Geometria bezpieczeństwa: Jak mierzyć odporność systemów

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje koncepcję geometrii bezpieczeństwa jako kluczowego narzędzia do mierzenia odporności systemów infrastruktury krytycznej. Autor wskazuje na konieczność zrozumienia sieciowej architektury powiązań zamiast prostego gromadzenia zasobów. Wykorzystując teorię grafów oraz teorię gier, tekst pokazuje, jak matematycznie modelować interakcje między systemem a zagrożeniami. W kontekście współczesnych wyzwań geopolitycznych przywołano ramy prawne takie jak dyrektywy CER, NIS2 oraz rozporządzenie DORA. Podkreślono, że bezpieczeństwo nowoczesnego państwa zależy od niewidzialnej geometrii połączeń, która decyduje o zdolności do przetrwania w warunkach ekstremalnego stresu, awarii czy sabotażu. To interdyscyplinarne spojrzenie łączy inżynierię, ekonomię i prawo w służbie niezawodności usług podstawowych.

This article examines the concept of security geometry as a key tool for measuring the resilience of critical infrastructure systems. The author points to the need to understand the network architecture of connections rather than simply pooling resources. Using graph theory and game theory, the text demonstrates how to mathematically model interactions between systems and threats. Legal frameworks such as the CER, NIS2, and DORA directives are referenced in the context of contemporary geopolitical challenges. It emphasizes that the security of a modern state depends on the invisible geometry of connections, which determines the ability to survive conditions of extreme stress, failure, or sabotage. This interdisciplinary perspective combines engineering, economics, and law in the service of the reliability of essential services.

Monografia Sambora Guze podejmuje próbę zdefiniowania infrastruktury krytycznej nie jako zbioru statycznych aktywów, lecz jako dynamicznej anatomii przetrwania współczesnego państwa. Autor, odrzucając publicystyczny patos na rzecz surowej

dyscypliny matematycznej, stawia tezę, że kluczem do bezpieczeństwa systemowego jest głębokie zrozumienie gęstej sieci zależności. Wykorzystując teorię grafów i teorii gier, Guze przekłada abstrakcyjne zjawiska systemowe na precyzyjne parametry, umożliwiając inżynierom i decydentom identyfikację punktów krytycznych oraz modelowanie awarii kaskadowych. Publikacja ta stanowi głos w debacie nad przejściem od biernej ochrony obiektów do aktywnego budowania odporności, wymuszonego przez współczesne regulacje, takie jak dyrektywy CER, NIS2 czy rozporządzenie DORA. W dobie narastającej konwergencji cyberfizycznej, autor ostrzega przed konformizmem poznawczym i pokusą nadmiernej złożoności, która często maskuje strukturalną kruchość systemów. Praca ta jest nie tylko inżynieryjnym podręcznikiem, lecz manifestem metodologicznym, który uczy, jak w świecie niepewności i rosnących zagrożeń geopolitycznych, świadomie zarządzać architekturą naszych fundamentów cywilizacyjnych, odróżniając realną redundancję od kosztownych pozorów bezpieczeństwa.

SŁOWA KLUCZOWE

infrastruktura krytyczna | geometria bezpieczeństwa | teoria grafów | odporność systemów | dyrektywa CER | NIS2 | rozporządzenie DORA | topologia sieci | zarządzanie ryzykiem | niezawodność | węzły i krawędzie | teoria gier | bezpieczeństwo operacyjne | modelowanie matematyczne | automatyzacja ochrony

Infrastruktura krytyczna jako anatomia przetrwania

Była niegdyś pewna wspólnota, która z niemal dziecięcą ufnością chlubiła się stanem swojego posiadania, wierząc głęboko, że nowoczesność jest po prostu trwałym i niezbywalnym przywilejem. W jej inwentarzu znajdowało się wszystko: od światła i wody, przez magistrale przesyłowe, aż po lśniące centra danych i sztaby ludzi przekonanych, że świat jest jedynie zbiorem gotowych produktów. Dopiero gdy zawiódł jeden, pozornie nieistotny element, owa zbiorowość odkryła bolesną prawdę, którą cywilizacje zazwyczaj dostrzegają o krok za późno. Nie wystarczy bowiem gromadzić zasoby, gdyż kluczem do trwania jest zrozumienie głębokiej architektury ich współistnienia, a nie tylko ich fizyczna obecność. Nowoczesne państwo nie upada wszak z powodu

nagłego braku dóbr, lecz przez fundamentalne niezrozumienie gęstej sieci zależności między nimi. W tym ujęciu infrastruktura krytyczna nie jest magazynem aktywów. Jest anatomią przetrwania.

Monografia Sambora Guze wyrasta właśnie z tej intuicji, przy czym jej siła nie opiera się na taniej retoryce alarmu, lecz na surowej dyscyplinie myślenia. Autor nie serwuje nam efektownych metafor katastroficznych, budując zamiast tego precyzyjny aparat do badania mechanizmów podtrzymujących życie zbiorowe pod presją awarii, błędu czy sabotażu. Centralna teza pracy brzmi niepokojąco jasno: krytyczne systemy można i należy modelować za pomocą teorii grafów, czyli metody odwzorowania infrastruktury jako sieci powiązanych węzłów i krawędzi. Równie istotna okazuje się teoria gier, czyli matematyczne badanie interakcji między systemem a naturą lub agresorem, co pozwala na strategiczne planowanie ochrony. Ta matematyczna prostota nie jest słabością, lecz warunkiem koniecznym, by wypracowane modele znalazły realne zastosowanie w świecie technicznym. Największym zagrożeniem bywa bowiem akademicka pycha, która tworzy konstrukcje zbyt subtelne, by inżynier mógł z nich skorzystać w chwili, gdy naprawdę płonie stacja.

Książka Guze posiada wymiar zarazem inżynieryjny, ekonomiczny, prawny oraz kulturowy, co nadaje jej wywodowi głęboko interdyscyplinarny charakter. Perspektywa ekonomiczna przypomina nam, że każda redundancja kosztuje, a każda oszczędność poczyniona w niewłaściwym miejscu mści się z bezlitosnym procentem składanym w czasie kryzysu. Z kolei wymiar kulturowy obnaża iluzję beztarciowej ciągłości, w której żyją społeczeństwa późnej nowoczesności, oczekując, że system płatniczy zawsze autoryzuje ich codzienne wybory. Wszystko ma działać bezszelestnie aż do momentu, gdy okaże się, że nasza cywilizacja cyfrowa jest równie materialna i podatna na zniszczenie jak średniowieczny most. Tyle że jej konstrukcyjne belki pozostają ukryte pod gładką warstwą interfejsów, co sprawia, że rzadko dostrzegamy moment, w którym struktura zaczyna trzeszczeć pod ciężarem własnej złożoności.

Współczesny paradygmat naukowy i legislacyjny coraz wyraźniej potwierdza, że infrastruktury nie wolno postrzegać wyłącznie jako zbioru statycznych obiektów wymagających fizycznej ochrony. Unijna dyrektywa CER ujęła ten problem w języku odporności, czyli zdolności systemu do przygotowania się na zagrożenia oraz szybkiego odzyskania funkcji po wystąpieniu zakłócenia. Równolegle dyrektywa NIS2 rozszerzyła wspólną ramę cyberbezpieczeństwa na osiemnaście kluczowych sektorów, uznając cyfrową stabilność za fundament bezpieczeństwa usług podstawowych. Z kolei rozporządzenie DORA ustanawia w sektorze finansowym rygorystyczny reżim operacyjny, czyniąc z odporności twardy obowiązek regulacyjny, a nie tylko opcjonalny dodatek do zarządzania ryzykiem. Te zmiany prawne odzwierciedlają przejście od biernego oznaczania infrastruktury ku aktywnemu zarządzaniu jej zdolnością do przetrwania w warunkach ekstremalnego stresu.

W polskim porządku prawnym oficjalna architektura ochrony infrastruktury krytycznej pozostaje szeroka, obejmując energię, łączność, finanse, a nawet systemy związane z żywnością, wodą i ratownictwem. Katalog ten, podobnie jak amerykańska perspektywa CISA obejmująca szesnaście sektorów, dowodzi, że mimo różnic jurysdykcyjnych rdzeń problemu pozostaje wszędzie wspólny. Bezpieczeństwo nie zaczyna się bowiem od subiektywnego poczucia spokoju, lecz od zdolności precyzyjnego nazwania i zrozumienia struktury ryzyka wewnątrz skomplikowanych układów. Państwo trwa dokładnie tak długo, jak długo sprawnie funkcjonują systemy, których większość obywateli nie dostrzega, dopóki te nagle nie zamilkną, obnażając naszą kruchość. Ostatecznie to właśnie ta niewidzialna geometria połączeń decyduje o tym, czy nasza wspólnota przetrwa próbę czasu, błędu ludzkiego oraz nieprzewidzianych konfliktów geopolitycznych.

Matematyczna demaskacja: Grafy jako fundament odporności

Wyobraźmy sobie wspólnotę, która zamiast wznosić coraz wyższe mury, postanawia wreszcie zrozumieć anatomię własnych fundamentów. Monografia Guze jawi się na tym tle jako praca osobliwie trzeźwa, niemal ascetyczna w swej intelektualnej rzetelności. Autor nie ulega pokusie pogoni za modnymi terminami, choć bez trudu mógłby ubrać swoje wywody w piórka współczesnego żargonu bezpieczeństwa. Zamiast żonglować pojęciami takimi jak ryzyko systemowe czy konwergencja cyberfizyczna, wybiera on drogę znacznie bardziej wymagającą i surową. Pyta mianowicie, jak te zjawiska policzyć, jak odwzorować ich wewnętrzną logikę i ująć w precyzyjne parametry to, co w publicystyce zbyt często zamienia się w gęste, słowne dymy. Jest to decyzja metodologiczna o fundamentalnym znaczeniu dla jakości debaty publicznej.

W dyskusji o infrastrukturze krytycznej, czyli zbiorze kluczowych zasobów niezbędnych do funkcjonowania państwa, panuje bowiem chroniczny nadmiar patosu przy jednoczesnym niedoborze dyscypliny modelowej. Powszechnie akceptujemy tezę, że wszystko jest istotne, lecz rzadko potrafimy wskazać, które konkretnie zależności decydują o stabilności całości. Tutaj właśnie wkracza modelowanie grafowe, czyli metoda odwzorowania infrastruktury jako sieci powiązanych węzłów i krawędzi o określonej dynamice. Nie służy ono jako matematyczna dekoracja, lecz jako precyzyjny język opisu porządku ukrytego pod powierzchnią instytucji i urządzeń. Dzięki niemu to, co w języku administracyjnym bywa mgłą, w ujęciu matematycznym staje się czytelną strukturą. Węzeł przestaje być martwym obiektem, stając się punktem sprzężenia, sterowania lub krytycznego tranzytu.

W tym ujęciu graf staje się narzędziem demaskacji prawdziwego ustroju sieci, obnażając jej ukryte słabości i punkty ciężkości. Wielką zaletą analizy Guze jest to, że nie zatrzymuje się ona na poziomie podręcznikowych truizmów o prostych połączeniach. Autor wskazuje na przejście od topologii statycznej do topologii funkcjonalnej, co ma znaczenie wręcz ontologiczne dla rozumienia systemów. Sama informacja o istnieniu połączenia nie mówi nam wszak nic o tym, jak system żyje, starzeje się lub odzyskuje równowagę po wstrząsie. Dopiero przypisanie wag i konkretnych funkcji do krawędzi umożliwia analizę o charakterze rzeczywiście inżynierskim. To pozwala wydobyć infrastrukturę z pułapki zbyt ubogiego modelu, który ignoruje różnorodność przepływów.

Sieć nie składa się przecież z relacji równoważnych, o czym boleśnie przekonujemy się w momentach nagłych awarii lub celowych ataków. Jedna krawędź może przenosić marginalny ruch lokalny, podczas gdy inna obsługuje krytyczny wolumen energii decydujący o przetrwaniu aglomeracji. Jeden węzeł jest jedynie dogodnym punktem na mapie, inny zaś okazuje się całkowicie niezastępowalnym sercem systemu. Niezawodność, czyli prawdopodobieństwo poprawnego działania układu w konkretnych warunkach, zależy od zrozumienia tych właśnie niuansów. Niektóre elementy dają się odtworzyć w kilka godzin, inne wymagają miesięcy pracy i skomplikowanych łańcuchów dostaw. Bez tej wiedzy każda strategia ochrony pozostaje jedynie zbiorem pobożnych życzeń.

W tym miejscu ekonomista rozpoznaje natychmiast własny, odwieczny problem rzadkości zasobów i konieczności dokonywania trudnych wyborów. Nie ma bowiem odporności bez kosztu alternatywnego ani bezpieczeństwa bez decyzji, które aktywa należy uprzywilejować kosztem innych. Infrastruktura krytyczna nie jest magazynem aktywów, lecz anatomią przetrwania, w której każda redundancja konkuruje z efektywnością kapitałową. Maksymalizacja niezawodności musi nieustannie mierzyć się z presją minimalizacji kosztów operacyjnych. To sprawia, że monografia Guze zasługuje na uwagę nie tylko inżynierów, ale i ekonomistów instytucjonalnych. Pokazuje ona, że błąd w wycenie ryzyka infrastrukturalnego bywa błędem cywilizacyjnym, a nie tylko budżetowym.

Również prawnik dostrzeże w tej pracy zapowiedź głębokiej zmiany normatywnej, która przesuwa akcent z ochrony obiektów na budowanie odporności. Odporność, czyli zdolność systemu do adaptacji oraz szybkiego powrotu do sprawności, staje się dziś nowym standardem odpowiedzialności operatorów. Unijna dyrektywa CER oraz regulacje NIS2 czynią z cyberbezpieczeństwa element obowiązkowego ładu operacyjnego, a nie tylko techniczny dodatek. W sektorze finansowym rozporządzenie DORA idzie jeszcze dalej, uznając zależność od dostawców technologii za źródło ryzyka systemowego. Język matematycznego modelowania przestaje być

zatem luksusem poznawczym dla nielicznych ekspertów. Staje się on niezbędną infrastrukturą dowodową dla nowoczesnego zarządzania i nadzoru.

Współczesne raporty międzynarodowe, w tym najnowsze opracowania OECD, coraz mocniej akcentują potrzebę projektowania odporności już na etapie finansowania i budowy. Obecny krajobraz zagrożeń unaocznia nam wszystkim wysoki koszt nadmiernej koncentracji i zależności od nielicznych dostawców technologicznych. Ryzyko łańcucha dostaw oraz złożoność wzajemnych powiązań stanowią dziś główne bariery w osiąganiu realnej stabilności systemowej. W tym kontekście intuicje badawcze Guze okazują się niemal prorocze, trafiając w samo sedno współczesnych dylematów bezpieczeństwa. Matematyczna demaskacja struktury sieci pozwala nam bowiem widzieć wcześniej i rozumieć głębiej. To tylko tyle i aż tyle.

Geometria odporności: Jak topologia definiuje bezpieczeństwo

Sieć nie jest jedynie sumą rozproszonych komponentów, lecz stanowi ustrój wzajemnych zależności, w którym każda niedoszacowana relacja wystawi nam kiedyś bolesny rachunek. Warto przy tym zrewidować samo pojęcie niezawodności, czyli prawdopodobieństwa poprawnego działania systemu w określonym czasie i warunkach, gdyż w debacie publicznej bywa ono niebezpiecznie banalizowane. Niezawodność nie oznacza bowiem, że coś po prostu „działa” w sposób ciągły, lecz wymaga precyzyjnego określenia standardów oraz horyzontu czasowego. Pytamy przecież o zachowanie struktury pod konkretnym obciążeniem, wobec specyficznych zakłóceń i przy zachowaniu odpowiedniego marginesu bezpieczeństwa. Z perspektywy infrastruktury krytycznej kluczowe jest nie tylko to, czy system funkcjonuje, lecz jaką funkcję zachowuje i jak długo potrafi ją utrzymać.

Tu właśnie ujawnia się przewaga modeli wielostanowych nad dwustanową naiwnością, która dzieli świat na sferę pełnej sprawności oraz całkowitej zapaści. Systemy techniczne rzadko przechodzą do stanu „śmierci” jednym gwałtownym ruchem, ponieważ zazwyczaj najpierw tracą jakość, potem przepustowość, a następnie elastyczność i zdolność buforowania. Kto nie uwzględnia tej dynamiki w swoich modelach, ten projektuje infrastrukturę niczym lekarz opisujący chorobę wyłącznie kategoriami: żywy albo martwy. A przecież to, co decyduje o ostatecznym przetrwaniu, rozgrywa się właśnie w owej szarej strefie stopniowej degradacji funkcji. Notatka źródłowa słusznie akcentuje wagę opisu topologicznego jako uniwersalnego paradygmatu niezawodnościowego dla struktur sieciowych, co zasługuje na głębsze rozwinięcie. Topologia jest bowiem tym poziomem opisu, na

którym najwyraźniej widać, czy system został zaprojektowany jako struktura promieniowa, pętlowa, kratowa czy może hybrydowa.

Te różnice formalne nie są jedynie estetycznym wyborem inżyniera, lecz niosą ze sobą konkretny i unikalny profil ryzyka operacyjnego. Sieci promieniowe bywają tanie i przejrzyste, niemniej są one najbardziej podatne na odcięcie końcowych odbiorców przy pojedynczej awarii. Z kolei sieci kratowe, choć znacznie kosztowniejsze w budowie, oferują wielość alternatywnych ścieżek przesyłu i wyższą zdolność rekonfiguracji. Sieci bezskalowe imponują efektywnością w normalnych warunkach, lecz wystawiają nas na katastrofalne skutki precyzyjnego uderzenia w kluczowe węzły, czyli huby. Podobnie sieci małego świata, które zachwycają skrótami dystansu, często ukrywają niebezpieczną koncentrację funkcji w miejscach rozsadzających lokalną stabilność. Topologia jest zatem polityką bezpieczeństwa zapisaną w geometrii połączeń, określającą granice naszej odporności na nieprzewidziane zdarzenia.

W tym kontekście dochodzimy do jednego z najbardziej twórczych elementów pracy Guze, czyli wykorzystania parametrów dominacji grafowej do badania podatności. Zamiast operować nieostrą nowomową o „wąskich gardłach" czy „obiektach strategicznych", autor wprowadza rygorystyczne miary pozwalające przejść od intuicji do rygoru. Liczba dominacji pokazuje nam bowiem, jaki minimalny zbiór węzłów wystarcza do sprawowania pełnej kontroli nad całą strukturą. Różne odmiany liczby uwiązania ujawniają natomiast, jak niewielka ingerencja w system może drastycznie zwiększyć koszt utrzymania kontroli lub rozbić jego spoistość. To fundamentalne spostrzeżenie, gdyż odporność, czyli zdolność systemu do adaptacji i szybkiego odzyskania funkcji po zakłóceniu, nie polega na posiadaniu ogromnej liczby nadmiarowych elementów. Odporność polega na tym, że uszkodzenie niewielu ogniw nie wywołuje nieproporcjonalnie dużej degradacji funkcji. To tylko tyle i aż tyle.

W świecie operatorów infrastruktury to rozróżnienie oddziela systemy prawdziwie solidne od tych, które jedynie sprawiają wrażenie potężnych. Można przecież zbudować sieć kosztowną i politycznie efektowną, która w obliczu kryzysu okaże się matematycznie krucha. Można też zaprojektować system z umiarem, lecz z wysoką inteligencją topologiczną, która przetrwa próbę czasu i stresu. Nie każda złożoność jest siłą, wszak czasem bywa ona jedynie bardzo drogo ubraną słabością, maskującą brak głębszej logiki projektowej. Z perspektywy kulturoznawczej uderza tutaj fakt, że infrastruktura krytyczna stanowi jeden z najczystszych przykładów współczesnej niewidzialności pracy cywilizacyjnej. Im lepiej ona działa, tym mniej o niej myślimy, uznając jej niezawodność za naturalne tło, a nie historyczne osiągnięcie wymagające podtrzymywania.

Z tego powodu wspólnoty późnokapitalistyczne mają chroniczną skłonność do niedoinwestowania systemów, które powinny być nudne, a nie widowiskowe. Transformator nie wygrywa wyborów, a

magistrala światłowodowa rzadko budzi zbiorowe wzruszenie, choć to one rozstrzygają o naszym przetrwaniu. Rezerwowa trasa przesyłowa nie jest wdzięcznym symbolem politycznym, niemniej to ona decyduje, czy wspólnota działa jak organizm, czy jak przypadkowy zbiór urządzeń. Guze uderza w samo serce kultury konformizmu infrastrukturalnego, pokazując, że cywilizacja nie trwa dzięki sloganom o innowacyjności, lecz dzięki zrozumieniu redundancji. Bezpieczeństwo nie zaczyna się od poczucia bezpieczeństwa, lecz od zdolności nazwania struktury ryzyka i świadomego zarządzania awaryjnością.

Nie mniej doniosła jest tutaj rola teorii gier, czyli narzędzia matematycznego służącego do modelowania interakcji między atakującym a obrońcą. Jeżeli teoria grafów daje nam język topologii, to teoria gier dostarcza języka konfliktu, decyzji oraz wszechobecnej niepewności. Pozwala ona na strategiczne planowanie ochrony i przewidywanie scenariuszy rozwoju sytuacji kryzysowych w sposób znacznie bardziej wyrafinowany niż prosta ekstrapolacja. Optymalizacja, czyli proces poszukiwania najlepszych rozwiązań przy uwzględnieniu ograniczeń zasobowych, zmusza nas do przejścia od diagnozy do konkretnych projektów. A infrastruktura krytyczna nie jest magazynem aktywów, jest anatomią przetrwania, wymagającą od nas rygoru zamiast życzeniowego myślenia. Kto widzi tylko ostatni etap, ten widzi za mało i widzi za późno.

Od teorii gier do algorytmów: Matematyka w służbie odporności

Infrastruktura krytyczna, czyli zbiór kluczowych zasobów i systemów niezbędnych do funkcjonowania państwa, nie unosi się w próżni fizycznej ani tym bardziej w próżni intencji. Funkcjonuje ona w świecie gęstym od zdarzeń, gdzie natura, ślepy przypadek i błąd ludzki nieustannie spotykają się z wrogim aktorem oraz presją ekonomiczną. W tym strategicznym teatrze działań każda awaria techniczna może stać się zarzewiem kryzysu politycznego, a niedobór zasobów wymusza brutalne ograniczenie czasu reakcji. Dlatego modelowanie gier z naturą czy schematów typu atakujący-obrońca nie jest jedynie kaprysem teoretyka zakochanego w formalizmie. To próba uchwycenia realnej sytuacji decyzyjnej, w której operator lub administrator publiczny musi zarządzać ryzykiem pod ogromną presją. Bezpieczeństwo nie zaczyna się od poczucia bezpieczeństwa, lecz od zdolności nazwania struktury ryzyka.

Szczególnie ożywcze wydaje się sprzęgnięcie teorii gier, czyli narzędzia matematycznego służącego do modelowania interakcji między stronami, z klasyczną analizą SWOT. W powszechnym odbiorze SWOT bywa dziś instrumentem korporacyjnej banalności, rodzajem konsultingowego lustra, w którym organizacje podziwiają własną, zazwyczaj zawyżoną samoocenę. U Guze zostaje on jednak

wprzęgnięty w rygorystyczną strukturę gry decyzyjnej, co nadaje mu zupełnie nowy ciężar gatunkowy. Oznacza to przejście od statycznego katalogowania mocnych i słabych stron do dynamicznego modelowania wyboru strategii w obliczu niepewnych stanów otoczenia. To ruch o wiele poważniejszy, niż mogłoby się wydawać na pierwszy rzut oka. Wszak infrastruktura krytyczna nie jest magazynem aktywów, lecz anatomią przetrwania.

Jeszcze ciekawszy jest algorytm strażaka, który pozwala symulować rozprzestrzenianie się zagrożeń i badać, ile elementów systemu da się uratować przy danym reżimie interwencji. Kryje się w tym coś niemal parabolicznego, co przypomina nam o dawnych wspólnotach walczących z żywiołem przy pomocy prymitywnych barier. Najpierw ogień zajmuje jeden punkt, później drugi, a w końcu trawi całą strukturę, jeśli nikt nie przewidział kierunku wiatru. Kto zawczasu nie policzył, które tamy trzeba postawić i w jakiej kolejności, ten w chwili kryzysu będzie jedynie improwizował na gruzach własnej pewności siebie. Matematyka staje się tu zatem narzędziem pokory wobec nieuchronności zdarzeń losowych. Współczesna praktyka brutalnie potwierdza słuszność tej optyki, pokazując, że teoretyczne modele mają swoje krwawe odbicie w rzeczywistości.

Ataki na sektor energetyczny czy skoordynowane incydenty w infrastrukturze przemysłowej pokazują, że granica między awarią techniczną a paraliżem systemowym staje się niebezpiecznie cienka. W Polsce raporty CERT Polska z 2026 roku informowały o uderzeniach wymierzonych w instalacje OZE oraz elektrociepłownie, niosących realne ryzyko odcięcia ciepła dla setek tysięcy odbiorców. To nie jest już tylko sucha teoria z podręcznika bezpieczeństwa, lecz twarde przypomnienie o naszej zbiorowej wrażliwości. Energetyka, cyberprzestrzeń i ciągłość życia codziennego stanowią dziś jeden, nierozerwalnie połączony organizm ryzyka. Właśnie dlatego na tak dużą uwagę zasługuje rozdział poświęcony optymalizacji, czyli procesowi poszukiwania najlepszych rozwiązań przy ograniczonych zasobach. Większość sporów o infrastrukturę cierpi bowiem na tę samą, chroniczną chorobę braku realizmu.

Z jednej strony polityczna wyobraźnia chętnie szafuje hasłem maksimum bezpieczeństwa, które brzmi dumnie, ale niewiele wyjaśnia. Z drugiej strony ekonomiczna praktyka przypomina, że nie istnieje bezpieczeństwo absolutne, które nie wiązałoby się z astronomicznym kosztem. Pomiędzy tymi biegunami rozciąga się prawdziwe pole decyzji, którego Guze nie próbuje w magiczny sposób zlikwidować. Przeciwnie, uznaje on konflikt celów za stan normalny i dlatego odwołuje się do optymalności Pareto. W świecie systemów krytycznych nie szuka się rozwiązania doskonałego, ponieważ takie w naturze zazwyczaj nie występuje. Szuka się natomiast rozwiązania, które poprawia jedno dobro bez nieuzasadnionego pogarszania innych parametrów układu.

To podejście jest zarazem głęboko techniczne, bo dotyczy parametrów sieci, jak i par excellence polityczne. Każdy punkt na froncie Pareto jest w gruncie rzeczy decyzją o tym, ile społeczeństwo

chce zapłacić za określony poziom odporności. Najbardziej wywrotowym elementem tej części monografii jest jednak redukcja złożonego problemu optymalizacji do binarnego problemu plecakowego. W świecie akademickim często panuje cichy przesąd, że rozwiązanie bardziej wyrafinowane matematycznie jest z definicji rozwiązaniem lepszym. Guze wybiera pozycję odwrotną, wykazując się przy tym rzadko spotykanym, antysnobistycznym pragmatyzmem. Jeżeli da się przekształcić problem w postać prostszą, ale nadal wierną funkcjonalnie, należy to bez wahania zrobić.

Nie chodzi tu o spłycanie teorii, lecz o umożliwienie jej realnej pracy w warunkach polowych, gdzie czas jest towarem deficytowym. Inżynier nie potrzebuje modelu, który zachwyci recenzenta w zaciszu gabinetu, lecz takiego, który zadziała pod presją niepełnych danych. W tym sensie redukcja do problemu plecakowego ma wartość większą niż czysto techniczna, stając się swoistym manifestem metodologicznym. Mówi nam ona, że elegancja nauki polega nie na komplikowaniu świata, lecz na takim uproszczeniu, które niczego istotnego nie gubi. Nie każda złożoność jest siłą, czasem jest tylko drogo ubraną słabością, która zawodzi w najmniej odpowiednim momencie. Także wykorzystanie algorytmów ewolucyjnych nie jest tu jedynie modą na bioinspirację, lecz odpowiedzią na ogromną przestrzeń możliwych konfiguracji.

Infrastruktura krytyczna rzadko pozwala się zoptymalizować ręcznie i linearnie, ponieważ zmienne decyzyjne są zbyt liczne, a kryteria wzajemnie sprzeczne. Algorytm ewolucyjny, działający na populacjach rozwiązań, pozwala eksplorować kompromisy i unikać pułapki zamknięcia w lokalnym ekstremum. To znów doskonale współgra z naturą problemu, gdyż infrastruktura nie jest systemem dążącym do jednego, statycznego ideału. Jest raczej polem nieustannego przeszukiwania konfiguracji, które są możliwie dobre pod wieloma względami jednocześnie. Lecz równie ważne jak podejście dyskretne jest ujęcie ciągłe, które wydobywa pełen sens autorskich rodzin grafów ważonych. Modelowanie grafowe, czyli metoda odwzorowania sieci jako powiązanych węzłów i krawędzi, zyskuje tu zupełnie nową głębię.

Gdy wagi krawędzi i węzłów stają się funkcjami zmiennych opisujących czas, obciążenie czy koszt, możliwe staje się zastosowanie zaawansowanych metod gradientowych. Otwiera się wtedy przestrzeń analizy nie tylko projektowej, ale przede wszystkim operacyjnej, która pozwala reagować na bieżąco. Sieć nie jest już martwym rysunkiem architekta, lecz procesem, który żyje, starzeje się i reaguje na każde najmniejsze zakłócenie. Takie ujęcie jest szczególnie cenne dla analiz online oraz zarządzania ruchem w sytuacjach, gdy liczy się każda sekunda. Przejście od grafu jako statycznej mapy do grafu jako żywego organizmu staje się możliwe właśnie dzięki ciągłemu ujęciu wag. Można powiedzieć jeszcze ostrzej: to przejście od geometrii połączeń do ontologii działania, gdzie liczy się nie tylko to, co jest połączone, ale jak to połączenie oddycha pod obciążeniem. Toteż matematyka w

służbie odporności przestaje być tylko zestawem wzorów, a staje się strategią przetrwania w niepewnym jutrze.

Geometria zależności: Dlaczego infrastruktura wymaga nowego języka

Kto w dobie inteligentnych sieci energetycznych i dynamicznych łańcuchów dostaw analizuje infrastrukturę krytyczną wyłącznie w sposób statyczny, ten przypomina obserwatora usiłującego zrozumieć tętniący organizm na podstawie czarno-białej fotografii. Zdjęcie, choćby najbardziej kunsztowne, pozostaje jedynie martwym zapisem chwili, który w żaden sposób nie pozwala na sprawne sterowanie przepływem krwi w żyłach systemu. Właśnie w tym miejscu ujawnia się fundamentalny błąd poznawczy wielu współczesnych strategów bezpieczeństwa, którzy mylą inwentaryzację zasobów z ich rzeczywistym, operacyjnym funkcjonowaniem. Infrastruktura krytyczna nie jest bowiem magazynem aktywów, lecz anatomią przetrwania, wymagającą języka zdolnego opisać ruch, a nie tylko trwanie. Bez zrozumienia tej dynamiki pozostajemy zakładnikami iluzji kontroli, która pryska przy pierwszym poważniejszym wstrząsie systemowym.

Warto w tym kontekście powrócić do przypowieści o wspólnocie, która przez pokolenia poszukiwała źródła swojej niezłomności w coraz to nowszych paradygmatach. Początkowo sądziła ona, że jej siła tkwi w samych zasobach, by później uznać, iż to sztywne procedury stanowią ostateczną gwarancję bezpieczeństwa. Jeszcze później, zachłyśnięta postępem, uwierzyła, że panaceum na wszelkie bolączki jest powszechna cyfryzacja, czyli proces nasycania rzeczywistości rozwiązaniami informatycznymi. Dopiero seria bolesnych zakłóceń uświadomiła jej, że zasoby bez mapy zależności stają się bezużytecznym ciężarem, a procedury pozbawione modelu są jedynie jałową liturgią. Ostatecznie zrozumiała, że cyfryzacja bez odporności to tylko sposób na przyspieszone rozchodzenie się błędu w skali całego organizmu.

To właśnie w tym punkcie należy ulokować właściwą recepcję monografii Sambora Guze, która wyrasta ponad ramy typowej publikacji technicznej o teorii grafów. Autor występuje tutaj jako rzecznik walki z konformizmem poznawczym, czyli tendencją do upraszczania rzeczywistości w celu dopasowania jej do znanych schematów myślowych. Przypomina nam on dobitnie, że bezpieczeństwo nie zaczyna się od błogiego poczucia bezpieczeństwa, lecz od surowej zdolności nazwania struktury ryzyka. Książka ta nie jest zatem kolejnym podręcznikiem matematyki dyskretnej, ale ważnym głosem w debacie o tym, jak przestać patrzeć, a zacząć widzieć. Bez tej fundamentalnej zmiany optyki każda próba ochrony nowoczesnego państwa będzie skazana na reaktywność i wieczne spóźnienie wobec zagrożeń.

Dzisiejszy paradygmat bezpieczeństwa nie pyta już wyłącznie o to, jak skutecznie otoczyć murem pojedynczy, odizolowany obiekt infrastrukturalny. Zamiast tego stawia on pytania o sposoby zarządzania współzależnością sektorów oraz o metody łączenia fizycznych i cybernetycznych wymiarów ryzyka w jedną, spójną całość. Kluczowe staje się modelowanie awarii kaskadowych, czyli zjawisk, w których drobne zakłócenie w jednym węźle wywołuje lawinę problemów w odległych częściach systemu. Musimy nauczyć się rozpoznawać ryzyko koncentracji oraz identyfikować pojedyncze punkty awarii, których uszkodzenie paraliżuje funkcjonowanie całych regionów lub gałęzi gospodarki. To wyzwanie dotyczy zarówno ochrony usług podstawowych przed ekstremalną pogodą, jak i zabezpieczania ich przed wyrafinowanymi cyberatakami czy napięciami geopolitycznymi.

Współczesne organizacje międzynarodowe, takie jak OECD, coraz głośniej akcentują potrzebę odporności integrowanej już na etapie planowania, finansowania i późniejszego utrzymania systemów. Z kolei NIST definiuje odporność wspólnot jako aktywną zdolność do przygotowania się, adaptacji, wytrzymania uderzenia oraz błyskawicznego odzyskiwania kluczowych funkcji po wystąpieniu incydentu. Równolegle ENISA podkreśla, że dyrektywa NIS2 znacząco wzmacnia bezpieczeństwo sektorów krytycznych poprzez radykalne zaostrzenie wymogów w zakresie cyberbezpieczeństwa i ciągłości świadczonych usług. Te trzy odmienne języki – administracyjny, naukowy oraz techniczny – znajdują wspólny mianownik właśnie w aparacie pojęciowym, który proponuje w swojej pracy Guze. Spotykają się one w obszarze precyzyjnego modelowania zależności oraz matematycznej optymalizacji odporności całego układu.

Obrona tez źródłowych zawartych w tej monografii jest dziś intelektualnie mocna nie dlatego, że świat nagle pokochał abstrakcyjną teorię grafów. Dzieje się tak, ponieważ coraz boleśniej odkrywamy granice myślenia sektorowego, liniowego i biurokratycznie odseparowanego od rzeczywistych przepływów. Energetyka nie kończy się już na granicach elektrowni, transport nie jest zamkniętym systemem logistycznym, a sektor ICT nie istnieje w próżni cyfrowej. Każdy z tych systemów staje się dla pozostałych zarazem niezbędnym zasobem, warunkiem koniecznym działania, a także potencjalnym wektorem kryzysu. W tak splecionym świecie potrzebujemy nauki, która nie boi się stosować narzędzi pozornie prostych, o ile niosą one ze sobą głębię strukturalną.

W tym miejscu monografia wykonuje swój najważniejszy ruch, odchodząc od ogólnikowego języka troski o bezpieczeństwo na rzecz precyzyjnego języka struktur i relacji. To przejście nie jest jedynie techniczną zmianą słownika, lecz stanowi wyraz zmiany cywilizacyjnego poziomu powagi w podejściu do ochrony państwa. Operatorzy, regulatorzy oraz projektanci muszą zrozumieć, że albo nauczą się rzetelnie liczyć swoje zależności, albo zapłacą za nie w przyszłości cudzym cierpieniem. Przerwany przepływ, ogromna strata gospodarcza czy kompromitacja instytucjonalna to realna

cena za ignorowanie ukrytej geometrii naszych systemów. Modelowanie infrastruktury w ujęciu Guze ma charakter rygorystyczny, lecz nie jest to jałowy rygor scholastyczny, służący jedynie teoretycznym rozważaniom.

Autor tworzy aparat pojęciowy nie po to, by zamknąć rzeczywistość w martwej symbolice, lecz aby wydobyć z niej to, co dla bezpieczeństwa systemowego jest naprawdę decydujące. Z tej perspektywy teoria grafów przestaje być tylko działem matematyki dyskretnej, a staje się swoistą epistemologią zależności, czyli nauką o granicach i metodach poznawania powiązań. Uczy ona widzieć system jako uporządkowany układ relacji między obiektami, które pełnią odmienne role i mają skrajnie różną wagę dla całości. Pozwala zrozumieć, że poszczególne komponenty mają różną podatność na zagrożenia oraz odmienny horyzont awaryjności, co determinuje ich zdolność do przejmowania funkcji. Rozdział poświęcony modelowaniu należy zatem czytać jako próbę ustanowienia języka prawdy infrastrukturalnej w świecie zdominowanym przez puste deklaracje.

W przestrzeni publicznej o bezpieczeństwie mówi się zazwyczaj w trybie życzeniowym, opierając się na przekonaniu, że system jest bezpieczny, bo posiada odpowiednie procedury. Twierdzi się, że infrastruktura jest odporna, ponieważ istnieją plany kryzysowe, oraz nowoczesna, gdyż wyposażono ją w najnowsze komponenty cyfrowe. Tymczasem z punktu widzenia inżynierii systemów takie zapewnienia są niewiele warte, dopóki nie poznamy rzeczywistej topologii sieci, czyli układu połączeń między jej elementami. Musimy wiedzieć, gdzie znajdują się punkty koncentracji, które węzły pełnią rolę dominującą i jakie krawędzie mają charakter krytyczny dla stabilności. Bez analitycznego sprawdzenia profilu przepływu oraz identyfikacji sprzężeń zwrotnych, wszelkie ćwiczenia i plany pozostają jedynie kosztowną dekoracją.

Infrastruktura krytyczna nie jest po prostu zbiorem odrębnych sektorów, lecz skomplikowanym układem współzależnych sieci, które nieustannie przenikają się funkcjonalnie. Energetyka warunkuje pracę systemów teleinformatycznych, które z kolei sterują transportem, finansami oraz kluczowymi elementami samej sieci energetycznej. Transport podtrzymuje logistykę paliw i części zamiennych, a administracja publiczna całkowicie zależy od usług cyfrowych, zasilanych energią i telekomunikacją. W tym sensie nowoczesne państwo nie przypomina już federacji pionów, lecz staje się niezwykle splątaną architekturą przepływów. Współczesne europejskie ramy prawne, zwłaszcza dyrektywy CER i NIS2, idą dokładnie w tym kierunku, kładąc nacisk na utrzymanie funkcji żywotnych.

Z tego powodu autor wprowadza kluczowe rozróżnienie między zależnością a współzależnością, co na pierwszy rzut oka może wydawać się jedynie niuansem terminologicznym. W rzeczywistości jest to dystynkcja o znaczeniu strategicznym, gdyż zależność oznacza relację jednostronną, podczas gdy współzależność opisuje relację wzajemną. Należy jednak pamiętać, że wzajemność w tym ujęciu

wcale nie musi oznaczać symetrii wpływów między poszczególnymi elementami systemu. Wiele katastrof infrastrukturalnych bierze swój początek z błędnego założenia, że skoro systemy są powiązane, to ich oddziaływanie na siebie jest w przybliżeniu równe. Tymczasem rzeczywistość pokazuje, że jedna zależność może być strukturalnie decydująca, podczas gdy inna pełni jedynie rolę pomocniczą.

Czasem zasilanie awaryjne okazuje się ważniejsze niż nominalna przepustowość sieci, a pojedynczy węzeł telekomunikacyjny ma większe znaczenie niż kilka dużych obiektów fizycznych. Modelowanie jest w tym kontekście sztuką obnażania pozorów, ponieważ sieć może wydawać się gęsta i solidna, a w rzeczywistości pozostawać niezwykle krucha. Może ona imponować nowoczesnością, a jednocześnie nie posiadać żadnych realnych marginesów rekonfiguracji, czyli zdolności do zmiany układu połączeń w sytuacji kryzysowej. Dlatego monografia tak silnie akcentuje znaczenie topologii, która nie jest tutaj geometryczną ciekawostką, lecz ontologią działania. To właśnie ona rozstrzyga o tym, czy utrata jednego połączenia rozetnie system, czy też węzły zdołają przejąć funkcje uszkodzonych komponentów.

Na tym tle szczególnie cenne wydaje się przejście od grafu prostego do grafów ważonych oraz do autorskich rodzin grafów, w których wagi przyjmują postać funkcji ciągłych. Ten krok ma rangę prawdziwego przełomu metodologicznego, ponieważ wiele klasycznych analiz sieciowych zatrzymuje się na binarnej informacji o istnieniu połączenia. Guze idzie znacznie dalej, pozwalając na opisanie subtelnych różnic w intensywności i charakterze relacji między poszczególnymi elementami infrastruktury. Dzięki temu model przestaje być jedynie statycznym schematem, a staje się dynamicznym narzędziem zdolnym do przewidywania zachowań systemu w warunkach stresu. To tylko tyle i aż tyle, by móc realnie zarządzać bezpieczeństwem w świecie, gdzie każda złożoność może być drogo ubraną słabością.

Matematyka przetrwania: Jak mierzyć prawdziwy próg bólu sieci

W świecie infrastruktury krytycznej, która wszak nie jest jedynie magazynem aktywów, lecz prawdziwą anatomią przetrwania, sama obecność połączeń to zaledwie wstęp do rzetelnej analizy. Musimy bowiem precyzyjnie rozumieć, co konkretnie płynie przez daną krawędź grafu, z jaką przepustowością oraz przy jakim poziomie ryzyka awaryjnego. Istotne staje się tu znaczenie strategiczne każdego elementu, uwikłane w skomplikowaną dynamikę czasową oraz zmienne obciążenia, które definiują codzienność systemów przesyłowych. Dopiero takie wielowymiarowe spojrzenie sprawia, że abstrakcyjny model matematyczny zaczyna rzetelnie odpowiadać brutalnej

rzeczywistości technicznej. To naturalnie prowadzi nas do fundamentalnego pytania o niezawodność – termin często nadużywany w debacie publicznej i pozbawiany swojej pierwotnej ostrości.

W ścisłym ujęciu inżynieryjnym niezawodność, czyli prawdopodobieństwo poprawnego działania systemu w określonych warunkach i czasie, przestaje być jedynie technicznym parametrem. To sformułowanie, choć na pierwszy rzut oka wydaje się suche, zawiera w sobie całą filozofię odpowiedzialności za stabilność państwa. Nie wystarczy przecież zaprojektować układu, który funkcjonuje bez zarzutu wyłącznie w warunkach idealnych, laboratoryjnych czy czysto teoretycznych. Prawdziwym wyzwaniem jest zrozumienie, jak system zachowuje się w czasie, jak postępuje jego nieuchronna degradacja oraz jak reaguje na uszkodzenia cząstkowe. Musimy wiedzieć, co dzieje się z jego funkcją pierwotną, zanim nastąpi ostateczna i całkowita utrata operacyjności, paraliżująca życie milionów obywateli.

Właśnie z tego powodu autor słusznie zestawia klasyczne podejście dwustanowe z modelem wielostanowym oraz rozwiązaniami o charakterze mieszanym. Podejście dwustanowe, operujące prostą logiką zero-jedynkową, bywa użyteczne jedynie wtedy, gdy priorytetem jest szybkość estymacji w sytuacjach skrajnie uproszczonych. Model wielostanowy staje się jednak absolutnie konieczny, gdy chcemy rzetelnie uchwycić proces starzenia się komponentów oraz częściową utratę zdolności przesyłowych. W praktyce infrastrukturalnej stan degradacji jest bowiem znacznie częściej regułą niż wyjątkiem, co wymaga od nas porzucenia binarnych schematów myślowych. Można to ująć w formule niemal aforystycznej: system nie umiera nagle, lecz najpierw słabnie, tracąc kolejno elastyczność i przepustowość.

Kto widzi tylko ostatni etap, ten widzi za mało i widzi za późno, tracąc szansę na skuteczną interwencję wyprzedzającą. Tu właśnie zaczyna się kluczowy rozdział analityczny poświęcony podatności i odporności, gdzie monografia dokonuje rzeczy w polskiej literaturze rzadkiej. Nie zadowala się ona moralnym słownikiem alarmu, lecz proponuje ścisłe wskaźniki pozwalające matematycznie opisać kruchą naturę oraz siłę sieci. Centralne miejsce zajmują tu liczby dominacji oraz parametry oparte na pojęciu uwiązania, które nadają analizie głęboki sens operacyjny. Każda sieć potrzebuje bowiem minimalnego zbioru węzłów pozwalających zachować nad nią kontrolę, monitoring czy niezbędne pokrycie funkcjonalne.

Jeżeli niewielkie usunięcie krawędzi istotnie zwiększa koszt kontroli lub rozrywa wymaganą spoistość układu, mamy do czynienia z podatnością policzalną. Właśnie dlatego bondage number, czyli parametr określający minimalną liczbę krawędzi, których usunięcie zwiększa liczbę dominacji grafu, zasługuje na szczególne uznanie. Jest to próba wydobycia z topologii tego, co dla bezpieczeństwa najistotniejsze, czyli zestawu uszkodzeń zdolnych wywołać nieproporcjonalny efekt

degradacyjny. To narzędzie intelektualnie eleganckie i jednocześnie praktycznie bezlitosne, gdyż nie pyta ono, czy system wygląda na solidny. Ono bada, ile naprawdę potrzeba, by sieć przestała zachowywać własną zdolność do dominacji oraz spójności w warunkach kryzysowych.

Dla ekonomisty taki aparat matematyczny ma dodatkową, niemal rewolucyjną wartość, pozwalając wyjść poza powierzchowną logikę kosztów jednostkowych. Pozwala on dostrzec koszty marginalne utraty odporności, co stanowi bardzo ważną korektę wobec klasycznego, często krótkowzrocznego myślenia księgowego. W świecie infrastruktury krytycznej problemem nie jest tylko cena budowy dodatkowej redundancji czy zabezpieczenia nowego, strategicznego węzła. Prawdziwym wyzwaniem jest oszacowanie, ile kosztuje brak takiego zabezpieczenia w punkcie, którego matematyczne znaczenie dla całości jest skrajnie wysokie. Transformator nie wygrywa wyborów, więc politycy często tną wydatki na to, co niewidoczne, dopóki system nie przestanie działać. Księgowość pyta o koszt komponentu, natomiast inżynieria bezpieczeństwa pyta o koszt utraty jego funkcji dla całego, złożonego układu.

Między tymi dwoma pytaniami rozciąga się przepaść, w której tonęło już niejedno państwo oraz niejedna potężna spółka infrastrukturalna. Nie mniej interesująca jest integracja teorii grafów z teorią gier, która pozwala opisać działanie systemu w warunkach konfliktu. Gdy sieć zostanie już opisana topologicznie, pozostaje kwestia podejmowania decyzji w obliczu niepewności oraz celowego działania przeciwnika. Tu właśnie pojawiają się gry z naturą oraz zaawansowany model atakujący-obrońca, który nie jest jedynie teoretycznym ozdobnikiem. Stanowi on logiczne dopełnienie całego projektu, ponieważ infrastruktura nie istnieje w sterylnym laboratorium, lecz w świecie pełnym realnych zagrożeń.

Przeciwnikiem może być zarówno świadomy ludzki sprawca, jak i ślepa siła losowa, gwałtowne zjawisko pogodowe czy błąd wykonawczy. Każde z tych zagrożeń generuje inny profil strat, inny rytm eskalacji oraz wymaga odmiennego porządku interwencji służb technicznych. Teoria gier pozwala przekształcić ten nieprzewidywalny świat z narracji o niebezpieczeństwie w precyzyjny model konkretnej sytuacji decyzyjnej. Bardzo wymowna jest tu obecność algorytmu strażaka, który posiada wartość nie tylko techniczną, ale wręcz głęboko antropologiczną. Uświadamia on nam, że w nowoczesnych systemach najważniejsze nie jest samo pojawienie się zagrożenia, lecz tempo jego rozprzestrzeniania.

Musimy wiedzieć, jaką część struktury można jeszcze ocalić przy ograniczonych zasobach obronnych, co stanowi istotę logiki współczesnych kryzysów. Nie wszystko da się zatrzymać od razu, toteż trzeba wiedzieć, które węzły są warte natychmiastowej osłony kosztem innych. To okrutne pytania o priorytetyzację strat, ale cywilizacja dojrzała zadaje je zawczasu, przygotowując się na najgorsze możliwe scenariusze. Tylko cywilizacja infantylna udaje, że nie będzie musiała ich

zadawać wcale, licząc na wieczne trwanie w stanie nienaruszonej stabilności. W tym sensie podejście Guze idealnie odpowiada współczesnemu paradygmatowi odporności, który jest konsekwentnie rozwijany przez organizacje takie jak NIST czy OECD.

Odporność, czyli zdolność systemu do adaptacji i szybkiego odzyskania funkcji po zakłóceniu, nie jest tam rozumiana jako mityczna niewrażliwość. NIST ujmuje ją w czteroelementowym cyklu obejmującym przygotowanie, wytrzymanie uderzenia oraz sprawną regenerację zasobów po wystąpieniu incydentu. Z kolei OECD podkreśla znaczenie planowania oraz priorytetyzacji inwestycji przez cały cykl życia infrastruktury, co wymaga ścisłego zarządzania ryzykiem. Takie podejście przesuwa punkt ciężkości z pasywnej ochrony na aktywną zdolność przetrwania w warunkach permanentnego stresu systemowego. Ostatecznie matematyka przetrwania staje się narzędziem, które pozwala nam nie tylko mierzyć ból sieci, ale przede wszystkim nim zarządzać.

Sztuka wyboru: Jak optymalizacja cywilizuje konflikty celów

Monografia Guze pozostaje z tym nurtem zadziwiająco zgodna, choć autor kroczy własną drogą i buduje autorski aparat pojęciowy. Kiedy przechodzimy do optymalizacji, czyli procesu poszukiwania najlepszych rozwiązań przy ograniczonych zasobach, cała wcześniejsza architektura myśli zaczyna pracować z pełną mocą. Modelowanie daje język, analiza dostarcza wskaźniki, a teoria gier narzuca logikę decyzji. Niemniej to dopiero optymalizacja zmusza system do odpowiedzi na pytanie, jak przejść od diagnozy do projektu. Tu pojawia się wielka zaleta książki: autor nie osuwa się ani w fetyszyzm obliczeniowy, ani w banał konsultingowy.

Guze wie, że infrastruktura krytyczna, czyli zbiór kluczowych zasobów niezbędnych do funkcjonowania państwa, jest polem sprzecznych celów. Niezawodność, czyli miara sprawności systemu w określonym czasie, kosztuje, podobnie jak redundancja czy bezpieczeństwo cybernetyczne. Jednocześnie brak tych elementów kosztuje więcej, tyle że w walucie bardziej brutalnej niż budżet inwestycyjny. Zastosowanie optymalności Pareto staje się zatem ruchem koniecznym, gdyż w świecie CNI niemal nigdy nie istnieje rozwiązanie idealne. Trzeba wybierać efektywne kompromisy i wiedzieć, gdzie wzrost niezawodności uzasadnia nakłady, a gdzie generuje jedynie kosztowny nadmiar.

Należy rozstrzygać, czy bardziej opłaca się wzmacniać węzły sieci, czy może jej krawędzie, czyli połączenia decydujące o przepływach. Trzeba decydować, kiedy inwestować w fizyczną redundancję, a kiedy w zdolność do szybkiej rekonfiguracji systemu. Front Pareto nie usuwa

konfliktu celów, on go cywilizuje. Pozwala to na świadome zarządzanie odpornością, czyli aktywną zdolnością systemu do przetrwania i adaptacji w warunkach stresu. Wszak w inżynierii bezpieczeństwa każda decyzja ma swoją wagę i cenę, której nie da się uniknąć.

Jeszcze bardziej znacząca jest propozycja redukcji złożonych problemów wielokryterialnych do binarnego problemu plecakowego. W tej decyzji zawiera się cała filozofia autora: prostota nie jest rezygnacją z jakości, lecz sztuką zachowania rdzenia problemu. To postawa cenna w epoce, która myli nieraz komplikację z głębią. Guze pokazuje, że model dobry to nie ten najbardziej imponujący, lecz taki, który nadaje się do decyzji operacyjnej i zarządczej. To tylko tyle i aż tyle.

Przypowieść mówi dalej tak: wspólnota, która przetrwała wstrząs, zebrała mędrców, lecz ich eleganckie wykresy nie przyniosły ratunku. Najmniej efektowny z nich rozłożył prosty plan sieci i wskazał miejsca, których utraty nie przeżyją bez ceny politycznej i gospodarczej. Wspólnota obraziła się na tę prostotę, bo obnażała ona pustkę dekoracji, w których żyli zbyt długo. Lecz dopiero gdy nauczyli się czytać własną sieć bez złudzeń, zaczęli naprawdę budować bezpieczeństwo. Bezpieczeństwo nie zaczyna się od poczucia bezpieczeństwa; zaczyna się od zdolności nazwania struktury ryzyka.

Geometria wrażliwości: Jak grafy ujawniają prawdę o systemach

Na tym etapie rozważań musimy postawić sprawę jasno, bez zbędnych uników czy akademickiej kurtuazji. Monografia Sambora Guze zasługuje na szeroką promocję nie dlatego, że dorzuca kolejną cegiełkę do gmachu wyspecjalizowanych technik analizy grafowej, lecz z powodu przywrócenia nauce o infrastrukturze krytycznej rzeczy fundamentalnej, czyli dyscypliny proporcji. Autor precyzyjnie wskazuje, co faktycznie należy modelować, co mierzyć i co optymalizować, a czego pod żadnym pozorem nie wolno mylić z realną odpornością systemu. W dobie strategicznego przeciążenia informacyjnego, gdzie szum informacyjny często udaje sygnał, takie osiągnięcie jest znacznie istotniejsze, niż mogłoby się wydawać na pierwszy rzut oka. To tylko tyle i aż tyle.

Największym wrogiem współczesnego bezpieczeństwa bywa bowiem nie brak danych, lecz brak trafnego, operacyjnego modelu ich interpretacji. Musimy wreszcie zejść z bezpiecznych wyżyn czystej metodologii na poziom brutalnej próby ognia, gdyż każda teoria infrastruktury staje się poważna dopiero wtedy, gdy wytrzymuje kontakt z rzeczywistością. Systemy istniejące w konkretnej geopolityce, ekonomii i technice nie wybaczają teoretycznych błędów, toteż studia przypadków w rekonstrukcji monografii Guze przestają być jedynie ilustracją, a stają się twardym

argumentem. Wszak bezpieczeństwo nie zaczyna się od poczucia bezpieczeństwa, lecz od zdolności nazwania struktury ryzyka.

Sieci rurociągów w USA i Arabii Saudyjskiej, Baltic Ports Network czy skomplikowane układy transportowe i energetyczne nie stanowią tutaj zestawu egzotycznych ciekawostek. Są to raczej laboratoria prawdy infrastrukturalnej, które udowadniają, że graf nie jest jedynie szkolnym szkicem, lecz precyzyjnym instrumentem ujawniającym anatomię zależności, koncentracji i podatności. W czasach, gdy język bezpieczeństwa bywa inflacyjny i pełen pustych haseł, taki walor demonstracyjny ma znaczenie wręcz kolosalne dla praktyki zarządzania. Nie wystarczy bowiem deklarować, że dany system jest ważny, gdyż trzeba jeszcze umieć pokazać, w którym dokładnie miejscu i dlaczego on pęka.

Rozważmy najpierw rurociągi, które w potocznym wyobrażeniu jawią się jako proste linie służące do transportu surowca z punktu A do punktu B. Z perspektywy teorii sieci są one jednak strukturami o znacznie wyższym stopniu złożoności, gdzie przepływ fizyczny, sterowanie i monitorowanie tworzą jeden organizm operacyjny. Infrastruktura krytyczna nie jest magazynem aktywów, lecz anatomią przetrwania, w której awaria techniczna błyskawicznie przelewa się na grunt ekonomiczny, polityczny i społeczny. Każdy krytyczny odcinek czy węzeł przesyłowy posiada znaczenie strategiczne, ponieważ lokalna utrata funkcji niemal zawsze uruchamia nielokalny, niszczycielski efekt kaskadowy.

Współczesne analizy odporności, czyli zdolności systemu do adaptacji i szybkiego odzyskania sprawności po szoku, kładą nacisk na planowanie już na etapie projektowania i utrzymania. OECD słusznie podkreśla, że naprawa po wystąpieniu zakłócenia jest zawsze kosztowniejsza niż inwestycja uprzedzająca, która uwzględnia dynamikę potencjalnych zagrożeń. Sambor Guze, analizując rurociągi poprzez modelowanie grafowe, czyli metodę odwzorowania infrastruktury jako sieci powiązanych węzłów i krawędzi, wpisuje się idealnie w tę logikę. Pokazuje on dobitnie, że pytanie o bezpieczeństwo przesyłu jest w swojej istocie pytaniem o topologię wrażliwości całego układu.

Infrastruktura jako węzeł: Od optymalizacji do odporności

Przypadek Arabii Saudyjskiej oraz szerzej pojętej infrastruktury energetycznej ukazuje nam dobitnie, że współczesna sieć przestała być wyłącznie domeną inżynierów, stając się kluczowym komponentem ładu geopolitycznego. Węzeł eksportowy czy magistrala przesyłowa to dziś nie tylko stal i beton, lecz naczynia krwionośne bezpieczeństwa państwowego oraz stabilności całych

regionów. Każdy punkt obejścia wąskiego gardła morskiego staje się w tej optyce strategicznym bezpiecznikiem, który reguluje globalne ceny i nastroje na rynkach. Zrozumienie tej zależności wymaga jednak porzucenia perspektywy pojedynczego obiektu na rzecz analizy jego relacyjnej pozycji w skomplikowanej geometrii połączeń. Infrastruktura krytyczna nie jest bowiem magazynem aktywów, lecz stanowi prawdziwą anatomię przetrwania współczesnych organizmów państwowych.

W tym kontekście modelowanie grafowe, czyli metoda odwzorowania infrastruktury jako sieci powiązanych węzłów i krawędzi, przestaje być jedynie jałowym ćwiczeniem formalnym dla matematyków. Zamienia się ono w precyzyjne narzędzie rozpoznania strategicznego, które pozwala dostrzec to, co dla niewprawnego oka pozostaje ukryte w gąszczu kabli i rur. To, co w potocznym dyskursie politycznym nazywamy bezpieczeństwem energetycznym, w modelu Guze zostaje rozpisane na konkretną strukturę ścieżek, redundancji oraz parametrów podatności. Takie podejście pozwala nam nazwać strukturę ryzyka, zanim jeszcze przerodzi się ono w realny kryzys paraliżujący życie milionów obywateli. Bezpieczeństwo nie zaczyna się wszak od subiektywnego poczucia spokoju, lecz od rzetelnej zdolności do modelowania i zrozumienia sieciowych zależności.

Współczesne ramy bezpieczeństwa coraz częściej traktują powiązania fizyczne i cybernetyczne jako wspólny, nierozerwalny obszar ryzyka, co jest szczególnie widoczne w sektorach energii i transportu. Agencja ENISA wskazuje wyraźnie, że dyrektywa NIS2 zaostrza wymogi wobec sektorów krytycznych właśnie dlatego, że ciągłość ich usług stała się dobrem ponadbranżowym. Każda awaria systemu informatycznego może dziś skutkować fizycznym zablokowaniem przepływu surowców, co czyni z cyberbezpieczeństwa integralny element ochrony fizycznej. Nie możemy już dłużej oddzielać świata bitów od świata atomów, gdyż w nowoczesnej infrastrukturze stanowią one jeden, wzajemnie przenikający się ekosystem. Kto widzi tylko ostatni etap tego procesu, ten widzi zdecydowanie za mało i zazwyczaj dostrzega zagrożenie zbyt późno.

Niemniej wymowny jest przypadek sieci portów bałtyckich, gdzie port przestaje być postrzegany wyłącznie jako miejsce przeładunku towarów z morza na ląd. Jest on w rzeczywistości wielowymiarowym skrzyżowaniem przepływów handlowych, energetycznych, wojskowych oraz cyfrowych, które podlegają surowym reżimom prawnym i środowiskowym. Każda analiza portu jako odizolowanego obiektu jest z natury zbyt uboga, gdyż ignoruje jego rolę jako węzła wielosystemowego w globalnej sieci. Z punktu widzenia teorii grafów to miejsce koncentracji relacji o nierównej sile, gdzie lokalna awaria błyskawicznie przechodzi w zakłócenie całych łańcuchów dostaw. Port staje się zatem punktem krytycznym, w którym zbiegają się interesy ekonomiczne, wymogi bezpieczeństwa narodowego oraz skomplikowane procedury nadzorcze.

Z perspektywy ekonomii politycznej port jest miejscem, w którym drobne opóźnienie może wywołać gwałtowny wzrost kosztów transakcyjnych i wymusić zmianę trajektorii światowego handlu. W obszarze prawa oznacza to, że obowiązek zachowania ciągłości działania i należytej staranności nabiera charakteru dowodowego, wykraczając daleko poza zwykłą sprawność operacyjną. Studium portów bałtyckich stanowi zatem znakomitą demonstrację głównej tezy monografii, głoszącej, że krytyczność nie wynika ze skali obiektu, lecz z jego pozycji relacyjnej. Analogicznie należy interpretować systemy transportowe, w tym układy drogowe i miejskie, które w debacie publicznej często bywają spychane do roli problemów czysto komunalnych. Tymczasem w warunkach kryzysowych każde skrzyżowanie może stać się lokalnym generatorem kaskady, paraliżującym ruch służb ratunkowych lub blokującym trasy zaopatrzeniowe.

Współczesne badania nad odpornością, czyli zdolnością systemu do adaptacji i szybkiego odzyskania funkcji po zakłóceniu, podkreślają konieczność projektowania układów z myślą o usterkach. Systemy inteligentne muszą być przygotowane na ataki i anomalie klimatyczne, a nie tylko na optymalną wydajność w idealnych, nominalnych warunkach eksploatacji. To podejście jest niezwykle bliskie intuicji Guze, według której ruch, energia i dane tworzą dziś jeden żywy, pulsujący układ regionalny. Musimy zrozumieć, że nie każda złożoność jest siłą, gdyż czasem bywa ona jedynie drogo ubraną słabością, podatną na najmniejsze nawet drgnienie sieci. Kto w procesie planowania optymalizuje jedynie przepustowość, zapominając o odporności, ten w rzeczywistości buduje prędkość pozbawioną trwałości.

Od teorii do praktyki: operacyjna siła modeli grafowych

W tym punkcie powraca fundamentalne zagadnienie analiz online, które autor zasygnalizował wcześniej z chirurgiczną precyzją, a które teraz domaga się pełnego wybrzmienia. Modelowanie grafowe, czyli metoda odwzorowania infrastruktury jako sieci powiązanych węzłów i krawędzi o określonej przepustowości, w ujęciu Guze nie służy wyłącznie projektowaniu ex ante. Jego prawdziwa, operacyjna siła ujawnia się w momencie, gdy sieć już tętni życiem i wymaga zarządzania w czasie rzeczywistym. To kluczowa dystynkcja, bowiem wiele modeli inżynieryjnych doskonale radzi sobie na deskach kreślarskich, lecz kapituluje w starciu z brutalną praktyką eksploatacji. Autor dąży do tego, aby aparat matematyczny nie tylko chłodno przewidywał przyszłość, lecz aktywnie wspierał reakcję na kryzys poprzez redystrybucję energii lub danych. A infrastruktura krytyczna nie jest magazynem aktywów. Jest anatomią przetrwania.

Współczesne ramy regulacyjne w Europie podążają dokładnie tym samym szlakiem, porzucając teoretyczne abstrakcje na rzecz twardej rzeczywistości operacyjnej. ENISA, opracowując techniczne

wytyczne dla zarządzania ryzykiem w reżimie dyrektywy NIS2, kładzie nacisk na mechanizmy wdrażalne, które realnie zapewnią ciągłość usług i odporność na incydenty. W obliczu kryzysu prosta, działająca teoria okazuje się nieskończenie cenniejsza niż najbardziej wyrafinowane konstrukcje myślowe, których nie sposób uruchomić pod presją czasu. To prowadzi nas do istotnej kwestii recepcji dzieła Guze, które nie jest głosem z akademickiego marginesu, lecz uderza w samo serce dzisiejszego paradygmatu naukowego. Powinniśmy czytać tę monografię jako narzędzie dla tych, którzy muszą podejmować decyzje tu i teraz. To tylko tyle i aż tyle.

Obecny paradygmat, w którym osadzona jest praca, definiuje kilka rewolucyjnych cech zmieniających nasze postrzeganie bezpieczeństwa systemowego. Po pierwsze, odchodzi on od naiwnej ochrony pojedynczych obiektów na rzecz zarządzania odpornością funkcji całego organizmu technicznego. Po drugie, traktuje ryzyko jako wypadkową skomplikowanych współzależności międzysektorowych, a nie tylko sumę wewnętrznych słabości danego układu. Po trzecie, integruje wymiar fizyczny i cyfrowy, uznając, że cyberodporność jest dziś integralną częścią fundamentów infrastrukturalnych, a nie odrębnym, wirtualnym światem. Wreszcie, przyjmuje perspektywę całego cyklu życia, gdzie projektowanie, utrzymanie i odbudowa stanowią etapy tej samej, nieubłaganej logiki. OECD wskazuje ten kierunek jako jedyną drogę do stabilności nowoczesnego państwa.

NIST definiuje odporność jako zdolność do przygotowania, adaptacji, wytrzymania i szybkiego odzyskiwania sprawności, co ENISA przekłada na konkretne wymogi operacyjne. Guze dostarcza do tego procesu precyzyjny aparat modelowy, tworząc rzadko spotykane w literaturze, niezwykle mocne współbrzmienie teorii z praktyką inżynieryjną. Z perspektywy ekonomicznej szczególnie wartościowa jest jego nieufność wobec nadmiernie skomplikowanych metod tam, gdzie prostsze rozwiązania okazują się wystarczające. Takie stanowisko może wprawdzie razić akademickich estetów, lecz z punktu widzenia metodologii jest ono głęboko zdrowe i uzasadnione. W świecie infrastruktury krytycznej liczy się bowiem nie tylko matematyczna elegancja, ale przede wszystkim koszt poznawczy i operacyjny wdrożenia modelu. Nie każda złożoność jest siłą. Czasem jest tylko drogo ubraną słabością.

W rzeczywistości systemów CNI, czyli kluczowych zasobów niezbędnych do funkcjonowania państwa, nie ma miejsca na luksus uprawiania czystej, oderwanej od realiów teorii. Każda zbędna komplikacja drastycznie obniża szanse na skuteczną implementację, stając się wrogim elementem w strukturze zarządzania kryzysowego. Z tego powodu redukcja problemów wielokryterialnych do klasycznego problemu plecakowego oraz wykorzystanie algorytmów ewolucyjnych mają sens nie tylko techniczny, ale i instytucjonalny. Jest to swoista logika gospodarowania ograniczoną złożonością, gdzie każda subtelność musi udowodnić swoją przydatność w boju o utrzymanie usług.

Jeśli dany model wymaga nadmiaru danych i długich godzin obliczeń, staje się bezużyteczny dla operatora walczącego z awarią. Warto to ująć jeszcze mocniej, patrząc przez pryzmat odpowiedzialności za trwanie wspólnoty.

Wróćmy na chwilę do obrazu wspólnoty, która buduje swoje struktury nie tylko po to, by trwać, ale by móc się odrodzić po każdej burzy. Tak jak dawni budowniczowie łączyli geometrię z instynktem przetrwania, tak współczesny inżynier musi łączyć grafy z etyką odpowiedzialności za ciągłość życia społecznego. Niezawodność, czyli prawdopodobieństwo poprawnego działania systemu w określonym czasie, przestaje być wtedy suchym parametrem technicznym, a staje się obietnicą bezpieczeństwa. Guze rozumie tę ontologię działania, w której matematyka służy wspieraniu decyzji administratorów stojących na pierwszej linii frontu technicznego. Ostatecznie chodzi o to, by system był zdolny do adaptacji, gdy wszystkie inne zabezpieczenia zawiodą. Żywy albo martwy.

Między formalizmem a odpornością: Dlaczego modelowanie wygrywa z audytem

W epoce zdominowanej przez wszechobecne dashboardy, audyty oraz rozbuchane systemy zgodności pojawia się fundamentalne niebezpieczeństwo poznawcze. Operatorzy infrastruktury krytycznej, czyli kluczowych zasobów niezbędnych do funkcjonowania państwa, toną dziś w proceduralnym nadmiarze. Nie zyskują oni jednak przy tym żadnej proporcjonalnej przewagi w zrozumieniu realnych zagrożeń. Monografia Guze stanowi odważną próbę przeciwdziałania temu niepokojącemu dryfowi w stronę biurokracji. Autor proponuje aparat matematyczny, który jest uderzająco prosty w swojej konstrukcji, lecz jednocześnie niezwykle głęboki strukturalnie. Taka postawa jest bliska klasycznym zasadom ekonomii instytucjonalnej, gdzie liczy się przede wszystkim efektywność reguł.

Dobre reguły oraz skuteczne narzędzia nie są tymi, które generują najwięcej papierowej dokumentacji lub rekordową liczbę wskaźników KPI. Prawdziwa wartość tkwi w rozwiązaniach obniżających ryzyko błędu decyzyjnego w punktach o znaczeniu strategicznym. Ta intelektualna trzeźwość jest nam dzisiaj szczególnie potrzebna, gdyż regulacje europejskie słusznie podnoszą poprzeczkę dla sektorów kluczowych. Istnieje jednak realne ryzyko, że w praktyce wdrożeniowej popadniemy w jałowy formalizm bez solidnej warstwy modelowej. Właśnie tutaj praca Guze pełni niezwykle istotną funkcję korekcyjną dla całego systemu. Przypomina ona dobitnie, że zgodność z przepisami bez głębokiego zrozumienia sieci jest tylko formą kosztownej autoiluzji.

Z perspektywy prawnej należy dopowiedzieć rzecz o znaczeniu absolutnie zasadniczym dla bezpieczeństwa publicznego. Współczesne ramy unijne nie próbują już budować bezpieczeństwa wyłącznie poprzez system zakazów i sztywnych obowiązków ochronnych. Zamiast tego ciężar zostaje przesunięty na odporność, czyli aktywną zdolność systemu do adaptacji i przetrwania wstrząsów. Dyrektywa CER ustanawia ramy wzmacniania tej odporności na rynku wewnętrznym poprzez nadzór i środki pomocowe. Równolegle NIS2 podnosi standardy cyberbezpieczeństwa, obejmując swoim zasięgiem znacznie szerszy katalog sektorów gospodarki. Z kolei rozporządzenie DORA w sektorze finansowym skupia się niemal wyłącznie na cyfrowej odporności operacyjnej.

Wspólny mianownik tych wszystkich aktów prawnych jest dla analityka całkowicie jasny i klarowny. Liczy się przede wszystkim zdolność do utrzymania funkcji żywotnych oraz wykazania pełnego zrozumienia własnych zależności. To właśnie sprawia, że aparatura grafowa, miary dominacji czy analiza podatności przestają być domeną wyłącznie teoretyków matematyki. Stają się one integralną częścią zaplecza dowodowego, które potwierdza zachowanie należytej staranności przez operatora. W niedalekiej przyszłości spory regulacyjne i odszkodowawcze będą dotyczyć tego, czy skutki sieciowe można było przewidzieć. Infrastruktura krytyczna nie jest bowiem magazynem aktywów, lecz prawdziwą anatomią przetrwania całego społeczeństwa.

Z perspektywy antropologicznej monografia odsłania prawdę, która zazwyczaj bywa spychana na margines oficjalnych dokumentów politycznych. Człowiek w systemie technologicznym wcale nie znika, mimo postępującej cyfryzacji i automatyzacji procesów. Nowoczesne sieci są wyposażone w tysiące sensorów i protokołów zdalnego sterowania, lecz nadal wymagają obecności decydentów. Autor słusznie zaznacza kluczową rolę czynnika ludzkiego w procedurach restartu systemów po wystąpieniu poważnej awarii. Jest to punkt o znaczeniu znacznie większym, niż skłonna jest przyznać dzisiejsza doktryna technokratyczna. Cywilizacja techniczna zbyt często ulega niebezpiecznemu mitowi o bezzałogowej doskonałości maszyn.

Tymczasem najważniejsze momenty budowania odporności zdarzają się wtedy, gdy człowiek musi ocenić sytuację niepełną i niepewną. To on wykonuje krytyczne przełączenie, odseparowuje uszkodzony segment sieci i samodzielnie dobiera priorytety działania. NIST definiuje odporność jako własność projektową obejmującą wiarygodność oraz zdolność do działania mimo silnych zakłóceń. Nie ma w takim ujęciu żadnej sprzeczności z aktywną rolą operatora czy inżyniera systemowego. Przeciwnie, im bardziej złożony staje się dany układ, tym bardziej musimy wiedzieć, gdzie kończy się automatyzacja. W tym miejscu zaczyna się bowiem decyzja obarczona pełną odpowiedzialnością prawną i moralną.

Dzisiejsza kultura zarządzania niefortunnie lubi przeciwstawiać człowieka systemowi, jakby ten pierwszy był wyłącznie źródłem błędu. Monografia Guze w sposób niezwykle precyzyjny podważa to

szkodliwe i nazbyt uproszczone widzenie rzeczywistości technicznej. Prawdziwy problem nie polega na samej obecności człowieka, lecz na źle zaprojektowanej relacji między informacją a architekturą. Dobrze zbudowany model sieciowy nie ma na celu usunięcia człowieka z pętli decyzyjnej, lecz wzmocnienie jego kompetencji. Z tego punktu widzenia teoria grafów oraz teoria gier stają się instrumentami dyscyplinowania ludzkiej intuicji. To różnica fundamentalna, która decyduje o sukcesie lub porażce w obliczu kryzysu.

Człowiek pozbawiony solidnego modelu jedynie improwizuje, co w warunkach zagrożenia życia bywa tragiczne w skutkach. Z kolei model bez człowieka zawiedzie wszędzie tam, gdzie kryzys wykracza poza ramy przewidzianego wcześniej skryptu. Dopiero ich rozsądne sprzężenie daje nam odporność dojrzałą, zdolną do przetrwania w nieprzewidywalnym środowisku zewnętrznym. Wracając do przypowieści o wspólnocie, możemy teraz dostrzec w niej znacznie głębszy sens moralny. Pierwszy doradca kazał kupować więcej urządzeń, drugi mnożyć procedury, a trzeci wdrażać nowsze systemy cyfrowe. Dopiero czwarty doradca zadał wspólnocie te naprawdę niewygodne i bolesne pytania o strukturę.

Zapytał on, czy wiedzą, które węzły sieci są naprawdę krytyczne i jak w rzeczywistości rozchodzi się kaskadowa awaria. Chciał wiedzieć, gdzie kończy się realna redundancja, a gdzie zaczyna się jedynie kosztowny pozór bezpieczeństwa technicznego. Wspólnota początkowo uznała go za człowieka zbyt surowego, a jego metody za niepotrzebnie skomplikowane i abstrakcyjne. Szybko jednak odkryła, że tylko on potrafił odróżnić realne bezpieczeństwo od jego czysto dekoracyjnej i biurokratycznej formy. Właśnie dlatego recepcja tej monografii powinna być ambitna i wykraczać poza wąskie grono akademickich specjalistów. Nie jest to jedynie uczony dodatek do debat, lecz propozycja konkretnego aparatu rozpoznania rzeczywistości.

Centralna intuicja autora jest dzisiaj znacznie bardziej aktualna niż w momencie, gdy powstawały pierwsze szkice tej pracy. Świat staje się jednocześnie coraz bardziej gęsto sieciowy, a przy tym niepokojąco niestabilny pod względem politycznym. Zmiany klimatyczne zwiększają presję na systemy fizyczne, a zależności cyfrowe komplikują profil ryzyka w sposób nieliniowy. Geopolityka odzyskuje swoją brutalność, a nowoczesne regulacje słusznie przestają ufać samym deklaracjom składanym bez twardego dowodu. W takich warunkach rośnie wartość narzędzi pozwalających zrozumieć, co w systemie jest naprawdę krytyczne i niezbędne. Musimy umieć szukać trudnych kompromisów między kosztem ochrony a realną zdolnością do przetrwania szoku.

Trzeźwe spojrzenie wymaga, aby powiedzieć rzecz niepopularną, która może uderzać w samozadowolenie wielu współczesnych elit zarządzających. Największym ryzykiem dla infrastruktury nie jest wyłącznie atak hakerski, awaria techniczna czy gwałtowna katastrofa pogodowa. Bywa nim przede wszystkim konformizm poznawczy decydentów, którzy wolą mówić o

odporności, zamiast ją matematycznie testować. Wolą oni posiadać pięknie brzmiącą politykę bezpieczeństwa, niż znać rzeczywistą topologię połączeń w swoim systemie. Często wybierają wskaźnik zgodności z normą zamiast rzetelnej mapy krytycznych zależności, które decydują o ciągłości działania. To tylko tyle i aż tyle, a jednak zmienia wszystko.

Monografia Guze uderza bezpośrednio w ten konformizm, przypominając, że infrastruktura krytyczna nigdy nie wybacza nam samozachwytu. Systemy techniczne wybaczą czasem braki zasobów, ale rzadko wybaczą przyjęcie błędnego modelu otaczającej nas rzeczywistości. Pozostaje teraz problem najtrudniejszy, który obnaża intelektualną dojrzałość badaczy, regulatorów oraz samych operatorów tych złożonych układów. Jak myśleć o optymalizacji, kiedy wiadomo już, że infrastruktura nie jest neutralnym układem ani prostą sumą aktywów. Jest ona siecią kosztownych współzależności, które pod presją zdarzeń skrajnych zachowują się bardziej jak organizm niż magazyn. W tym punkcie praca Sambora Guze osiąga swój najistotniejszy ciężar gatunkowy.

Autor nie proponuje nam infantylnej obietnicy rozwiązania idealnego, które rozwiąże wszystkie problemy za dotknięciem czarodziejskiej różdżki. Proponuje coś znacznie cenniejszego: uczy, jak rozpoznawać granice kompromisu i jak ważyć bezpieczeństwo wobec rosnących kosztów. Pomaga odróżniać redundancję konieczną do przetrwania od redundancji dekoracyjnej, która jedynie obciąża budżet bez zwiększania odporności. Właśnie dlatego front Pareto staje się w tej pracy nie tylko narzędziem matematycznym, ale figurą rozsądku politycznego. Nie mówi nam, co jest absolutnie najlepsze, gdyż w infrastrukturze krytycznej rzadko dopuszcza się istnienie ideałów. Wskazuje natomiast, które kompromisy są efektywne, a które stanowią jedynie formę kosztownego samooszukiwania się.

Takie podejście dobrze współbrzmi ze współczesnym nurtem zarządzania, w którym OECD akcentuje potrzebę inwestycji wyprzedzających i planowania. Unikanie fałszywej oszczędności jest kluczowe, gdyż obniża ona zdolność całego systemu do absorpcji szoku i odbudowy funkcji. W sensie ekonomicznym optymalizacja infrastruktury jest zawsze trudną sztuką gospodarowania rzadkością pod ogromną presją niepewności. Każdy dodatkowy segment rezerwowy czy wzmocniony węzeł generuje konkretny koszt kapitałowy, operacyjny oraz poznawczy dla organizacji. Zarazem koszt braku takich rozwiązań rośnie zazwyczaj w sposób nieliniowy, prowadząc do gwałtownej utraty zaufania społecznego. Nie każda złożoność jest siłą. Czasem jest tylko drogo ubraną słabością.

Teza o poszukiwaniu prostych, lecz potężnych narzędzi optymalizacyjnych nie jest kapitulacją wobec złożoności, lecz próbą jej skutecznego zdyscyplinowania. Redukcja części problemów do binarnego problemu plecakowego pozwala przenieść spór z poziomu próżności na poziom operacyjny. W infrastrukturze krytycznej model nie może być wyłącznie poprawny matematycznie,

musi być przede wszystkim w pełni wdrażalny. To punkt, który współczesna administracja publiczna i korporacyjna powinna wreszcie przyswoić dla wspólnego dobra nas wszystkich. Nie każde narzędzie robiące wrażenie na audytorze zwiększa realną odporność, czasem wręcz przeciwnie, zwiększa jedynie koszt poznawczy.

OECD wprost wskazuje dzisiaj, że odporność wymaga praktycznych ram inwestycyjnych, a nie wyłącznie górnolotnych deklaracji politycznych. W tym miejscu najwyraźniej ujawnia się przewaga podejścia Guze nad wieloma modnymi obecnie dyskursami o szeroko pojętym bezpieczeństwie. Duża część debaty publicznej lubi mówić o odporności językiem moralnym, organizacyjnym, a nawet psychologicznym. Mówi się o gotowości, świadomości oraz kulturze bezpieczeństwa, co brzmi dobrze, lecz rzadko przekłada się na inżynierię. Bezpieczeństwo nie zaczyna się od poczucia bezpieczeństwa. Zaczyna się od zdolności nazwania struktury ryzyka w sposób ścisły. Dopiero wtedy możemy realnie zarządzać tym, co dla naszej cywilizacji jest naprawdę krytyczne.

Matematyka odporności: Od teorii grafów do praktyki operacyjnej

Wszystko to jest fundamentalne, lecz bez precyzyjnego aparatu modelowego zbyt łatwo osuwa się w liturgię dobrych intencji. Monografia słusznie przypomina, że odporność, czyli aktywna zdolność systemu do przetrwania w warunkach stresu, nie może pozostać wyłącznie figurą normatywną. Musi stać się własnością opisywalną, porównywalną i optymalizowalną w konkretnych scenariuszach operacyjnych. Tu właśnie ujawnia się głęboka zgodność z definicjami NIST, które postrzegają resilience jako proces przygotowania, adaptacji oraz szybkiego odzyskiwania funkcji. Ta definicja jest z pozoru oszczędna, ale właśnie w tej powściągliwości kryje się jej największa wartość. Łączy ona dynamikę zmian i wytrzymałość w jeden spójny szkielet pojęciowy, pozwalający zrozumieć anatomię przetrwania.

Guze wykonuje dla infrastruktury sieciowej tytaniczną pracę, przekładając te intuicje na język grafów, miar dominacji oraz procedur optymalizacyjnych. Szczególnej uwagi wymaga tu ciągłe podejście do optymalizacji, oparte na funkcjach wagowych przypisanych poszczególnym węzłom i krawędziom modelu. To właśnie ono pozwala wyjść poza statyczne wyobrażenie infrastruktury i zobaczyć ją jako żywy system, którego parametry nieustannie ewoluują. W świecie rzeczywistym przepustowość, obciążenie czy prawdopodobieństwo degradacji nie są danymi martwymi, lecz zmiennymi zależnymi od pogody i decyzji zarządczych. Jeżeli model ma nadążać za rzeczywistością, musi potrafić uchwycić tę płynność.

W tym sensie rodziny grafów ważonych funkcjami ciągłymi nie są jedynie dodatkiem formalnym, lecz warunkiem przejścia od opisu do skutecznej regulacji. Dopiero takie ujęcie pozwala na sensowne zastosowanie metod gradientowych lub bezgradientowych, takich jak algorytm Neldera-Meada, który świetnie radzi sobie z funkcjami niegładkimi. Metody te odpowiadają realiom pracy z niepełnymi danymi, gdzie czas na podjęcie decyzji jest zasobem skrajnie deficytowym. To bardzo trzeźwa decyzja metodologiczna, która odrzuca akademickie marzenia o pełnej gładkości matematycznej na rzecz operacyjnej skuteczności. Świat operatorów infrastruktury krytycznej rzadko przypomina sterylne laboratorium.

Właśnie na tym styku teorii i praktyki ujawnia się ukryta siła prostoty, która bywa mylnie utożsamiana z brakiem głębi. Prostota nie jest dziecięcym marzeniem o łatwym świecie, lecz trudną sztuką znalezienia takiej postaci modelu, która nie zdradza złożoności rzeczywistości. Monografia Guze idzie pod prąd pokusie utożsamiania komplikacji formalnej z wyższą rangą poznawczą, co w nauce o CNI jest stanowiskiem niemal etycznym. Nie wszystko, co trudne, jest głębokie, a czasem to, co najistotniejsze, polega na odważnym odrzuceniu zbędnych komplikacji. Nie każda złożoność jest siłą, czasem jest tylko drogo ubraną słabością, która zawodzi w najmniej odpowiednim momencie.

Gdy system naprawdę się chwieje, nikt nie pyta o to, czy zastosowany model był modny lub wystarczająco skomplikowany. Kluczowe staje się pytanie, czy ocalił on funkcję systemu i pozwolił wspólnocie przetrwać najtrudniejszy moment próby. Tu jednak trzeba dołożyć jeszcze jeden wymiar, dziś absolutnie centralny, a mianowicie postępującą konwergencję świata fizycznego i cyfrowego. Współczesne infrastruktury krytyczne są coraz rzadziej strukturami czysto materialnymi, stając się systemami cyberfizycznymi o ogromnej skali powiązań. Ich niezawodność, czyli prawdopodobieństwo poprawnego działania w określonym czasie, zależy dziś w równym stopniu od zasilania, co od architektury chmurowej. Pamiętajmy, że infrastruktura krytyczna nie jest magazynem aktywów, lecz anatomią przetrwania.

Odporność systemów jako nowy kontrakt cywilizacyjny

To nie jest suma dwóch odrębnych porządków, lecz jeden spójny i bezlitosny porządek podatności. Właśnie dlatego NIS2, czyli unijna dyrektywa o wysokim wspólnym poziomie cyberbezpieczeństwa, obejmuje dziś osiemnaście sektorów uznanych za krytyczne i ważne dla funkcjonowania państwa. Dokument ten sankcjonuje przekonanie, że bezpieczeństwo sieci i systemów informatycznych nie stanowi opcjonalnego dodatku do usług podstawowych, lecz jest jednym z ich fundamentalnych filarów. Europa przestała traktować cyfryzację jako zewnętrzną warstwę nakładaną na

rzeczywistość, uznając ją za tkankę łączną nowoczesnej cywilizacji. W tym nowym paradygmacie nie ma już miejsca na podział na świat cyfrowy i fizyczny, gdyż istnieje tylko jedna, wspólna przestrzeń ryzyka.

ENISA, czyli Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, w 2025 roku opublikowała techniczne wytyczne wdrożeniowe, które rzucają nowe światło na wymogi zarządzania ryzykiem. Eksperci agencji wprost podkreślili znaczenie praktycznych środków ochrony, dowodów ich realnego wdrożenia oraz mapowania wymogów na codzienną działalność podmiotów infrastrukturalnych. To niezwykle ważny sygnał płynący z Brukseli, świadczący o głębokiej zmianie mentalnej w strukturach unijnych. Europa zaczyna wymagać nie tyle deklaratywnego bezpieczeństwa, opartego na wypełnianiu formularzy, ile realnej odporności operacyjnej zdolnej do udowodnienia swojej skuteczności w praktyce. W tym kontekście intuicje badawcze Guze okazują się szczególnie płodne i trafne.

Jego aparat pojęciowy pozwala bowiem zrozumieć, że cyberfizyczna konwergencja nie oznacza jedynie mechanicznego dodania nowych ryzyk do starych, znanych nam systemów. Oznacza ona całkowite przekształcenie samej topologii krytyczności, czyli układu najważniejszych powiązań i zależności wewnątrz struktury państwa. Krawędź, która dawniej była wyłącznie fizycznym połączeniem kablowym, dziś staje się nośnikiem krytycznych informacji sterujących i decyzyjnych. Węzeł, który dawniej pełnił funkcję prostej stacji technicznej, dziś staje się jednocześnie punktem agregacji danych, sterowania zdalnego oraz monitoringu. W takim układzie awaria cyfrowa niemal natychmiast wywołuje skutki fizyczne, paraliżując realne procesy produkcyjne czy logistyczne.

Współczesna krytyczność jest z natury relacyjna i wielowarstwowa, przez co stare podziały sektorowe tracą swoją dawną siłę wyjaśniającą. Teoria grafów, czyli matematyczna metoda opisu sieci jako zbioru punktów i ich połączeń, nadaje się do opisu takiego świata znacznie lepiej niż proste listy aktywów. Jeśli wzbogacimy ją o funkcje wagowe oraz logikę gier, otrzymamy narzędzie zdolne do modelowania dynamicznych interakcji między systemem a zagrożeniem. Pozwala to na strategiczne planowanie ochrony, które uwzględnia nie tylko statyczne zasoby, ale przede wszystkim dynamikę ich wzajemnych oddziaływań. Bezpieczeństwo nie zaczyna się od poczucia spokoju, lecz od zdolności precyzyjnego nazwania struktury ryzyka.

Równocześnie musimy jednak zachować zdrowy sceptycyzm, bo nie każda obietnica cyfrowej inteligencji realnie zwiększa odporność naszych systemów. Nie każda złożoność jest siłą, bo czasem okazuje się ona jedynie drogo ubraną słabością, która maskuje brak fundamentalnej stabilności. Część rozwiązań typu „smart” bywa w istocie mechanizmem koncentracji ryzyka w coraz bardziej skomplikowanej i nieprzejrzystej formie. Im większa centralizacja sterowania i zależność od wspólnych dostawców, tym większa pokusa mówienia o efektywności przy jednoczesnym

zwiększaniu systemowej podatności. W tym sensie współczesna infrastruktura staje przed paradoksem, w którym cyfryzacja poprawia obserwowalność, ale tworzy nowe punkty pojedynczej awarii.

Właśnie dlatego potrzebna jest nam analiza, która nie będzie entuzjastyczna, lecz rygorystyczna i pozbawiona technokratycznych złudzeń. Nie wystarczy już pytać, czy dana technologia działa w optymalnych warunkach, bo to pytanie zbyt płytkie i niewystarczające. Trzeba pytać, jakie relacje dominacji ona zmienia, jakie przesuwa centra ciężkości ryzyka oraz jak wpływa na możliwości rekonfiguracji systemu. Należy badać, jakie nowe formy uwiązania tworzy ona w całym systemie i czy nie osłabiają one zdolności do autonomicznego działania w sytuacjach kryzysowych. W tym świetle szczególnie cenne staje się prawne przesunięcie od ochrony obiektów do odporności podmiotów krytycznych.

Dyrektywa CER z 2022 roku, dotycząca odporności podmiotów krytycznych, nie mówi już tylko o prostej identyfikacji i ochronie fizycznej infrastruktury. Tworzy ona nowoczesne ramy wzmacniania odporności podmiotów na rynku wewnętrznym, odchodząc od wcześniejszej, znacznie węższej logiki czysto ochronnej. To bardzo znaczące przesunięcie akcentów, które pokazuje ewolucję myślenia o bezpieczeństwie w skali całego kontynentu. Prawodawca europejski uznał de facto, że krytyczność nie jest wyłącznie cechą obiektu, lecz cechą relacji między organizacją, usługą a społecznym skutkiem zakłócenia. To ujęcie doskonale wzmacnia sens pracy Guze, nadając jej matematycznym modelom głęboki kontekst prawny i społeczny.

Matematyczne modelowanie CNI nie służy już tylko temu, by wiedzieć więcej o strukturze sieci dla samej satysfakcji poznawczej. Służy ono przede wszystkim temu, by wykazać, że dana organizacja rozumie własne zależności i potrafi nimi zarządzać zgodnie z rosnącymi standardami. Należyta staranność, odporność operacyjna i odpowiedzialność nadzorcza stają się w ten sposób mierzalnymi parametrami, a nie tylko pustymi hasłami w raportach. W świecie, w którym infrastruktura krytyczna nie jest magazynem aktywów, lecz anatomią przetrwania, takie podejście jest jedynym racjonalnym wyborem. Pozwala ono przejść od pasywnej, reaktywnej ochrony do aktywnego budowania systemowej zdolności do trwania.

Nie wolno nam przy tym pominąć sektora finansowego, który bywa traktowany jako mniej materialny, a przecież stanowi jedno z najbardziej infrastrukturalnych ogniw ładu. Rozporządzenie DORA, stosowane od stycznia 2025 roku, ustanowiło w Unii Europejskiej wiążący reżim cyfrowej odporności operacyjnej dla wszystkich podmiotów finansowych. Koncentruje się ono na zarządzaniu ryzykiem ICT, testowaniu odporności oraz nadzorze nad kluczowymi zewnętrznymi dostawcami usług technologicznych, takimi jak dostawcy chmury. To niezwykle ważne z punktu widzenia teorii sieci, ponieważ finanse coraz wyraźniej ujawniają nową naturę współczesnej

krytyczności. Pokazują one, że stabilność systemu zależy dziś od elementów, które często znajdują się poza jego formalnymi granicami.

Krytyczność bywa bowiem pochodną nie tylko funkcji własnej danej instytucji, lecz przede wszystkim koncentracji zależności u wspólnych dostawców technologicznych. Niektóre najbardziej niebezpieczne punkty sieci nie znajdują się już wewnątrz pojedynczej organizacji, lecz na styku wielu podmiotów korzystających z tych samych usług. Ta koncentracja ryzyka znakomicie wpisuje się w logikę grafową, pokazując, że czasem najbardziej krytyczny węzeł leży poza klasycznie rozumianym sercem systemu. Leży on tam, gdzie zbiegają się zależności wielu systemów naraz, tworząc niewidoczne, ale niezwykle groźne punkty zapalne. Z perspektywy ekonomicznej, prawnej i antropologicznej razem wziętych daje to obraz systemu o wysokim stopniu współzależności.

Infrastruktura krytyczna to ostatecznie nie tylko rzecz, obiekt czy nawet najbardziej zaawansowana usługa techniczna. To fundamentalny kontrakt cywilizacyjny pomiędzy techniką, instytucją a społeczeństwem, który określa warunki naszego wspólnego bezpieczeństwa. Społeczeństwo powierza systemom swoje życie codzienne, zdrowie, możliwość komunikacji oraz podstawowe warunki egzystencji, takie jak ciepło czy woda. Instytucje biorą na siebie obowiązek utrzymania tych funkcji, a technika staje się narzędziem realizacji tego moralnego i politycznego zobowiązania. Gdy technika zawodzi, zawodzi nie tylko metal ani kod, lecz rozpada się istotna część naszego porządku zbiorowego i zaufania.

Dlatego optymalizacja infrastruktury krytycznej nie jest chłodnym problemem technicznym, który można zamknąć w ramach wąskiej specjalizacji inżynierskiej. Jest to problem moralny, polityczny i cywilizacyjny, choć musi być rozwiązywany przy użyciu najbardziej rygorystycznych narzędzi nauk ścisłych. To właśnie ta dwoistość czyni pracę Guze tak cenną, gdyż łączy ona matematyczną precyzję z bardzo poważnymi konsekwencjami społecznymi. Autor nie ucieka przy tym ani w tani sentymentalizm, ani w technokratyczną ślepotę, zachowując rzadką równowagę między teorią a praktyką. Przypowieść o wspólnocie, która prowadzi nas przez ten tekst, może więc zostać rozwinięta jeszcze o jeden, niezwykle istotny obraz.

Architektura przetrwania: Od fasad do geometrii zależności

Wyobraźmy sobie wspólnotę, która przez dekady budowała swoje poczucie bezpieczeństwa na fundamencie tego, co widoczne i łatwe do sfotografowania. Inwestowała w lśniące fasady, nowoczesne aplikacje i opasłe tomy dokumentacji, które miały świadczyć o jej niezłomnej

odporności przed światem zewnętrznym. Jednak gdy nadeszła nieunikniona seria zakłóceń, ta estetyczna tarcza pękła z przerażającą łatwością, ujawniając bolesną prawdę o kruchości fundamentów. Okazało się bowiem, że prawdziwa siła nie tkwi w tym, co wystawione na pokaz, lecz w ukrytej geometrii zależności, której nikt wcześniej nie chciał dostrzec ani tym bardziej zrozumieć. Wtedy właśnie zrozumiano, że bezpieczeństwo nie jest kojącą opowieścią, jaką organizacja snuje o sobie w chwilach spokoju, lecz surową strukturą, którą potrafi ona obronić, gdy wszystko inne zawodzi. To bodaj najważniejszy bon mot, jaki wyłania się z ducha tej monografii: przetrwanie to nie kwestia wizerunku, lecz architektury.

W świecie nowoczesnego zarządzania kryzysowego obowiązuje żelazna logika: nie da się zarządzać tym, czego nie potrafimy precyzyjnie zmapować, ani mapować tego, czego nie umiemy właściwie nazwać. Prawidłowe nazewnictwo wymaga jednak głębokiego zrozumienia rzeczywistości w kategoriach relacji, a nie tylko izolowanych przedmiotów, urządzeń czy budynków. Na tym etapie wyłania się wniosek o fundamentalnym znaczeniu, wskazujący na specyficzną lukę w naszej współczesnej wiedzy o systemach. Choć obecny paradygmat naukowy sprzyja pracom o takim charakterze, to zarazem potrzebuje ich znacznie bardziej, niż skłonni są to przyznać akademiccy ortodoksi. W rzeczywistości przesyconej regulacjami, potokami danych i wszechobecnymi dashboardami coraz trudniej zachować intelektualną dyscyplinę, która pozwala odróżnić to, co rzeczywiście krytyczne, od tego, co jest jedynie głośne. Monografia Sambora Guze proponuje nam aparaturę pojęciową, która tę utraconą dyscyplinę przywraca, oferując narzędzia do nawigacji w gąszczu współczesnych sieci.

Autor pokazuje z niezwykłą precyzją, jak modelować infrastrukturę krytyczną, czyli zbiór kluczowych zasobów niezbędnych do funkcjonowania państwa, by wydobyć na światło dzienne jej rzeczywistą naturę. Analizuje podatność i odporność systemów, czyli ich zdolność do adaptacji i szybkiego odzyskiwania funkcji po wystąpieniu nieprzewidzianego zakłócenia, co stanowi serce nowoczesnej strategii obronnej. W tym ujęciu niezawodność, czyli prawdopodobieństwo poprawnego działania systemu w określonym czasie, przestaje być jedynie stanem psychicznego komfortu decydentów. Staje się ona parametryzowalną własnością systemu, którą można i należy poddać ścisłym obliczeniom inżynieryjnym. Guze zręcznie korzysta z teorii grafów oraz teorii gier, nie popadając przy tym w formalistyczny narcyzm ani publicystyczną mgłę, która często spowija debaty o bezpieczeństwie. To rzadkie osiągnięcie, zwłaszcza dziś, gdy tak wielu ekspertów chętnie debatuje o odporności, lecz tak niewielu ma odwagę rzetelnie policzyć warunki jej zaistnienia.

Pozostaje już tylko synteza ostateczna, moment, w którym wszystkie nici trzeba związać nie w katalog pojęć, lecz w jedną, mocną tezę o naturze współczesnej cywilizacji technicznej. Teza ta brzmi następująco: krytyczne infrastruktury sieciowe nie stanowią jedynie technicznego zaplecza

państwa, lecz są jego ukrytym ustrojem funkcjonalnym. Nie żyjemy już obok skomplikowanych sieci energetycznych, wodociągowych czy informacyjnych; my żyjemy głęboko wewnątrz nich, całkowicie od nich zależni w każdym aspekcie życia. Nie są one dodatkiem do porządku społecznego, lecz jego fundamentalnym warunkiem materialnym, ekonomicznym, prawnym i symbolicznym. Dlatego właśnie modelowanie CNI nie jest jedną z wielu wyspecjalizowanych nisz badawczych dla wąskiego grona teoretyków. Jest to w istocie próba uchwycenia architektury zbiorowego trwania, bez której nasza nowoczesność rozpadłaby się w mgnieniu oka pod wpływem pierwszego poważniejszego wstrząsu.

Kto tego nie rozumie, ten nieuchronnie myli politykę z pustą retoryką, gospodarkę z prostą księgowością, a bezpieczeństwo z ulotnym poczuciem psychologicznego spokoju. Monografia Sambora Guze zasługuje na szczególną uwagę właśnie dlatego, że z żelazną konsekwencją unika tak powszechnych dziś pomyłek poznawczych. Autor uporczywie powraca do kwestii najbardziej niewdzięcznej i najmniej medialnej – do struktury wzajemnych zależności, która spaja system w jedną, żywą całość. Nie pyta on naiwnie, jak dana infrastruktura wygląda na zdjęciach satelitarnych czy w raportach rocznych, lecz docieka, od czego ona realnie zależy i gdzie koncentrują się jej punkty krytyczne. Analizuje, jak system się degraduje, gdzie może nastąpić pęknięcie i jakie kompromisy trzeba zawrzeć, by w obliczu katastrofy nie utracić funkcji żywotnych. To fundamentalne przesunięcie od opisu statycznych obiektów do analizy dynamicznych relacji jest najważniejszym osiągnięciem intelektualnym całej tej konstrukcji.

W istocie praca ta mówi rzecz prostą, choć dla wielu środowisk skrajnie niewygodną: katastrofy infrastrukturalne rzadko wynikają z całkowitego braku wiedzy technicznej. Znacznie częściej są one owocem wiedzy źle zorganizowanej, sektorowo podzielonej i niesprowadzonej do spójnego modelu, który ujawnia hierarchię krytyczności. Właśnie dlatego teoria grafów staje się w rękach autora czymś więcej niż tylko matematycznym instrumentem – staje się językiem odczarowania instytucjonalnych złudzeń. Pokazuje ona dobitnie, że nie wszystkie połączenia w sieci są równorzędne i nie wszystkie węzły można bezkarnie zastąpić innymi w razie awarii. Dowodzi również, że nie każda redundancja faktycznie buduje odporność, a infrastruktura krytyczna nie jest magazynem aktywów, lecz anatomią przetrwania. Czasem system najbardziej efektowny wizualnie okazuje się po prostu najdroższą formą kruchości, bo nie każda złożoność jest siłą – czasem jest tylko drogo ubraną słabością.

Współczesny paradygmat naukowy i regulacyjny wyraźnie przesuwa się w stronę takiego właśnie, relacyjnego rozumienia problemu bezpieczeństwa. Dyrektywa CER ustanawia nowe ramy wzmacniania odporności podmiotów krytycznych, odchodząc od archaicznej koncepcji biernej ochrony poszczególnych obiektów na rzecz aktywnego zarządzania ryzykiem. Komisja Europejska

podkreśla, że dyrektywa ta, obowiązująca od 16 stycznia 2023 roku, ma służyć kompleksowemu ujęciu fizycznej i cyfrowej odporności kluczowych sektorów. Równolegle NIS2 wzmacnia cyberbezpieczeństwo poprzez narzucenie ostrzejszych wymagań, co ENISA opisuje wprost jako narzędzie zwiększania odporności unijnych struktur krytycznych. Z kolei rozporządzenie DORA, które obowiązuje od 17 stycznia 2025 roku, czyni cyfrową odporność operacyjną sektora finansowego elementem wiążącego porządku prawnego. Całość tego krajobrazu dopełnia standard NIST, ujmujący odporność jako zdolność do adaptacji i błyskawicznego odzyskania funkcji po zakłóceniu, co ostatecznie domyka proces przejścia od intuicji do twardych parametrów.

Architektura zależności jako fundament trwania cywilizacji

Wszystkie te intelektualne nurty zbiegają się ostatecznie w jednym, niemal egzystencjalnym punkcie. Liczy się bowiem nie sama fizyczna obecność rur, kabli czy serwerów, lecz zdolność do utrzymania ich funkcji w warunkach ekstremalnego stresu systemowego. To właśnie na tym polu praca Sambora Guze okazuje się propozycją wyjątkowo aktualną i potrzebną. Z perspektywy ekonomicznej końcowy sens tej monografii można ująć w sposób jeszcze bardziej bezlitosny. Infrastruktura krytyczna, czyli zbiór kluczowych systemów niezbędnych do funkcjonowania państwa, stanowi ostateczny test naszej dojrzałości w gospodarowaniu rzadkością. Każde nowoczesne społeczeństwo marzy przecież o sieciach, które byłyby jednocześnie tanie, wydajne, odporne i cyfrowo zintegrowane.

Rzeczywistość rzadko jednak bywa tak hojna i nie rozdaje podobnych prezentów bezwarunkowo. W świecie ograniczonych zasobów musimy nieustannie wybierać, ważyć racje, przesuwać nakłady oraz szukać bolesnych nieraz kompromisów. Projektowanie redundancji, czyli nadmiarowości elementów systemu, ma sens tylko tam, gdzie buduje ona realną odporność, a nie jedynie drogi komfort psychiczny decydentów. Dlatego optymalność Pareto staje się tutaj czymś znacznie głębszym niż tylko suchą techniką matematyczną. Jest ona w istocie filozofią odpowiedzialnej decyzji publicznej, w której szukamy punktu równowagi między bezpieczeństwem a kosztem. Nie chodzi przecież o mityczne maksimum wszystkiego, bo dążenie do ideału w każdym wymiarze bywa zazwyczaj jedynie kosztowną iluzją.

Prawdziwa sztuka polega na takim ułożeniu wektora decyzji, w którym poprawa jednego dobra nie niszczy bez potrzeby innych zasobów krytycznych. Monografia Guze trafnie dowodzi, że stosunkowo proste narzędzia optymalizacyjne mają głęboki sens praktyczny. Wykorzystanie algorytmów ewolucyjnych czy redukcja złożonych dylematów do problemu plecakowego nie wynika

z naiwnego przekonania, że świat jest prosty. Wręcz przeciwnie, dzieje się tak dlatego, że współczesne organizacje muszą działać w warunkach niepełnych danych i ogromnej presji czasu. Kto w obliczu kryzysu wybiera model zbyt skomplikowany, by był używalny, ten de facto wybiera intelektualny luksus kosztem bezpieczeństwa. W świecie realnych zagrożeń elegancja matematyczna musi ustąpić miejsca skuteczności operacyjnej.

Z perspektywy prawnej wniosek płynący z tej lektury jest równie mocny i brzemienny w skutki. Prawo coraz wyraźniej odchodzi od jałowych pytań o to, czy dana organizacja posiada jedynie formalny zestaw martwych polityk. Zamiast tego ustawodawca zaczyna pytać o realne zrozumienie własnych zależności oraz o faktyczną zdolność do zarządzania ryzykiem. Kluczowa staje się umiejętność wykazania należytej staranności w warunkach zakłócenia, co przesuwa ciężar dowodu na płaszczyznę merytoryczną. Niezawodność, rozumiana jako prawdopodobieństwo poprawnego działania systemu w określonym czasie, przestaje być domeną inżynierów. Staje się ona twardym, prawnym standardem oceny odpowiedzialności zarządów i instytucji państwowych.

Jesteśmy świadkami ogromnej zmiany cywilizacyjnej, która redefiniuje nasze podejście do techniki i bezpieczeństwa. Matematyczne modelowanie CNI zaczyna bowiem pełnić rolę nie tylko poznawczą, lecz przede wszystkim dowodową. Staje się ono niezbędnym zapleczem dla nowoczesnej odpowiedzialności regulacyjnej oraz organizacyjnej w dobie niepewności. Można wręcz zaryzykować twierdzenie, że nadchodzące spory o awarie infrastrukturalne będą dotyczyły kwestii znacznie głębszych niż sam fakt usterki. Pytania będą dotyczyły tego, czy dało się racjonalnie przewidzieć skutki sieciowe oraz czy poprawnie rozpoznano koncentrację ryzyka. W tym nowym paradygmacie teoria grafów i teoria gier przestają być jedynie abstrakcyjnymi dyscyplinami matematycznymi.

Teoria grafów, czyli metoda odwzorowania infrastruktury jako sieci powiązanych węzłów, staje się w ten sposób narzędziem odpowiedzialności instytucjonalnej. Z perspektywy antropologicznej przesłanie pracy Sambora Guze jest jednak znacznie bardziej dotkliwe i niepokojące. Pokazuje ona, że nowoczesne społeczeństwa cierpią na swoisty paradoks infrastrukturalnej niewidzialności, który usypia naszą czujność. Im lepiej i sprawniej działa dana sieć, tym rzadziej jest ona dostrzegana przez przeciętnego użytkownika. Niestety, im mniej coś jest widoczne, tym łatwiej o polityczne zaniedbania i cięcia budżetowe w imię doraźnych zysków. Transformator nie wygrywa wyborów, więc rzadko staje się bohaterem politycznych obietnic.

Dzisiejszy świat uwielbia opowiadać barwne historie o innowacjach, ale rzadko chce finansować nudną i mało fotogeniczną architekturę odporności. Tymczasem brutalna prawda o trwałości naszych struktur społecznych jest uderzająco prosta i pozbawiona zbędnych ozdobników. Wspólnoty nie rozpadają się wcale dlatego, że nagle zabrakło im pięknych opowieści o postępie czy

demokracji. One kruszeją wtedy, gdy w godzinie próby przestają działać systemy dostarczające ciepło, wodę, energię czy łączność. Książka Guze jest zatem w dużej mierze lekcją pokory wobec materialnych warunków istnienia ładu społecznego. Przypomina nam dobitnie, że cywilizacja nie stoi na sloganach, lecz na sieciach, których zazwyczaj nie chcemy widzieć.

Przypowieść, która prowadziła nas przez cały ten wywód, może teraz zostać ostatecznie i w pełni domknięta. Wspólnota przez długi czas wierzyła naiwnie, że jej jedyną i prawdziwą siłą są posiadane zasoby materialne. Potem uznała, że kluczem do sukcesu są sztywne procedury, a następnie pokładała nadzieję w samej cyfryzacji. Wreszcie zaczęła sądzić, że jej potęga płynie z samego powtarzania modnego słowa „odporność", traktowanego niemal jak magiczne zaklęcie. Każda z tych wiar była jednak tylko częściowa i okazywała się tragicznie niewystarczająca, gdy przychodził realny szok. Dopiero bolesna lekcja nauczyła tę wspólnotę, jak należy czytać swoją własną, skomplikowaną sieć powiązań.

Prawdziwe bezpieczeństwo zaczęło się budować dopiero wtedy, gdy nauczono się odróżniać węzły pozornie ważne od tych naprawdę krytycznych. Kluczowe okazało się mierzenie podatności, ważenie trudnych kompromisów oraz projektowanie systemów z myślą o ich kontrolowanej degradacji. Morał tej opowieści jest jasny i nie wymaga od nas żadnych dodatkowych, retorycznych upiększeń. Nie przetrwa bowiem ten, kto zgromadził najwięcej dóbr, lecz ten, kto najlepiej rozumie własną architekturę zależności. Dlatego końcowa ocena monografii Sambora Guze musi być jednoznaczna i pozbawiona zbędnej kurtuazji. Jest to praca cenna, dojrzała i przede wszystkim intelektualnie uczciwa wobec czytelnika.

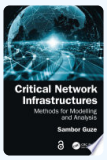
Siła tej publikacji nie polega na pogoni za efekciarską nowością, lecz na konsekwentnym łączeniu prostoty narzędzi z ogromną głębią problemu. Autor oferuje nam modelowanie CNI jako precyzyjny język opisu naszej technicznej rzeczywistości. Analiza tych struktur staje się językiem rozpoznania podatności, a optymalizacja – językiem trudnego kompromisu między bezpieczeństwem a trwałością. Wreszcie, niezawodność systemów zostaje przedstawiona jako język odpowiedzialności za ciągłość naszego wspólnego, zbiorowego życia. To osiągnięcie znacznie większe, niż mogłoby się wydawać w epoce informacyjnego szumu i strukturalnego bezładu. Można zatem podsumować ten materiał stwierdzeniem, które najlepiej oddaje jego głęboki sens.

Krytyczna infrastruktura sieciowa jest prawdziwym lustrem dojrzałości współczesnego państwa, wolnego rynku oraz każdej świadomej wspólnoty. Kto umie ją poprawnie modelować i optymalizować, ten nie tylko lepiej rozumie technikę, ale i warunki trwania świata. Kto zaś tej sztuki nie opanuje, ten wcześniej czy później odkryje, że największe katastrofy rzadko zaczynają się od huku. One biorą swój początek w ciszy źle zrozumianej zależności, która nagle i bezlitośnie przerywa ciągłość naszego istnienia. A infrastruktura krytyczna nie jest przecież magazynem

aktywów, lecz stanowi samą anatomię przetrwania. To tylko tyle i aż tyle w świecie, który zapomniał o fundamentach.

> Infrastruktura krytyczna nie jest jedynie technicznym tłem naszej egzystencji, lecz milczącym kontraktem, od którego zależy trwanie społeczeństwa. W świecie, w którym każda złożoność może okazać się drogo ubraną słabością, nasze przetrwanie zależy od tego, czy potrafimy dostrzec geometrię zależności ukrytą pod gładką taflą interfejsów. Pytanie brzmi: czy zdołamy przełożyć tę matematyczną wiedzę na realną odpowiedzialność, zanim nasza cywilizacja odkryje, że jej fundamenty były jedynie złudzeniem?

Inspiracje

[1] 

"Critical Network Infrastructures: Methods for Modelling and Analysis" Sambor Guze

2026 | CRC Press | ISBN: 9781003661450

Sambor Guze, dr hab. inż., jest doświadczonym profesorem nadzwyczajnym na Uniwersytecie Morskim w Gdyni, gdzie pracuje w Katedrze Matematyki na Wydziale Nawigacyjnym. Posiada doktorat z transportu oraz doktorat z nauk technicznych. Jego działalność naukowa i badawcza koncentruje się na matematyce stosowanej, badaniach operacyjnych i informatyce w kontekście systemów transportowych. Jego kluczowe osiągnięcia obejmują wiedzę specjalistyczną w zakresie planowania sieci transportowych, optymalizacji oraz modelowania bezpieczeństwa i niezawodności systemów technicznych. Wykorzystuje teorię grafów, teorię gier i wielokryterialną analizę decyzji do rozwiązywania luk w zabezpieczeniach krytycznych infrastruktur sieciowych. Dr Guze jest autorem licznych publikacji w czasopismach naukowych i członkiem wielu organizacji branżowych, w tym Europejskiego Stowarzyszenia Bezpieczeństwa i Niezawodności oraz Polskiego Towarzystwa Matematycznego.

***Sambor Guze**, Ph.D., D.Sc. (Eng), is an experienced associate professor at Gdynia Maritime University, Poland, where he serves in the Department of Mathematics at the Faculty of Navigation. He holds a Ph.D. in Transport and a D.Sc. in Technical Science. His academic and research work focuses on applied mathematics, operational research, and computer science as they relate to transportation systems. His key contributions include expertise in transportation network planning, optimization, and the modeling of safety and reliability in technical systems. He utilizes graph theory, game theory, and multi-criteria decision analysis to address vulnerabilities in critical network infrastructures. Dr. Guze has published extensively in scientific journals and is a member of several professional organizations, including the European Safety and Reliability Association and the Polish Mathematical Association.*

Gdynia Maritime University

Literatura uzupełniająca

Książki

Literatura pokrewna (Google Scholar):

[1] "Manuale di economia politica"

Vilfredo Pareto

1906 | Nabu Press | ISBN: 9781295492848

[2] "Trattato di sociologia generale"

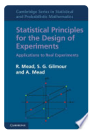
Vilfredo Pareto

1916 | Nabu Press | ISBN: 9781294680116

[3] "Generalized Linear Models"

Peter McCullagh, John Nelder

1989 | Chapman and Hall | ISBN: 978-0-412-31760-6



[4] "Statistical Principles for the Design of Experiments: Applications to Real Experiments"

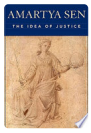
Roger Mead, Steven G. Gilmour, Andrew Mead

2012 | Cambridge University Press | ISBN: 9781139576642

[5] "The Design of Experiments: Statistical Principles for Practical Application"

Roger Mead

1988 | Cambridge University Press | ISBN: 978-0521245128



[6] "The Idea of Justice"

Amartya Sen

2009 | Harvard University Press | ISBN: 9780674036130

[7] "The Ethics of Artificial Intelligence"

S. Matthew Liao

2020 | Oxford University Press

[8] "Ethics of Artificial Intelligence"

S. Matthew Liao

2020 | Oxford University Press

Artykuły naukowe

Autorzy przywoływani:

[1] "Il massimo di utilità dato dalla libera concorrenza"

Vilfredo Pareto

1894 | Giornale degli Economisti

Google Scholar

[2] "The New Theories of Economics"

Vilfredo Pareto

1897 | Journal of Political Economy

Google Scholar

[3] "Moral Rightness Comes in Degrees"

Martin Peterson

2022 | Journal of the American Philosophical Association

Google Scholar

[4] "Generalized Linear Models"

John Nelder, Robert Wedderburn

1972 | Journal of the Royal Statistical Society: Series A (General) | DOI: 10.2307/2344614

Google Scholar

[5] "A Simplex Method for Function Minimization"

John Nelder, Roger Mead

1965 | The Computer Journal | DOI: 10.1093/comjnl/7.4.308

Google Scholar

[6] "The ethics of algorithms: Mapping the debate"

Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, Luciano Floridi

2016 | Big Data & Society

Google Scholar

[7] "Optimization's Neglected Normative Commitments"

Benjamin Laufer, Thomas Krendl Gilbert, Helen Nissenbaum

2023 | ACM Conference on Fairness, Accountability, and Transparency (FAccT)

Google Scholar

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

Article ID: b5314a5c-e1ec-4d03-ad26-b21d724680db