluzja kontroli i pułapka nadmiarowych zabezpieczeń

W instytucjach publicznych informacja pośrednia przybiera formę raportów, dashboardów, statystyk, wskaźników wykonania, ankiet, modeli predykcyjnych czy notatek służbowych i streszczeń dla decydentów. Im wyżej w hierarchii, tym rzadziej obcuje się z rzeczywistością, a częściej z jej syntetycznym odbiciem. Taka synteza bywa konieczna, lecz bywa też niebezpieczna – państwo zarządzane wyłącznie przez wskaźniki może przestać dostrzegać ludzi, których te wskaźniki nie potrafią policzyć.

Perrow zwraca szczególną uwagę na systemy transformacyjne: jądrowe, chemiczne, biologiczne czy genetyczne. W ich przypadku nie chodzi o zwykły montaż elementów, lecz o przemianę materii lub energii w warunkach wysokiego ciśnienia, temperatury, promieniowania bądź reaktywności chemicznej i biologicznej. Procesy te są często częściowo niewidoczne, modelowane probabilistycznie lub po prostu niedostatecznie zrozumiane. Prowadzi to do niewygodnego wniosku: możemy zbudować system, którego nie rozumiemy w pełni w stanach granicznych. Możemy sprawnie eksploatować go w warunkach normalnych, pozostając ślepymi na jego zachowania w konfiguracjach awaryjnych. A przecież katastrofy rzadko przebiegają zgodnie z podręcznikiem – są właśnie momentem, w którym system przechodzi w stan nieprzewidziany. Tu pojawia się granica inżynieryjnej pychy.

Nowoczesność zakłada, że skoro coś działa, to znaczy, iż jest zrozumiane. Perrow odpowiada: niekoniecznie. System może funkcjonować, bo warunki normalne są stabilne, personel doświadczony, a odchylenia niewielkie. Jednak gdy kilka anomalii nałoży się na siebie, system może wejść w obszar, którego nikt naprawdę nie zna. Dotyczy to również systemów społecznych. Możemy latami zarządzać państwem, rynkiem czy platformą cyfrową w warunkach względnej stabilności, lecz kryzys ujawnia zachowania niewidoczne na co dzień. Pandemia, wojna, masowy napływ uchodźców, załamanie łańcuchów dostaw czy cyberatak to odpowiedniki stanów granicznych. Pokazują one nie tyle codzienną sprawność systemu, ile to, co naprawdę potrafi, gdy przestaje być uprzejmy.

Jedną z najbardziej prowokacyjnych tez Perrowa jest krytyka bezrefleksyjnej redundancji. W tradycyjnym ujęciu bezpieczeństwa więcej zabezpieczeń ma oznaczać większe bezpieczeństwo: jeśli

zawiedzie jeden system, zastąpi go drugi, a w ostateczności uratuje sytuację trzeci. Brzmi to rozsądnie i często takie jest, ale nie zawsze. W systemie interakcyjnie złożonym każde dodatkowe zabezpieczenie staje się nowym elementem układu. Posiada własne czujniki, procedury, zasilanie i punkty awarii. Może chronić przed jednym scenariuszem, jednocześnie tworząc nowe ryzyka w innym; może dawać fałszywe poczucie niezależności, komplikować obraz operatora lub uruchamiać automatyczne reakcje, które zostaną źle zinterpretowane. Redundancja jest wartościowa, gdy upraszcza ratunek; staje się szkodliwa, gdy mnoży labirynt. Nie jest to argument przeciwko zabezpieczeniom, lecz przeciwko fetyszowi zabezpieczeń.

Bezpieczeństwo nie polega na nieskończonym dokładaniu warstw, lecz na projektowaniu systemu tak, by dodatkowe ogniwa były czytelne, niezależne i testowalne, a nie tworzyły ukrytych ścieżek awarii. W organizacji publicznej redundancją staje się podwójny nadzór, kolejna akceptacja, dodatkowy formularz czy nowa komórka kontrolna. Choć może to być potrzebne, często prowadzi do sytuacji, w której nikt nie odpowiada za całość, bo każdy pilnuje swojego fragmentu kontroli. Wtedy nadzór nie zwiększa bezpieczeństwa, lecz rozprasza odpowiedzialność. Nadmiar zabezpieczeń rodzi najgroźniejszą z organizacyjnych iluzji: wszyscy coś sprawdzili, ale nikt niczego nie zrozumiał.

Złożoność interakcyjna zmienia sens kompetencji. W prostym systemie wystarczy znać swój odcinek; w złożonym specjalizacja jest niewystarczająca, gdyż awaria potrafi przeskakiwać między sektorami. Potrzebna jest wiedza o relacjach i całości, lecz tu pojawia się paradoks: im bardziej system jest złożony, tym silniej organizacja dzieli wiedzę na wąskie specjalizacje. Każdy wie bardzo dużo o swoim fragmencie, a coraz mniej o powiązaniach między nimi. W rutynie to działa, w kryzysie zawodzi. Operator A rozumie pompę, B wskaźnik, inżynier C procedurę, menedżer D harmonogram, a regulator E wymóg formalny. Katastrofa jednak wydarza się „pomiędzy" tymi elementami.

Kto rozumie to, co dzieje się pomiędzy? W systemach wysokiego ryzyka kluczowa staje się zatem nie tylko wiedza specjalistyczna, ale wiedza integracyjna – zdolność widzenia powiązań i rozpoznania, że objaw w jednym miejscu może być skutkiem zdarzenia w innym. To wymaga gotowości do kwestionowania pierwszej interpretacji i uznania, że system może zachowywać się niezgodnie z podręcznikiem. Prowadzi to do praktycznej zasady: organizacje muszą budować nie tylko procedury, lecz także wyobraźnię systemową. Bez niej procedury będą jedynie mapą miasta sprzed trzęsienia ziemi.

Przenosząc kategorię Perrowa na grunt państwowy, dostrzeżemy, że wiele współczesnych instytucji publicznych ma cechy systemów interakcyjnie złożonych. Decyzja budżetowa wpływa na kadry, te na czas rozpatrywania spraw, co z kolei kształtuje zachowania obywateli i przedsiębiorców. Te

zachowania obciążają sądy, co wpływa na koszty administracji, a te na politykę. Polityka zmienia prawo, które wraca do administracji jako nowy obowiązek. To nie jest prosta linia.

Interakcyjna złożoność jako źródło nieprzewidywalności i rozmycia odpowiedzialności

To sieć. W takim systemie reforma może przynieść skutki odwrotne do zamierzonych. Uproszczenie jednej procedury często zwiększa obciążenie innej. Cyfryzacja przyspieszy obsługę spraw typowych, ale może sparaliżować te nietypowe. Centralizacja poprawi kontrolę, lecz osłabi lokalną zdolność reagowania; decentralizacja zaś zwiększy elastyczność kosztem rozproszenia odpowiedzialności. Nowe narzędzie nadzoru może ukrócić nadużycia, ale jednocześnie wydłużyć procesy do granic absurdu. Państwo interakcyjnie złożone nie znosi haseł prostych jak cep, choć polityka je uwielbia: „Wystarczy zmienić ustawę", „Wystarczy dać więcej pieniędzy", „Wystarczy rozliczyć winnych", „Wystarczy scentralizować", „Wystarczy sprywatyzować" czy „Wystarczy zinformatyzować".

Takie zdania brzmią dobrze w telewizji, bo mają rytm młotka. Problem polega na tym, że system złożony nie jest gwoździem. Tutaj każda interwencja staje się nowym elementem systemu, a każdy nowy element może otworzyć nową ścieżkę awarii. Perrow dowodzi, że złożoność nie jest wyłącznie kwestią techniczną – to także kwestia władzy. Projektant systemu decyduje bowiem, kto otrzyma informacje, kto poniesie odpowiedzialność, kto zyska czas na reakcję, kto będzie żył z ryzykiem, a kto czerpać korzyści z wydajności. Złożoność bywa wygodna dla organizacji, gdyż utrudnia przypisanie winy. Im więcej podsystemów, procedur, dostawców i audytów, tym łatwiej po katastrofie stwierdzić, że była to „nieprzewidywalna kombinacja". Czasem jest to prawda, jednak często nieprzewidywalność zostaje wyprodukowana przez samą strukturę zarządzania: outsourcing, presję kosztową, rozproszenie kompetencji i brak realnego właściciela całości. Analiza złożoności staje się więc aktem obywatelskiej higieny. Pozwala zapytać, czy system jest skomplikowany, bo wymaga tego rzeczywistość, czy dlatego, że złożoność ma ukrywać odpowiedzialność. Czy dodatkowe procedury chronią obywatela, czy raczej instytucję przed winą? Czy cyfryzacja upraszcza życie, czy jedynie przenosi kolejkę z korytarza do portalu, który nie działa w piątek po południu?

Złożoność nie jest grzechem sama w sobie, ale pozbawiona odpowiedzialności staje się zaproszeniem dla normalnego wypadku. Złożoność interakcyjna to nie liczba części, lecz liczba nieoczywistych relacji między nimi. To ukryte ścieżki, wspólne tryby awarii, pętle zwrotne i zabezpieczenia, które czasem same stają się problemem. Perrow uczy, że w takim systemie nie wystarczy pytać, co się zepsuło. Należy zapytać: jak awaria przeskoczyła między podsystemami? Jakie sygnały widzieli operatorzy? Czy wskaźniki pokazywały stan rzeczy, czy tylko stan elementów

sterujących? Czy zabezpieczenia były naprawdę niezależne i czy procedury pasowały do realnej konfiguracji zdarzenia?

Czy specjalizacja wiedzy nie przesłoniła relacji między częściami? Czy organizacja rozumiała swój system w stanach granicznych, czy jedynie w warunkach normalnej pracy? Najgroźniejsze w systemie złożonym nie jest to, że składa się z wielu elementów. Najgroźniejsze jest to, że on sam nie wie, jakie relacje ujawni dopiero w chwili kryzysu. I właśnie dlatego złożoność interakcyjna stanowi pierwszą połowę teorii Perrowa. Druga połowa jest jeszcze bardziej bezlitosna: ścisłe sprzężenie.

Ścisłe sprzężenie i brak luzu odbierają czas na reakcję

Nawet w złożonym systemie można czasem uratować sytuację, o ile dysponuje się czasem, przestrzenią i buforem pozwalającym na zatrzymanie procesu oraz izolację awarii. Prawdziwy problem zaczyna się jednak wtedy, gdy złożoność spotyka brak luzu. Złożoność interakcyjna wyjaśnia, dlaczego awarie w pewnych systemach stają się nieczytelne; pokazuje, jak drobne usterki mogą przeskakiwać między podsystemami, maskować się wzajemnie i uruchamiać ukryte pętle sprzężenia zwrotnego, zmuszając operatorów do działania na podstawie sprzecznych lub fałszywych informacji. Sama złożoność nie musi jednak oznaczać katastrofy. Uniwersytet jest systemem złożonym. Administracja publiczna jest złożona. Duże miasto czy Internet są złożone. Rodzina w niedzielny poranek też bywa złożona, zwłaszcza gdy wszyscy naraz szukają ładowarki, kluczy i sensu życia.

Złożoność jest trudna, lecz nie zawsze śmiertelna. Prawdziwy dramat w teorii Charlesa Perrowa zaczyna się wtedy, gdy spotyka ona drugi warunek: ścisłe sprzężenie (tight coupling). To właśnie połączenie złożoności interakcyjnej i ścisłego sprzężenia tworzy środowisko, w którym „normalny wypadek" staje się nie tylko możliwy, lecz strukturalnie wpisany w działanie systemu. Ścisłe sprzężenie oznacza, że procesy są silnie zależne od siebie, zachodzą szybko, mają sztywną kolejność i nie dają marginesu błędu, co uniemożliwia łatwą izolację uszkodzonego elementu. W takim systemie awaria nie czeka grzecznie, aż człowiek ją zrozumie. Ona biegnie dalej.

Jeżeli złożoność odbiera przejrzystość, ścisłe sprzężenie odbiera czas. Kluczowym pojęciem pozwalającym to zrozumieć jest luz – slack. To nadmiar czasu, zasobów i alternatywnych ścieżek; wszystko to, co pozwala systemowi nie pękać od razu i nie przenosić zakłócenia bezpośrednio na kolejne ogniwa. Luz bywa lekceważony, bo w spokojnych warunkach wygląda jak marnotrawstwo. Nadmiarowy personel, zapas części czy bufor czasowy są postrzegane jako koszt lub nieefektywność. Możliwość zatrzymania produkcji to spadek wydajności, alternatywna ścieżka decyzyjna – biurokratyczny luksus, a rezerwa finansowa – zamrożony kapitał.

W logice optymalizacji luz jest podejrzany. W logice bezpieczeństwa luz jest tlenem. System pozbawiony luzu może działać imponująco w warunkach normalnych: jest szybki, tani i smukły. Ale właśnie dlatego jest kruchy. Nie ma czym amortyzować zakłóceń; wystarczy mała awaria, by system nie miał gdzie jej przyjąć. Brakuje poduszki, bocznicy czy rezerwy. Nie ma człowieka, który mógłby przejąć zadanie, ani czasu na weryfikację wskaźników. W systemach wysokiego ryzyka luz nie jest luksusem – jest formą odpowiedzialności.

Pierwszą cechą ścisłego sprzężenia jest wysoka zależność od czasu. Procesy zachodzą zbyt szybko, by można je było dowolnie zatrzymać. Reakcja chemiczna nie poczeka na zebranie zarządu, ciśnienie w instalacji nie poczeka na opinię prawną, a rdzeń reaktora nie doczeka się spokojnej analizy raportu. Samolot w powietrzu nie może „zaparkować na chwilę", by załoga odbyła warsztat refleksyjny. W systemie ściśle sprzężonym czas staje się czynnikiem materialnym; nie jest tłem decyzji, lecz jej współautorem.

Ma to ogromne znaczenie poznawcze i organizacyjne. Gdy awaria jest niejasna, ale czas reakcji długi, można zbierać dane i testować hipotezy. Jednak gdy czas jest krótki, operator musi działać, zanim zrozumie. A działanie przed zrozumieniem jest zawsze hazardem, choć często koniecznym. Perrow zauważa, że w takich warunkach oczekiwanie, iż operator „powinien był właściwie zdiagnozować sytuację", bywa niesprawiedliwe. Diagnoza wymaga czasu, którego system nie daje. W efekcie operator nie tyle rozwiązuje problem, co próbuje go dogonić.

W organizacjach publicznych zależność czasowa ujawnia się w kryzysach: podczas powodzi, epidemii, cyberataków czy paniki finansowej. Wtedy decyzje administracyjne nie dojrzewają w rytmie konsultacji – muszą być podejmowane w ruchu. Państwo nie może dopiero wtedy odkrywać, gdzie leżą kompetencje i realne procedury. Dlatego systemy kryzysowe trzeba projektować przed kryzysem. W jego trakcie projektuje się już tylko improwizację.

Sztywność sekwencji i brak alternatyw jako źródła paraliżu

Drugą cechą ścisłego sprzężenia jest niezmienność sekwencji. Pewne działania muszą nastąpić w ściśle określonej kolejności; nie da się przeskoczyć etapu, wykonać procesu od końca, odłożyć półproduktu czy bezpiecznie zamienić kroków. W systemach luźno sprzężonych istnieje przestrzeń na improwizację: jeśli jeden dział zawodzi, zadanie przejmuje inny, a zablokowana droga skłania do objazdu. System posiada alternatywne rytmy. W systemach ściśle sprzężonych kolejność staje się prawem. Jeśli B musi nastąpić po A, brak tego pierwszego blokuje drugie. Gdy proces wymaga

konkretnego ciśnienia, temperatury czy synchronizacji, każde odchylenie przestaje być niedogodnością, a staje się początkiem awarii. Sztywna sekwencja jest groźna, gdyż drastycznie ogranicza pole manewru. Operator nie może po prostu powiedzieć: „zróbmy to inaczej". Procedury awaryjne są zazwyczaj wbudowane w projekt systemu, a nie tworzone doraźnie – jeśli pasują do sytuacji, mogą ratować, lecz jeśli nie, przyspieszą katastrofę.

W administracji odpowiednikiem sztywnej sekwencji są procedury prawne i budżetowe, terminy ustawowe, etapy zamówień publicznych czy hierarchie zatwierdzania. W warunkach normalnych zapewniają one legalność i porządek, lecz w kryzysie mogą stać się stalową obręczą. Gdy prawo wymaga pięciu kroków, a rzeczywistość daje czas na dwa, państwo odkrywa, że formalna poprawność nie zawsze idzie w parze ze zdolnością działania. Nie chodzi tu o pochwałę bezprawia, lecz o projektowanie prawa tak, by w sytuacjach granicznych posiadało legalne tryby elastyczności. Państwo bez procedur jest chaosem, ale państwo z procedurami pozbawionymi buforów jest automatem do produkcji bezradności.

Trzecią cechą ścisłego sprzężenia jest unifinalność – sytuacja, w której system posiada tylko jedną zasadniczą drogę osiągnięcia celu. Brak tu alternatywnych metod, substytutów czy równoległych kanałów działania; awaria jednego kluczowego elementu zagraża całemu procesowi. Unifinalność jest atrakcyjna dla projektantów wydajności, gdyż upraszcza produkcję: jedna droga, jeden standard i jedna logika. W idealnych warunkach działa to znakomicie, jednak bezpieczeństwo nie interesuje się ideałami, lecz pyta, co stanie się, gdy droga zostanie zablokowana. Jeśli system posiada alternatywy, awarię można zneutralizować obejściem. Bez nich pojedynczy błąd staje się awarią całości. To logika wąskiego gardła: dopóki przepływ trwa, nikt go nie zauważa; gdy się zatyka, wszyscy nagle odkrywają, że cała organizacja oddychała przez słomkę.

W państwie unifinalność objawia się centralizacją krytycznych funkcji: jeden system wypłat, jeden rejestr, jedna platforma komunikacyjna czy jedna osoba decyzyjna. Centralizacja daje kontrolę, ale tworzy jednocześnie pojedynczy punkt paraliżu. Doświadczenie systemowe podpowiada zasadę: im bardziej krytyczna funkcja, tym ostrożniej należy pytać, czy naprawdę powinna mieć tylko jedną drogę wykonania. Jedna droga jest elegancka na schemacie, lecz w kryzysie elegancja bywa pierwszą ofiarą.

Czwartą cechą ścisłego sprzężenia jest trudność zastępowalności ludzi, materiałów i urządzeń. W systemach luźno sprzężonych można użyć zamiennika, przesunąć pracownika lub pożyczyć zasób. W systemach ściśle sprzężonych zasoby są wyspecjalizowane, proporcje precyzyjne, a tolerancja odchyleń minimalna. Dotyczy to nie tylko przemysłu. W nowoczesnych instytucjach istnieją funkcje niezastąpione: administrator kluczowego systemu, ekspert od rzadkiej procedury czy prawnik znający niszową regulację. Organizacje często oszczędzają właśnie na tej niewidzialnej redundancji

kompetencji. Dopóki ekspert jest dostępny, wszystko działa. Gdy jednak choruje lub nie odbiera telefonu w niedzielę o trzeciej nad ranem, organizacja odkrywa, że „procedura” była w rzeczywistości człowiekiem. To jeden z najbardziej lekceważonych wymiarów bezpieczeństwa: zależność systemu od wiedzy ukrytej. Nie wszystko, co istotne, zapisano w instrukcji; część wiedzy mieszka w praktyce, doświadczeniu i intuicji operacyjnej ludzi.

Paradoks centralizacji i społeczne sprzężenie systemu

Jeżeli organizacja redukuje personel do minimum i udaje, że wszystko da się opisać w procedurach, buduje system papierowo odporny i praktycznie kruchy. W świetle NAT redukcja "nadmiarowego" personelu może wyglądać na sukces kosztowy, a w rzeczywistości być demontażem bufora bezpieczeństwa.

Piątą cechą ścisłego sprzężenia jest konieczność wcześniejszego zaprojektowania środków ratunkowych. W systemach luźno sprzężonych można czasem dokonać naprawy doraźnej: obejść uszkodzony fragment, użyć improwizowanego narzędzia, zmienić procedurę, zatrzymać proces lub przetestować rozwiązanie. W systemach ściśle sprzężonych improwizacja jest ograniczona albo niemożliwa, ponieważ tempo i ryzyko nie pozwalają na eksperymentowanie. Ma to ambiwalentne skutki. Z jednej strony wymusza profesjonalne projektowanie zabezpieczeń, z drugiej zaś sprawia, że system staje się zależny od wyobraźni projektantów. Jeżeli nie przewidzieli oni danej konfiguracji awarii, operatorzy mogą nie mieć bezpiecznego sposobu reakcji.

Tu pojawia się dramat normalnego wypadku: system może znaleźć się w stanie, którego projekt nie przewidział, a jednocześnie nie dać ludziom przestrzeni na bezpieczną improwizację. Złożoność mówi: "nie rozumiesz jeszcze, co się dzieje", podczas gdy ścisłe sprzężenie nakazuje: "musisz działać natychmiast". To jest organizacyjny imadło.

W administracji podobny problem występuje, gdy procedury awaryjne są przygotowane na katalog znanych kryzysów, lecz rzeczywistość produkuje kryzys hybrydowy. System prawny posiada tryby na powódź, epidemię, awarię infrastruktury, migrację czy cyberatak – ale co, jeśli kilka zdarzeń zachodzi jednocześnie? Czy procedury się łączą, czy blokują? Czy organy współpracują, czy czekają na właściwość? Czy dane przepływają, czy każdy pilnuje swojego silosu? Czy ktoś ma prawo przeciąć węzeł, zanim węzeł przeciśnie państwo?

Perrow wskazuje na istotną konsekwencję organizacyjną: systemy ściśle sprzężone wymuszają centralizację. Ponieważ reakcje muszą być szybkie, a sekwencje sztywne, zarządzanie kryzysem nie może polegać na długich konsultacjach. Potrzebne są jasne decyzje, automatyczne procedury,

dyscyplina wykonania i hierarchia. Jednak systemy interakcyjnie złożone wymagają czegoś przeciwnego: decentralizacji, lokalnej wiedzy, interpretacji, elastyczności oraz zdolności do improwizowania i rozumienia nietypowych konfiguracji. Tam, gdzie awaria jest niejasna, osoby najbliżej systemu muszą mieć możliwość myślenia, kwestionowania sygnałów i łączenia danych spoza standardowej procedury.

Tworzy to paradoks organizacyjny, który w notatce źródłowej został trafnie nazwany napięciem typu Pushme-pullyou: złożoność ciągnie organizację w stronę decentralizacji, a ścisłe sprzężenie pcha ją w stronę centralizacji. Organizacja ma być jednocześnie swobodna i posłuszna; kreatywna i proceduralna; lokalna i centralna; elastyczna i natychmiastowa. Ma myśleć jak sieć i reagować jak automat.

To nie jest drobny problem menedżerski, lecz głęboka sprzeczność architektury systemów wysokiego ryzyka. W praktyce organizacje rozwiązują ten paradoks błędnie na dwa sposoby. Pierwszy polega na nadmiernej centralizacji: wszyscy czekają na decyzję góry, choć ta dysponuje gorszymi informacjami i ma za mało czasu. Drugi to chaotyczna decentralizacja: każdy działa lokalnie, lecz bez wspólnego obrazu i koordynacji. Obie ścieżki mogą prowadzić do katastrofy.

Dojrzała organizacja musi zatem odróżniać sytuacje wymagające automatycznej dyscypliny od tych, w których konieczne jest przerwanie automatu i uruchomienie interpretacji. Łatwo to powiedzieć, trudniej zaprojektować, ale właśnie tu leży różnica między organizacją, która posiada procedury, a taką, która ma zdolność przetrwania.

Ścisłe sprzężenie systemu technicznego często wzmacnia się przez sprzężenie ekonomiczne. Proces nie może czekać, bo reakcja chemiczna trwa, ale nie może też czekać, ponieważ każda godzina przestoju generuje koszty. Nie można wyłączyć instalacji ze względu na plan produkcji, zwiększyć obsady z powodu budżetu, opóźnić startu przez harmonogram ani przyznać, że system jest niepewny, by nie nadwyrężyć reputacji. Tight coupling nie jest tylko cechą maszyn; może być cechą całej organizacji działającej pod presją wyniku.

Gdy presja ekonomiczna, polityczna albo wizerunkowa usuwa margines ostrożności, organizacja staje się ściślej sprzężona społecznie. Wtedy pojawiają się "błędy wymuszone". Ludzie obchodzą procedury nie z lekkomyślności, lecz dlatego, że system wymaga jednocześnie bezpieczeństwa i tempa, których nie da się pogodzić. Pracownik ma nie ryzykować, ale musi wykonać normę. Lekarz ma działać zgodnie ze standardem, lecz obsłużyć nierealną liczbę pacjentów. Urzędnik ma skrupulatnie badać sprawy, a jednocześnie skracać kolejki. Menedżer ma dbać o bezpieczeństwo, choć premia zależy od wyniku. Państwo ma konsultować prawo, ale musi natychmiast reagować na kryzys medialny.

To są społeczne odpowiedniki ścisłego sprzężenia: brak czasu, luzu, alternatyw i rezerw oraz zbyt kosztowne zatrzymanie procesu. Najgorsze organizacje deklarują wtedy, że "bezpieczeństwo jest priorytetem", a następnie projektują warunki, w których jest ono praktycznie niewykonalne. To nie hipokryzja jednostek, lecz sprzeczność systemowa ubrana w ładne hasła.

Teorie organizacyjnego uczenia się zakładają, że system może wyciągać wnioski z błędów.

Rozluźnianie sprzężeń jako jedyna realna metoda budowania odporności

Perrow jest sceptyczny wobec tej nadziei w środowiskach ściśle sprzężonych i interakcyjnie złożonych. Powód jest prosty: aby się uczyć, potrzeba powtarzalności, czasu na analizę i możliwości eksperymentowania bez katastrofalnych skutków. W systemach ściśle sprzężonych błędy bywają zbyt kosztowne, by mogły stać się dobrym materiałem dydaktycznym. Nie można spokojnie „uczyć się” na stopieniu rdzenia, eksplozji zakładu chemicznego czy skażeniu środowiska. Niektóre błędy są zbyt wielkie, by traktować je jako opłatę za wiedzę.

Poza tym każda katastrofa w systemie złożonym może być konfiguracją wyjątkową. Organizacja uczy się więc często nie ogólnej prawdy, lecz konkretnego scenariusza, który już wystąpił. Dopisuje zabezpieczenie przeciw poprzedniej katastrofie, podczas gdy następna nadchodzi inną ścieżką. To trochę jak zamykanie drzwi, przez które wszedł włamywacz, podczas gdy dom ma dwadzieścia okien, piwnicę i kuzyna z zapasowym kluczem. Uczenie się bywa też zniekształcone politycznie.

Po awarii organizacja dąży do odzyskania zaufania, uniknięcia odpowiedzialności, uspokojenia regulatora i ochrony menedżerów, szukając przyczyny wystarczająco konkretnej, by móc zamknąć sprawę. Sprzyja to prostym narracjom: zawiódł człowiek, procedura była niepełna lub sprzęt wymaga modernizacji. Rzadziej prowadzi to do wniosku, że cały system działa na granicy niedopuszczalnej złożoności i braku luzu. A jednak to właśnie taka konkluzja może być najważniejsza.

Dla równowagi należy zaznaczyć: Perrow nie twierdzi, że każdy złożony system musi natychmiast prowadzić do katastrofy. Kluczowa jest kombinacja złożoności i sprzężenia. System złożony, lecz luźno sprzężony, może być trudny w zarządzaniu, ale jest odporniejszy. Ma czas na interpretację, posiada alternatywne drogi i potrafi izolować błędy. Pozwala lokalnym jednostkom eksperymentować oraz zatrzymać część procesu bez niszczenia całości. Uniwersytety są złożone, lecz zazwyczaj luźno sprzężone – awaria jednego wydziału nie musi zniszczyć całej instytucji. Poczta, według klasycznych przykładów Perrowa, jest bardziej liniowa i luźniej sprzężona.

Lotnictwo, choć ryzykowne, dysponuje buforami, procedurami treningowymi, symulacjami oraz ogromną liczbą powtarzalnych operacji, dzięki którym błędy mogą być analizowane przed wystąpieniem katastrofy.

Luźne sprzężenie nie oznacza braku organizacji; oznacza zdolność absorbowania zakłóceń. System z luzem potrafi przyjąć cios, zanim odda go całej strukturze. Dla państwa jest to szczególnie ważna lekcja. Dobra decentralizacja może być formą luźnego sprzężenia. Lokalne zdolności działania, rezerwy, alternatywne kanały komunikacji, samodzielność operacyjna, pluralizm dostawców i rozproszone kompetencje – wszystko to zwiększa odporność, o ile istnieje koordynacja i wspólny obraz sytuacji. Luźne sprzężenie nie może oznaczać anarchii; musi oznaczać zaprojektowaną zdolność oddechu.

Współczesny świat coraz mocniej się sprzęga. Łańcuchy dostaw działają w systemie „just in time", systemy finansowe reagują automatycznie, a infrastruktura cyfrowa spaja administrację, bankowość, energetykę, transport i komunikację. Media społecznościowe skracają czas reakcji politycznej niemal do zera, przez co kryzysy lokalne błyskawicznie stają się globalne. Informacja, panika, kapitał i presja opinii publicznej przepływają szybciej niż zdolność instytucji do ich rozumienia. W takim świecie tight coupling przestaje być kategorią zarezerwowaną dla elektrowni i rafinerii – staje się kategorią cywilizacyjną.

Gospodarka bez zapasów, państwo bez rezerw kadrowych, system ochrony zdrowia bez wolnych łóżek czy administracja zależna od jednego systemu informatycznego – to wszystko są systemy ściśle sprzężone. Polityka reagująca na każdy impuls medialny jest ściśle sprzężona emocjonalnie. Organizacja, w której każdy termin jest „na wczoraj", a każda decyzja „pilna", sama produkuje środowisko normalnego wypadku.

To paradoks nowoczesnej efektywności. Im bardziej eliminujemy zapasy, opóźnienia, nadmiary i lokalne autonomie, tym sprawniej system wydaje się działać – aż do pierwszego poważnego zakłócenia. Wtedy okazuje się, że to, co nazywaliśmy efektywnością, było często jedynie brakiem amortyzatorów. Świat bez luzu wygląda dynamicznie, ale przy pierwszym zderzeniu zachowuje się jak szkło hartowane: długo wytrzymuje, a potem rozsypuje się naraz.

Dla praktycznej analizy instytucji, przedsiębiorstwa albo państwa warto sformułować zestaw pytań diagnostycznych. Nie są one ozdobą akademicką, lecz narzędziem myślenia systemowego: Czy proces można bezpiecznie zatrzymać? Czy awarię można odizolować lokalnie? Czy istnieją alternatywne drogi osiągnięcia celu? Czy można zastąpić kluczowy zasób: człowieka, dostawcę lub system? Czy reakcja musi być natychmiastowa? Czy kolejność działań jest sztywna? Czy zabezpieczenia są zaprojektowane z góry, czy możliwa jest improwizacja? Czy organizacja ma

rezerwy czasu, personelu, finansów i informacji? Czy presja ekonomiczna lub polityczna usuwa margines ostrożności? Czy zatrzymanie procesu jest traktowane jako dopuszczalna decyzja bezpieczeństwa, czy jako porażka?

Odpowiedzi na te pytania pokazują, czy system ma zdolność przeżywania własnych zakłóceń. Celem dojrzałego projektowania nie jest stworzenie systemu, który nigdy nie doświadczy awarii – to mrzonka. Celem jest stworzenie systemu, w którym awaria nie musi natychmiast stać się katastrofą. Jeżeli złożoność interakcyjna jest często trudna do całkowitego usunięcia, jednym z najważniejszych sposobów ograniczania ryzyka jest rozluźnianie sprzężeń. Oznacza to tworzenie buforów, rezerw, alternatywnych ścieżek, możliwości zatrzymania procesu, lokalnej autonomii, niezależnych źródeł informacji oraz zapasów czasu na diagnozę.

Luz systemowy i różnica między awarią a wypadkiem

Rozluźnianie brzmi mało heroicznie. Nie ma w nim blasku wielkiej reformy, nie nadaje się na konferencję prasową; trudno przeciąć wstęgę na „buforze czasowym". A jednak to właśnie on często decyduje o tym, czy system przetrwa. W praktyce oznacza to: nie projektować wszystkiego na styk. Nie traktować zapasów jako przejawu lenistwa. Nie mylić centralizacji z kontrolą i nie uzależniać krytycznych funkcji od jednego kanału. Nie usuwać personelu tylko dlatego, że w normalnym dniu „nie jest w pełni wykorzystany". Nie tworzyć procedur, które nie przewidują własnego zawieszenia w sytuacji nietypowej. Nie nagradzać wyłącznie szybkości, jeśli ta niszczy zdolność rozpoznania. Najkrótszy bon mot brzmi: system bez luzu nie jest sprawny; jest tylko jeszcze nienaruszony. Ścisłe sprzężenie wyjaśnia, dlaczego w niektórych systemach drobna awaria tak szybko zamienia się w lawinę. Nie chodzi jedynie o to, że elementy są powiązane, lecz o to, że są one połączone bez marginesu, bez czasu, bez obejścia, bez rezerwy i często bez możliwości improwizacji. Gdy taki system jest jednocześnie interakcyjnie złożony, powstaje najgroźniejsza konfiguracja Perrowa: człowiek nie rozumie w pełni tego, co się dzieje, a mimo to musi działać natychmiast; procedury są konieczne, ale mogą być niedopasowane; zabezpieczenia istnieją, lecz mogą komplikować sytuację; organizacja dąży do centralizacji, choć potrzebuje lokalnej wiedzy; wszyscy pragną bezpieczeństwa, podczas gdy system nagradza tempo. To nie jest zwykła awaria. To przepis na normalny wypadek.

Po omówieniu dwóch podstawowych wymiarów teorii Charlesa Perrowa – złożoności interakcyjnej i ścisłego sprzężenia – należy przejść do pytania, które decyduje o sile jego koncepcji: czym właściwie różni się zwykła awaria od wypadku systemowego? To rozróżnienie jest kluczowe, gdyż język potoczny zaciera różnice. Mówimy: „była awaria", „doszło do katastrofy", „system zawiódł",

„operator popełnił błąd", „zabezpieczenie nie zadziałało". Wszystko ląduje w jednym worku. Perrow ten worek rozcina.

Pokazuje on, że nie każdy wypadek ma tę samą strukturę, a różnica między awarią komponentu a wypadkiem systemowym nie jest kwestią skali, lecz rodzaju. Zwykła usterka może być groźna – może zabić ludzi, doprowadzić do strat lub ujawnić zaniedbania. Jednak wypadek systemowy jest czymś bardziej niepokojącym: powstaje z nieprzewidzianych interakcji wielu awarii, często w różnych i pozornie niezależnych podsystemach. To nie sytuacja, w której jedna część pęka, a reszta biernie ponosi konsekwencje; to moment, w którym system zaczyna działać w konfiguracji, której nikt nie przewidział. Perrow proponuje myśleć o złożonych technologiach warstwowo.

Na najniższym poziomie mamy części: śruby, uszczelki, przewody, czujniki, styki, zawory czy elementy elektroniczne. Wyżej znajdują się jednostki, czyli zespoły części pełniące określoną funkcję: pompa, wskaźnik, generator, zawór bezpieczeństwa czy panel sterowania. Jeszcze wyżej sytuują się podsystemy: układ chłodzenia, system zasilania, system awaryjnego wtrysku wody, układy sterowania i komunikacji. Dopiero na końcu mamy system jako całość: elektrownię, zakład chemiczny, statek, samolot, sieć energetyczną, szpital, państwo czy administrację kryzysową.

Wypadek systemowy to nieliniowa konfiguracja interakcji

Ta hierarchia nie jest akademicką pedanterią, lecz narzędziem rozpoznawania rodzaju awarii. Gdy psuje się element, mamy do czynienia z awarią części; gdy przestaje działać pompa – z problemem jednostki; jeśli zaś uszkodzenie obejmuje układ chłodzenia, mówimy o awarii podsystemu. Wypadek systemowy zaczyna się jednak wtedy, gdy kilka zakłóceń w różnych miejscach oddziałuje na siebie w sposób nieprzewidziany przez procedury, projekt czy operatorów. Inaczej mówiąc: awaria części ma lokalizację. Wypadek systemowy ma konfigurację.

Najniższym poziomem zdarzenia jest incydent. Może on zatrzymać pracę, uruchomić alarm, wymagać naprawy lub generować koszty, jednak jego sens pozostaje zasadniczo czytelny. Wiadomo, co się stało, gdzie wystąpił problem i jak zdarzenie wpływa na resztę systemu. W systemach liniowych większość awarii ma właśnie taki charakter. Jeśli na linii produkcyjnej pęknie pas transmisyjny, produkcja staje w konkretnym miejscu. Jeśli w urzędzie padnie drukarka, instytucja może być zirytowana, ale nie traci konstytucyjnej tożsamości. Gdy jeden samochód blokuje drogę, tworzy korek, lecz przyczyna jest widoczna – można usunąć pojazd, wyznaczyć objazd lub naprawić pas.

Incydent może być poważny, ale jego logika jest zazwyczaj liniowa: element zawodzi, skutek pojawia się w przewidywalnym miejscu, a reakcja jest możliwa. W takim świecie klasyczne zarządzanie bezpieczeństwem sprawdza się stosunkowo dobrze – wymieniamy część, poprawiamy procedurę, szkolimy ludzi, zwiększamy kontrolę lub tworzymy plan zapasowy. Wypadek systemowy jest inny. Nie dlatego, że jest „większy", lecz dlatego, że jest mniej czytelny.

Perrow odróżnia wypadki systemowe od tych spowodowanych awarią komponentu. Wypadek komponentowy może mieć ciężkie konsekwencje, ale jego mechanizm pozostaje zrozumiały; awaria postępuje znaną ścieżką, a przyczyna i skutek są połączone w sposób przewidywalny. Nawet przy zaniedbaniach, błędach projektowych czy złym nadzorze, można odtworzyć sekwencję zdarzeń. Przykładem mogą być niektóre katastrofy tam lub kopalń. Są one śmiertelnie groźne, lecz niekoniecznie muszą mieć charakter wypadku systemowego w sensie Perrowa. Jeśli tama pęka z powodu wad projektu, złych materiałów, błędnej oceny podłoża lub zaniedbanej kontroli, mamy do czynienia z tragedią, której mechanizm może być liniowy. Podobnie w kopalni: wypadek na skutek znanego zagrożenia, złej wentylacji, wybuchu metanu czy zawalenia stropu jest wydarzeniem poważnym, lecz zasadniczo zrozumiałym.

To rozróżnienie bywa moralnie niewygodne, gdyż można by błędnie uznać, że „liniowy" oznacza mniej ważny. Nie – liniowy wypadek może być katastrofą społeczną i ludzką. Perrow wskazuje jedynie na inną strukturę poznawczą i organizacyjną. Można mu przeciwdziałać klasycznymi metodami: poprawą projektu, kontrolą materiałów, egzekwowaniem norm, lepszym nadzorem, szkoleniami czy konserwacją. Wypadek systemowy jest trudniejszy, ponieważ jego przyczyna nie tkwi w jednej części, lecz w relacjach między nimi.

Wypadek systemowy powstaje, gdy kilka awarii lub zakłóceń wchodzi ze sobą w nieoczekiwaną interakcję. Nie wynika on z jednej znanej sekwencji, lecz z przecięcia kilku z nich. Podsystemy, które miały być odseparowane, zaczynają na siebie wpływać. Zabezpieczenia zamiast izolować problem, mogą go zamaskować; wskaźniki zacząć mylić, a procedury stać się nieadekwatne. Operatorzy otrzymują zniekształcony obraz systemu.

Wypadek systemowy cechuje zatem kilka właściwości. Po pierwsze: jest nieliniowy – małe zdarzenie może wywołać skutki nieproporcjonalne do swojej skali. Po drugie: jest nieprzejrzysty – uczestnicy nie widzą od razu, co naprawdę się dzieje. Po trzecie: jest interakcyjny – katastrofa nie jest prostą sumą usterek, lecz efektem ich wzajemnego oddziaływania. Po czwarte: jest czasowo wymagający – w systemach ściśle sprzężonych brakuje czasu na spokojne rozpoznanie sytuacji. Po piąte: jest organizacyjnie mylący – ex post łatwo wskazać pojedyncze błędy, lecz w czasie rzeczywistym ich znaczenie było ukryte.

Wypadek systemowy można porównać do choroby wielonarządowej. Nie wystarczy stwierdzić, że „zawiodło serce” lub „zawiodły płuca”. Problem polega na tym, że organizm jako całość wszedł w stan, w którym zaburzenia jednego układu zmieniają funkcjonowanie innych, a leczenie jednego objawu może pogorszyć drugi. Podobnie jest w systemach technologicznych i organizacyjnych: leczenie lokalne nie wystarczy, jeśli choroba ma charakter systemowy. Tradycyjna analiza ryzyka często próbuje przewidywać awarie poprzez rozpisywanie prawdopodobieństw: co się stanie, gdy zawiedzie pompa, zawór, zasilanie lub gdy operator zareaguje zbyt późno?

Katastrofa to nie pech, lecz cecha architektury

Takie podejście jest potrzebne, choć ma swoje ograniczenie: łatwiej analizować pojedyncze ścieżki niż ich nieprzewidywalne kombinacje. W systemach złożonych liczba możliwych interakcji rośnie szybciej niż liczba samych elementów. Nie chodzi jedynie o ilość części, lecz o to, że każda z nich może oddziaływać na inne w różnych stanach: podczas pracy, awarii, przeciążenia, konserwacji czy testowania, a także w sytuacjach obejścia procedur, presji czasu lub błędnego odczytu. Projektanci zazwyczaj przewidują awarie znane, prawdopodobne lub wyobrażalne w ramach dotychczasowego modelu systemu. Wypadek systemowy pojawia się często w przestrzeni między tym, co przewidziane, a tym, co możliwe. To obszar „nieznanych znanych”: elementy są nam znane, ale ich konkretna konfiguracja nie została wcześniej pomyślana. Po katastrofie wszystko wydaje się logiczne; przed nią zaś wiele konfiguracji uznawano za zbyt nieprawdopodobne, by traktować je poważnie. Tu działa bezlitosny paradoks: system może generować zdarzenia rzadkie, lecz strukturalnie możliwe, a ponieważ występują one rzadko, organizacja łatwo uczy się je lekceważyć. W tym miejscu należy wrócić do paradoksu zawartego w pojęciu „normalnego wypadku”. Dla Perrowa normalność nie oznacza, że takie zdarzenia muszą występować codziennie, lecz że wynikają one z immanentnych właściwości systemu. Są statystycznie rzadkie, ale nie stanowią anomalii logicznej.

Organizacje po katastrofach często bronią się argumentem o „nadzwyczajnym zbiegu okoliczności”. Perrow nie zaprzecza nadzwyczajności tego zbiegu, pyta jednak: czy system został zbudowany tak, że taki splot zdarzeń mógł przekształcić się w katastrofę? Jeśli tak, stwierdzenie „mieliśmy pecha” jest niewystarczające. Pech jest prywatnym słowem na publicznie źle zaprojektowane sprzężenie. Normalny wypadek jest więc rzadki, ale nie zewnętrzny; przypomina możliwość choroby wpisaną w organizm. Nie chorujemy codziennie, lecz pewne schorzenia wynikają ze sposobu działania ciała. Podobnie system nie ulega katastrofie każdego dnia, jednak niektóre z nich są bezpośrednim wynikiem sposobu jego organizacji.

Po każdej awarii można zadać pytanie na trzech poziomach. Pierwszy brzmi: co się zepsuło? To poziom techniczny – szukamy konkretnej części, błędu, usterki lub nieprawidłowego odczytu. Drugi poziom pyta: kto co zrobił? To perspektywa operacyjna; analizujemy decyzje ludzi, reakcje operatorów, działania kierownictwa i zastosowane procedury. Trzeci poziom brzmi: dlaczego system umożliwił taką konfigurację zdarzeń? To pytanie Perrowa – najtrudniejsze i najważniejsze. Tu badamy relacje, sprzężenia, nieczytelność, brak buforów, wspólne tryby awarii, presję produkcyjną oraz strukturę władzy i odpowiedzialności. Organizacje chętnie zatrzymują się na pierwszych dwóch poziomach, gdyż dają one konkret: można wymienić element, przeszkolić człowieka lub dopisać procedurę. Trzeci poziom jest kosztowny, ponieważ może obnażyć błędy całej architektury działania. A architektury nie naprawia się komunikatem prasowym.

Jednym z największych wrogów rzetelnej analizy wypadków jest złudzenie wiedzy po fakcie. Znając wynik, łatwo układamy zdarzenia w spójną opowieść. Widzimy, który sygnał był kluczowy, który alarm należało potraktować poważnie, który wskaźnik kłamał i jaki manewr należało wykonać. Operatorzy jednak nie znali zakończenia tej historii – byli w jej środku. To zasadnicza różnica między analizą historyczną a działaniem operacyjnym: historyk katastrofy dysponuje pełną sekwencją zdarzeń.

Błąd operatora to często tylko widoczny skutek architektury systemu

Operator dysponuje jedynie migawkami. Komisja natomiast ma pełną dokumentację. Operator mierzy się z dźwięczącymi alarmami, presją czasu i niepełnymi danymi; ekspert analizujący zdarzenie po fakcie korzysta z komfortu rekonstrukcji. Człowiek w kryzysie ma obowiązek podjęcia decyzji, dlatego Perrow sprzeciwia się łatwemu moralizowaniu. Nie chodzi tu o uniewinnianie każdego działania, lecz o uczciwość poznawczą. Aby rzetelnie ocenić decyzję, należy odtworzyć nie tylko to, co obiektywnie działo się w systemie, ale przede wszystkim to, co było widoczne i możliwe do zinterpretowania w danym momencie. Jeśli system generował fałszywy obraz, operator mógł działać racjonalnie w ramach tej fałszywej rzeczywistości.

Raporty powypadkowe są niezbędne, lecz często niosą ryzyko uproszczenia. Instytucje mają interes w tym, by wskazać przyczynę konkretną, naprawialną i ograniczoną – im bardziej lokalnie wygląda źródło problemu, tym mniej groźne są konsekwencje dla całego systemu. W efekcie raporty często wskazują na niewłaściwą reakcję operatora, braki w szkoleniu, złą komunikację, wadliwy element czy nieaktualną procedurę.

Wszystko to może być prawdą, ale rzadko jest wystarczające. Perrow kazałby sprawdzić, czy raport nie popełnia błędu "przyczyny ostatniej". Ostatnia decyzja przed katastrofą jest najbardziej widoczna, lecz niekoniecznie najważniejsza. Człowieka, który nacisnął przycisk, opisuje się znacznie łatwiej niż system, który sprawił, że naciśnięcie tego przycisku wydawało się rozsądne. Analiza normalnych wypadków wymaga zatem dyscypliny metodologicznej: nie wolno mylić widoczności przyczyny z jej rzeczywistym znaczeniem. To, co widać najlepiej, często jest jedynie punktem, w którym głębsze zależności wyszły na powierzchnię.

Katastrofa w Three Mile Island stanowi jeden z kluczowych przykładów w teorii Perrowa, gdyż obrazuje różnicę między awarią komponentu a wypadkiem systemowym. Nie była to pojedyncza usterka prowadząca liniowo do kryzysu, lecz konfiguracja wielu zdarzeń: problemy z urządzeniami pomocniczymi, zablokowane zawory, zacięcie zaworu PORV, mylące wskaźniki oraz decyzje podejmowane na podstawie sprzecznych danych. Kluczowe nie jest to, że zawiódł jeden element, lecz fakt, iż awarie i informacje o nich weszły ze sobą w mylące relacje. System nie tylko tracił chłodziwo – system tracił przejrzystość.

Operatorzy nie widzieli po prostu „prawdy o reaktorze”; widzieli odczyty sugerujące stan inny niż rzeczywisty. Ich działania, krytykowane post factum, były częścią konfiguracji stworzonej przez sam system. TMI pokazuje zasadę: wypadek systemowy to nie suma awarii i błędu człowieka. To splot usterki, błędnych informacji, presji czasu, procedur i ukrytych sprzężeń, które uniemożliwiają natychmiastowe rozpoznanie sytuacji. Dlatego stwierdzenie, że „operatorzy popełnili błąd”, jest zbyt wąskie w stosunku do skali zdarzenia. Może być częściowo prawdziwe, ale jako wyjaśnienie pozostaje ubogie. To jak powiedzieć, że powódź była skutkiem mokrej wody.

Zmiana architektury zamiast szukania winnych

Anegdota o pękniętym dzbanku, kluczach, sąsiedzie i strajku autobusów działa dlatego, że w miniaturze obrazuje strukturę wypadku systemowego. Żadne z tych zdarzeń osobno nie jest wystarczające; każde posiada potencjalne obejście. Problem polega na tym, że te obejścia same zawodzą lub okazują się zależne od innych warunków. To kluczowy aspekt normalnych wypadków: zabezpieczenia nie tylko mogą zawieść, ale bywają powiązane z tym samym środowiskiem, które wywołało pierwotny problem. Zapasowy klucz jest świetnym rozwiązaniem, dopóki nie zostanie oddany. Sąsiad stanowi doskonały plan B, dopóki jego samochód działa. Autobus pozostaje alternatywą do momentu strajku, a taksówka – dopóki nie wszyscy potrzebują jej w tym samym czasie. System awaryjny przestaje być awaryjny, gdy zależy od tych samych warunków, które zawodzą w kryzysie. To samo dotyczy wielkich instytucji.

Plan B bywa tylko planem A w innym folderze. Rezerwa często okazuje się pozorna. Alternatywna procedura wymaga tych samych ludzi, tego samego systemu informatycznego, tej samej decyzji przełożonego czy budżetu. W takim przypadku organizacja nie posiada redundancji, lecz papierową redundancję. Przeniesienie typologii Perrowa na grunt państwa pozwala lepiej rozumieć awarie instytucjonalne. Państwo doświadcza incydentów: lokalnego błędu urzędu, awarii systemu, opóźnienia decyzji czy błędnej interpretacji przepisu. Doświadcza też wypadków komponentowych: źle napisanej ustawy, niesprawnej instytucji, wadliwego systemu informatycznego lub niewydolnego procesu zamówień. Najpoważniejsze są jednak wypadki systemowe państwa. Dochodzi do nich wtedy, gdy kilka pozornie niezależnych słabości zaczyna się wzajemnie wzmacniać. Niejasne prawo spotyka przeciążone sądy; te z kolei zderzają się z niepewnością inwestorów. Niepewność potęgują opóźnienia administracyjne, które napotykają presję polityczną. Presja ta wymusza pośpieszne nowelizacje, a te produkują kolejne niejasności.

Nikt pojedynczo „nie wysadził państwa". A jednak system generuje skutki, których nikt nie chciał i za które wszyscy częściowo odpowiadają. Tak wyglądają normalne wypadki instytucjonalne. Nie zawsze towarzyszy im dramatyczny moment eksplozji; czasem są długim osuwaniem się zdolności działania. Państwo nie wybucha. Państwo coraz częściej nie dowozi. Jest to mniej widowiskowe niż katastrofa techniczna, lecz społecznie równie groźne. Wypadek systemowy jest politycznie niewygodny, ponieważ osłabia prostą narrację winy. Polityka kocha personalizację: winny minister, urzędnik, dyrektor, poprzednik, następca, opozycja czy media. Taka narracja ma energię, konflikt i dostarcza dobrych kadr telewizyjnych.

Analiza systemowa jest mniej efektowna. Wskazuje, że problem nie tkwi wyłącznie w człowieku, lecz w architekturze relacji, presjach, braku buforów, błędnym projekcie kompetencji czy sprzężeniach między instytucjami. To nie oznacza, że nikt nie ponosi odpowiedzialności – przeciwnie, jest ona głębsza. Nie wystarczy usunąć człowieka; trzeba zmienić układ, który będzie produkował podobne zdarzenia z innymi ludźmi. Dlatego myślenie Perrowa jest tak istotne dla kultury państwowej. Uczy, że dymisja nie jest reformą, raport nie jest naprawą, a nowa procedura nie gwarantuje bezpieczeństwa. Znalezienie winnego nie oznacza zrozumienia przyczyny.

Z praktycznego punktu widzenia typologia Perrowa pozwala po każdym zdarzeniu zadać serię pytań: Czy mieliśmy do czynienia z awarią części, jednostki, podsystemu czy całego systemu? Czy sekwencja zdarzeń była liniowa i przewidywalna? Czy pojawiły się interakcje między niezależnymi podsystemami? Czy operatorzy dysponowali bezpośrednią informacją o stanie systemu, czy jedynie pośrednimi wskaźnikami?

Czy zabezpieczenia uprościły sytuację, czy dodały nowe zależności? Czy presja czasu uniemożliwiła diagnozę? Czy wypadek był wynikiem jednej usterki, czy konfiguracji wielu drobnych awarii? Czy

proponowane środki naprawcze usuwają przyczynę systemową, czy tylko ostatni widoczny objaw? Te pytania są ważniejsze niż rytualne „kto zawinił?”. Pytanie o winę jest niezbędne w prawie i etyce, ale pytanie o strukturę jest kluczowe dla prewencji. Można ukarać winnego, nie zmniejszając ryzyka. Można też zrozumieć system i dopiero wtedy sensownie przypisać odpowiedzialność. Wypadek systemowy nie jest większą wersją zwykłej awarii – to inny rodzaj zdarzenia. Zwykła awaria ma linię przyczynową; wypadek systemowy ma sieć interakcji. Tę pierwszą często można naprawić lokalnie, ten drugi wymaga zmiany relacji między elementami. Zwykła awaria pyta: co się zepsuło? Wypadek systemowy pyta: jak system umożliwił, by kilka drobnych zakłóceń stworzyło katastrofę?

To rozróżnienie stanowi serce teorii Perrowa. Bez niego każde poważne zdarzenie będziemy sprowadzać do błędu człowieka, wady części lub braku procedury. Wtedy będziemy naprawiać świat tak, jakby pożar był problemem zapałki, a nie składu materiałów łatwopalnych, wentylacji, nadzoru i zamkniętych wyjść ewakuacyjnych. Perrow każe myśleć trudniej. Ale właśnie dlatego jest potrzebny.

> W świecie obsesyjnie dążącym do optymalizacji i eliminacji wszelkich nadmiarów, zapominamy, że to właśnie 'luz' – ten nieefektywny z punktu widzenia kosztów margines czasu i zasobów – jest jedyną rzeczą, która oddziela zwykłą awarię od nieodwracalnej katastrofy. System bez buforów może wyglądać na dynamiczny i sprawny, lecz w rzeczywistości przypomina szkło hartowane: wytrzymuje ogromne napięcia, by w jednej sekundzie rozsypać się w pył. Czy zatem nasza nowoczesna definicja efektywności nie jest w istocie systematycznym demontażem bezpieczników, który czyni wielki wybuch jedynie kwestią czasu?

Inspiracje

[1] 

"Normal Accidents" Charles Perrow

Princeton University Press | ISBN: 9781400828494

Charles Perrow (1925–2019) był wybitnym amerykańskim socjologiem i teoretykiem organizacji. Przez wiele lat wykładał na Uniwersytecie Yale, gdzie był emerytowanym profesorem socjologii. Perrow jest najbardziej znany ze swojej pionierskiej pracy w dziedzinie teorii organizacji, a w szczególności z opracowania „Teorii Przypadków Normalnych", która zakłada, że w złożonych, ściśle powiązanych systemach wypadki są nieuniknione, a nie wyłącznie wynikiem błędu ludzkiego. Jego badania wywarły głęboki wpływ na socjologię, zarządzanie i inżynierię bezpieczeństwa. W trakcie swojej kariery koncentrował się na funkcjonowaniu dużych organizacji i biurokracji, często krytykując koncentrację władzy i ryzyko związane ze złożonymi systemami technologicznymi. Jego wkład naukowy pozostaje fundamentalny dla zrozumienia zachowań organizacyjnych, zarządzania ryzykiem oraz socjologicznych badań nad technologią i społeczeństwem.

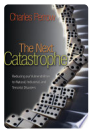
Charles Perrow *(1925–2019) was a prominent American sociologist and organizational theorist. He served as a professor at Yale University for many years, where he was an emeritus professor of sociology. Perrow is best known for his pioneering work in organizational theory, specifically his development of 'Normal Accident Theory,' which posits that in complex, tightly coupled systems, accidents are inevitable rather than the result of human error alone. His research profoundly influenced the fields of sociology, management, and safety engineering. Throughout his career, he focused on how large-scale organizations and bureaucracies function, often critiquing the concentration of power and the risks associated with complex technological systems. His scholarly contributions remain foundational to understanding organizational behavior, risk management, and the sociological study of technology and society.*

Yale University

Literatura uzupełniająca

Książki

Autorzy przywoływani w artykule:



[1] "The Next Catastrophe"

Charles Perrow

2011 | Princeton University Press | ISBN: 9780691150161

[2] "Organizing America"

Charles Perrow

2009 | Princeton University Press | ISBN: 9781400825080

[3] "Authority, Goals and Prestige in a General Hospital"

Charles Perrow

1960

[4] "Organizational Analysis"

Charles Perrow

1974

[5] "Complex Organizations"

Charles Perrow

1979 | Pearson Scott Foresman

[6] "A Society of Organizations"

Charles Perrow

1990 | ISBN: 9788479190170

Literatura pokrewna (Google Scholar):

[7] "Good Strategy Bad Strategy The Difference and Why It Matters Richard Rumelt"

[8] "Outliers Malcolm Gladwell"

[9] "Humble Pi A Comedy of Maths Errors Matt Parker"

[10] "Why Stock Markets Crash Didier Sornette"

[11] "Judgment under Uncertainty Heuristics and Daniel Kahneman"

Artykuły naukowe

Artykuły pokrewne (Google Scholar):

[1] "Normal Accidents: Living with High Risk Technologies"

A. J. Grimes, Charles Perrow

1985 | Academy of Management Review | DOI: 10.2307/257982

Google Scholar

[2] "Ambiguity and Choice in Organizations."

Charles Perrow, James G. March, Johan P. Olsen

1977 | Contemporary Sociology A Journal of Reviews | DOI: 10.2307/2064777

Google Scholar

[3] "A Framework for the Comparative Analysis of Organizations"

Charles Perrow

1967 | American Sociological Review | DOI: 10.2307/2091811

Google Scholar

[4] "Complex Organizations: A Critical Essay"

Neil Fligstein, Charles Perrow

1990 | Teaching Sociology | DOI: 10.2307/1318250

Google Scholar

[5] "The Logic of Collective Action: Public Goods and the Theory of Groups."

Charles Perrow, Mancur Olson

1973 | Social Forces | DOI: 10.2307/2576430

Google Scholar

[6] "Insurgency of the Powerless: Farm Worker Movements (1946-1972)"

J. Craig Jenkins, Charles Perrow

1977 | American Sociological Review | DOI: 10.2307/2094604

Google Scholar

[7] "Organizational Analysis: A Sociological View"

Charles Perrow

1970 | Medical Entomology and Zoology

Google Scholar

Tekst opracowany z udziałem sztucznej inteligencji.
Redakcja i kontrola merytoryczna: Fundacja Dobre Państwo.
APA ONE Publishing System

Article ID: 8b3b7aa9-bf45-4146-85e3-8cdc340a37e8