ZAGADNIENIA
NAUKOZNAWSTWA
2–4 (224–226) 2020
PL ISSN 0044-1619

Krzysztof Michalski
Politechnika Rzeszowska im. I. Łukasiewicza
Katedra Nauk Humanistycznych i Społecznych
e-mail: michals@prz.edu.pl
ORCID: https://orcid.org/0000-0002-2089-2160

Fałszywe obietnice bezpieczeństwa?
Nauka normalna wobec zagrożeń wynikających z rosnącej złożoności systemów technicznych

DOI: http://dx.doi.org/10.12775/ZN.2020.012

Abstrakt. W artykule dokonano przeglądu zagrożeń strukturalnych (organicznych, kombinacyjnych i kumulacyjnych) wynikających z ekspansji i gwałtownego wzrostu złożoności systemów technicznych oraz współczesnych uwarunkowań eksploatacji takich systemów i wprowadzania technologicznych innowacji. Wobec rosnącej społecznej awersji do sąsiedztwa instalacji technicznych i produktów przemysłowych oraz rosnącej nieufności do naukowych poświadczeń bezpieczeństwa autor artykułu poszukuje odpowiedzi na pytanie, czy społeczne obawy przed szkodliwymi oddziaływaniami czynników technicznych są zasadne. Na podstawie teoretycznej analizy strategii poznawczych stosowanych w ocenie bezpieczeństwa w wybranych domenach działalności technicznej autor wykazuje, że część zagrożeń ze strony czynników technicznych jest poznawczo nieuchwytna dla normalnej nauki. Jako przyczyny wymienia ograniczenia poznawcze, błędy, ułomności i nadużycia, które podważają wiarygodność naukowych poświadczeń bezpieczeństwa i skłaniają do gruntownej rewizji dotychczasowych strategii poznawczych. Autor postuluje zastąpienie procedur ekspercko-laboratoryjnych normalnej nauki modelami postnormalnymi, opartymi na uzgodnieniach z osobami narażonymi.

Słowa kluczowe: metodologia; nauka o bezpieczeństwie; ocena technologii; bezpieczeństwo techniczne; ocena oddziaływań; szacowanie ryzyka; nauka postnormalna

False Promises of Safety?
Normal Science in the Face of Threats Resulting from the Growing Complexity of Technical Systems

Abstract. The article reviews structural (organic, combinational and cumulative) threats resulting from the expansion and rapid increase in the complexity of technical systems and the contemporary conditions for the operation of such systems and the introduction of technological innovations. Given the growing social aversion to the proximity of technical installations and industrial products or the growing distrust of scientific safety certificates, the author of the article seeks an answer to the question of whether social fears of harmful effects of technical factors are justified. Based on a theoretical analysis of cognitive strategies used in safety assessment in selected domains of technical activity, the author of the article demonstrates that some threats from technical factors are cognitively elusive to normal science. The causes are indicated by cognitive limitations, errors, deficiencies and abuses that undermine the credibility of scientific safety certificates and prompt a thorough revision of previous cognitive strategies. The author postulates replacing the expert-laboratory procedures of normal science with post-normal models based on agreements with risk-exposed persons.

Keywords: methodology; safety and security science; technology assessment; technical safety; impact assessment; risk assessment; post-normal science

Sytuacja problemowa

Uwarunkowania niezawodnego funkcjonowania systemów technicznych i oddziaływania takich systemów na człowieka należą do najbardziej złożonych zjawisk, jakie kiedykolwiek stanowiły przedmiot naukowego poznania. Złożoność środowiska życia współczesnego człowieka, gwałtownie wzrastająca pod wpływem galopujących transformacji technologicznych spowodowanych ekspansją technologii (np. teleinformatycznych) na niemal wszystkie sfery życia indywidualnego i zbiorowego, stawia dotychczasowe systemy bezpieczeństwa, które dotąd mniej lub bardziej skutecznie chroniły społeczeństwo przed zagrożeniami ze strony „czynników technicznych”[1], przed nowymi, nieznanymi dotąd wyzwaniami. Chaotyczna, bezrefleksyjna modernizacja powodująca szybki wzrost uzależnienia człowieka w najprostszych czynnościach życiowych od niezawodnego funkcjonowania coraz bardziej skomplikowanych i coraz bardziej autonomicznych[2] (inteligentnych) systemów technicznych, których działanie, wzajemne interakcje i oddziaływania na otoczenie są dla nauki poznawczo coraz bardziej nieuchwytne, a dla większości ludzi coraz bardziej niezrozumiałe, stawia pod znakiem zapytania adekwatność dotychczasowych wyobrażeń o bezpieczeństwie technicznym, sposobów percepcji zagrożeń powodowanych przez „czynniki techniczne” oraz strategii ochrony ludności przed takimi zagrożeniami. Niektóre z zagrożeń rozpatrywanych w dalszej części artykułu – zagrożeń wynikających zarówno ze zmiany ontologicznego statusu techniki, która w toku czterech rewolucji przemysłowych (mechanizacja, elektryfikacja, automatyzacja, autonomizacja) ze zbioru użytecznych narzędzi i niewinnych gadżetów, sztucznych tworzyw i wypróbowanych receptur wymyślonych w celu poprawienia niedoskonałości przyrody niepostrzeżenie przekształciła się w potężny, wszechobecny, niszczycielski żywioł, przed którym nie ma ucieczki, jak i z braku odpowiedniej poznawczej lub operacyjnej kontroli nad rosnącą złożonością systemów technicznych, ich coraz bardziej skomplikowanymi wzajemnymi interakcjami i rosnącym potencjałem ich oddziaływań – to zagadnienia nowe, nieobjęte dotąd systematycznymi badaniami. Większość problemów poruszonych w niniejszym opracowaniu jest jednak dobrze znana nauce i była od dawna przedmiotem badań na gruncie różnych dyscyplin i nurtów, zwłaszcza na gruncie teorii krytycznej szkoły frankfurckiej (zob. Habermas 1977) i w nurcie studiów nad technonauką (STS) (zob. Bińczyk 2012). Ze względu na ograniczenia objętościowe artykułu omówienie uwarunkowań bezpieczeństwa współczesnych systemów technicznych ograniczy się jedynie do kwe-

[1] Określenie „czynnik techniczny” zaczerpnięto z rozpowszechnionej w naukach o bezpieczeństwie typologii zagrożeń, która kategoryzuje zagrożenia ze względu na ich źródło pochodzenia lub przyczynę sprawczą (czynnik naturalny, czynnik ludzki, czynnik techniczny).

[2] Więcej na temat autonomizacji techniki i jej wpływu na bezpieczeństwo zob. Michalski 2017a.

stii techniczno-strukturalnych, związanych z gwałtownym wzrostem złożoności, zagęszczenia i interaktywności (interoperacyjności) coraz bardziej konwergujących systemów technicznych oraz destrukcyjnej roli normalnej nauki[3], dla której redukcjonistycznych modeli poznawczych wiele problemów istotnych z punktu widzenia bezpieczeństwa jest coraz bardziej nieuchwytnych i która – dodatkowo uwikłana za sprawą postępującej komercjalizacji w „niebezpieczne związki" z przemysłem wytwarzającym niebezpieczne produkty w niebezpiecznych procesach z użyciem niebezpiecznych instalacji – swoimi poświadczeniami bezpieczeństwa legitymizuje coraz bardziej ryzykowne praktyki techniczne, dostarczając opinii publicznej brzemienne w skutkach, fałszywe poczucie bezpieczeństwa, które nieuchronnie prowadzi do rozczarowań podważających społeczne zaufanie do nauki. Natomiast wiele interesujących splotów uwarunkowań odpowiedzialnych za rosnącą skłonność systemów technicznych do katastrof oraz do systematycznego wytwarzania niewidzialnych, rozsianych, czasoprzestrzennie nieograniczonych łańcuchów szkód – zagadnień częściowo omówionych przez autora w innej pracy (Michalski i Jurgilewicz 2021) – zostało z konieczności pominiętych, choć zrozumienie skomplikowanej struktury kooperacyjnej sprzyjającej konstelacjom technologicznym i rozwiązaniom organizacyjnym gwarantującym wysoką podatność na katastrofy (Hofmann 2008, s. 39) – struktury powstającej w wyniku

[3] Pojęcie „normalnej nauki" zostało wprowadzone w 1962 roku przez Thomasa S. Kuhna (Kuhn 1968) na określenie tradycyjnego sposobu uprawiania nauki akademickiej, sprowadzającego się do prac porządkowych w obrębie obowiązujących w danej dziedzinie lub dyscyplinie wzorców postępowania naukowego, akceptowanych przez określoną wspólnotę uczonych i wpajanych młodym adeptom sztuki naukowej. Na wzorce tworzące zwartą tradycję badawczą, zwaną paradygmatem, składają się takie heterogeniczne elementy jak: prawa, teorie, autorytety, zastosowania oraz obowiązkowy w danej dyscyplinie ekwipunek badacza. Badania w nauce normalnej sprowadzają się do weryfikowania ograniczonego zakresu przewidywań wynikających z założeń leżących u podstaw panującego paradygmatu za pomocą ograniczonego zasobu pojęciowych „szufladek". Takie badania rzadko dostarczają zaskakujących rezultatów, ponieważ nauka normalna unika nowych odkryć, które mogłyby zakwestionować wygodny system szufladek i zagrozić zmianą paradygmatu – czyli rewolucją naukową, która wiązałaby się z koniecznością wzmożonego wysiłku uczenia się. Aby zapobiec rewolucjom, nauka normalna systematycznie ignoruje zjawiska, które mogłyby podważyć jej fundamentalne założenia, a rozwój naukowy polega nie na nowatorskim budowaniu teorii bardziej adekwatnych do rzeczywistości, lecz na wzroście zróżnicowania i specjalizacji. Dopiero gdy nagromadzone sprzeczności w teorii osiągają krytyczny poziom, pojawiają się warunki do podważenia dotychczas wyznawanych fundamentalnych zasad. Wtedy zwykle dochodzi do rewolucji, w toku której nauka na krótko powraca do rozwiązywania istotnych zagadek poznawczych do czasu ukształtowania się nowego paradygmatu (więcej na ten temat zob. Michalski 2019, s. 77 i n.). Fatalne skutki niechęci nauki do zmiany wygodnych paradygmatów szczególnie wyraźnie widać w badaniach bezpieczeństwa i zarządzaniu bezpieczeństwem, gdzie ze względu na dynamiczne zmiany w środowisku bezpieczeństwa dotychczasowe paradygmaty szybko się starzeją. Trudno byłoby obecnie wskazać inną dziedzinę działalności, w której przepaść między aktualnym stanem wiedzy naukowej i zdolnościami nauki do poznawczej obróbki problemów a społecznymi potrzebami byłaby równie duża (por. Jurgilewicz, Michalski 2020, s. 16). Zamiast rozpoznawać aktualne, społecznie istotne problemy, rozwiązywać zagadki poznawcze oraz eliminować luki i sprzeczności w wiedzy międzydyscyplinowej, nauki badające wpływ systemów technicznych, obiektów infrastruktury technicznej i przemysłowych produktów na różne aspekty życia ludzkiego brną w coraz większe wewnętrzne zróżnicowania, coraz węższą specjalizację oraz w konsekwentne zawyżanie standardów naukowej ścisłości, skutkujące wyłączeniem niemierzalnych, nieobliczalnych lub niepewnych aspektów rzeczywistości poza obszar naukowych zainteresowań.

wzajemnych interakcji między polityką i administracją publiczną, prywatnym biznesem a normalną nauką – mogłoby rzucić dodatkowe światło na skomplikowane uwarunkowania bezpieczeństwa współczesnych systemów technicznych.

Ponieważ poziom bezpieczeństwa – obok obiektywnych przedmiotowych uwarunkowań (np. powagi zastanych zagrożeń) – determinują również zdolności systemów bezpieczeństwa do reagowania na zagrożenia, dużego znaczenia z punktu widzenia efektywnego zarządzania bezpieczeństwem nabierają kwestie adekwatnej poznawczej identyfikacji zagrożeń. Tej ostatniej nie sprzyja jednak niewłaściwa, niepełnowymiarowa percepcja aspektów funkcjonowania nowoczesnych technologii istotnych z punktu widzenia bezpieczeństwa człowieka – percepcja oparta na anachronicznym, „rzeczowo-operacyjnym" rozumieniu techniki, redukującym technikę do rangi niesamoistnych i niezdolnych do działania bez człowieka środków wspomagających ludzkie ciało i umysł w bardziej efektywnym przekształcaniu środowiska przyrodniczego i społecznego zgodnie z potrzebami człowieka, zajmujących w hierarchii bytów miejsce poniżej najprostszych mikroorganizmów – a także receptur na ich wytwarzanie i użytkowanie. Mimo że technika niezauważalnie przekształciła się ze świata użytecznych artefaktów w skomplikowany i coraz mniej przyjazny dla człowieka świat superstruktur, które za sprawą tajemniczych połączeń, wewnętrznych interakcji i synergii posiadły zdolność do samoorganizacji, samoodtwarzania i samorzutnego, spontanicznego działania bez wiedzy i udziału człowieka, zgodnie z własną, niezrozumiałą dla człowieka logiką – systemy bezpieczeństwa w większości dziedzin ludzkiej działalności wciąż bazują na „rzeczowo-operacyjnym" rozumieniu techniki, bagatelizującym jej rzeczywiste, coraz bardziej niekontrolowane, niszczycielskie oddziaływania. Aby skuteczniej chronić ludność przed rosnącymi zagrożeniami ze strony czynników technicznych, należy przede wszystkim zrewidować dotychczasowe nieadekwatne strategie poznawcze, na których opiera się społeczny monitoring zagrożeń, oraz dopasować je do nowych wymagań i uwarunkowań, wynikających ze zmiany ontologicznego statusu, właściwości i znaczenia czynników technicznych.

Zagrożenia rozwijające się na żyznym gruncie współczesnych transformacji technologicznych

Nowego rodzaju złożone zagrożenia towarzyszące współczesnym transformacjom technologicznym wynikają z jednej strony ze zmieniających się właściwości czynników technicznych, z drugiej z uwarunkowań organizacyjnych, ekonomicznych, zmian społecznych i czynników kulturowych. Spośród nowych uwarunkowań technicznych na szczególną uwagę zasługują:

- technologie wysokiego ryzyka – systemy cechujące się wysokim prawdopodobieństwem zaburzeń o katastrofalnych, nieodwracalnych albo długo utrzymujących się skutkach. W złożonych systemach bazujących na nieliniowych interakcjach i zbyt sztywnych połączeniach komponentów – systemach, do których zaliczają się m.in. energetyka atomowa, GMO, inżynieria chemiczna, cywilny transport lotniczy, załogowe loty kosmiczne czy składowiska niebezpiecznych odpadów, katastrofy są czymś normalnym[4];
- technologie wysoce inwazyjne, cechujące się głębokimi ingerencjami w procesy naturalne, a zarazem wysoką skutecznością takich ingerencji (np. technologie kontrolowanej mutagenezy umożliwiające wytwarzanie syntetycznych organizmów działających autonomicznie i samoreplikujących się);
- technologie o wysokim potencjale transformacyjnym, zdolnym do wywoływania radykalnych zmian cywilizacyjnych (np. technologie IT);
- technologie wysoce innowacyjne o potencjałach rozwojowych, scenariuszach zastosowań i potencjałach oddziaływań trudnych do oszacowania ze względu na brak wzorców ekstrapolacyjnych;
- technologie organiczne, cechujące się wysokimi zdolnościami do samoodtwarzania i samoorganizacji. Takie technologie potrzebują tylko impulsu początkowego, po którym działają samodzielnie bez udziału – a często nawet bez wiedzy – człowieka. Wysoka produktywność takich systemów wynika z niestabilności, która ogranicza możliwości ingerencji ze strony człowieka (por. Michalski 2019, s. 113). Warto przyjrzeć się bliżej tej ostatniej właściwości współczesnych systemów technicznych, która – mimo rosnącego znaczenia – jest wciąż powszechnie pomijana albo bagateli-

[4] Charles Perrow – amerykański badacz katastrof przemysłowych wykorzystujący narzędzia analizy systemowej do identyfikacji przyczyn rzeczywistych wypadków – już w latach 80. zidentyfikował w złożonych systemach technicznych i organizacyjnych struktury, które mogą zagrażać swoim własnym funkcjom oraz wszystkiemu, co znajdzie się w zasięgu ich oddziaływania. Perrow skoncentrował się w swoich analizach na dwóch wzajemnie niezależnych strukturalnych cechach złożonych systemów – rodzajach interakcji (liniowe – nieliniowe) oraz rodzajach połączeń między elementami systemów (luźne – sztywne). Z połączenia obu wymiarów powstała matryca heurystyczna (por. Perrow 1984, s. 97) przydatna w analizach bezpieczeństwa systemów technicznych nadająca się również do wykorzystania w badaniu zagrożeń i ryzyk systemowych poza pierwotnym obszarem działalności przemysłowej. Na podstawie analizy rzeczywistych wypadków Perrow wykazał, że złożone systemy oparte na nieliniowych interakcjach i sztywnych sprzężeniach cechuje szczególna skłonność do wypadków i katastrof, które w systemach o takich cechach strukturalnych są czymś normalnym mimo podjęcia wszystkich niezbędnych środków ostrożności. Prace Perrowa stanowią przełom w badaniach nad bezpieczeństwem technicznym, w których wcześniej przyczynę wypadków i katastrof technicznych upatrywano wyłącznie w błędach człowieka (błędy projektanta, błędy operatora, lekceważenie przepisów bezpieczeństwa itp.) (więcej na ten temat zob. Perrow 1984, 1994, 2007). Do podobnego przełomu nie doszło niestety w systemach prawnych, gdzie na ławę oskarżonych o nieumyślne spowodowanie katastrofy wciąż zbyt często trafiają zwykli pechowcy – projektanci, kierownicy robót, inspektorzy nadzoru i wiele innych osób – pod naciskiem opinii publicznej, żądającej znalezienia i ukarania winnych. Siła przyzwyczajenia jest tak duża, że ludziom – zwłaszcza osobom poszkodowanym – trudno się pogodzić z myślą, że do wypadku mogło dojść wskutek niekontrolowanego zbiegu okoliczności, z powodu niedających się przewidzieć interakcji między czynnikami technicznymi lub naturalnymi, bez winy konkretnego człowieka.

zowana zarówno w naukowych analizach i ocenach bezpieczeństwa, jak i w praktyce zarządzania bezpieczeństwem technicznym.

Zagrożenia strukturalne: systemowe (organiczne), kumulacyjne i kombinacyjne – martwe strefy w polu widzenia normalnej nauki

Pomimo popularyzacji ekologii, która jako pierwsza dyscyplina nauk przyrodniczych zerwała z siedemnastowiecznym mechanistyczno-redukcjonistycznym obrazem świata, ciągle dominującym w innych gałęziach przyrodoznawstwa, i postawiła na holistyczne, „systemowe" rozumienie zjawisk w przyrodzie bez konieczności ich rozbierania na części, wciąż tyko niewielka część społeczeństwa zdaje sobie sprawę z istnienia systemów, ma świadomość zdolności, jakimi systemy dysponują, oraz właściwie rozumie ich znaczenie. Kształtowaniu świadomości „systemowej" z pewnością nie sprzyja szeroko rozpowszechnione inflacyjne użycie słowa „system", które stało się obecnie „gumą do żucia" stosowaną na określenie różnych złożonych obiektów lub struktur, które w sensie ścisłym systemami nie są. Chociaż od kilkunastu lat w różnych dyscyplinach naukowych wzrasta zainteresowanie zagrożeniami i ryzykami systemowymi[5], dotąd nie wypracowano jednolitej, uniwersalnej, powszechnie uznawanej definicji takich zagrożeń i ryzyk. Różnica między zagrożeniami i ryzykami systemowymi a niesystemowymi jest zatem intuicyjna i opiera się na ogólnych właściwościach systemów: organiczności, ogólnoustrojowości, zdolności do samoorganizacji i autonomicznego działania, wewnętrznych powiązaniach wszystkiego z wszystkim, synergiach itp. Mianem „systemowe" będą określane w dalszej części artykułu zagrożenia

[5] Powszechnie uważa się, że impulsem do rozpoczęcia badań nad zagrożeniami i ryzykami systemowymi był kryzys finansowy, do jakiego doszło w USA w latach 2001–2002 w następstwie zdemaskowania nadużyć finansowych Enronu i WorldComu. W obliczu gwałtownego spadku wartości indeksu Nasdaq i serii spektakularnych bankructw czołowych spółek technologicznych (IT) – zjawiska niezrozumiałego w epoce gwałtownego rozwoju cyfryzacji i ekspansji komputerów – teoretycy finansów i bankowości jako pierwsi w wyjaśnianiu przyczyn kryzysu posłużyli się narzędziami teorii systemów i analizy systemowej, które szybko znalazły zastosowania w analizie ryzyka (zob. Kaufmann i Scott 2003). Kulminacyjna fala zainteresowań naukowych zagrożeniami i ryzykami systemowymi na gruncie różnych dyscyplin zbiegła się w czasie z nadejściem jeszcze większego, ogólnoświatowego kryzysu finansowego lat 2008–2009, spowodowanego zapaścią na amerykańskim rynku kredytów hipotecznych wysokiego ryzyka – zapaścią, której symboliczną zapowiedzią było ogłoszenie upadłości czwartego co do wielkości amerykańskiego banku inwestycyjnego Lehman Brothers pod koniec września 2008 roku. Zagrożenia systemowe wynikające z rosnącej złożoności systemów technicznych dopiero od niedawna są przedmiotem systematycznych badań (zob. m.in. Hellström 2007; Renn i Keil 2008; Helbing 2009; Rothkegel, Banse i Renn 2010; Büscher 2011; Cleeland 2011; Orwat 2011; Michalski 2020a, 2020c). Dzięki intensyfikacji badań udało się dotąd zidentyfikować szereg wzajemnie współzależnych czynników strukturalnych wspólnych złożonym systemom technicznym, zwiększających prawdopodobieństwo zaskakujących, nieprzewidywalnych zachowań lub utrudniających kontrolowanie procesów rozprzestrzeniania się zaburzeń, a tym samym tworzących „żyzny grunt" dla zagrożeń i ryzyk o charakterze systemowym (zob. International Risk Governance Council, IRGC 2010, 2011).

wynikające z tajemniczych, niekontrolowanych synergii między strukturami, procesami lub czynnikami, które – rozpatrywane oddzielnie – same często nie niosą ryzyka poważnych zdarzeń szkodowych, ale dzięki przypadkowym koincydencjom, wzajemnym interakcjom, krzyżowym wpływom, kumulacjom, synergiom i skomplikowanym pętlom zwrotnych sprzężeń mogą prowadzić do zaskakujących niebezpiecznych sytuacji lub zdarzeń wymykających się poznawczej i operacyjnej kontroli, mogących poważnie zagrozić wszystkiemu, co znajdzie się w zasięgu ich oddziaływania. Mianem „systemowych" określa się czasami również zagrożenia związane z niepożądanymi wtórnymi lub tercjarnymi skutkami „rozsianymi", trudnymi do jednoznacznego zdefiniowania, dla których brakuje metod efektywnego szacowania strat (np. straty moralne lub wizerunkowe) oraz określania krytycznych, dopuszczalnych wartości lub w przypadku których trudno wykazać istnienie jednoznacznej zależności przyczynowej, mogącej stanowić podstawę ewentualnych roszczeń w postępowaniu prawnoadministracyjnym (por. Michalski 2020a, s. 15). Pojęcie „systemu" będzie poniżej używane w duchu klasycznej teorii systemów oraz synergetyki (zob. Haken 1982). W myśl tego pojęcia systemami są dające się wyodrębnić z otoczenia dynamiczne układy wzajemnie zależnych i współdziałających ze sobą elementów wykazujące skłonności samozachowawcze, posiadające zdolność do spontanicznej samoorganizacji i autonomicznego działania dzięki efektywności czerpanej z tajemniczych wewnętrznych synergii (Bertalanffy 1950, s. 143). Mimo braku ośrodka sterowania jakaś tajemnicza, niewidzialna siła (niewidzialna ręka) spaja pojedyncze oddziaływania w harmonijną całość i utrzymuje taki zmienny układ w dynamicznej równowadze (stabilność poprzez ciągłą zmianę), dzięki czemu jest on w stanie przetrwać nawet gwałtowne egzo- lub endogenne zaburzenia, dopóki te nie przekroczą określonego krytycznego poziomu. Tajemniczej integralności działania takich skomplikowanych układów oraz ich nadzwyczajnej produktywności nie da się zrozumieć ani wyjaśnić poprzez ich elementaryzację – rozłożenie całości na pierwotne części składowe celem poznania, jak działają one osobno we wzajemnej izolacji. Ze znajomości właściwości i sposobu działania pojedynczych komponentów w izolacji nie da się również wywnioskować, jaki będzie ostateczny efekt ich współoddziaływań, gdy komponenty te wejdą w skomplikowane wzajemne interakcje. Rozumienie działania takich złożonych układów wymaga całościowego ujęcia i jest zwykle rezultatem wielokrotnych iteracji. W toku rozwoju cybernetyki wypracowano użyteczne narzędzia analityczne zwiększające rozdzielczość obserwacji i opisu systemów pod kątem oddziaływań i konsekwencji ich złożoności i wewnętrznego zróżnicowania, umożliwiające pomniejszanie tego, co duże, powiększanie tego, co małe, i upraszczanie tego, co zbyt złożone (por. Büscher 2011, s. 5). Systemy mają pod wieloma względami paradoksalną konstytucję bytową. Z jednej strony są kruchymi złożeniami permanentnie zagrożonymi rozpadem i gwałtownie reagującymi na niewielkie nawet zaburzenia, z drugiej zaś superstabilnymi strukturami

potrafiącymi dopasowywać się do zmian otoczenia dzięki zdolnościom do spontanicznej reorganizacji i wysokiej produktywności czerpanej z synergii. Trwałość systemów zależy od ich zdolności do neutralizowania zaburzeń. Systemy nabywają taką zdolność poprzez spontaniczne produkowanie przypadkowych operacji powodujących ciągły wzrost wewnętrznej złożoności oraz wzrost specjalizacji pojedynczych komponentów. Wzrost złożoności oraz specjalizacji umożliwia generowanie nowych lub coraz wydajniejszych synergii między częściami składowymi i powstawanie dodatkowych funkcji, których nie posiadają pojedyncze komponenty systemu, gdy działają osobno. Im bardziej wewnętrznie złożony jest dany system, tym większą wykazuje autonomię, stabilność i odporność na zaburzenia, dopóki te nie przekroczą określonego krytycznego poziomu. Istnieją jednak górne granice złożoności, których przekroczenie powoduje dysfunkcjonalność systemu i zwiększa jego podatność na destabilizację (por. Michalski 2020a, s. 208). Dzięki zdolnościom do spontanicznej samoorganizacji oraz czerpanej z synergii dodatkowej produktywności, umożliwiającej wzajemne wzmacnianie efektów działania pojedynczych komponentów i pojawianie się nowych, niedających się przewidzieć funkcji i oddziaływań, złożone systemy wykazują skłonność do zaskakujących zachowań mogących poważnie zagrozić wszystkiemu, co znajdzie się w zasięgu ich oddziaływania[6].

Zmienność, której złożone systemy zawdzięczają swoje zdolności przystosowywania się do zmian otoczenia, ma przeważnie charakter losowy, polegający na uczeniu się metodą prób i błędów. Jednak oprócz przypadkowości zmian złożone systemy mają wiele innych wspólnych cech strukturalnych zwiększających ryzyko nieprzewidywalnych zachowań, czyniących z nich źródło poważnych zagrożeń dla otoczenia. Nieoczekiwanym, niepożądanym zachowaniom i oddziaływaniom złożonych systemów sprzyja przede wszystkim wspomniana wcześniej zdolność do wytwarzania wewnętrznych synergii umożliwiających zwiększanie wydajności zasobów, przy czym granic dodatkowej produktywności z reguły nie da się wywnioskować na podstawie analizy produktywności pojedynczych komponentów. Zachowania systemów cechują ponadto bifurkacje, czyli skokowe zmiany własności jakościowych systemu spowodowane niewielkimi ciągłymi zmianami jego parametrów. Nieliniowe interakcje między częściami składowymi oraz nieliniowe zależności między zachowaniem pojedynczych komponentów a zachowa-

[6] Odkrycia na gruncie matematycznej teorii chaosu nie pozostawiają wątpliwości, że możliwości kontrolowania bezpieczeństwa złożonych systemów technicznych były dotąd powszechnie przeceniane. Okazuje się bowiem, że nawet bardzo proste układy mogą zachowywać się chaotycznie (zob. Wang i Chen 2012). Modelowym przykładem prostego układu mechanicznego zachowującego się w sposób nieprzewidywalny jest podwójne wahadło. Współczesne systemy techniczne są oczywiście nieporównanie bardziej skomplikowane. Odkąd w połowie lat 80. XX wieku Charles Perrow zwrócił uwagę na wspólne cechy systemów technicznych i organizacyjnych odpowiedzialne za strukturalną podatność tych systemów na destabilizacje, w badanych systemach dokonał się skokowy postęp złożoności – przede wszystkim za sprawą rewolucji cyfrowej.

niem całego systemu sprawiają, że przyczyny i skutki zaburzeń oraz siła bodźców i siła reakcji nie są wzajemnie proporcjonalne. W konsekwencji niezauważalne zmiany parametrów pojedynczego komponentu mogą mieć zaskakująco poważne skutki dla zachowania całego systemu i odwrotnie: duże zmiany parametrów pojedynczych komponentów mogą w pewnych warunkach pozostawać bez wpływu na zachowanie całego układu. Rozprzestrzenianiu się zaburzeń sprzyja skłonność do zbyt sztywnych połączeń między komponentami. To właśnie brak „luzów" pełniących ważną funkcję marginesów bezpieczeństwa sprawia, że nawet bardzo niepozorne zaburzenia zachowania pojedynczego komponentu potrafią wywoływać kaskady zaburzeń innych komponentów, grożące destabilizacją całego systemu i jego przejściem w inny, mniej pożądany stan. Luźne sprzężenia umożliwiają pojedynczym komponentom swobodne działanie zgodnie z własną logiką, zapewniając wewnętrzną amortyzację zaburzeń, które dzięki temu nie destabilizują działania całego systemu. Nadmierne „luzy" zwiększające wzajemną niezależność działania komponentów mogą jednak niekorzystnie wpływać na synergie między nimi oraz grozić niebezpiecznymi, trudnymi do przewidzenia interakcjami lub utratą zdolności do amortyzowania i kompensowania zaburzeń poprzez ich rozłożenie na zbyt wiele buforów bezpieczeństwa. Złożone systemy przejawiają szczególną skłonność do zachowań fazowych, progowych, polegających na nagłych skokowych zmianach stanu dopiero z chwilą przekroczenia określonego krytycznego progu. Chociaż wczesne rozpoznawanie zbliżającej się gwałtownej zmiany stanu jest niezwykle trudne, przejścia fazowe nie muszą być całkowicie nieprzewidywalne. Istnieją bowiem zarówno uniwersalne, jak i specyficzne dla pewnych klas systemów słabe sygnały zapowiadające zbliżanie się krytycznego progu i rychłego przejścia systemu w nowy stan. W przypadku niektórych systemów takim sygnałem są „krytyczne fluktuacje" (częstsze i większe zaburzenia), w przypadku innych bywa nim „krytyczne spowolnienie" (coraz wolniejsze wychodzenie z zaburzeń) (zob. Scheffer i in. 2009). Ze skłonnością systemów do zachowań fazowych wiąże się określona bezwładność, która sprawia, że zaburzenia nie pociągają za sobą zwykle natychmiastowej reakcji systemu. Ponieważ zmiany stanu wymagają często głębokiej reorganizacji wewnętrznej struktury, złożone systemy „odkładają" przechodzenie do nowej równowagi do czasu, aż dotychczasowa równowaga osiągnie stan krytyczny. Opóźnienia reakcji miewają różną, trudną do przewidzenia długość. Złożone systemy posiadają pamięć ścieżki (histereza), czyli zależność aktualnego stanu od stanów go poprzedzających, co oznacza, że gdy system pod wpływem bodźca lub zaburzeń przechodzi do nowego stanu, po usunięciu bodźca lub ustaniu zaburzeń nie powraca do poprzedniego stanu wzdłuż tej samej ścieżki, o ile taki powrót w ogóle jest możliwy. Cechuje je ponadto występowanie zwrotnych sprzężeń, których częstym efektem bywa pozytywne zwrotne wzmocnienie. Takie układy reagują na pierwotne zaburzenia, dodatkowo je wzmacniając, co powoduje, że niewielkie z pozoru zaburzenie może za sprawą pozytywnego wzmocnienia

całkowicie zdestabilizować system. Określenie „pozytywne" nie ma w tym kontekście nic wspólnego z oceną zmian pod kątem użyteczności, oznacza bowiem jedynie zgodność kierunku zmian. To, jak duże możliwości zwrotnych sprzężeń oferuje dany system, zależy przede wszystkim od tego, jak silnie połączone są ze sobą jego elementy, nie zaś od stopnia złożoności. Istnieją bowiem proste systemy cechujące się silnym zwrotnym wzmocnieniem. Wskaźnikami dodatniej dynamiki zwrotnych sprzężeń są zaskakująco radykalne zmiany zachowania systemu pod wpływem nieproporcjonalnie słabych bodźców (por. Michalski 2020c, s. 20–23). Czynnikiem istotnie ograniczającym możliwości przewidywania zachowań złożonych systemów jest różna podatność takich systemów na zaburzenia tego samego rodzaju. Te same bodźce wpływają na różne systemy lub elementy systemów niejednakowo, co wobec braku wzorców ekstrapolacyjnych utrudnia odpowiednio wczesną identyfikację ewentualnych zdarzeń szkodowych oraz szacowanie ich prawdopodobieństwa, konsekwencji i dolegliwości. Podatność złożonych dynamicznych systemów na zaburzenia podlega ciągłym zmianom w czasie. Przeoczenie istotnych różnic w podatności lub zmian podatności w czasie grozi brzemiennym w skutkach przeszacowaniem lub niedoszacowaniem ryzyka określonych zdarzeń oraz błędnymi prognozami dotyczącymi jego trendów (ryzyko rosnące, ryzyko malejące). Z ewolucyjnego punktu widzenia zachowanie złożonych systemów może ponadto cechować zmienność mająca charakter losowy, polegająca na przystosowaniach metodą prób i błędów. Pod tym względem szczególnym przypadkiem są złożone systemy adaptacyjne (CAS) posiadające zdolność uczenia się. Przypadkowość „mutacji" czyni zachowania systemowe jeszcze bardziej nieprzewidywalnymi i trudnymi do kontrolowania (Helbing 2009).

Ze względu na swoją osobliwą konstytucję bytową systemy zagrażają człowiekowi zasadniczo na dwa sposoby, w związku z czym o zagrożeniach systemowych można mówić w dwóch znaczeniach, co często prowadzi do nieporozumień. W przypadku systemów, których niezawodne funkcjonowanie jest warunkiem zaspokajania ważnych potrzeb życiowych człowieka, niebezpieczne bywają wszelkiego rodzaju anomalie w zachowaniach systemu – anomalie, których spektrum sięga od niewielkich odchyleń, poprzez niepożądane zmiany stanów i trwałe destabilizacje, aż po całkowite i nieodwracalne zniszczenie systemu. Niepożądane zachowania systemów „krytycznych" (np. systemy zasilania), od których zależne są w swoim funkcjonowaniu inne systemy o kluczowym znaczeniu egzystencjalnym, mogą powodować brzemienne w skutkach kaskady niepożądanych zdarzeń. Istotniejsze z punktu widzenia dalszych rozważań są jednak zagrożenia systemowe innego rodzaju, wynikające ze spontanicznych procesów samoorganizacyjnych inicjujących skomplikowane, wielkoskalowe, poznawczo lub operacyjnie niedające się kontrolować interakcje i synergie między zjawiskami, procesami lub strukturami, które – rozpatrywane we wzajemnej izolacji – same często nie stanowią poważnego zagrożenia dla człowieka. W przeciwieństwie do zagrożeń

pierwszego typu źródło problemu stanowią w takim przypadku poznawcza nieuchwytność skomplikowanych wzajemnych strukturalno-funkcjonalnych zależności i interakcji między komponentami oraz odporność systemu na zaburzenia ograniczająca możliwości ingerencji ze strony człowieka.

Do gwałtownego wzrostu złożoności systemów technicznych przyczyniła się w ostatnich trzech dekadach rewolucja cyfrowa. Upowszechnienie mikroprocesorów, komputerów, Internetu, łączności bezprzewodowej i sztucznej inteligencji nadało transformacjom technologicznym całkowicie nową dynamikę. Wzrost złożoności, wzajemnych niedopasowań i podatności systemów technicznych na zaburzenia wynika przede wszystkim z połączenia technologii „różnych prędkości starzenia się”[7] w skomplikowane, wielokomponentowe systemy cyberfizyczne (*Cyber-Physical-Systems*, w skrócie: CPS). Różnice w długości cykli życia poszczególnych komponentów i odmienne tempo zmian innowacyjnych w gałęziach przemysłu je obsługujących wymagają ciągłych strukturalnych dopasowań i reorganizacji. W połączeniu z pozytywnymi zwrotnymi sprzężeniami, wynikającymi z konieczności wbudowywania w rozrastające się systemy posiadające zdolności uczenia się (adaptacji do zmieniających się warunków otoczenia) coraz to nowych komponentów technologicznych (np. kontrolery, warstwy zabezpieczeń, zapory ogniowe, bariery ochronne, systemy przechodzenia w tryb awaryjny itp.), co z kolei prowadzi do powstania beznadziejnej spirali rosnącego uzależnienia od wzajemnej niezawodności, wszystko to przyczynia się do gwałtownego wzrostu strukturalnej złożoności systemów technicznych, zwiększającej ryzyko nagłego występowania nieprzewidywalnych, niepożądanych zdarzeń, interakcji, synergii i kumulacji.

Złożone systemy mają jednak również pewne wspólne cechy ograniczające prawdopodobieństwo występowania zaskakujących groźnych zachowań. Im bardziej wewnętrznie złożony jest dany system, tym większe są z reguły jego zdolności adaptacyjne i samoorganizacyjne, od których zależy jego odporność na zaburzenia i destabilizacje. Wzajemnie niezależne komponenty tworzące system potrafią zmieniać swoje zachowanie w odpowiedzi na zmiany warunków zewnętrznych, a taka dokonująca się w sposób niezależny adaptacja zapewnia systemowi wytrzymałość na zaburzenia, dopóki te nie przekroczą pewnego ściśle określo-

[7] Do szacowania orientacyjnej długości cyklu życia komponentów IT w zarządzaniu technologiami powszechnie wykorzystywano prawo Moore’a. Gordon Moore – niegdyś szef Intela – w latach 90. XX wieku zaobserwował prawidłowość, zgodnie z którą mniej więcej co 18 miesięcy następował dwukrotny wzrost mocy obliczeniowej mikroprocesorów przy dwukrotnym spadku ich cen i dwukrotnej miniaturyzacji. Aby wymusić na użytkownikach odpowiednio częste wymiany sprzętu i oprogramowań na nowsze wersje i zabezpieczyć sobie stabilność rynków zbytu, producenci stosują wyrafinowane strategie (m.in. projektowanie planowej trwałości/żywotności, wygaszanie aktualizacji i usług wsparcia, wycofywanie produktów i części zamiennych z rynku, zmiany standardów kompatybilności). Infrastruktury fizyczne z oczywistych względów nie są w stanie dotrzymać kroku infrastrukturom IT w tempie modernizacji, co bywa przyczyną chronicznych niedopasowań i poważnych problemów zwłaszcza w systemach cechujących się zbyt sztywnymi połączeniami obu rodzajów komponentów.

nego krytycznego poziomu. Zdolności samoorganizacyjne pozwalają na zwiększanie wydajności zasobów, którymi dysponuje złożony system, aż do uzyskania pożądanego poziomu niezawodności. Zdolności te można wykorzystać w zarządzaniu bezpieczeństwem do ograniczania ryzyka systemowego (Helbing 2009), oczywiście pod warunkiem, że adekwatnie się je rozpozna. Pierwszym krokiem w zarządzaniu ryzykiem systemowym winno być więc określenie, czy rozpatrywany system jest złożony w sensie omówionym powyżej. Następnie należy ustalić wewnętrzne, endogeniczne czynniki, które mogą wpływać na występowanie niekontrolowanych, niepożądanych zdarzeń. Szczególną uwagę należy zwracać na istniejące w systemie marginesy bezpieczeństwa. Utrata takich marginesów, wynikająca np. z nadmiernej złożoności, przeciążeń, skrócenia i nadmiernego usztywnienia połączeń lub wzmocnienia wzajemnych zależności między komponentami, może w sposób istotny zwiększać podatność systemów na destabilizacje, ograniczając dodatkowo i tak niewielką przewidywalność ich przyszłych zachowań. Pozostawianie lub odbudowa odpowiednich marginesów bezpieczeństwa (buforów, rezerw, luzów, elastyczności itp.), stosowanie „zapór ogniowych" zapobiegających rozprzestrzenianiu się zaburzeń (np. uszkodzeń) między komponentami systemu, stosowanie barier chroniących systemy przed błędami lub złośliwymi ingerencjami ze strony człowieka oraz budowanie struktur systemowych o większej redundancji (dublowanie ważnych funkcji) lub większej odporności, które powodują, że każdy komponent systemu istotny z punktu widzenia bezpieczeństwa jest wspomagany przez inne komponenty, a jednocześnie dysponuje odpowiednią samowystarczalnością gwarantującą zachowanie funkcji nawet w przypadku poważnej awarii całego układu (por. Cleeland 2011, s. 17), to sprawdzone sposoby ograniczania ryzyka niepożądanych zachowań złożonych systemów oferowane przez współczesną inżynierię bezpieczeństwa. Koniecznym warunkiem możliwości skutecznego zarządzania bezpieczeństwem takich systemów lub skutecznej ochrony przed ich niebezpiecznymi lub szkodliwymi oddziaływaniami jest jednak poznawcze zapanowanie nad złożonością takich superstruktur. Realizacji tego celu nie sprzyjają jednak różnego typu pozastrukturalne czynniki i uwarunkowania (m.in. polityczne, prawne, ekonomiczne, organizacyjne, społeczne, kulturowe) eksploatacji niebezpiecznych systemów technicznych oraz wprowadzania ryzykownych innowacji, w tym również sytuacja panująca obecnie w świecie profesjonalnej nauki, której nieadekwatne strategie poznawcze służą w większości dziedzin działalności technicznej za podstawę społecznego monitoringu zagrożeń. Postępująca konwergencja infrastruktur fizycznych i infrastruktur teleinformatycznych stała się obecnie źródłem poważnych zagrożeń związanych z bezprawnymi ingerencjami czynnika ludzkiego możliwymi dzięki otwartości infrastruktury bazującej na sieci, obsługiwanej z poziomu wielu terminali. Gwałtownie rosnąca liczba cyberataków – w połączeniu z rosnącą strukturalną złożonością systemów technicznych sprzyjającą powstawaniu i rozprzestrzenianiu się zabu-

rzeń oraz ograniczającą możliwości poznawczej i operacyjnej kontroli – stawia ludzkość przed widmem katastrof, które w przypadku wysoce złożonych systemów o dużym udziale komponentów technologicznych należy traktować jako coś najzupełniej normalnego. Ze względu na współzależność oddziaływań wymienionych powyżej czynników w przypadku złożonych systemów należy się w związku z tym w każdej chwili liczyć z nagłym wystąpieniem nieznanych, nieoczekiwanych, niebezpiecznych zdarzeń i sytuacji, którymi trudno racjonalnie i odpowiedzialnie zarządzać z powodu ograniczeń poznawczych wynikających przede wszystkim z nadmiernej złożoności oraz zbyt dużej liczby danych wymagających obróbki (wyzwania czasu rzeczywistego). Wystąpienie krytycznych zaburzeń w takich systemach rozpoznaje się zresztą zwykle dopiero po fakcie, kiedy takie poznanie ma już ograniczoną praktyczną przydatność. O innych pozastrukturalnych czynnikach sprzyjających powstawaniu zagrożeń systemowych mowa będzie nieco dalej.

W kontekście bezpieczeństwa technicznego i ochrony ludności przed szkodliwymi oddziaływaniami przedsięwzięć technicznych, obiektów, instalacji, procesów czy produktów przemysłowych znacznie częściej niż o zagrożeniach systemowych mówi się o zagrożeniach skumulowanych i kombinacyjnych (hybrydowych), które wraz z zagrożeniami systemowymi (organicznymi) tworzą ukryty, strukturalny wymiar bezpieczeństwa – w dużej mierze niewykrywalny dla normalnej nauki i dla systemów monitoringu zagrożeń opartych na jej procedurach. O zagrożeniach skumulowanych mówi się przeważnie w odniesieniu do sytuacji, w których na ograniczonym terenie występuje duże zagęszczenie źródeł potencjalnie szkodliwych lub niebezpiecznych oddziaływań podobnego typu o niewielkim lub umiarkowanym poziomie ryzyka. Obiekty przemysłowe posiadające niewielki potencjał niebezpiecznego oddziaływania własnego w warunkach dużego zagęszczenia mogą stwarzać poważne zagrożenie dla samych siebie i otoczenia w przypadku jednoczesnego wystąpienia niebezpiecznych zdarzeń na terenie wielu obiektów. Niekontrolowane uwolnienie szkodliwych związków chemicznych na terenie jednego zakładu w następstwie wypadku może prowadzić do niebezpiecznych kumulacji szkodliwych oddziaływań wielu źródeł zagrożeń na niewielkim terenie i konieczności przerwania pracy w sąsiednich zakładach z powodu przekroczenia dopuszczalnych wartości stężeń. Konieczność prowadzenia działań ewakuacyjnych lub ratowniczych na terenie jednego obiektu w razie wypadku albo przerwa w pracy takiego obiektu spowodowana awarią lub planowym wyłączeniem mogą ograniczać istotne funkcje systemów bezpieczeństwa sąsiednich obiektów, zwiększając ryzyka związane z normalną działalnością do nieakceptowalnych poziomów. Przykładem problemów z kumulacją zagrożeń jest bliskie sąsiedztwo stacji benzynowych i zakładów o dużym ryzyku pożaru, magazynów niebezpiecznych chemikaliów lub środków pirotechnicznych. Indywidualne potencjały niebezpiecznych oddziaływań dla każdego z takich obiektów w sytuacji normalnej

mogą mieścić się w granicach ryzyka tolerowanego, wystarczającego do uzyskania niezbędnych pozwoleń, ale skumulowany rachunek ryzyka uwzględniający wiele źródeł zagrożeń łącznie nakazywałby w wielu przypadkach cofnąć wydane wcześniej pozwolenia. Rozwiązywanie problemów zagrożeń skumulowanych wymaga nowoczesnych instrumentów prawnych, politycznych, planistycznych, technicznych oraz komunikacyjnych umożliwiających zintegrowane zarządzanie ryzykiem na większym terenie, zamiast dotychczasowego wycinkowego zarządzania ryzykiem ograniczonego do pojedynczych, wzajemnie izolowanych obiektów. Mianem „hybrydowych" określa się natomiast zagrożenia będące kombinacjami dwóch lub więcej potencjalnie niebezpiecznych heterogenicznych czynników, między którymi dochodzi do wzajemnych krzyżowych oddziaływań zwiększających poziomy ryzyka określonych niepożądanych zdarzeń przyjęte dla każdego z tych czynników działających osobno lub grożących wystąpieniem dodatkowych zdarzeń, które nie byłyby możliwe w przypadku niewystąpienia któregoś z tych czynników. Źródłem zagrożeń hybrydowych mogą być koincydencje lub wzajemne interakcje typu: „czynnik techniczny – czynnik naturalny" (np. katastrofy wielkich zapór wodnych – Shimantan-Bangiao, sierpień 1975, katastrofa jądrowa w Fukushimie z 11/12.03.2011, katastrofa naftowa Deepwater Horizon z 22.04.2010 lub zagrożenia wynikające z pozalaboratoryjnego stosowania GMO), „czynnik techniczny – czynnik ludzki" (np. katastrofa jądrowa w Czarnobylu z 26.04.1986, zamachy terrorystyczne z 11.09.2001 czy katastrofa Airbusa A320-211 linii Germanwings w Alpach Zachodnich z 24.03.2015), „czynnik ludzki – czynnik naturalny" (np. epidemia koronawirusa z Wuhan) albo współoddziaływania trzech wymienionych czynników. Ilość wariantów takich kombinacji jest ograniczona tylko ludzką wyobraźnią. W przypadku większości tego typu zagrożeń efekt wzajemnego wzmocnienia podnosi akceptowalne ryzyko zdarzeń elementarnych do poziomu nieakceptowalnego dla ich koincydencji. Pojęcie „zagrożeń hybrydowych" pojawiało się dotąd częściej w kontekście zagadnień obronności i było kojarzone z prowadzeniem operacji zbrojnych na wielu polach walki równocześnie (np. klasyczny konflikt zbrojny połączony z wojną informacyjną albo cyberatakami). Wiele problemów związanych z zagrożeniami kombinacyjnymi nie zostało dotąd naukowo rozpoznanych, wyraźnie zdefiniowanych i rozwiązanych, a działania ochronne sporadycznie podejmowane w związku z nimi można uznać najwyżej za kosmetykę zagrożeń. Wiele systemów technicznych wysokiego ryzyka posiada wymagane prawem systemy ochrony zabezpieczające je przed normalnymi ryzykami eksploatacyjnymi, takimi jak awarie czy niepożądane zdarzenia spowodowane nieumyślnymi błędami obsługi. Systemy te są zwykle wyposażone w odpowiednie marginesy bezpieczeństwa wystarczające w przypadku różnego typu zdarzeń losowych, ale większość z tych systemów nie posiada wbudowanych zabezpieczeń przed ich celowym zniszczeniem, umyślnym uwolnieniem niszczących oddziaływań lub wykorzystaniem jako narzędzia do złośliwego ataku. Mode-

lowym przykładem szokującego „nadużycia", którego nie brano pod uwagę przy konfigurowaniu systemów bezpieczeństwa w cywilnym transporcie lotniczym, było wykorzystanie rejsowych samolotów pasażerskich jako pocisków do ataku terrorystycznego na Pentagon i WTC. W obliczu realnego zagrożenia zamachami terrorystycznymi oraz cyberterrorystycznymi pilnie potrzebne są nowe koncepcje ochrony przed kombinacyjnymi zagrożeniami wynikającymi z potencjalnie niszczycielskich interakcji typu „złośliwość ludzka – technologia wysokiego ryzyka". Różnica między zagrożeniami skumulowanymi, kombinacyjnymi i systemowymi ma charakter analityczny, w sytuacjach rzeczywistych zagrożenia te przeważnie występują łącznie w skomplikowanych, niepowtarzalnych konstelacjach.

Czynniki i uwarunkowania pozastrukturalne sprzyjające ryzykownym przedsięwzięciom technicznym

W dyskusjach o pozastrukturalnych czynnikach i uwarunkowaniach stwarzających żyzny grunt dla powstawania w złożonych systemach technicznych zaburzeń i oddziaływań zagrażających ludziom i środowisku zwraca się coraz częściej uwagę na zaskakująco zgodne konstelacje interesów w utrzymywaniu bezpieczeństwa takich systemów na najniższym możliwym poziomie wbrew deklaracjom o zaangażowaniu w poprawę bezpieczeństwa. Na szczegółowe omówienie pełnego spektrum takich czynników i uwarunkowań nie pozwalają ograniczenia objętościowe niniejszego artykułu, ale z pewnością warto wspomnieć o najistotniejszych determinantach, które wyostrzą świadomość powagi sytuacji.

Poprawie bezpieczeństwa systemów technicznych z pewnością nie sprzyjają obecne determinizmy ekonomiczne skłaniające przedsiębiorstwa – zarówno producentów towarów, wykonawców usług, jak i operatorów instalacji i infrastruktur – do ryzykownych i społecznie nieodpowiedzialnych praktyk biznesowych. Odkąd mianowicie pod wpływem rozwoju nowoczesnych, wysokowydajnych technik wytwarzania, rosnącego nasycenia rynków zbytu oraz globalizacji gospodarczej głównym czynnikiem przewagi konkurencyjnej stała się innowacyjność, przedsiębiorstwa oraz gospodarki narodowe prześcigają się w pochopnym wprowadzaniu innowacji, zanim nauka w pełni rozpozna wynikające z nich konsekwencje. Ponieważ wiele zagrożeń związanych z niepożądanymi oddziaływaniami innowacyjnych procesów lub produktów ujawnia się dopiero w późnych fazach procesu ich rozwoju, a więc po tym, jak przedsiębiorstwo poniosło już spore koszty inwestycyjne, zrozumiałe są opory firm przed rezygnacją z niebezpiecznych procesów lub wycofywaniem niebezpiecznych produktów zwłaszcza w sytuacji, kiedy nie istnieją jednoznaczne, niepodważalne eksperymentalne dowody ich szkodliwości, które mogłyby stanowić podstawę roszczeń sądowych.

Jeśli dane przedsiębiorstwo poczyniło wcześniej poważne inwestycje w innowację lub spodziewa się uzyskać strategiczne korzyści z jej wprowadzenia, wówczas trudno oczekiwać, że zdecyduje się przerwać projekt, gdy innowacyjny produkt okaże się niebezpieczny lub zostaną rozpoznane jego szkodliwe oddziaływania. W praktyce nic nie skłania przedsiębiorstw wytwarzających niebezpieczne produkty w niebezpiecznych procesach przy użyciu niebezpiecznych instalacji, do rzeczywistej troski o bezpieczeństwo narażonych, zwłaszcza że w każdym kraju świata niebezpieczny przemysł może liczyć na przychylność organów państwa, czerpiących zyski z licencjonowania i opodatkowania takiej działalności. Ponieważ państwo zyskuje na wzroście inwestycji, wzroście produkcji i wzroście sprzedaży, w interesie fiskalnym państwa nie leży wydawanie zakazów produkcji podejrzanych produktów wytwarzanych w podejrzanych procesach z użyciem podejrzanych urządzeń, zwłaszcza w sytuacji braku zniewalających naukowych dowodów na ich szkodliwość[8]. Szczególną ochronę państwa zapewnia interesom przemysłów wysokiego ryzyka plaga lobbingu i korupcji. Odkąd przemysł odkrył, że losy innowacji w większej mierze, niż od ich rynkowej siły przebicia, zależą od uwarunkowań politycznych, a sukces lub niepowodzenie inwestycji w innowacje zależą od tego, czy wcześniej przygotowało się odpowiednie warunki polityczne, aby innowacje miały pewny rynek zbytu na mocy prawa, które zmusi konsumentów do ich zakupu, powszechną praktyką stały się lobbing i korupcja, które gwarantują bezryzykowne finansowanie wprowadzania innowacyjnych produktów i procesów na rynek przy minimalnym wkładzie własnego kapitału. Zamiast sporych wydatków na proces badawczo-rozwojowy, poprawę bezpieczeństwa i reklamę nowego produktu firmy wolą przeznaczać stosunkowo niewielkie kwoty na wynagrodzenia dla lobbystów, PR i korupcję, ponieważ politycy będący obiektem zabiegów firm stanowią prawo w sposób gwarantujący sukces każdej – nawet społecznie wysoce szkodliwej lub niebezpiecznej – innowacji[9]. Nawet jeśli w pewnych sytuacjach organy państwa zdecydują się uznać prymat interesów bezpieczeństwa i ochrony obywateli nad krótkowzrocznymi interesami gospodarczymi i próbują przeciwdziałać społecznie szkodliwym lub niebezpiecznym praktykom

[8] Gospodarcze priorytety państw i pozorowanie zainteresowania ochroną własnych obywateli przed zagrożeniami ze strony niebezpiecznego przemysłu zdemaskowała niedawno globalna afera wokół glifosatu. Wbrew długoletnim protestom ekologów, wbrew ostrzeżeniom Międzynarodowej Agencji Badań nad Rakiem (IARC), która już w marcu 2015 roku ogłosiła, że związek ten jest prawdopodobnie rakotwórczy, a także wbrew formułowanym przez środowiska lekarskie wezwaniom do zakazania glifosatu państwa członkowskie Unii Europejskiej po wielu miesiącach impasu opowiedziały się pod koniec listopada 2017 roku za odnowieniem licencji na stosowanie glifosatu na pięć lat. Tylko nieliczne kraje unijne: Francja, Włochy, Holandia i Belgia zdecydowały się wprowadzić u siebie ograniczenia stosowania glifosatu (zob. https://biznes.interia.pl/firma/news/bayer-przegrywa-przed-sadem-w-sprawie-glifosatu,2607585,1852, dostęp: 30.03.2019).

[9] Przykładem niezawodnego funkcjonowania mechanizmów gwarantujących wysoką podatność współczesnych systemów socjotechnicznych na ryzyka są – będące efektem lobbingu wpływowych grup interesu – polityczne i prawne uwarunkowania handlu emisjami CO_2, które doprowadziły do powstania globalnych infrastruktur wymuszających rozwój elektromobilności.

prywatnego biznesu poprzez odmowę wydania zezwoleń lub restrykcyjny urzędowy nadzór, mają w praktyce bardzo ograniczone możliwości działania. W przypadku wydania urzędowego zakazu lub nakazu ograniczenia działalności stanowiącej zagrożenie dla ludzi lub środowiska firmy żądają zniewalających naukowych dowodów potwierdzających szkodliwość swoich oddziaływań, dobrze wiedząc, jakiego rodzaju oddziaływania są nieuchwytne dla nauki. Największymi możliwościami wczesnego rozpoznawania zagrożeń i ryzyk, których źródłem są procesy, produkty lub instalacje przemysłowe w prywatnych przedsiębiorstwach, dysponują osoby pracujące w takich przedsiębiorstwach. Ale sytuacja zawodowa tych osób (np. brak regulacji gwarantujących demaskatorom – zwanym często sygnalistami, whistleblowerami – ochronę przed działaniami odwetowymi ze strony pracodawców) nie ułatwia im ostrzegania otoczenia przed zagrożeniami wynikającymi z działalności własnego przedsiębiorstwa. Znane z historii ponure biografie osób, które w poczuciu społecznej odpowiedzialności zdecydowały się poinformować opinię publiczną o niebezpieczeństwach wynikających z działalności własnej firmy, z pewnością nie zachęcają innych do pójścia w ich ślady. Systematycznej produkcji zagrożeń w systemach technicznych sprzyja ponadto dynamiczny rozwój tzw. przemysłów ryzyka – wysokomarżowej branży produkcji i usług, którą tworzą m.in. firmy ubezpieczeniowe, producenci środków leczniczych, dostawcy sprzętu ratowniczego czy firmy zajmujące się usuwaniem zniszczeń i odbudową. Usuwanie skutków katastrof i niepożądanych skutków ubocznych „po szkodzie" z pewnością nie jest najlepszym wariantem zarządzania bezpieczeństwem, ale na rynku ryzyka nie brakuje podmiotów, które profitują z takich działań. Niebezpieczeństwa i ryzyka, które dotrą do świadomości potencjalnych poszkodowanych, rozbudzają nowe potrzeby bezpieczeństwa i ograniczania ryzyka strat, co przyczynia się do powstania wielu nowych gałęzi przemysłu i usług. Ponieważ konsolidujący się przemysł profituje z zagrożeń, które sam wytwarza, nie należy oczekiwać ze strony przemysłu większego zaangażowania w ich eliminowanie. Jeśli dodatkowo weźmie się pod uwagę fakt, że potencjalnie poszkodowani, licząc na wypłaty sowitych odszkodowań i rekompensat, również są w niewielkim stopniu zainteresowani zapobieganiem szkodom, wówczas nasuwa się pytanie, komu w tych warunkach zależy jeszcze na utrzymaniu bezpieczeństwa systemów technicznych na odpowiednim poziomie i powstrzymaniu niebezpiecznych przemysłów przed narażaniem ludności na nieograniczone łańcuchy szkód (por. Rothkegel, Banse i Renn 2010, s. 156). Jeśli ten ponury obraz sytuacji dopełni się zawartymi w dalszej części artykułu wynikami obserwacji rzeczywistego zaangażowania nauki w adekwatne rozpoznanie zagrożeń ze strony czynników technicznych i rozwijanie strategii przeciwdziałania tym zagrożeniom oraz ochrony przed nimi, trudno oprzeć się wrażeniu, że – oprócz czynników strukturalnych nadzwyczaj sprzyjających niebezpiecznym, niekontrolowanym zachowaniom i szkodliwym oddziaływaniom złożonych systemów technicznych – istnieje również zaskakująca

zgodność interesów w utrzymaniu bezpieczeństwa systemów technicznych na najniższym możliwym poziomie. W konsekwencji w większości dziedzin działalności technicznej prowadzi się tylko kosmetykę zagrożeń zamiast eliminowania ich prawdziwych przyczyn.

Badania analityków katastrof technicznych oraz statystyki ubezpieczeniowe wskazujące na stały wzrost liczby katastrof, wypadków i różnego typu zdarzeń szkodowych z udziałem systemów technicznych (zob. Schweizerische Rückversicherungsgesellschaft 2008) zgodnie potwierdzają trafność konkluzji wynikających z powyższych analiz: możliwości poznawczego i operacyjnego kontrolowania bezpieczeństwa złożonych systemów opartych na komponentach technologicznych oraz złożonych, wieloagentowych strukturach organizacyjnych były dotąd powszechnie przeceniane i duża w tym zasługa profesjonalnej nauki, która stosując nieadekwatne, redukcjonistyczne, selektywne strategie poznawcze do monitorowania zagrożeń ze strony czynników technicznych, dostarczała i nadal dostarcza społeczeństwu fałszywego poczucia bezpieczeństwa.

Wątpliwa rola nauki w monitorowaniu zagrożeń i ochronie społeczeństwa przed szkodliwymi oddziaływaniami czynników technicznych

Coraz bardziej złożone, nieprzewidywalne i niebezpieczne otoczenie, w którym wszystko jest w skomplikowany i niezrozumiały dla człowieka sposób połączone ze wszystkim i w którym każda, nawet najbardziej niepozorna zmiana zachowania jednego elementu może powodować zaskakujące niepożądane reakcje innych elementów, a w sytuacjach skrajnych wywoływać brzemienne w skutkach kaskady zaburzeń błyskawicznie rozprzestrzeniające się wzdłuż łańcuchów zbyt sztywnych połączeń, zdolne pokonać wszelkie bariery ochronne wymyślone przez człowieka i zdolne zagrozić wszystkiemu, co znajdzie się w zasięgu ich oddziaływania (Büscher 2011, s. 4), stawia pod znakiem zapytania przydatność normalnej nauki jako narzędzia wspomagania procesów zarządzania bezpieczeństwem technicznym i ochrony ludności przed niepożądanymi oddziaływaniami systemów technicznych. Adekwatnej identyfikacji zagrożeń wynikających z szybko rosnącej złożoności systemów technicznych z pewnością nie sprzyja sytuacja panująca obecnie w nauce. Procesy komercjalizacji niepostrzeżenie przekształcają działalność naukową z bezinteresownego poszukiwania prawdy w służbie społeczeństwu w płatne usługi wsparcia dla prywatnego biznesu. Odkąd zainteresowania badawcze zaczął wyznaczać szybki zwrot kapitału, a kariera naukowa bardziej niż od pasji badawczej stała się zależna od umiejętności pozyskiwania grantów i sponsorów, nauka skupiła wysiłki na poszukiwaniu nowych sposobów na pod-

niesienie skuteczności działania, a poznanie w naukach szczegółowych zaczęło się ograniczać do precyzyjnego, ale coraz bardziej wycinkowego opisu pojedynczych zjawisk podporządkowanego praktycznym celom gospodarczego wykorzystania uzyskanej w ten sposób wiedzy. W konsekwencji dziedziny nauki, które nie są interesujące finansowo, szybko pustoszeją, a nauka bezwiednie poddająca się naciskom praw rynku unika odkryć, które mogłyby zaszkodzić interesom finansującego ją prywatnego biznesu. Normalna nauka – coraz bardziej uzależniona od prywatnego kapitału i uwikłana w „niebezpieczne związki" z przemysłem wytwarzającym niebezpieczne produkty w niebezpiecznych procesach z użyciem niebezpiecznych instalacji – nie może liczyć na nieograniczone społeczne zaufanie do poświadczeń bezpieczeństwa, których dostarcza, również z powodów bardziej zasadniczych. Zagrożenia organiczne, kombinacyjne i skumulowane wynikające ze złożoności systemów technicznych pozostają w dużej mierze poznawczo nieuchwytne dla nauk laboratoryjnych, które mają w wielu dziedzinach monopol na rozstrzyganie kwestii bezpieczeństwa. Nauki te operują bowiem nieadekwatnymi, mechanistyczno-redukcjonistycznymi modelami poznania opartymi na elementaryzacji, coraz węższej specjalizacji oraz przesadnie zawyżonych wymaganiach ścisłości stawianych naukowym dowodom. Kartezjański, mechanistyczny model poznania uznający redukowanie złożonych zjawisk do elementarnych części składowych i prostych liniowych zależności kauzalnych oraz dogłębne badanie, jak części te działają we wzajemnej izolacji, za właściwą drogę do rozumienia rzeczywistości, w połączeniu z metodycznym sceptycyzmem, który za jedyną prawomocną strategię obiektywizacyjną uznaje kwantyfikowalność, skutkuje wyłączeniem złożonych, niemierzalnych i nieobliczalnych aspektów rzeczywistości poza obszar zainteresowań nauki i uznaniem ich za domenę niepewnych faktów i „teorii spiskowych" (Jurgilewicz i Michalski 2020, s. 16). Możliwość arbitralnego pomijania niemierzalnych oddziaływań w analizie i ocenie ryzyka pod pretekstem „obiektywizacji" jest nagminnie wykorzystywana do sztucznego zaniżania rzeczywistych poziomów ryzyka w celu budowania społecznej akceptacji dla kontrowersyjnych projektów. W konsekwencji normalna nauka w sposób bardziej lub mniej zamierzony wznosi wokół niebezpiecznej działalności przemysłowej prywatnego biznesu „wały ochronne" w postaci niepewności faktów, która skutkuje „domniemaniem niewinności" i umożliwia narażającym nieograniczone kwestionowanie roszczeń narażonych i poszkodowanych. W związku z tym naukowe dowody nie tylko coraz rzadziej rozwiewają wątpliwości związane z bezpieczeństwem przedsięwzięć, obiektów, procesów i produktów technologicznych, ale wobec akceleracji zmian technologicznych czas oczekiwania na takie dowody jest zdecydowanie zbyt długi, aby można było ludność skutecznie ochronić przed narażeniem na szkody i niebezpieczeństwa wynikające z działalności technologiczno-przemysłowej prywatnego biznesu, któremu udaje się wmówić opinii publicznej, że technologiczne innowacje są największym dobrodziejstwem ludzkości.

Głównym powodem brzemiennej w skutkach utraty z pola widzenia wielu zagrożeń „organicznych" ukrywających się za skomplikowanymi wielopoziomowymi interakcjami i współoddziaływaniami złożonych struktur różniących się od siebie pod względem sposobu działania jest stosowanie nieadekwatnych, liniowo-deterministycznych modeli naukowego poznania, rozpowszechnione w większości obszarów zarządzania bezpieczeństwem (bezpieczeństwo leków i żywności, bezpieczeństwo procesowe, bezpieczeństwo stanowisk pracy, bezpieczeństwo obiektów i ochrona mienia itp.). Będąca „mitem założycielskim" pozytywizmu newtonowska mechanistyczna wizja świata, widząca właściwą drogę do rozumienia i przewidywania złożonych zjawisk w redukowaniu ich do elementarnych części składowych i prostych liniowych zależności przyczynowych, w połączeniu z kartezjańskim metodycznym sceptycyzmem, którego konsekwencjami są zawyżone wymagania ścisłości stawiane naukowym „dowodom" faworyzujące nauki eksperymentalne oraz „domniemanie niewinności" oddziaływań nieznajdujących laboratoryjno-eksperymentalnego potwierdzenia, czynią współczesną profesjonalną naukę integralną częścią struktur systemowych odpowiedzialnych za dyskretne, nieograniczone generowanie szkód, którym laboratoryjna nauka konsekwentnie zaprzecza. Wielu skomplikowanych systemowych uwarunkowań powstawania poważnych zagrożeń i systematycznej produkcji ryzyka – szczególnie zagrożeń ukrytych, które nie ujawniły się dotąd w postaci rzeczywistych katastrof – nie można modelować jako prostych liniowych łańcuchów przyczynowo-skutkowych, dających się eksperymentalnie potwierdzić w drodze laboratoryjnych symulacji. Ograniczenia możliwości eksperymentowania wynikają nie tylko z samej złożoności rozpatrywanych tutaj oddziaływań, ale także długich okresów ekspozycji. Zatem nawet gdyby skomplikowane sploty organicznych współoddziaływań udało się bez uszczerbku dla ich całościowego rozumienia rozłożyć na jednokierunkowe łańcuchy przyczynowo-skutkowe pozwalające na ich symulację, to i tak ograniczony czas trwania eksperymentu laboratoryjnego wyklucza możliwość symulacji procesów trwających w rzeczywistości wiele lat i narażonych w tak długim czasie na różnorodne krzyżowe interakcje. Tymczasem w sytuacji braku możliwości eksperymentalnego potwierdzenia jednoznacznych liniowych związków przyczynowo-skutkowych między podejrzanym czynnikiem a określonymi zdarzeniami szkodowymi kartezjański program metodycznego sceptycyzmu będący filarem zachodniej racjonalności i kultury prawnej zaleca wątpienie, natomiast epistemologia współczesnej nauki nakazuje rozstrzygać wszelkie wątpliwości… na niekorzyść wątpliwości (por. Hofmann 2008, s. 29), co skutkuje przyjęciem zasady domniemania niewinności każdego podejrzanego czynnika do czasu, aż pojawią się niepodważalne eksperymentalne dowody jego szkodliwości. Wobec gwałtownie wzrastającej złożoności środowiska bezpieczeństwa do rzadkości należą obecnie zagrożenia, które powstają w sposób odosobniony i które można wyjaśnić jednoczynnikowo, a wynikające z nich ryzyka ograniczać, działając na

jedną przyczynę, dającą się zidentyfikować i w sposób nieograniczony kontrolować. Większość współczesnych zagrożeń ma złożoną genezę i sieciową lub organiczną strukturę, więc ich badanie pod kątem wczesnej wykrywalności, potencjału szkodowego lub możliwości skutecznej ochrony przed niepożądanymi skutkami wymaga przyjęcia innej perspektywy niż dotychczasowe – coraz bardziej „wycinkowe" – ujęcia, będące konsekwencją postępującej specjalizacji w nauce. Silne tendencje separatystyczne cechujące normalną naukę nie sprzyjają wzajemnej konstruktywnej krytyce i wypracowywaniu metod i narzędzi integrujących różne nośniki wiedzy, przydatnych w całościowych, interdyscyplinarnych syntezach. Czynnikiem poważnie ograniczającym możliwości poznawczego zapanowania nad złożonością oddziaływań systemowych, a w konsekwencji przewidywalność ewentualnych niepożądanych efektów skomplikowanych synergii są granice matematycznego modelowania. Niedorozwój naukowych narzędzi umożliwiających adekwatne, całościowe, wysokorozdzielcze odwzorowywanie złożoności – najlepiej prospektywne albo przynajmniej w czasie rzeczywistym – w połączeniu z nieuchronną selektywnością scjentystycznych ujęć związaną z ograniczaniem się w percepcji zagrożeń do parametrów mierzalnych odpowiadających wymaganiom obliczalności ryzyka gwarantują niewykrywalność szerokiego spektrum zagrożeń. Takie „martwe strefy" w polu widzenia podważają jednak sensowność wielu restrykcji wprowadzanych dla poprawy bezpieczeństwa i sprawiają, że „odcinkowa" nadgorliwość zarządzających bezpieczeństwem bywa często bezużyteczna, a czasami wręcz kontrproduktywna.

Selektywność scjentystycznych odwzorowań sztucznie wyizolowujących wycinki rzeczywistości cechujące się ścisłym determinizmem i nadające się do prostej ilościowej obróbki bez konieczności uwzględniania skomplikowanych współzależności i interakcji występujących w ich „naturalnym" otoczeniu wynika ze złożonych uwarunkowań, na których szczegółowe omówienie nie pozwalają ograniczenia objętościowe niniejszego artykułu. Mierzalność i obliczalność bywają wygodną i skuteczną strategią obiektywizacyjną, tyle że w przypadku szerokiego spektrum oddziaływań trudno wypracować jednolite, akceptowalne dla wszystkich i akceptowane przez wszystkich kryteria porównywalności i priorytetyzacji oddziaływań należących do różnych kategorii, w tym także oddziaływań niemierzalnych. Aby ten problem rozwiązać, w praktyce ignoruje się te wymiary oddziaływań, których kwantyfikacja oraz – w razie potrzeby – monetaryzacja są szczególnie kłopotliwe. Głównym problemem epistemologicznym, z jakim borykają się analizy i oceny ryzyka, są jednak trudności z empirycznym wykazaniem istnienia wystarczająco silnego związku przyczynowo-skutkowego między niepożądanym zdarzeniem szkodowym (np. zgon, niezdolność do pracy, strata finansowa) a pojedynczym czynnikiem podejrzanym o jego spowodowanie w warunkach skomplikowanego splotu egzo- i endogenicznych uwarunkowań. W efekcie analizy ryzyka

często ograniczają się więc do oddziaływań, dla których istnieje możliwość wykazania ścisłego determinizmu[10].

Takie redukcje uważa się powszechnie za usprawiedliwione z punktu widzenia konieczności zachowania ścisłości danych. Uznanie innych wymiarów oddziaływań za niemające istotnego wpływu na podejmowanie decyzji i pominięcie ich w ilościowej analizie ryzyka jest jednak akceptowalne tylko pod warunkiem, że decydent traktuje rezultaty takiej analizy wyłącznie jako jeden z wielu elementów swojego zaplecza decyzyjnego, a pominięte w niej oddziaływania niewymierne lub niedające się zmierzyć z przyczyn pragmatycznych uzupełni danymi z innych źródeł. W praktyce zarządzania bezpieczeństwem możliwość arbitralnego pomijania określonych wymiarów szkodliwych oddziaływań w analizie i ocenie ryzyka pod pretekstem jej obiektywizacji jest nagminnie wykorzystywana do sztucznego zaniżania rzeczywistych poziomów zagrożenia w celu budowania społecznej akceptacji wokół kontrowersyjnych projektów.

Ze względu na ograniczoną poznawalność przyszłości wczesna identyfikacja niepożądanych sytuacji, zdarzeń lub oddziaływań zagrażających realizacji celów oraz ocena ich znaczenia, która coraz częściej przybiera postać sformalizowanej analizy ryzyka – o ile w ogóle są możliwe – zamiast być procesem refleksyjnym, samoświadomym i samokrytycznym, są często mniej lub bardziej przypadkową sekwencją pomiarów i obliczeń przeplatających się z czynnościami intuicyjnymi, rutynowymi oraz arbitralnymi rozstrzygnięciami o charakterze aksjonormatywnym. Niepewność dotycząca przyszłych zdarzeń nie wynika bowiem jedynie z wpływu przypadkowości lub nieznajomości związków przyczynowych łączących obecne sytuacje i zdarzenia z ich następstwami w przyszłości, ale także stąd, że same decyzje dotyczące ryzyka są źródłem zaburzeń wpływających na zachowanie rozpatrywanych systemów w przyszłości i jako takie niszczą konieczne warunki możliwości weryfikacji trafności prognoz, na których się opierają. W przypadku innowacyjnych procesów oraz towarzyszących im skomplikowanych, nieliniowych łańcuchów przyczynowych, łączących czynniki inicjujące z niepożądanymi „odchyleniami" zagrażającymi ciągłości działania, realizacji celów albo prawnie chronionym dobrom, co może dostarczać podstawy do roszczeń osób trzecich,

[10] W przypadku szacowania ryzyka na gruncie medycznej koncepcji czynników ryzyka zdrowotnego ścisły determinizm oznaczający, że rozpatrywany czynnik ryzyka jest zarazem koniecznym i wystarczającym warunkiem zachorowania na określoną chorobę, wymaga istnienia liniowej zależności między dawką czynnika a skutkiem (1) – zależności przejawiającej się tym, że liczba zachorowań wzrasta wprost proporcjonalnie do wzrostu wartości czynnika ryzyka; zgodności rezultatów badań przeprowadzonych niezależnie dla różnych populacji (2) oraz w różnych dziedzinach (np. obserwacje kliniczne, studia epidemiologiczne, analizy patologiczne itp.) (3); istnienia przekonujących potwierdzeń podobnego oddziaływania czynnika ryzyka na procesy komórkowe (4) oraz odpowiedniego potwierdzenia przez rezultaty studiów interwencyjnych (Banse i Bechmann 1998, s. 32). Takie warunki spełnia tylko niewielka część oddziaływań na ludzkie zdrowie, co operatorzy niebezpiecznych urządzeń i producenci niebezpiecznych produktów skrzętnie wykorzystują jako alibi, aby zaprzeczać społecznym oskarżeniom formułowanym w obronie narażonych lub poszkodowanych.

postępowanie rutynowe oparte na dotychczasowych doświadczeniach z sytuacjami problemowymi arbitralnie uznanymi za podobne przysparza często więcej problemów i w konsekwencji naraża na ryzyka nie mniejsze od tych wynikających z całkowitego zignorowania określonych zagrożeń. Uczenie się rozpoznawania zagrożeń o wysokim potencjale niszczącym lub nieodwracalnych skutkach i reagowania na takie zagrożenia metodą prób i błędów nie wydaje się zatem dobrą koncepcją bezpieczeństwa, właściwą z punktu widzenia ochrony ludności przed zagrożeniami systemowymi.

Sprawdzonym w wielu dziedzinach działalności człowieka sposobem produktywnego obcowania z nieprzewidywalnością i niepewnością przyszłych zdarzeń jest zarządzanie ryzykiem. Ma ono coraz częściej postać sformalizowanego postępowania, na które składają się: wyznaczanie możliwie pełnego spektrum niepożądanych zdarzeń mogących zagrażać realizacji celów, określanie częstości występowania interesujących zdarzeń w podobnych sytuacjach, indukcyjne wyprowadzanie wniosków dotyczących prawdopodobieństwa powtórzenia się określonych zdarzeń w zdefiniowanym przedziale czasu, szacowanie i wzajemne bilansowanie spodziewanych kosztów szkód i strat, jakie mogą być następstwem takich zdarzeń, wyznaczanie spektrum dostępnych działań umożliwiających zapobieganie takim zdarzeniom, ograniczanie prawdopodobieństwa ich wystąpienia lub ograniczanie grożących strat, szacowanie wysokości związanych z tym nakładów, a w końcu porównawcza ocena racjonalności wyboru każdej z dostępnych opcji działania w świetle przyjętych preferencji i progów ryzyka (ryzyko akceptowane, ryzyko tolerowane, ryzyko resztkowe) (zob. Michalski 2020c). W niektórych obszarach, takich jak bezpieczeństwo leków i żywności, bezpieczeństwo procesowe, bezpieczeństwo środowiskowe czy bezpieczeństwo stanowisk pracy, systematyczne analizy ryzyka oparte na ocenach mierzalnych – przede wszystkim fizycznych – oddziaływań i wyznaczaniu wartości granicznych dla takich oddziaływań są obligatoryjnym narzędziem zarządzania bezpieczeństwem wymaganym przepisami prawa. Podstawę zarządzania ryzykiem stanowi jego szacowanie (ocena), a standardowym narzędziem szacowania ryzyka jest klasyczna matematyczna formuła ryzyka bazująca na rachunku prawdopodobieństwa. Odkąd Andriej N. Kołmogorow nadał podstawowym zasadom rachunku prawdopodobieństwa postać aksjomatyczną (zob. Kolmogorow 1933), klasyczna matematyczna formuła definiująca ryzyko jako obliczalną wielkość zależną od dwóch zmiennych: wartości strat i wartości prawdopodobieństwa ich wystąpienia[11] rozpoczęła swój „trium-

[11] W niektórych domenach zarządzania bezpieczeństwem, gdzie zdarzenia szkodowe stanowiące względnie jednorodny zbiór odpowiednio często się powtarzają i gdzie dysponuje się w związku z tym rozległą bazą zagęszczonych danych historycznych, zamiast prawdopodobieństwa bazuje się w szacowaniu ryzyka na częstości występowania zdarzeń. W nowszych teoriach ryzyka uwzględnia się również inne zmienne, takie jak np. współczynnik ekspozycji, określający czas lub stopień narażenia – np. w BHP, albo grupowe lub indywidualne czynniki podatności – np. w epidemiologii.

falny marsz", który w wielu dziedzinach teorii i praktyki miał umożliwić poznawcze lub operacyjne zapanowanie nad niepewnością przyszłości.

Niewątpliwa elegancja i prostota klasycznej matematycznej formuły ryzyka, umożliwiającej jednolite klasyfikowanie wszystkich możliwych ilościowych opisów zdarzeń, a także wrażenie solidnej naukowej podbudowy, jakie stwarzają obliczenia z zakresu rachunku prawdopodobieństwa, przyczyniają się do przesadnego zaufania do zawężonego, sformalizowanego pojęcia ryzyka – pojęcia, które opiera się na wielu niesprawdzonych, niesprawdzalnych lub nieprzekonujących założeniach i z którego zastosowaniami wiąże się wiele niejasności, nieścisłości i konieczność dokonywania mniej lub bardziej arbitralnych rozstrzygnięć natury normatywnej – oraz do bezkrytycznego ekstrapolowania tego pojęcia użytecznego w niektórych obszarach strategicznego zarządzania[12] na obszary ludzkiej działalności niespełniające często nawet najbardziej podstawowych warunków jego stosowalności. Operowanie tradycyjnym, zmatematyzowanym pojęciem ryzyka wymaga przyjęcia wielu kontrowersyjnych założeń, m.in. że podobne sytuacje decyzyjne regularnie się powtarzają, niepożądane zdarzenia tworzące odpowiednio zagęszczony, jednorodny zbiór są wzajemnie niezależne i dają się dobrze obserwować, wynikające z nich straty można definiować jako obiektywne, obliczalne wielkości, a ich tolerancja nie ulega zmianom w okresie wyznaczającym horyzont analizy. W wielu obszarach, w których rozpowszechniło się wąskie matematyczne pojęcie ryzyka, warunki te nie są jednak spełnione. Nieadekwatność ujęcia ryzyka w takich przypadkach sprawia, że niewzruszone przekonanie o posiadaniu pełnej kontroli nad sytuacją czerpane ze ścisłości obliczeń jest iluzją – tym bardziej niebezpieczną, im dalej odbiega od rzeczywistości. Opieranie

[12] Zarządzanie strategiczne jest tutaj rozumiane szeroko jako rozległa dziedzina planowania realizacji celów w środowisku o zmiennych, niepewnych uwarunkowaniach, na które jednostka lub organizacja mają ograniczony wpływ. Planowanie w takich warunkach wymaga przewidywania przyszłych sytuacji, oceny wynikających z nich szans i zagrożeń dla realizacji celów oraz wypracowywania strategii optymalizacyjnych minimalizujących konsekwencje błędnych, nietrafionych decyzji, strat lub odchyleń od założonych celów. Modelowymi dziedzinami produktywnych zastosowań analiz i ocen ryzyka są zarządzanie projektami oraz zarządzanie ryzykiem na rynkach finansowych. W pierwszym przypadku analiza ryzyka przypisująca zmiennym krytycznym, od których zależy powodzenie projektu, odpowiednie rozkłady prawdopodobieństw stanowi narzędzie pomocnicze analizy wrażliwości badającej wpływ zmian procentowych zmiennych na wskaźniki powodzenia projektu. Pod warunkiem dostępności odpowiedniej bazy danych historycznych dotyczących podobnych projektów ilościowe analizy ryzyka dostarczają analitykom użytecznych statystyk dotyczących wskaźników ekonomiczno-finansowej wydajności projektu: oczekiwanych wartości, standardowych odchyleń, współczynników zmienności itp. (por. Michalski 2020b, s. 49 i n.). Natomiast szacowanie ryzyka na rynkach finansowych opiera się najczęściej na pojęciu wartości zagrożonej (*Value at Risk*, VaR), która jest ogólną, uniwersalną miarą ryzyka wyznaczającą graniczny poziom straty wartości rynkowej (np. instrumentu finansowego, portfela pozycji/produktów itp.) przy granicznym tolerowanym poziomie prawdopodobieństwa jej osiągnięcia α w przyjętym okresie. Taka uniwersalna miara rozwiązuje uciążliwy problem porównań ryzyka wielu pozycji i umożliwia agregację ryzyka metodą portfela (zob. Dowd 1998; Sawczyk 1999; Jajuga 2000; Butler 2001). Warunkiem stosowalności VaR jest normalne funkcjonowanie rynku gwarantujące przewidywalność strat przy określonych, niezmiennych założeniach dotyczących horyzontów czasowych prognoz oraz przyjętych poziomów tolerancji strat.

się na obliczalności ryzyka w takich sytuacjach przynosi zwykle więcej szkody niż pożytku, a w najlepszym razie prowadzi do kontrowersji, dezorientacji i rozczarowań – podobnych do tych, jakie wywołuje np. profilaktyka raka piersi polegająca na przesiewaniu metodą mammografii[13].

Jak niebezpieczną pułapką bywają obietnice bezpieczeństwa oparte na wierze w obliczalność rzeczywistości i w możliwość obiektywnej identyfikacji i oceny ryzyka, pokazują techniczne katastrofy (budowlane, transportowe, przemysłowe itp.) oraz codzienne prawie-katastrofy (sytuacje, w których katastrofa była „o włos", ale ostatecznie nie doszło do niej z powodu skutecznego, szybkiego reagowania lub zbiegu okoliczności niebranych wcześniej pod uwagę w procesie analizy ryzyka i oceny bezpieczeństwa). Pułapka obliczalności polega na tym, że sytuacje decyzyjne jawią się jako bardziej matematyczne i regularne, niż są w rzeczywistości. Obliczalność świata wydaje się jednak powszechnie przeceniana i każdy, kto w nią przesadnie wierzy, prędzej czy później znajdzie się w pułapce. Towarzyszące większości wypadków uwarunkowanych technicznie doświadczenie utraty kontroli nad procesami i zależnościami, które wcześniej powszechnie uważano za w pełni kontrolowane, uświadamia dotychczas nieznane, nieuwzględniane lub uznawane za nieistotne z punktu widzenia bezpieczeństwa cechy i zachowania systemów tech-

---

[13] Badania przeprowadzone przez Szpital Uniwersytecki w Zurychu wykazały, że dobroczynne skutki badań przesiewowych metodą mammografii są powszechnie przeceniane. Z analizy danych statystycznych wynika, że na każde 1000 kobiet w wieku powyżej 50 lat regularnie co dwa lata przesiewanych metodą mammografii umarłoby w następnych 20 latach na raka piersi ok. 16 pań, czyli mniej więcej o cztery mniej (2%) w porównaniu z grupą kontrolną nieobjętą takim profilaktycznym programem badań przesiewowych. Autorzy raportu nie przemilczają jednak istotnych wad takiej metody przesiewania. Mammografia jako nieprecyzyjna metoda diagnostyczna daje spory odsetek wyników fałszywie dodatnich, a także pewien odsetek wyników fałszywie ujemnych. U mniej więcej jednej czwartej pań w wieku 50+ objętych regularnym (co dwa lata) przesiewaniem z użyciem mammografii rozpoznaje się niepokojącą zmianę kwalifikującą się do bardziej precyzyjnej, ale jednocześnie inwazyjnej diagnostyki (np. biopsja), przy czym u mniej więcej trzech czwartych z nich zmiana okazuje się finalnie niezłośliwa, co stawia pod znakiem zapytania sensowność narażania tak wielu pań na cierpienia fizyczne i wtórne ryzyka związane z inwazyjną diagnostyką oraz cierpienia psychiczne związane z lękiem przed chorobą i śmiercią, stresem i niepewnością w okresie oczekiwania na końcową diagnozę. U części z 6,5% ogółu pań objętych programami profilaktyki z użyciem mammografii – pań, u których diagnoza końcowa brzmi „rak piersi", w mammografii wykrywa się niewielkie zmiany, które – choć finalnie okazują się złośliwe – rozwijają się na tyle powoli, że nie stanowią realnego zagrożenia dla dalszego trwania życia. Te pacjentki poddawane są jednak rutynowo – w wielu przypadkach zupełnie niepotrzebnie – uciążliwym procedurom leczenia chirurgicznego, chemio- lub radioterapii tylko dlatego, że współczesna medycyna często nie dysponuje możliwościami jednoznacznej oceny, które zmiany są niebezpieczne, a które nie. Zdarzają się też oczywiście sytuacje odwrotne, kiedy zmiana złośliwa jest niewidoczna w mammografii i fałszywie negatywny wynik daje na kolejne dwa lata złudne poczucie bezpieczeństwa, skłaniając do bagatelizowania symptomów rozwijającej się choroby. W kilkunastu przypadkach na tysiąc mammografia pomaga wykryć zmiany nieuleczalne, które oznaczają tylko długie cierpienie zamiast obiecywanego długiego życia. Stosunkowo niewielkie dawki promieniowania rentgenowskiego stosowane w mammografii mogą w rzadkich przypadkach indukować zmiany w komórkach inicjujące lub przyspieszające rozwój raka. Dwuletnie interwały przesiewania bywają również w nielicznych przypadkach wystarczające do rozwoju nowotworów złośliwych do stadiów trudno- albo nieuleczalnych. Wszystkie te okoliczności mogą nastrajać część opinii publicznej sceptycznie do takich kosztownych programów profilaktyki, zwłaszcza że podmioty w nich uczestniczące rzadko uczciwie informują swoje pacjentki o wszystkich wadach i ryzykach tej metody przesiewania. Por. https://www.usz.ch/krankheit/mammografie/.

nicznych i ich elementów, uwarunkowania ich funkcjonalności i bezpieczeństwa, niesprawdzone lub nieweryfikowalne założenia dotyczące funkcjonalności, wytrzymałości lub nieuszkadzalności systemów i ich elementów w sytuacjach skrajnych, a także rozmaite niekompatybilności w relacjach człowiek–maszyna (por. Banse 2013, s. 23).

Wbrew dominującemu w większości obszarów zarządzania bezpieczeństwem modelowi percepcji i oceny zagrożeń opartemu na ich elementaryzacji i linearyzacji w niektórych dziedzinach badań ryzyka – np. farmakologii, epidemiologii czy toksykologii – poświęca się sporo uwagi interakcjom i oddziaływaniom krzyżowym między wieloma niebezpiecznymi czynnikami oraz efektom kumulacyjnym, a badanie ryzyk kombinacyjnych już od dziesięcioleci jest metodologicznym standardem. Krytyczna analiza rozpowszechnionych w sektorze farmaceutycznym procedur bezpieczeństwa opartych w sposób modelowy na wierze w obliczalność ryzyka odsłania nieusuwalną wybiórczość, subiektywność, szacunkowość i arbitralność wielu czynności składających się na skomplikowany proces certyfikacji środków leczniczych pod kątem ich bezpieczeństwa. Podstawą oceny bezpieczeństwa leków są zwykle bilanse korzyści i ryzyka (*Risk-Benefit-Balancing*, RBB), będące odmianą analizy kosztowej wspomaganej rachunkiem prawdopodobieństwa, zastępującej pojęcie kosztów pojęciem ryzyka. Ponieważ bezpieczeństwo traktuje się jako pojęcie względne, oceny bezpieczeństwa bazujące na bilansach korzyści i ryzyka mają zwykle charakter porównawczy. Oznacza to, że warunkiem dopuszczenia nowego środka leczniczego jest pozytywna ocena bilansu spodziewanych korzyści i ryzyk związanych z zastosowaniem danego środka na tle bilansów sporządzonych dla alternatywnych środków leczniczych. Korzyści terapeutyczne mogą wynikać z większej skuteczności leku, wyeliminowania lub ograniczenia niepożądanych skutków ubocznych, szerszego pod względem rodzajów schorzeń lub objawów, grup pacjentów lub niepożądanych interakcji z innymi lekami spektrum zastosowań, łatwości podawania (np. smakowitości – istotnej zalety w przypadku leków dla dzieci lub produktów weterynaryjnych), krótszego okresu stosowania, elastyczniejszego dawkowania, niższych kosztów wytwarzania i większej cenowej dostępności dla określonych grup pacjentów i wielu innych. Ocena ryzyka w przypadku produktów leczniczych przeznaczonych dla ludzi jest względnie łatwa i możliwa za pomocą metod ilościowych, odnosi się bowiem w zasadzie jedynie do problemów nieskuteczności leku, niedopasowania dawek, niepożądanych krzyżowych interakcji z innymi lekami, uczuleń, niepożądanych skutków ubocznych lub wiarygodności danych i informacji, na których oparta jest analiza. Podstawą analizy oddziaływań środków leczniczych i ocen ich ryzyka są zwykle ekstrapolacje rezultatów symulacyjnych badań laboratoryjnych przeprowadzanych na modelach zwierzęcych lub modelach molekularnych, potwierdzone statystycznymi analizami danych historycznych opisujących niepożądane zdarzenia i częstość ich występowania, pochodzących z testów klinicznych oraz zgłoszeń od lekarzy-terapeutów

stosujących dany lek. W analizie ryzyka bierze się zwykle pod uwagę to, w jakim stopniu dany produkt można uznać za przyczynę niepożądanego zdarzenia, jak poważne i prawdopodobne mogą być jego konsekwencje, jak ryzyko zachowuje się w czasie (wzrasta, maleje, utrzymuje się na tym samym poziomie), czy ryzyko utrzymuje się po zaprzestaniu przyjmowania leku, jak można zapobiec lub zminimalizować ryzyko niepożądanych skutków ubocznych lub skutecznie reagować w przypadku ich wystąpienia, na ile informacje użyte do charakterystyki ryzyka są wiarygodne i spolegliwe, a także to, jakie ryzyka grożą w razie niepodjęcia leczenia lub w razie wyboru innego środka leczniczego. W sytuacji, kiedy na rynku istnieją porównywalne produkty o podobnym działaniu, ze względów etycznych testy kliniczne pod kątem skuteczności nowego produktu przeprowadza się zwykle na zasadzie porównania efektów leczenia różnymi środkami (w tym tzw. produktami referencyjnymi), aby uniknąć niepotrzebnego cierpienia pacjentów zakwalifikowanych do grupy kontrolnej nieobjętej leczeniem. Takie postępowanie – zrozumiałe z etycznego punktu widzenia – dostarcza jednak tylko względnych bilansów korzyści i ryzyka. Istnieje wiele pojęć, ujęć i sposobów szacowania ryzyka (statystyczne, postrzegane, prognozowane, rzeczywiste) i niezależne posłużenie się dwoma różnymi sposobami szacowania prowadzi często do wzajemnie przeciwstawnych bilansów korzyści i ryzyka dla numerycznie tych samych obiektów. Zwłaszcza w sytuacjach ambiwalentnych, grożących konfliktami poznawczymi, konfliktami interesów lub wartości, analizy korzyści i ryzyka pomimo niewątpliwej elegancji, jaką zawdzięczają matematycznemu aparatowi, są często źródłem poważnych rozczarowań, ponieważ bilanse sporządzone niezależnie od siebie na podstawie innego sposobu percepcji ryzyka dostarczają w takich sytuacjach sprzecznych rezultatów. Istnieją co prawda sposoby rozwiązania tego problemu poprzez wbudowanie w proces analizy porównania różnych rodzajów ryzyka i uśredniania jego wartości, ale znacząco komplikuje to i wydłuża proces analizy w czasie, więc nie w każdych okolicznościach można sobie pozwolić na takie poszerzenie bazy analitycznej. Wbrew oczekiwaniom oraz deklaracjom w wielu obszarach zastosowań analizy ryzyka nie mają i nie mogą mieć charakteru czysto ilościowego, a próby narzucania takiego reżimu prowadzą do niebezpiecznych zniekształceń i obietnic bezpieczeństwa, których fałszywość rzeczywistość demaskuje czasami w brutalny sposób.

Problem porównywalności i obliczalności ryzyka ma jeszcze bardziej złożoną strukturę w przypadku weterynaryjnych produktów leczniczych ze względu na inny profil rozpatrywanych zagrożeń, na który – w zależności od charakterystyki produktu – oprócz zdrowia i bezpieczeństwa zwierząt docelowych składają się zdrowie i bezpieczeństwo konsumenta produktów pochodzenia zwierzęcego, bezpieczeństwo hodowcy, bezpieczeństwo środowiska, ryzyka epidemiologiczne, wzrost oporności drobnoustrojów chorobotwórczych na środki lecznicze itp. Uwzględniając tak szerokie spektrum zagrożeń, nie można w sposób równie prosty, jak w przypadku produktów leczniczych przeznaczonych dla ludzi, bilansować korzy-

ści i ryzyka oraz ustalać równowag między nimi. Ponieważ ocena bezpieczeństwa bazująca na bilansie korzyści i ryzyka jest miarą względną, porównywalną ocenę uzyskuje produkt o wysokiej skuteczności cechujący się wysokim ryzykiem niepożądanych skutków ubocznych oraz produkt o niskiej skuteczności, ale niemający stwierdzonych skutków ubocznych. Aby rozwiązać ten problem, na potrzeby oceny korzyści i ryzyka środków leczniczych agencje regulacyjne określają zwykle minimalne, możliwe do zaakceptowania wymagania dla skuteczności nowo dopuszczanych środków farmaceutycznych (zob. EMA 2009). Oprócz spełnienia materialnych wymagań formalną podstawą dopuszczenia produktów farmaceutycznych są przede wszystkim wysoka naukowa jakość i wiarygodność procesów badawczych, wymagany zestaw i poziom wiarygodności danych oraz staranny, zgodny z wymaganiami sposób sporządzenia dokumentacji. W sytuacjach, kiedy procesy badawcze nie spełniają wymagań autoryzacyjnych, analizę korzyści i ryzyka uzupełnia się bilansem ryzyka-ryzyka, polegającym na wzajemnym porównaniu ryzyk wynikających z niedopuszczenia danego produktu leczniczego z ryzykami jego dopuszczenia na podstawie zestawu danych niespełniających wymagań. Takie oceny mają jednak charakter intuicyjny, subiektywny i arbitralny, co naraża oparte na nich procedury na wpływy lobbingu. Z metodologicznego punktu widzenia bilanse korzyści i ryzyka cechują ułomności i ograniczenia strukturalne podobne do tych, które są powodem gruntownej krytyki kierowanej pod adresem analiz kosztów-korzyści w ogólności (zob. Kelman 1981). Ze względu na wymienione metodologiczne ułomności i ograniczenia szacowanie ryzyka, zarządzanie ryzykiem oraz formułowane na ich podstawie solenne obietnice bezpieczeństwa w warunkach złożonych systemów same bywają źródłem poważniejszych zagrożeń niż zagrożenia „źródłowe", które skłaniały do ich podjęcia.

Obiecującą metodą monitoringu, analizy i oceny zagrożeń z założenia otwartą na zagrożenia skumulowane, w pewnym stopniu również na zagrożenia kombinacyjne i systemowe, jest metoda wartości granicznych wywodząca się z toksykologii i znajdująca obecnie coraz szersze zastosowania w zarządzaniu bezpieczeństwem i higieną pracy, dietetyce czy inżynierii procesowej. W zależności od wariantu metoda wartości granicznych polega na określaniu maksymalnej tolerowanej wartości strat (1), maksymalnego tolerowanego prawdopodobieństwa wystąpienia określonych zdarzeń szkodowych (2), dopuszczalnego poziomu lub czasu narażenia (3), maksymalnych dawek szkodliwego czynnika (4) lub maksymalnych dawek zagregowanych (5). Najczęstszym punktem odniesienia i głównym wskaźnikiem w analizie oddziaływań jest wpływ na ludzki organizm, a naukowej podstawy do wyznaczania wartości granicznych dostarczają zwykle badania biomedyczne. Potencjalne szkodliwe oddziaływania na ludzkie zdrowie identyfikuje się za pomocą teoretycznych modeli rozprzestrzeniania się niebezpiecznego czynnika, szacowania średniej wartości spodziewanych strat lub metod indeksowania szkód na podstawie skumulowanej ekspozycji i w oparciu o nie określa się dopuszczalną sumę obcią-

żeń szkodliwymi czynnikami. Ostateczny rezultat agregacji oddziaływań różnorodnych czynników szkodliwych zależy jednak od mniej lub bardziej intuicyjnej i subiektywnej oceny znaczenia poszczególnych czynników i wynikającego z niej sposobu ich wagowania. W zarządzaniu bezpieczeństwem systemów technicznych graniczne wartości dopuszczalnego narażenia określa się na podstawie tzw. ryzyk referencyjnych, skalkulowanych dla zagrożeń naturalnych (np. ryzyka dla zdrowia wynikające z promieniowania pochodzenia naturalnego) lub normalnych zagrożeń cywilizacyjnych. Uznawanie zagrożeń naturalnych za miarę akceptowalności zagrożeń uwarunkowanych technicznie nie jest jednak przekonujące, skoro jedną z pierwotnych funkcji systemów technicznych była ochrona człowieka przed zagrożeniami naturalnymi. Diagnozy bezpieczeństwa formułowane na podstawie wartości granicznych można byłoby więc uznać za nazbyt ostrożne, a przyjęte poziomy dopuszczalnego narażenia za niepotrzebnie zaniżone, gdyby nie fakt, że przy ich ustalaniu nie bierze się pod uwagę ani pełnego spektrum niepożądanych oddziaływań, ani szerszego, pozafizycznego i pozamaterialnego „kontekstu" wpływającego w sposób istotny na percepcję, ocenę i tolerancję dla ryzyka. Przez wzgląd na wymogi obliczalności w metodzie wartości granicznych nie uwzględnia się w szczególności złożonych oddziaływań wtórnych i tercjarnych[14], a często także skutków odłożonych w czasie. Ustalone graniczne wartości narażenia są „sztywne" i nie uwzględniają indywidualnej podatności, dobrowolności, sprawiedliwości i proporcjonalności narażenia czy użyteczności źródła ryzyka i ogólnospołecznych lub indywidualnych korzyści mogących uzasadniać tolerancję dla wyższego poziomu narażenia (por. Michalski 2020b, s. 55 i n.). Ponieważ ustalanie wartości granicznych ma z konieczności charakter arbitralny i wybiórczy, opiera się na wielu nieuzasadnionych założeniach i intuicyjnych szacunkach, które cechują przybliżoność, subiektywność i przedziałowość typowa dla ocen punktacyjnych, czynności takie

[14] W badaniach nad wpływem antybiotyków lub promieniowania elektromagnetycznego na organizm człowieka nie uwzględnia się na przykład skutków pośrednich związanych ze szkodliwymi oddziaływaniami rozpatrywanych czynników na inne organizmy (np. mikroorganizmy) – oddziaływaniami mogącymi prowadzić do destabilizacji procesów w przyrodzie mających istotne znaczenie dla ludzkiego zdrowia. Modelowym przykładem „krótkowzroczności" naukowych ocen bezpieczeństwa jest powszechne ignorowanie zgubnych następstw szeroko rozpowszechnionej w polskim systemie ochrony zdrowia prewencyjnej antybiotykoterapii prowadzonej rutynowo, „na chybił trafił", z użyciem środków o niepotrzebnie szerokim spektrum rażenia, które nie tylko upośledzają funkcjonowanie systemu immunologicznego, ale także przyczyniają się do wzrostu antybiotykooporności mikroorganizmów chorobotwórczych. Niewłaściwie użyte środki służące pierwotnie do ograniczania ryzyka same stają się wtórnie – na zasadzie tzw. efektu bumerangowego – źródłem jeszcze większego ryzyka. Podobnie niepożądane efekty rykoszetowe spowodowało upowszechnienie benzoesanu sodu jako środka konserwującego. Trwałość, będąca główną zaletą tego środka biobójczego i powodem dopuszczenia go w stosunkowo dużych dawkach jako środka nieszkodliwego dla organizmu ludzkiego, z którego wydalany jest w postaci niezmienionej, utrudnia unieszkodliwianie go w procesie oczyszczania ścieków komunalnych. W efekcie czynnik ten w stosunkowo dużych stężeniach dostaje się do wód płynących, gdzie zaburza równowagę mikroorganizmów, przyczyniając się do nadmiernego rozwoju odpornych mikroorganizmów niszczących ikrę i wylęg, co znacząco zubaża naturalny rybostan.

nie uprawniają do formułowania twierdzeń kategorycznych, a taki charakter mają przecież normy określone w obowiązujących regulacjach prawnych.

Wiele zastrzeżeń zgłaszanych pod adresem różnych metod i technik oceny ryzyka wynika z osobliwości samego pojęcia ryzyka. Obiektywna niekonieczność, losowość i poznawcza niedostępność przyszłych zdarzeń miesza się w nim z różnymi sytuacjami niewiedzy lub niepewności, które rzadko trafnie się od siebie odróżnia i rozgranicza. Popularne w fachowej literaturze rozróżnienie na ryzyka subiektywne i ryzyka obiektywne (zob. Kaplan i Garrick 1993) jest coraz częściej kwestionowane. W przypadku większości ujęć ryzyka rolę nośnika obiektywności odgrywa prawdopodobieństwo zdarzeń, choć bywa ono różnie rozumiane – albo jako częstość występowania w sensie przedmiotowym, albo jako przewidywalność w sensie podmiotowym. Często oba te wymiary znaczeniowe są ze sobą pomieszane. Obiektywność prawdopodobieństwa jest utożsamiana z sytuacją, w której dwa racjonalne podmioty dysponujące taką samą informacją potrzebną do oszacowania ryzyka muszą dojść do takich samych szacunków prawdopodobieństwa (por. Nida-Rümelin i Schulenburg 2013, s. 21). W praktyce łatwo jednak zakwestionować istnienie klas referencyjnych (zob. Hajek 2007; Kahneman 2011), które jest koniecznym warunkiem możliwości określenia względnej częstości występowania interesujących zdarzeń będącej podstawą obiektywności szacunków prawdopodobieństwa.

W odniesieniu do poważnych zdarzeń szkodowych w świecie realnym, do których na szczęście dochodzi zbyt rzadko, aby możliwa była bezpośrednia obserwacja obiektywnych prawdopodobieństw, nasuwają się wątpliwości co do sensu rozgraniczania między „miękkim", podmiotowym pojęciem ryzyka związanym z poznawczą niepewnością a „twardym" pojęciem ryzyka opartym na powtarzalności zdarzeń. Refleksja nad strukturalną złożonością sytuacji poznawczych uprawnia do rozróżniania czterech modelowych sytuacji:

- znani znajomi (*known knowns*, świadoma wiedza – typowa sytuacja deterministyczna, w której działający wie, co wie, a między jego decyzją a rezultatem zachodzi relacja wzajemnie jednojednoznaczna – rezultat jest przyporządkowany tylko do określonej decyzji z prawdopodobieństwem równym 1);
- znani nieznajomi (*known unknowns*, świadoma niewiedza – sytuacja probabilistyczna, w której działający wie, czego nie wie, a niewiedza wynika stąd, że niektóre parametry opisujące sytuację są zmiennymi losowymi o znanych rozkładach prawdopodobieństwa. W takich sytuacjach pomimo niewiedzy można działać racjonalnie, kierując się np. regułą maksymalizacji sumy wszystkich użyteczności danego wyniku pomnożonych przez wartość ich prawdopodobieństwa;

- nieznani znajomi (*unknown knowns*, nieświadoma wiedza – działający nie wie, co wie. Sytuacja, w której fakty znane i przewidywalne z różnych powodów nie są brane pod uwagę);
- nieznani nieznajomi (*unknown unknowns*, nieświadoma niewiedza – działający nie wie, czego nie wie. Typowa sytuacja strategiczna, w której nie są znane parametry determinujące sytuację ani wartości, jakie może przyjmować każdy parametr. Przykładem takiej sytuacji jest rzucanie kostką o nieznanej liczbie ścian, nieznanej wartości wyniku i nieznanej liczbie prób) (por. Eckhardt i Rippe 2016, s. 59 i n.).

Szerokie spektrum sytuacji wymagających szacowania ryzyka sięga więc od sytuacji skrajnej niepewności, w których wiedza o prawdopodobieństwach jest tak marginalna, że twierdzenia o prawdopodobieństwie graniczą z zupełną dowolnością, aż po sytuacje tzw. czystego ryzyka, w których twierdzenia o prawdopodobieństwie są tak dobrze ugruntowane, że można je utożsamiać z istnieniem obiektywnych prawdopodobieństw. Każda z wymienionych sytuacji poznawczych wymaga odmiennych strategii zarządzania ryzykiem. Na przykład szeroko rozpowszechnione metody scenariuszowe są przydatnym narzędziem do rozwiązywania problemów niepewności w sytuacjach probabilistycznych („znani nieznajomi"), ale mają ograniczoną użyteczność w sytuacjach strategicznych („nieznani nieznajomi"), w których nie ma pewności, co się wie, a czego się nie wie. Ponieważ w przypadku większości zagrożeń towarzyszących innowacyjnym przedsięwzięciom technicznym nie jest dostępna ponadpodmiotowa perspektywa poznawcza umożliwiająca obiektywną obserwację ryzyka bazującą na danych historycznych uprawniających do wnioskowań o możliwości wystąpienia niepożądanych oddziaływań, nie można czyichś obaw traktować z góry jako imaginacji, aberracji lub bezpodstawnych uprzedzeń. Opinie ekspertów od bezpieczeństwa oparte na wycinkowych wglądach, zaokrągleniach, nieuprawnionych ekstrapolacjach i uogólnieniach należy traktować również jako jedną z wielu koncepcji ryzyka – nie bardziej wolną od arbitralnych założeń niż niektóre obawy laików.

Możliwość przeprowadzania komprehenzywnych, kompletnych, sytuacyjnie adekwatnych analiz bezpieczeństwa dodatkowo ograniczają trudności z pozyskiwaniem danych potrzebnych do analizy ryzyka i oceny bezpieczeństwa wynikające albo z ich poufności lub umyślnego utrzymywania w tajemnicy, albo z ograniczeń czasowych, finansowych lub etycznych utrudniających lub uniemożliwiających przeprowadzanie próbnych testów i eksperymentów weryfikujących na rzeczywistych obiektach w normalnych warunkach eksploatacyjnych. Z omówionych powyżej i wielu innych względów, którym z powodu ograniczeń objętościowych nie można poświęcić tutaj więcej miejsca, należy odnosić się zatem z dużą rezerwą do naukowych obietnic bezpieczeństwa, opartych na uprzywilejowanej pozycji ekspertów, mechanistycznych wyobrażeniach o rzeczywistości, liniowo-deterministycznym rozumieniu przyczynowości, przesadnych wymaganiach ścisło-

ści stawianych naukowym dowodom, metodycznym sceptycyzmie nakazującym domniemanie niewinności w razie braku zniewalających empirycznych potwierdzeń szkodliwości, a także wierze w moc obliczalności i kontrolowalność ryzyka.

Rosnąca społeczna świadomość tej sytuacji skłania coraz więcej osób do wątpienia w rzetelność i bezstronność naukowych ekspertów oraz jest powodem coraz powszechniejszego kwestionowania naukowych poświadczeń bezpieczeństwa, czego wyrazistym przykładem są dotychczasowe doświadczenia z *safety case*. To rodzaj raportu zawierającego informacje i opinie o bezpieczeństwie podziemnych składowisk odpadów radioaktywnych, będący w zachodnioeuropejskich systemach administracji publicznej obligatoryjnym dokumentem w procedurach wydawania zezwoleń oraz innych procesach decyzyjnych, np. związanych z wyborem lokalizacji (zob. NEA 2013, 2014). Takie raporty prezentują szerokie spektrum zagadnień i aspektów bezpieczeństwa transportu, rozładunku i podziemnego składowania odpadów radioaktywnych, w większości zużytego paliwa z elektrowni jądrowych, z uwzględnieniem lokalnych uwarunkowań (geologicznych, infrastrukturalnych, technicznych, społecznych itd.). Oceny bezpieczeństwa formułowane są na podstawie szczegółowonaukowych, dyscyplinowych ekspertyz, pomiarów oddziaływań, analiz zagrożeń i szacunków ryzyka, które w większości nie ograniczają się jedynie do długoterminowego bezpieczeństwa odpadów radioaktywnych po napełnieniu i zamknięciu składowiska, lecz uwzględniają niebezpieczne oddziaływania z perspektywy całego cyklu życia składowiska „od kołyski aż po grób" – od zagadnień technicznej wykonalności i bezpieczeństwa osób zatrudnionych przy budowie i napełnianiu składowiska, poprzez kwestie bezpieczeństwa ludności cywilnej i zabezpieczenia składowiska przed dostępem osób nieuprawnionych w trakcie napełniania i po jego zamknięciu. Koncepcja *safety case* opiera się na międzydziedzinowej i międzydyscyplinowej komunikacji i kooperacji między szczegółowymi naukami przyrodniczymi i technicznymi oraz kompletnym i transparentnym dokumentowaniu procesu poznawczego obejmującym zarówno przyjęte założenia, ocenę wiarygodności uzyskanych rezultatów, jak i pytania, na które nie udało się uzyskać odpowiedzi. W koncepcję tę ze względów pragmatycznych nie zostały jednak wbudowane mechanizmy obywatelskiej partycypacji ani procedury refleksyjne otwierające pola do konstruktywnej naukowej krytyki, które mogłyby grozić strategiczną obstrukcją i przewlekłością procesów społecznej oceny bezpieczeństwa. W całej Europie sporządzono dotąd kilka takich raportów, m.in. w Szwajcarii (zob. NAGRA 2002), we Francji (zob. ANDRA 2005), w Szwecji (zob. SKB 2011) oraz w Niemczech (zob. GRS 2013), jednak zarówno sama koncepcja *safety case*, jak i konkretne rezultaty nie cieszą się ani większym zainteresowaniem, ani szerszą akceptacją ze strony interesariuszy oraz opinii publicznej. O fiasku dotychczasowych postępowań administracyjnych opartych na *safety case* przesądziły zbyt duże rozbieżności między wizjami bezpieczeństwa oraz preferencjami i oczekiwaniami operatorów składo-

wisk, organów administracji publicznej wydających pozwolenia i nadzorujących procesy budowy i eksploatacji składowisk oraz społecznych interesariuszy dotyczącymi właściwego poziomu bezpieczeństwa, nadmierne naukowe skomplikowanie raportów sprawiające, że wielu interesariuszy uznało się za niekompetentnych i niezdolnych do tego, żeby wyrobić sobie i wyartykułować własną opinię o bezpieczeństwie projektowanego składowiska, a także pomijanie w eksperckich badaniach nad bezpieczeństwem prowadzonych często „zza biurka" wielu zagadnień i aspektów istotnych dla lokalnych interesariuszy, a wynikających z wiedzy „miejscowej" i osobistych doświadczeń. Brak wiary lokalnych społeczności w prawdziwość i szczerość obietnic bezpieczeństwa zawartych w *safety case* wynikał również z faktu, że wobec większości dotychczasowych raportów krytyczne środowiska naukowe wyrażały poważne zastrzeżenia dotyczące zarówno wzornictwa procesów badawczych i użytych metod, jak i sposobu doboru wykonawców. Społeczne uprzedzenia do *safety case* wynikały także ze świadomości, w jak dużym stopniu badania bezpieczeństwa ze względu na swoją przedmiotową oraz czynnościową złożoność otwierają pola do nadużyć, możliwości manipulowania rezultatami i strategicznego wpływania na oparte na nich procesy decyzyjne. Czynnikiem wpływającym na niewielkie społeczne zainteresowanie eksperckimi opiniami o bezpieczeństwie i społeczne uznanie dla rezultatów naukowych badań udokumentowanych w *safety case* jest również brak zaufania do bezstronności i niezależności wykonawców ekspertyz i autorów raportów, wynikający zarówno z postępującej komercjalizacji, upolitycznienia i koniunkturalizacji nauki, jak i pogłębiającego się kryzysu etosu naukowego. Wielu uczonych uczestniczących w pracach nad raportami traktuje krytyczny stosunek społeczeństwa do *safety case* jako odmowę konfrontacji z aktualnymi zasobami wiedzy naukowej wynikającą wyłącznie z bezpodstawnych uprzedzeń (por. Röhling i Eckhardt 2017, s. 104). Konsekwencją takiego podejścia jest uznanie laboratoryjnych testów i eksperckich ocen bezpieczeństwa przeprowadzanych za zamkniętymi drzwiami – bez udziału osób potencjalnie narażonych – oraz podawanie wyników do wiadomości opinii publicznej za właściwy sposób postępowania odpowiadający aktualnym wymaganiom bezpieczeństwa. Takie aroganckie podejście do obaw osób zaniepokojonych sąsiedztwem niebezpiecznych instalacji przemysłowych lub narażonych na nieznane oddziaływania obiektów lub produktów z pewnością nie sprzyja jednak eliminowaniu ewentualnych uprzedzeń. Taki sposób przeprowadzania ocen bezpieczeństwa może częściowo wynikać z przekonania, że uczestnictwo interesariuszy – osób potencjalnie narażonych – w procedurach kontroli bezpieczeństwa i tak istotnie nie zwiększy społecznego zaufania i akceptacji ich rezultatów, ponieważ niektóre z założeń arbitralnie przyjmowanych w tego typu postępowaniach i rozstrzygnięć o charakterze aksjonormatywnym (np. kryteria istotności, progi ryzyka, warunki dopuszczalności narażenia itp.), które – zdeterminowane indywidualną sytuacją „pozycyjną"

i osobistymi preferencjami (np. skłonnością albo awersją do ryzyka) – zawsze prowadzą do rozbieżności opinii, byłyby dla części interesariuszy z pewnością nie do zaakceptowania. Koncepcja *safety case* mogłaby odgrywać ważną rolę w ogólnospołecznym dialogu towarzyszącym realizacji ryzykownych, społecznie kontrowersyjnych przedsięwzięć technicznych, gdyby do udziału w przygotowaniu tego typu raportów dopuszczono wszystkich interesariuszy i zadbano o większą otwartość procesów oceny bezpieczeństwa na krytykę.

Wobec niezdolności normalnej nauki do pełnego poznawczego uchwycenia złożoności oddziaływań czynników technicznych i jednoznacznego wykazania szkodliwości niektórych z nich szybko spada zaufanie społeczeństwa do naukowych potwierdzeń bezpieczeństwa. W efekcie dochodzi do zaniku kolektywnej orientacji, wzrasta podatność społeczeństwa na dezinformację, propagandę i manipulację, a przedsięwzięcia techniczne wywołują coraz więcej kontrowersji i stają się źródłem ostrych konfliktów społecznych (zob. Michalski i Jurgilewicz 2021). Do wytwarzania chaosu wokół bezpieczeństwa produktów lub instalacji przemysłowych przyczyniają się same przedsiębiorstwa, odkąd systematyczne produkowanie wątpliwości wokół szkodliwości czynników technicznych stało się skutecznym, tanim i łatwym do zamaskowania środkiem bojowym stosowanym przez niebezpieczny przemysł do ochrony własnych komercyjnych interesów. W ten sposób krytycyzm i metodyczne wątpienie z jednej z najważniejszych zalet naukowego poznania zostało przekształcone w jedną z największych wad, która sprzyja rozprzestrzenianiu się relatywizmu i skłania coraz większą część społeczeństwa do utraty wiary w możliwość naukowego ustalenia prawdy. W ten sposób współczesne nauki eksperymentalne wpisują się również w generalny trend wiodący ludzkość ku erze postprawdy, którą cechuje stopniowe zacieranie granic między prawdą a fałszem oraz informacjami autentycznymi a zmanipulowanymi. Wobec coraz większej nierozróżnialności prawdy i fałszu coraz łatwiej przemycać kłamstwa i manipulować opinią publiczną. Kłamstwo, manipulacja i dezinformacja powszednieją i coraz więcej ludzi przestaje odczuwać potrzebę poznania prawdy (Keyes 2017, s. 6 i n.).

Mimo powierzchownego i wycinkowego potraktowania wielu wątków – nieuniknionego w obliczu ograniczeń objętościowych niniejszego artykułu – trudno nie zgodzić się z tezą, że wobec niezdolności normalnej nauki do poznawczego zapanowania nad złożonością współczesnych zagrożeń ze strony systemów technicznych oraz wobec społecznej nieufności do naukowych poświadczeń bezpieczeństwa, których nieadekwatność demaskują spektakularne katastrofy, codzienne prawie-katastrofy oraz świadectwa poszkodowanych, które zaufały naukowym zapewnieniom o nieszkodliwości jakiegoś produktu lub sąsiedztwa jakiejś instalacji, należy uznać, że strategie poznawcze, na których opierał się dotąd społeczny monitoring zagrożeń ze strony czynników technicznych, wymagają pilnej, gruntownej rewizji i modyfikacji.

Konkluzja: potrzebna zmiana strategii poznawczych w zarządzaniu bezpieczeństwem systemów technicznych

W obliczu rosnącego znaczenia zagrożeń strukturalnych, które ze względu na swoją złożoność oraz sytuację panującą obecnie w nauce wymykają się naukowej „obróbce" za pomocą standardowych metod i narzędzi nauk laboratoryjnych, zachodzi potrzeba gruntownej rewizji i rekonfiguracji dotychczasowych sposobów naukowego monitorowania zagrożeń oraz zmiany stosowanych dotąd strategii poznawczych. Aby w naukowym polu widzenia zagrożeń ograniczyć „martwe strefy", będące obecnie przyczyną brzemiennych w skutkach pominięć, niedoszacowań oraz niewystarczających marginesów bezpieczeństwa projektowanych dla systemów technicznych, należy zastąpić lub uzupełnić mechanistyczne, szczegółowonaukowe procedury identyfikacji zagrożeń i oceny ryzyka oparte na elementaryzacji, uznawanej za właściwą drogę do rozumienia złożoności, oraz zawężające horyzont uwagi do oddziaływań mierzalnych, dających się symulować bezpośrednio lub za pomocą modelowania w warunkach laboratoryjnych eksperymentów, alternatywnymi postnormalnymi strategiami poznawczymi ukierunkowanymi na całościowe, (eko-)systemowe, społecznie uzgodnione ujęcie środowiska bezpieczeństwa uwzględniające pełnię jego strukturalnej i funkcjonalnej złożoności oraz mnogość perspektyw i stylów poznawczych. Procesy naukowego monitorowania zagrożeń ze strony systemów technicznych należy otworzyć nie tylko na interdyscyplinarną współpracę, która umożliwiłaby bardziej adekwatną obróbkę złożoności współczesnego środowiska bezpieczeństwa dzięki wykorzystaniu synergii do optymalnego spożytkowania zasobów, jakimi dysponuje współczesna nauka, na filozoficzną krytykę i refleksję nad możliwościami i ograniczeniami naukowego poznania, ale przede wszystkim także na uczestnictwo interesariuszy. Skuteczne stawianie czoła niepożądanym synergiom mogącym przekształcić każdy złożony system techniczny w niszczycielski żywioł wymaga od nauki zdolności do lepszego wykorzystania synergii między własnymi „aktywami". Ponieważ kwestie bezpieczeństwa systemów technicznych są modelową domeną nauki postnormalnej, której sytuacje badawcze cechuje niepewność faktów, sporność wartości, wysoka stawka i potrzeba szybkich rozwiązań (zob. Funtowicz i Ravetz 1993a, 1993b), społecznie wiarygodna ocena bezpieczeństwa takich systemów wymaga konfrontowania przeciwstawnych perspektyw poznawczych: naukowych ekspertów – niezaangażowanych obserwatorów z perspektywami uczestników – interesariuszy bezpieczeństwa (zob. Böschen i Pfersdorf 2014), którym nie tylko należy się rzetelna informacja o granicach naukowej pewności, ale do których – jako potencjalnie narażonych – powinno w ogóle należeć ostatnie słowo w kwestiach akceptowalności wynikających stąd ryzyk. Taka konfrontacja kategorialnie odmiennych sposobów per-

cepcji powinna się dokonywać w otwartym dialogu prowadzonym na społecznie uczciwych warunkach (uczciwa reprezentacja, równość stron, wzajemny szacunek, brak uprzedzeń, otwartość rezultatu itp.). Udział osób potencjalnie narażonych w procesach badania i oceny bezpieczeństwa przedsięwzięć technicznych, instalacji, procesów lub produktów może przyczynić się do wzbogacenia tych procesów o perspektywę uczestników (m.in. niedostępna na innej drodze wiedza „lokalna", pochodząca z doświadczenia życiowego, postawy motywowane odpowiedzialnością za losy swoje i bliskich, a nie tylko ciekawością), wzmocnienia społecznej wiarygodności takich procesów oraz wzmocnienia ochrony społeczeństwa przed nieuzasadnionymi lękami, dezinformacją i manipulacją (por. Röhling i Eckhardt 2017, s. 105). Osoby potencjalnie narażone, obawiające się o swoje bezpieczeństwo, czuły się dotąd ignorowane lub lekceważone przez ekspertów, którzy z pozycji uprzywilejowanej traktowali obawy laików jako bezpodstawne lub przesadzone. Intuicja interesariuszy miewa jednak pozytywny wpływ na ustanawianie priorytetów i zdarza się nawet, że pod jej wpływem eksperci rewidują swoje pierwotne zapatrywania. Dotychczasowe doświadczenia z inkluzyjnymi procesami oceny bezpieczeństwa wskazują na to, że otwartość na wielość spojrzeń na zagrożenia i ryzyka korzystnie wpływa na jakość analiz ryzyka i racjonalność ocen bezpieczeństwa. Dlatego w procesach poznawczych należy unikać faworyzowania punktu widzenia ekspertów i pochopnego deprecjonowania obaw, zastrzeżeń i uprzedzeń interesariuszy (zob. Marti 2016). Ze względu na wymagania społecznej odpowiedzialności, które zabraniają faworyzowania doraźnych, krótkoterminowych korzyści kosztem narażenia ludności na długookresowe szkodliwe oddziaływania, należy zadbać o to, aby na ocenę zagrożeń i akceptację ryzyka nie wywierały wpływu krótkotrwałe mody, a osiągnięte w procesach oceny bezpieczeństwa kompromisy i konsensusy były trwałe, zapewniały długoterminową, długookresową kolektywną orientację oraz przewidywalność planowania, bez której aktywna, refleksyjna, sprawiedliwa i odpowiedzialna polityka bezpieczeństwa traktująca je jako wspólne dobro nie da się w obecnych warunkach urzeczywistnić. Racjonalne i społecznie odpowiedzialne obcowanie z zagrożeniami i ryzykami systemowymi, kombinacyjnymi i skumulowanymi wymaga – oprócz technicznych ingerencji w struktury systemowe służących monitorowaniu zagrożeń, wzmacnianiu niezawodności i odporności na zaburzenia, budowaniu buforów bezpieczeństwa i zapór chroniących przed rozprzestrzenianiem się zaburzeń – również przyjęcia strategii poznawczych umożliwiających rozumienie złożoności bez konieczności rozbierania jej na części i redukowania do bardziej elementarnego poziomu, co pozwoliłoby na uniknięcie poznawczych zniekształceń typowych dla czynności elementaryzacyjnych, które są częstą przyczyną „martwych stref" w polu widzenia normalnej nauki. Trudno o lepszą niż teoria systemów wyjściową perspektywę poznawczą umożliwiającą bardziej adekwatną i zintegrowaną percepcję złożonych zagrożeń oraz

bardziej kompleksowe zarządzanie takimi zagrożeniami. Integralnym elementem nowego podejścia do bezpieczeństwa i ochrony ludności przed zagrożeniami ze strony czynników technicznych powinno być również budowanie świadomości nieusuwalności ryzyka, uczciwe komunikowanie ograniczeń poznania naukowego i wynikających stąd wątpliwości, zrozumienie dla obaw i uprzedzeń osób, które poniosą konsekwencje ewentualnych błędów w ocenach bezpieczeństwa, a także społeczne uzgadnianie decyzji o dopuszczalności narażenia, rekompensatach i zasadach postępowania w razie wystąpienia szkody w uczciwym dialogu z interesariuszami – w myśl zasady, że narażenie jest społecznie dopuszczalne pod warunkiem, że sami narażeni wyrażą na nie zgodę. Zmiana nawyków związanych z percepcją zagrożeń ze strony czynników technicznych i zarządzaniem bezpieczeństwem złożonych systemów technicznych stanowi duże wyzwanie, ale jest koniecznym warunkiem przystosowania się do współczesnego, coraz bardziej skomplikowanego środowiska bezpieczeństwa.

Bibliografia

ANDRA – Agence Nationale pour la gestion des Déchets Radioactifs, 2005, *Dossier 2005*, www.andra.fr/international/pages/en/dossier-2005-1636.html (dostęp: 30.01.2020).

Banse G., 2013, „Sicherheit", w: A. Grunwald (red.), *Handbuch Technikethik*, Stuttgart–Weimar: J. B. Metzler, 22–27.

Banse G., Bechmann G., 1998, *Interdisziplinäre Risikoforschung. Eine Bibliographi*e, Opladen/Wiesbaden: Westdeutscher Verlag.

Beck U., 2002, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Warszawa: Scholar.

Bertalanffy L. von, 1950, „An Outline of General System Theory", *The British Journal for the Philosophy of Science* 1–2 (April): 134–165.

Bińczyk E., 2012, *Technonauka w społeczeństwie ryzyka. Filozofia wobec niepożądanych następstw praktycznego sukcesu nauki*, Toruń: Wydawnictwo Naukowe UMK.

Böschen S., Pfersdorf S., 2014, „Partizipation von zivilgesellschaftlichen Organisationen in Innovationsentwicklung und Risikobewältigung", *Forschungsjournal Soziale Bewegungen* 4: 50–59.

Büscher Ch., 2011, „Systemic Risk as a Perspective for Interdisciplinary Risk Research", *Technikfolgenabschätzung – Theorie und Praxis* 3(20): 4–12.

Butler C., 2001, *Tajniki Value at Risk: Praktyczny podręcznik zastosowań metody VaR*, Warszawa: Liber.

Cleeland B., 2011, „Contributing Factors to the Emergence of Systemic Risks", *Technikfolgenabschätzung – Theorie und Praxis* 3(20): 13–21.

Dowd K., 1998, *Beyond Value at Risk. The New Science of Risk Management*, Chichester: Wiley.

Eckhardt A., Rippe K.P., 2016, *Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle*, Zürich: ETH.

EMA – European Medicines Agency, 2009, *Recommendation on the Evaluation of the Benefit-Risk Balance of Veterinary Medicinal Products* (EMA/CVMP/248499/2007), London: EMA.

Funtowicz S. O., Ravetz J. R., 1993a, „Science for the Post-Normal Age", *Futures* 25: 739–755.

Funtowicz S. O., Ravetz J. R., 1993b, „The Emergence of Post-Normal Science", w: R. von Schomberg (red.), *Science, Politics and Morality. Scientific Uncertainty and Decision Making*, Dordrecht: Kluwer Academic Publisher, 85–124.

GRS – Gesellschaft für Anlagen- und Reaktorsicherheit mbH, 2013, *Vorläufige Sicherheitsanalyse für den Standort Gorleben. Synthesebericht für die VSG*, Bericht zum Arbeitspaket 13. GRS 290, Braunschweig.

Habermas J., 1977, *Technika i nauka jako ideologia*, tłum. M. Łukasiewicz, w: J. Szacki (red.), *Czy kryzys socjologii?*, Warszawa: Czytelnik, 342–395.

Hájek A., 2007, „The Reference Class Problem is Your Problem Too", *Synthese* 156: 185–215.

Haken H., 1982, *Synergetik*, Berlin–Heidelberg–New York: Springer.

Helbing D., 2009, *Systemic Risks in Society and Economics*, Geneva: IRGC, http://irgc.org/IMG/pdf/Systemic_Risks_Helbing2.pdf (dostęp: 23.01.2019).

Hellström T., 2007, „Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework", *Safety Science* 45(3): 415–430.

Hofmann M., 2008, *Lernen aus Katastrophen. Nach den Unfällen von Harrisburg, Seveso und Sandoz*, Berlin: Edition Sigma.

Jajuga K., 2000, „Miary ryzyka rynkowego. Część trzecia", *Rynek Terminowy* 8: 112–117.

Jänicke M., 1979, *Wie das Industriesystem von seinen Mißständen profitiert*, Opladen: Westdeutscher Verlag.

Jurgilewicz M., Michalski K., 2020, *Teoretyczno-metodologiczne podstawy nauki o bezpieczeństwie*, w: M. Jurgilewicz, K. Michalski, W. Krztoń (red.), *Badania nad bezpieczeństwem. Wybrane aspekty*, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej, 13–48.

Kahneman D., 2011, *Thinking, Fast and Slow*, New York: Penguin.

Kaplan S., Garrick J. B., 1993, „Die quantitative Bestimmung von Risiko", w: G. Banse (red.), *Risiko und Gesellschaft*, Opladen: Westdeutscher Verlag, 91–124.

Kaufman G. G., Scott K. E., 2003, „What is Systemic Risk and do Bank Regulators Retard or Contribute to it?", *Independent Review* 7(3): 371–391.

Kelman S., 1981, „Cost-Benefit Analysis: An Ethical Critique", *AEI Journal on Government and Society Regulation*, January/February: 33–40.

Keyes R., 2017, *Czas postprawdy. Nieszczerość i oszustwa w życiu codziennym*, Warszawa: Wydawnictwo Naukowe PWN.

Khazai B., Daniell J. E., Wenzel F., 2011, „The March 2011 Japan Earthquake. Analysis of Losses, Impacts, and Implications for the Understanding of Risks Posed by Extreme Events", *Technikfolgenanschätzung – Theorie und Praxis* 3(20): 22–33.

Kolmogorow A. N., 1933, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin: Julius Springer.

Kuhn T. S., 1968, *Struktura rewolucji naukowych*, Warszawa: PWN.

Marti M., 2016, *Risikoansichten*, ENTRIA-Arbeitsbericht-05, Zollikerberg.

Michalski K., 2011, „Dylemat ekspertowy w ocenie technologii. Zarys problemu", *Zeszyty Naukowe Politechniki Rzeszowskiej. Ekonomia i Nauki Humanistyczne* 18: 123–134.

Michalski K., 2017a, „Autonomizacja techniki i niepożądane skutki eliminowania człowieka jako źródła błędów", *Filo-Sofija. Z problemów współczesnej filozofii* 39(4) (t. 6: Człowiek i maszyna): 79–95.

Michalski K., 2017b, „Programy etyczne w zarządzaniu organizacjami zainteresowania publicznego", *Humanities and Social Sciences* XXII, 24(2): 181–196.

Michalski K., 2019, *Technology Assessment. Ocena technologii – nowe wyzwania dla filozofii nauki i ogólnej metodologii nauk*, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej.

Michalski K., 2020a, „Ochrona infrastruktur elektroenergetycznych przed zagrożeniami i ryzykami systemowymi – nowy paradygmat w zarządzaniu bezpieczeństwem energetycznym", *Rocznik Bezpieczeństwa Międzynarodowego* 1: 207–228.

Michalski K., 2020b, *Metodyka analizy ryzyka i oceny bezpieczeństwa*, w: M. Jurgilewicz, K. Michalski, W. Krztoń (red.), *Badania nad bezpieczeństwem. Wybrane zagadnienia*, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej, 49–84.

Michalski K., 2020c, *Ochrona przed zagrożeniami systemowymi jako nowy obszar badań i zadań dla polityki bezpieczeństwa*, w: M. Delong, J. Puacz-Olszewska (red.), *Współczesna polityka bezpieczeństwa w Europie Środkowo-Wschodniej. Uwarunkowania – wyzwania – zagrożenia*, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej, 9–54.

Michalski K., Jurgilewicz M., 2021, *Konflikty technologiczne – nowa architektura zagrożeń w epoce wielkich wyzwań*, Warszawa: Difin.

NAGRA – Nationale Genossenschaft für die Lagerung radioaktiver Abfälle, 2002, *Project Opalinus Clay – Safety Report: Demonstration of Disposal Feasibility for Spent Fuel, vitrified High-Level Waste and long-lived Intermediate-Level Waste*, NAGRA Technical Report NTB 02-05, Wettingen.

NEA – Nuclear Energy Agency, 2013, *The Nature and Purpose of the Post-Closure Safety Cases for Geological Repositories*, NEA/RWM/R (2013)1, Paris: OECD.

NEA – Nuclear Energy Agency, 2014, „The Safety Case for Deep Geological Disposal of Radioactive Waste: 2013 State of the Art", *Symposium Proceedings*, NEA/RWM/R (2013)9, Paris: OECD.

Nida-Rümelin J., Schulenburg J., 2013, „Risiko", w: A. Grunwald (red.), *Handbuch Technikethik*, Stuttgart–Weimar: J. B. Metzler, 18–22.

Orwat C., 2011, „Systemic Risks in the Electric Power Infrastructure?", *Technikfolgenabschätzung – Theorie und Praxis* 3(20): 47–55.

Perrow Ch., 1984, *Normal Accidents. Living with High-Risk Technologies*, New York: Basic Books.

Perrow Ch., 1994, „The Limits of Safety: The Enhancement of a Theory of Accidents", *Journal of Contingencies and Crisis Management* 2(4): 212–220.

Perrow Ch., 2007, *The Next Catastrophe*, Princeton: Princeton University Press.

Renn O., Keil F., 2008, „Systemische Risiken: Versuch einer Charakterisierung", *GAIA* 17(4): 349–354.

Röhlig K. J., Eckhardt A., 2017, „Primat der Sicherheit. Ja, aber welche Sicherheit ist gemeint?", *GAIA* 26(2): 105–107.

Röhlig K. J., Hocke P., 2016, „Safety Case, Interdisziplinarität und Transdisziplinarität", w: U. Smeddinck, S. Kuppler, S. Chaudry (red.), *Inter- und Transdisziplinarität bei der Entsorgung radioaktiver Reststoffe. Grundlagen – Beispiele – Wissenssynthese*, Wiesbaden: Springer Fachmedien, 77–87.

Rothkegel A., Banse G., Renn O., 2010, „Interdisziplinäre Risiko- und Sicherheitsforschung", w: P. Winzer, E. Schnieder, F.-W. Bach (red.), *Sicherheitsforschung – Chancen und Perspektiven*, Berlin–Heidelberg: Springer, 147–162.

Sawczyk A., 1999, „Wprowadzenie do metodologii pomiaru ryzyka. Value at Risk", *Rynek Terminowy* 6: 132–137.

Schäfer M. S., 2009, „From Public Understanding to Public Engagement. An Empirical Assessment of Changes in Science Coverage", *Science Communication* 30(4): 475–505.

Scheer J., 1987, „Grenzen der Wissenschaftlichkeit bei der Grenzwertfestlegung. Kritik der Low-Dose-Forschung", w: L. Burkart (red.), *Technik und sozialer Wandel*, Frankfurt am Main: Campus Verlag, 447–454.

Scheffer M., 2009, *Critical Transitions in Nature and Society*, Princeton NJ: Princeton University Press.

Scheffer M., Bascompte J., Brock W. A., Brovkin V., Carpenter S. R., Dakos V., Held H., van Nes E. H., Rietkerk M., Sugihara G., 2009, „Early-warning Signals for Critical Transitions", *Nature* 461(7260): 53–59.

SKB – Svensk Kärnbränslehantering AB, 2011, *Long-term Safety for the Final Repository for Spent Nuclear Fuel at Forsmark. Main Report of the SR-Site Project*, Technical Report TR-11-01, Stockholm: SKB.

Vogel S. A., 2009, „The Politics of Plastics: The Making and Unmaking of Disphenol A Safety", *American Journal of Public Health* 99(Suppl. 3): 559–566.

Wang X., Chen G., 2012, „A Chaotic System with Only One Stable Equilibrium", *Communications in Nonlinear Science and Numerical Simulation* 17: 1264–1272.