DOI: https://doi.org/10.34862/rbm.2020.1.12

Krzysztof Michalski
Politechnika Rzeszowska im. I. Łukasiewicza
michals@prz.edu.pl
https://orcid.org/0000-0002-2089-2160

Ochrona infrastruktur elektroenergetycznych przed zagrożeniami i ryzykami systemowymi[1] – nowy paradygmat w zarządzaniu bezpieczeństwem energetycznym

Streszczenie: Artykuł zawiera wyniki wstępnej eksploracji nowego pola problemowego na obszarze bezpieczeństwa energetycznego, obejmującego szerokie spektrum złożonych zagrożeń i ryzyk systemowych, przed jakimi staje przemysł elektroenergetyczny przechodzący gwałtowne transformacje w kierunku systemów cyberfizycznych. Celem eksploracji jest identyfikacja i wstępna teoretyczna analiza (stworzenie siatki pojęć, strukturalizacja itp.) kompleksów problemów poznawczych, decyzyjnych i projekcyjno-organizacyjnych, jakie dla bezpieczeństwa i niezawodności zaopatrzenia w energię elektryczną wynikają z gwałtownego wzrostu wewnętrznej złożoności oraz skomplikowanych synergii i współzależności, będących następstwem konwergencji technologii „dwóch prędkości": systemów energetycznych i technologii teleinformatycznych. Skłonności takich złożonych, turbulentnych systemów do zachowań chaotycznych oraz ich zdolności do zachowań samoorganizacyjnych „bez udziału człowieka" grożą nagłymi, nieprzewidywalnymi, niebezpiecznymi zdarzeniami inicjującymi, mogącymi wywoływać niekontrolowane kaskady zaburzeń zdolne pokonać wszelkie bariery ochronne, zapory ogniowe i warstwy zabezpieczeń. Widmo katastrofalnych konsekwencji wielkoobszarowych awarii zasilania stawia pod znakiem zapytania dotychczasowe modele zarządzania bezpieczeństwem bazujące na elementaryzacji zagrożeń, analizie podatności, ocenie ryzyka i reagowaniu kryzysowym i skłania do poszukiwania nowego paradygmatu w zarządzaniu

[1] Część autorów opowiada się za rozróżnieniem między niebezpieczeństwem (zagrożeniem) jako prawdopodobnym zdarzeniem szkodowym, którego wystąpienie nie jest konsekwencją decyzji, a ryzykiem jako prawdopodobnym zdarzeniem szkodowym zależnym od decyzji. Ze względu na daleko posunięte współczesne możliwości wczesnego rozpoznania nadciągających zagrożeń, wczesnego ostrzegania, a także techniczne, finansowe i organizacyjne zdolności do przeciwdziałania i obrony przed niepożądanymi zdarzeniami i sytuacjami oraz ochrony przed ich skutkami coraz więcej zagrożeń – w tym także zagrożeń naturalnych, takich jak trzęsienia ziemi, powodzie czy epidemie – definiuje się jako ryzyka, czyli sytuacje zależne od ludzkich decyzji i żąda ich społecznej legitymizacji (Rothkegel, Banse i Renn, 2010, s. 153). Aby uniknąć nieporozumień, autor niniejszego artykułu operuje tradycyjnym rozróżnieniem na zagrożenia i ryzyka, a niepewne, losowe zdarzenia traktuje jako źródła ryzyka jedynie pośrednio, gdy wpływają one na podejmowanie decyzji. Za ryzykowne uznaje jednak nie same takie zdarzenia, lecz ewentualne decyzje o ich zignorowaniu.

bezpieczeństwem, który pozwoliłby lepiej przygotować krytyczne infrastruktury energetyczne na „normalne katastrofy". Autor artykułu rozważa przydatność modelu bezpieczeństwa bazującego na zagrożeniach i ryzykach systemowych oraz zarządzaniu odpornością jako nowego paradygmatu bezpieczeństwa energetycznego.

Słowa kluczowe: bezpieczeństwo energetyczne, cyberbezpieczeństwo, inteligentne sieci, Internet energii, teoria systemów.

Protection of Power Infrastructure Against Threats and Systemic Risks - A New Paradigm in Energy Security Management

Summary: The article contains the results of the initial exploration of a new problem field in the area of energy security, covering a wide spectrum of complex threats and systemic risks facing the power industry undergoing rapid transformations towards cyber-physical systems. The purpose of the exploration, identification, and initial theoretical processing (conception, structuring, etc.) of the complexes of cognitive, decision-making and projection-organizational problems, which for the safety and reliability of the electricity supply, resulting from the rapid increase in internal complexity as well as complex synergies and interdependencies arising from the convergence of two-speed technologies - energy systems and information and communication technologies. The tendencies of such complex, turbulent systems for chaotic behavior and their ability to self-organizing behavior "without human intervention" threaten with sudden, unpredictable, dangerous initiating events that can cause uncontrolled cascades of disorders capable of overcoming all protective barriers, firewalls, and layers of protection. The spectrum of catastrophic consequences of large-scale power failures puts into question the current safety management model based on threat elementarization, vulnerability analysis, risk assessment, and crisis management, and prompts the search for a new paradigm in security management that would prepare critical energy infrastructures for 'normal disasters' better. The author of the article considers the usefulness of the security model based on systemic threats and risks as well as resilience management as a new energy security paradigm.

Keywords: security of power systems, cybersecurity, smart grid, Internet of energy, system theory.

Współczesne transformacje w sektorze elektroenergetycznym – żyzny grunt dla zagrożeń i ryzyk systemowych

Sektor elektroenergetyczny jest jednym z najbardziej newralgicznych obszarów krytycznej infrastruktury, od której niezawodności zależą wszystkie układy krążenia istotne dla przetrwania nowoczesnych społeczeństw bazujących w nawet najprostszych codziennych czynnościach na mikroelektronice, komputerach i łączności bezprzewodowej. Jednocześnie za sprawą konwergencji technologii energetycznych z technologiami teleinformatycznymi (IT) infrastruktury

energetyczne stały się obecnie obszarem najbardziej narażonym na cyberataki[2], dlatego wiele państw w swoich narodowych strategiach bezpieczeństwa uznaje podejmowanie wielofrontowych działań zmierzających do zwiększenia bezpieczeństwa sektora energetycznego za zadanie priorytetowe. W związku z niezwykle szybko postępującą cyfryzacją, komputeryzacją, usieciowieniem i wirtualizacją wszystkich sfer życia indywidualnego i zbiorowego, czwartą rewolucją przemysłową (*Industry 4.0*) oraz rozwojem Internetu rzeczy bazującego na technologiach sieciowych piątej generacji (5G) gwałtownie wzrasta uzależnienie ludzkości od bezpieczeństwa energetycznego i niezawodności dostaw energii elektrycznej, a także zapotrzebowanie na ciągłe, elastyczne, dostosowane do zmieniających się potrzeb zaopatrzenie w energię w dowolnym miejscu i każdym czasie, coraz częściej z opcją mobilnego poboru energii. Jednocześnie systemy energetyczne na świecie przechodzą od kilku lat głębokie transformacje w kierunku systemów cyberfizycznych (CPS), będących konsekwencją zmiany politycznego kursu (np. *Energiewende* w Niemczech), do jakiej doszło na przełomie tysiącleci pod wpływem idei zrównoważonej energetyki przyjaznej dla ludzi, środowiska i biznesu, czyli godzącej ekologiczne wymagania gospodarki niskoemisyjnej ze społecznymi wymaganiami bezpieczeństwa i sprawiedliwości oraz ekonomicznymi wymaganiami opłacalności i konkurencyjności. Główne trendy związane przede wszystkim z dekarbonizacją i denuklearyzacją, dywersyfikacją i decentralizacją źródeł energii, wzrostem znaczenia odnawialnych źródeł energii (OZE) – zwłaszcza energetyki wiatrowej i fotowoltaicznej – oraz konieczność obsługi niestabilnych dostaw energii z tego typu źródeł, transgraniczną integracją sieci elektroenergetycznych, w połączeniu z takimi problemami, jak starzenie się infrastruktury elektroenergetycznej i wzrost podatności na awarie oraz szybko zmieniające się regulacje i standardy techniczne, wymagające ciągłych dostosowań i modernizacji, zagrażających ciągłości pracy komponentów sieci, stawiają przemysł elektroenergetyczny przed nieznanymi dotąd wyzwaniami. Zarządzanie dostawami energii elektrycznej w takich warunkach wiąże się z koniecznością oparcia systemów na sieciach inteligentnych (*smart grid*)[3]

[2] W ostatnich latach liczba cyberataków na systemy elektroenergetyczne gwałtownie wzrosła (Dragos Inc., 2017; Sobczak, 2019) i systemy te przygotowywane są na dalszy wzrost liczby cyberincydentów.

[3] Do głównych atrybutów inteligentnej sieci należą m.in.: (1) systemy po stronie dostawcy umożliwiające monitorowanie stanu sieci i komponentów systemowych za pomocą nowoczesnych narzędzi komputerowej analizy danych, analizę obciążenia i wydajności przesyłu energii, wykrywanie i łagodzenie zakłóceń oraz równoważenie niestabilnych źródeł zasilania (np. farm wiatrowych), szybką lokalizację awarii

– oznaczających wzrost usieciowienia, zdalną obsługę, wzrost znaczenia sztucznej inteligencji oraz postępującą autonomizację (Internet energii) – nieodzowną z punktu widzenia poprawy integracji i optymalizacji wzajemnego zbilansowania procesów wytwarzania, przesyłu, dystrybucji i zużycia energii w coraz bardziej rozproszonych układach krążenia o nieregularnej pulsacji (Orwat, 2011, s. 47). Jak wszystkie inne rozwiązania technologiczne, również zwiększenie zaangażowania technologii IT w sektorze elektroenergetycznym cechują jednak silne ambiwalencje. Oprócz niewątpliwych zalet, takich jak wzrost efektywności ekonomicznej i energetycznej oraz niezawodności, należy się spodziewać pojawienia się nowych podatności na zagrożenia i ryzyka związanych z jednej strony z gwałtownym wzrostem złożoności i zjawiskami emergencyjnymi, z drugiej z szeroko rozumianymi problemami cyberbezpieczeństwa. Inteligentne zarządzanie bazujące na technologiach IT jest koniecznym elementem ograniczania ryzyka związanego z transformacjami w sektorze elektroenergetycznym, ale same struktury zarządzania bywają również źródłem ryzyka. Transformacje cyfrowe i nowy model zarządzania „inteligentną

i uszkodzeń pozwalającą na skrócenie czasu naprawy i przerw w zasilaniu, zdecentralizowane zarządzanie energią w myśl koncepcji wirtualnych elektrowni, a także systemy pozwalające na optymalne reagowanie na zapotrzebowanie i dostosowujące ceny energii do aktualnego popytu; (2) systemy po stronie odbiorcy, na które składają się zaawansowana infrastruktura pomiarowa (tzw. inteligentne liczniki) umożliwiająca gromadzenie, przechowywanie i przetwarzanie kompleksowych danych o zużyciu energii, przesyłanie danych o zużyciu energii w czasie rzeczywistym oraz aktualnej lub przewidywanej przyszłej cenie energii na inne urządzenia klienta, a także wykrywanie strat lub kradzieży, dwukierunkową komunikację między agentami systemu pozwalającą na wzajemną integrację i synchronizację wszystkich komponentów systemu elektroenergetycznego z wykorzystaniem różnych sieci (tzw. Internet energii) upraszczającą rozliczenia, mikrosieci i systemy zarządzania energią typu smart home, urządzenia prosumenckie do rozproszonego generowania lub magazynowania energii (np. elektryczne samochody lub inne urządzenia wyposażone w akumulatory), inteligentne urządzenia zdalnie sterowane lub programowalne na czas pracy optymalny z punktu widzenia dostępności energii, szczytowego zapotrzebowania lub ceny, a także (3) systemy ekonomiczne i nowe modele biznesowe bazujące na sprawnie funkcjonującej infrastrukturze teleinformatycznej i automatycznym przetwarzaniu dużej liczby danych transakcyjnych, pozwalające na optymalizację zakupów energii, zwiększające liczbę podmiotów uczestniczących w transakcjach na giełdach energii, otwierające nowe sektory usług doradczych specjalizujących się w optymalizacji zużycia energii, umożliwiające regulowanie zużycia energii przez odbiorców przy pomocy dynamicznych, tj. czasowo zróżnicowanych cen oraz umożliwiające instalowanie nowych i wykorzystanie istniejących rozproszonych mocy produkcyjnych (mikroturbiny gazowe, hydroelektrownie szybowe, lokalne elektrociepłownie oraz szybko rozwijające się systemy prosumenckie, głównie fotowoltaiczne) (Orwat, 2011, s. 48). W związku z rozwojem systemów łączności bezprzewodowej piątej generacji (5G) w niedalekiej przyszłości należy się spodziewać wzrostu autonomizacji infrastruktur technicznych oraz zastąpienia interakcji człowiek–człowiek i człowiek–maszyna interakcjami między maszynami wyposażonymi w sztuczną inteligencję. Wielkimi krokami zbliża się era Internetu rzeczy, z myślą o którym przygotowano już nawet specjalny system maszynowych rozliczeń finansowych bazujący na kryptowalucie IOTA.

siecią" prowadzą do niebezpiecznego wzajemnego uzależnienia infrastruktury teleinformatycznej od niezawodności systemu elektroenergetycznego, którego bezpieczeństwo zapewniają. W tych warunkach staje się oczywiste, że rosnące pod wpływem inteligentnych sieci uzależnienie sektora energetycznego od Internetu dodatkowo zwielokrotnia podatność nowoczesnych systemów zaopatrzenia w energię na zaburzenia. Ponadto postępująca konwergencja infrastruktur elektroenergetycznych i infrastruktur teleinformatycznych może stać się wkrótce źródłem poważnych zagrożeń i dodatkowego ryzyka nie tylko z powodu coraz większej otwartości infrastruktury bazującej na sieci, zwiększonej złożoności i rosnącego uzależnienia od niezawodności systemów łączności, wysokiej podatności tych systemów na zaburzenia i destabilizacje, widma cyberataków – a więc zagrożeń elementarnych, na których skupia się główna uwaga interesariuszy bezpieczeństwa energetycznego – ale także z powodu niepożądanych zdarzeń i sytuacji uwarunkowanych systemowo, które pozostawały dotąd w dużej mierze niezauważone. Inherentna niestabilność rozproszonych źródeł energii, niekontrolowany wzrost złożoności oraz zbyt sztywne połączenie dwóch najbardziej newralgicznych infrastruktur krytycznych o odmiennej dynamice zmian technologicznych w połączeniu z dużą liczbą punktów ataku oraz niskimi – jak na infrastruktury krytyczne – standardami niezawodności typowymi dla systemów otwartych, obsługiwanych przez wielu agentów z poziomu wielu terminali, narażają systemy elektroenergetyczne na nieznane dotąd złożone zagrożenia i ryzyka o charakterze skumulowanym, kombinacyjnym i systemowym, które stawiają pod znakiem zapytania – a w najlepszym razie przed trudnymi wyzwaniami – dotychczasowe standardy bezpieczeństwa, bazujące na elementaryzacji zagrożeń, rutynowej analizie podatności, szacowaniu ryzyka, zarządzaniu kryzysowym i podziale odpowiedzialności. Gwałtowny wzrost złożoności i nieliniowe interakcje między pojedynczymi komponentami rozproszonych systemów cyberfizycznych potęgowane przez różne prędkości, z jakimi rozwijają się konwergujące technologie energetyczne i technologie IT, grożą chaotycznymi, niekontrolowanymi zachowaniami systemów energetycznych i powstawaniem zdarzeń, które wykorzystując łańcuchy zbyt sztywnych połączeń, mogą inicjować kaskady zaburzeń zdolne pokonać wszelkie bariery ochronne i warstwy zabezpieczeń.

Zagrożenia i ryzyka systemowe

Od kilkunastu lat w badaniach bezpieczeństwa i analizach ryzyka infrastrukturalnego coraz częściej uwzględniane są zagrożenia i ryzyka systemowe (Hellström, 2007; Renn, Keil, 2008; Helbing, 2010; Hellström, 2009; Laperrouza, 2009; Rothkegel, Banse i Renn, 2010; Büscher, 2011; Cleeland, 2011; Orwat, 2011), ale prawdziwym impulsem do reaktywacji teorii systemów i pogłębionych badań nad ryzykami systemowymi był kryzys finansowy w USA spowodowany aferami Enronu i Worldcomu – kryzys, który w latach 2001–2002 pociągnął za sobą gwałtowny spadek wartości indeksu Nasdaq i serię bankructw wielu czołowych spółek internetowych. Nic więc dziwnego, że to właśnie na gruncie finansów i bankowości zapoczątkowano po 2002 r. badania nad zagrożeniami i ryzykami systemowymi (Kaufman, Scott, 2003), które przyczyniły się do reaktywacji teorii systemów[4]. Pojęcie zagrożeń systemowych i ryzyka systemowego jest nieprecyzyjne z powodu niejasności, niejednoznaczności jego składników. Nie ma powszechnie obowiązującej definicji zagrożeń systemowych i ryzyka systemowego, są one rozumiane w sposób intuicyjny i potrzebne są dalsze badania zmierzające do teoretycznego ugruntowania tych pojęć oraz opracowania metod i narzędzi do analizy tego nowego rodzaju zagrożeń i ryzyk. Pojęcie zagrożeń i ryzyk systemowych bywa wywodzone z pojęcia „bezpieczeństwo systemu", które ma powszechnie znaną strukturę hybrydową: pojęcie systemu może w tej formule występować w dwóch różnych znaczeniach: *security* (*genetivus objectivus*, system zagrożony – w dużym uproszczeniu: brak niebezpiecznych oddziaływań

[4] Ogólna teoria systemów jest teorią operacyjną dostarczającą sformalizowanych metod analizy i syntezy, a bazującą na budowaniu modeli (obrazowych rekonstrukcji) badanych obiektów lub fragmentów rzeczywistości traktowanych jako system, czyli złożony układ współzależności stanowiący całość dającą się jednoznacznie rozgraniczyć od otoczenia i wykazujący zdolności do samoorganizacji. Głównym celem teorii systemowej jest zrozumienie złożoności takich układów bez konieczności rozbierania ich na części i redukowania do bardziej elementarnego poziomu, którym to operacjom zawsze towarzyszą poznawcze zniekształcenia rozpatrywanego przedmiotu i ryzyka utraty z pola widzenia zjawisk, procesów lub powiązań istotnych z punktu widzenia funkcjonowania całości i całościowego rozumienia. Dlatego zamiast elementaryzacji stosuje się systematyzację, modele atomistyczne zastępuje holistycznymi, jednowymiarowość (liniowość) zastępuje wielowymiarowością, wielozmiennowością, a zamiast różnicowania i analizy stosuje się integrację i syntezę. Teoria systemów tradycyjnie dzieli się na synergetykę, czyli interdyscyplinarną naukę badającą procesy samoorganizacyjne na poziomie systemów (Haken, 1982) i cybernetykę, czyli teorię (zewnętrznego) sterowania systemami. Z teorii systemów wywodzi się analiza systemowa – rodzina metod opisu i analizy wysoce złożonych, skomplikowanych układów wzajemnych zależności wymagających logicznej obróbki nieliniowych strumieni danych i interdyscyplinarnej integracji różnych aspektów i nośników wiedzy. Analiza systemowa otwiera poznawczy dostęp do tego, co dzieje się na mikropoziomie z komponentami systemu zupełnie na innej drodze, niż umożliwiają to badania dyscyplinowe (Michalski, 2019, s. 137 i n., 393–395).

ze strony otoczenia lub ochrona systemu przed takimi oddziaływaniami) i *safety* (*genetivus subjectivus*, system zagrażający – w dużym uproszczeniu: niezawodność systemu lub brak niebezpiecznych oddziaływań na otoczenie). O zagrożeniach i ryzykach systemowych czasami mówi się więc w którymś z tych znaczeń, ale w pojęciu zagrożenia lub ryzyka „systemowego" w gruncie rzeczy chodzi o coś innego, co ma związek z zachowaniami typowymi dla złożonych systemów. Systemy są tutaj rozumiane jako wewnętrznie spójne złożenia elementów zdolnych również do oddzielnego istnienia, dynamiczne kompleksy dające się wyodrębnić z otoczenia, posiadające zdolność do spontanicznej samoorganizacji i autonomicznego działania będącego efektem tajemniczych synergii – działania, którego nie da się zrozumieć ani wyjaśnić poprzez dekompozycję, czyli rozłożenie na pierwotne części składowe i poznanie, jak poszczególne części działają osobno, we wzajemnej izolacji. Działaniem systemów rządzi „niewidzialna ręka" – mimo że nie posiadają one często żadnej scentralizowanej instancji sterującej lub kontrolnej, wykazują wysokie zdolności samoorganizacyjne. Systemy posiadają paradoksalną konstytucję bytową: z jednej strony są superstabilnymi superstrukturami, z drugiej kruchymi złożeniami elementów zagrożonymi rozpadem. Ich trwałość zależy od zdolności do neutralizacji zakłóceń (szumów) ze strony otoczenia poprzez produkowanie operacji powodujących wzrost wewnętrznej złożoności umożliwiający zwiększenie synergii między częściami składowymi – wykorzystanie funkcji i oddziaływań dodatkowych, których nie posiadają elementy systemu działające osobno. Im bardziej wewnętrznie złożony jest dany system, tym większe są z reguły jego autonomia, stabilność i odporność na uszkodzenia. Istnieje jednak górna granica złożoności, której przekroczenie powoduje dysfunkcjonalność systemu i zwiększenie podatności na zniszczenie lub destabilizację.

Odkąd w połowie lat 80. XX w. amerykański badacz katastrof Charles Perrow zwrócił uwagę na wspólne cechy systemów technologicznych i organizacyjnych odpowiedzialne za strukturalną podatność tych systemów na destabilizacje (Perrow, 1984), nastąpił w badanych systemach skokowy postęp złożoności. Wcześniej przyczynę wypadków i katastrof technicznych upatrywano wyłącznie w błędach człowieka (błędy konstruktora, błędy operatora, lekceważenie przepisów bezpieczeństwa itp.). Perrow skoncentrował się w swoich analizach na dwóch wzajemnie niezależnych strukturalnych cechach tzw. wysokich technologii (technologii wysoce złożonych, zaawansowanych i innowacyjnych)

– rodzajach interakcji (liniowe – nieliniowe) oraz rodzajach sprzężeń między elementami systemów (luźne – silne). Z połączenia obu wymiarów powstała matryca heurystyczna (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.

Rozwój inteligentnej sieci wymaga wysokowydajnych systemów łączności umożliwiających sprawną i tanią dwukierunkową komunikację w czasie rzeczywistym. Wykorzystanie Internetu jako powszechnie akceptowanego standardu komunikacji wydaje się naturalnym odruchem, ale otwartość Internetu naraża infrastruktury elektroenergetyczne na przypadkowe destabilizacje lub złośliwe ataki i zmusza do restrykcyjnego stosowania reżimów ochronnych polegających na szyfrowaniu, kontroli dostępu, uwierzytelnianiu itp. Dodatkowe zagrożenia wynikają z powszechnego w energetyce trendu do bazowania na komercyjnych usługach sieciowych, standardowym sprzęcie i standardowych oprogramowaniach, a także dołączenia nowych, inteligentnych aplikacji ze starszymi systemami. Szybkie tempo procesów starzenia się technologii w sektorze IT jest źródłem wielu wyzwań i dylematów, związanych z koniecznością coraz częstszych wymian sprzętu i oprogramowań. Z jednej strony szybko zmieniające się w czasie standardy kompatybilności, z drugiej zaś wygaszanie aktualizacji i usług wsparcia – stymulatory powszechnie stosowane przez producentów oprogramowań w celu zmotywowania użytkowników do zakupu nowszych produktów – czynią korzystanie w przemyśle elektroenergetycznym z kosztownych, ale zapewniających wyższy poziom cyberbezpieczeństwa, niestandardowych rozwiązań mało opłacalnym. Aby pogodzić przeciwstawne wymagania kompatybilności i opłacalności większość operatorów stosuje praktykę nadbudowywania starszych systemów IT nowymi technologiami inteligentnych sieci, co bywa źródłem jeszcze większych problemów z cyberbezpieczeństwem (Tervo, Wiander, 2010; Flick, Morehouse, 2011, s. 54 i n; Orwat, 2011, s. 50). Wzajemne interakcje między nowo dodawanymi aplikacjami a starszymi komponentami, zwłaszcza takimi, dla których wygasł serwis wsparcia, miewają trudne do przewidzenia konsekwencje. Ponadto ogromna ilość wrażliwych danych migrujących w inteligentnej sieci, w tym dane z urządzeń monitorujących i kontrolnych, dane pomiarowe z inteligentnych liczników, a także dane administracyjne i osobowe stosowane w rozliczeniach, podlega restrykcyjnym przepisom o ochronie wymagającym

odpowiedniego szyfrowania, do czego potrzebna jest skomplikowana i kosztowna w utrzymaniu infrastruktura zarządzania kluczami kryptograficznymi.

Również struktury organizacyjne i systemy zarządzania mogą same stwarzać warunki zagrażające swoim własnym funkcjom. Analiza zagrożeń systemowych i ocena ryzyka systemowego wymagają uwzględnienia procesów społecznych i czynników ludzkich (zarówno błędów, jak i czynników intencyjnych), które tworzą, utrzymują krytyczne infrastruktury elektroenergetyczne lub zagrażają im. Analiza winna obejmować przede wszystkim zachęty i ograniczenia wynikające z istniejących struktur organizacyjno-zarządczych, które wpływają m.in. na sposób percepcji zagrożeń i obsługi ryzyka przez poszczególne podmioty, kształtują indywidualne poczucie odpowiedzialności za bezpieczeństwo oraz motywacje. Jeśli struktury zarządzania nie stymulują ani nie wymagają innych zachowań, podmioty tworzące system elektroenergetyczny kierując się logiką ekonomiczną, mogą narażać system na zagrożenia i ryzyka poprzez ograniczanie nakładów na modernizację technologii IT, inżynierię bezpieczeństwa, usługi doradcze czy podnoszenie kompetencji w zakresie cyberbezpieczeństwa. Prywatyzacja i liberalizacja sektora energii stawia operatorów infrastruktur elektroenergetycznych pod silną presją konkurencyjności, prowadząc do radykalnego ograniczania marginesów bezpieczeństwa w ramach optymalizacji kosztowej poniżej poziomów pożądanych z punktu widzenia inżynierii bezpieczeństwa (Cohen, 2010, s. 62; Orwat, 2011, s. 50; Dynes, Goetz i Freemann, 2008; Van der Vleuten, Lagendijk, 2010). Do momentu wdrożenia Dyrektywy NIS operatorzy infrastruktur elektroenergetycznych nie czuli się zachęceni do zgłaszania informacji o problemach z niezawodnością, awariach oprogramowania lub zagrożeniach cybernetycznych, co nie sprzyjało społecznym procesom uczenia się, które mają kluczowe znaczenie z punktu widzenia racjonalnego obcowania z nieznanymi zagrożeniami i ryzykami. Certyfikacja systemów bezpieczeństwa bazuje na procesach elementaryzacji i modelowych procedurach dowodowych, pomijając zagrożenia i ryzyka o charakterze kombinacyjnym, skumulowanym lub systemowym w prawdziwym środowisku pracy. W praktyce w przypadku większości operatorów działania ochronne mają charakter pasywny i koncentrują się na zgodności z minimalnymi wymaganiami regulacyjnymi określonymi w przepisach o cyberbezpieczeństwie krytycznych infrastruktur i tylko w nielicznych przypadkach można zauważyć bardziej ofensywne i kompleksowe podejście do bezpieczeństwa. Wciąż brakuje wiarygodnych systemów certyfikacji

i przejrzystych systemów oznakowania produktów, co sprawia, że konsumenci energii są niewłaściwie informowani o zaletach bezpiecznych systemów i wykazują w związku z tym niewielką skłonność do płacenia wyższych cen za bardziej bezpieczne produkty (Orwat, 2011, s. 51; US GAO 2011, s. 23).

W systemach obsługiwanych przez wiele podmiotów bezpieczeństwo systemowe nabiera cech dobra publicznego, co z powodu braku koordynacji i odmowy współpracy (m.in. dylemat więźniów) prowadzi do nieefektywnego poziomu bezpieczeństwa ogólnego. Wzrost fragmentacji sektora elektroenergetycznego związany z rosnącą liczbą uczestników rynku oraz wzrost złożoności powiązań międzysektorowych skutkujący aktywnością coraz większej liczby regulatorów prowadzą do powstania coraz bardziej nieprzejrzystej konstelacji aktorów, która utrudnia efektywne zarządzanie bezpieczeństwem tego sektora i zwiększa ryzyko niepowodzeń w realizacji celów (Mayntz, 2009).

Rosnące zagęszczenie i postępujące usieciowienie struktur społecznych powodują wzrost współzależności między różnymi sferami życia jednostki i zbiorowości, gwałtownie zwiększając ekspozycję każdego elementu tych struktur na zagrożenia wynikające z egzo- lub endogennych zaburzeń, które za sprawą sieci powiązań szybko się rozprzestrzeniają i mogą tworzyć czasoprzestrzennie i społecznie nieograniczone łańcuchy szkód. Istnienie zagrożeń i ryzyk systemowych zauważa się zwykle dopiero po fakcie, ilekroć pomimo przedsięwziętych środków bezpieczeństwa chroniących przed zagrożeniami elementarnymi, izolowanymi nie udało się zapobiec katastrofie. Nasuwa się więc pytanie, czy można byłoby takie systemowe zagrożenia rozpoznawać wcześniej, aby móc skuteczniej niż dotychczas chronić się przed ich niszczącymi skutkami.

Nieadekwatność dotychczasowego modelu zarządzania bezpieczeństwem bazującego na elementaryzacji zagrożeń, analizie podatności, ocenie ryzyka i obsłudze incydentów

Zarządzanie bezpieczeństwem w sektorze elektroenergetycznym – podobnie jak w większości innych obszarów zbiorowej działalności technicznej – ciągle bazuje na nieadekwatnych pojęciach o świecie oraz jego poznawczej i operacyjnej kontrolowalności – pojęciach będących „wybuchową" mieszaniną antycznych i nowożytnych tradycji myślenia, m.in. arystotelesowskiej ontologii opartej na pojęciu substancji i wizji świata jako hierarchicznie uporządkowanego zbioru

odrębnych rzeczy, newtonowskiego deterministyczno-mechanicystycznego modelu naukowego poznania bazującego na wyjaśnianiu złożonych zjawisk poprzez ich rozczłonkowanie na elementy, kartezjańskiego sceptycyzmu metodycznego odpowiedzialnego za obecne, zawyżone standardy naukowego dowodu oraz szeroko rozpowszechnione „domniemanie niewinności", pascalowskiej wierze w obliczalność ryzyka, a także hobbesowskiej wizji społeczeństwa, dla którego naturalnym stanem jest „wojna wszystkich przeciw wszystkim". Coraz częstsze doświadczenie niespodziewanego fiaska w działaniu i utraty kontroli nad procesami, których pełne kontrolowanie wcześniej zakładano, boleśnie uświadamia współczesnemu człowiekowi, w jak skomplikowany, nieprzejrzysty i niezrozumiały sposób wszystko jest połączone ze wszystkim, a także to, że każda zmiana – choćby najbardziej niepozorna – nie pozostaje bez wpływu na inne elementy (Büscher, 2011, s. 4). Do znaczącego wzrostu świadomości „systemowej" w społeczeństwie przyczyniło się w ostatnich dwóch dekadach upowszechnienie edukacji ekologicznej. Dzięki ekologii coraz więcej osób rozumie istotę „systemowości" i posiada zdolność do całościowego rozumienia wielu zjawisk z uwzględnieniem złożoności interakcji między ich częściami składowymi (Cleeland, 2011, s. 14). Choć coraz więcej ludzi zdaje sobie sprawę z tego, że ponad rzeczami istnieją złożone wielopoziomowe superstruktury posiadające zdolności do samoistnego działania zgodnie z własną, nie zawsze zrozumiałą dla ludzi logiką, zdolności samoorganizacji i samoreprodukcji – a więc atrybuty zarezerwowane w tradycyjnej ontologii wyłącznie dla substancji – to jednak w zarządzaniu bezpieczeństwem nadal wydaje się dominować nieuzasadniony poznawczy i planistyczny optymizm, oparty na arystotelesowsko-oświeceniowym przekonaniu o panowaniu rozumu nad światem bezrozumnych rzeczy. W świetle najnowszych odkryć na gruncie matematycznej teorii chaosu (Magnitskii, 2018) wydaje się, że możliwości kontrolowania bezpieczeństwa złożonych systemów bazujących na komponentach technologicznych były dotąd powszechnie przeceniane[5].

O beznadziejnej niemożliwości uwolnienia się decydentów odpowiedzialnych za bezpieczeństwo sektora energetycznego od tych anachronicznych schematów myślenia dobitnie świadczą obowiązujące w Polsce i innych krajach regulacje

[5] Niedawno wykazano, że nawet prosty trójwymiarowy autonomiczny układ kwadratowy z pojedynczą stabilną równowagą skupioną na węźle może zachowywać się chaotycznie (Wang, Chen, 2012).

określające zasady zarządzania bezpieczeństwem i ochrony infrastruktur krytycznych[6].

W systemach zaopatrzenia w energię elektryczną infrastruktury techniczne odpowiadające za produkcję i dystrybucję energii są nie tylko połączone skomplikowaną siecią zależności ze zjawiskami i procesami przyrodniczymi oraz społeczno-ekonomicznymi, lecz także w skomplikowany sposób zrastają się z innymi krytycznymi infrastrukturami: informatycznymi, telekomunikacyjnymi i transportowymi, co skutkuje gwałtownym wzrostem złożoności i wzajemnej zależności. Są one odpowiedzialne za szczególną skłonność tych systemów do generowania i propagacji wewnętrznych zaburzeń, które rozprzestrzeniając się wzdłuż łańcuchów sztywnych sprzężeń, pozbawionych odpowiednich marginesów bezpieczeństwa, w sposób niekontrolowany mogą powodować kaskady niepożądanych zdarzeń włącznie z awariami ogólnosystemowymi, zdolne pokonać wszelkie zabezpieczenia. Takim niekorzystnym scenariuszom niewątpliwie sprzyjają sztywne sprzężenia zwrotne pomiędzy infrastrukturą elektroenergetyczną a infrastrukturą internetową oraz wzajemne niedostosowanie tempa rozwoju struktur zarządzania do tempa zmian technologicznych. Manifestacją niedostosowania jest szeroko rozpowszechniona elementaryzacja zagrożeń i ciągle bardzo ograniczone uwzględnianie zagrożeń i ryzyk systemowych w analizach podatności, na których opiera się zarządzanie bezpieczeństwem infrastruktur krytycznych. Ze względu na rosnącą złożoność wzajemnych zależności między infrastrukturą elektroenergetyczną a infrastrukturą

[6] W ciągu ostatnich kilku lat Unia Europejska i rządy wielu krajów zauważyły szereg zagrożeń i na nie odpowiedziały, przygotowując i wdrażając pakiety regulacji, głównie z zakresu cyberbezpieczeństwa, uznające ochronę infrastruktur krytycznych za priorytet bezpieczeństwa narodowego. Państwa rozpostarły nad sektorem elektroenergetycznym urzędowy parasol cyberbezpieczeństwa oraz nałożyły na operatorów infrastruktur restrykcyjne obowiązki związane z troską o bezpieczeństwo własnych systemów IT, ich ciągłe testowanie pod kątem podatności i udoskonalanie, bieżące prowadzenie analizy i oceny ryzyka, audytowanie i zgłaszanie groźnych incydentów organom właściwym w sprawach cyberbezpieczeństwa. W Polsce szczegółowe normy i narodowe standardy cyberbezpieczeństwa oraz wymagania dotyczące środków ochrony infrastruktur krytycznych przed niebezpiecznymi incydentami i sposobów reagowania na takie incydenty określały Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (2017), a następnie ustawa o krajowym systemie cyberbezpieczeństwa (2018) wraz z przepisami wykonawczymi – pakiet regulacji stanowiący implementację unijnej dyrektywy w sprawie bezpieczeństwa sieci i informacji (NIS) oraz uchwała Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (2019). Kierowane troską o powszechne bezpieczeństwo nadmierne ingerencje regulacyjne państwa w kwestie ochrony systemów IT operatorów krytycznych infrastruktur są jednak źródłem fałszywej obietnicy bezpieczeństwa, której kruchość brutalnie demaskują wielkoobszarowe awarie zasilania, do jakich co pewien czas dochodzi w różnych częściach świata.

teleinformatyczną oraz dynamikę rozwoju technologii IT już w chwili obecnej nie jest możliwa elementaryzacja potencjalnych zagrożeń i zidentyfikowanie kompleksowego ich wykazu wraz z oszacowaniem prawdopodobieństwa ich wystąpienia, bez których dotychczasowe koncepcje bezpieczeństwa bazujące na analizie podatności i klasycznym zarządzaniu ryzykiem okazują się bezużyteczne (NIST, 2014; Rossebo i in., 2017).

Brakuje ponadto adekwatnych modeli współpracy i regulacji określających w sposób jednoznaczny zakresy uprawnień (np. do monitorowania i zarządzania zależnościami ponadsektorowymi) i odpowiedzialności poszczególnych podmiotów – rozwiązań organizacyjnych niezbędnych w warunkach wzrastającej złożoności i nieprzejrzystości konstelacji aktorów i interesów, cechującej wzajemnie zależne sektory infrastruktur krytycznych. Ponieważ przemysł elektroenergetyczny należy do sektorów silnie regulowanych przez państwo, odpowiedzialność za rzeczywisty poziom bezpieczeństwa ulega niebezpiecznemu rozproszeniu, bowiem operatorzy systemów elektroenergetycznych czują się często zwolnieni z obowiązku aktywnego działania na rzecz podnoszenia bezpieczeństwa swoich systemów ponad poziom określony w prawnych regulacjach, czego wymownym przykładem są praktyki firm energetycznych na obszarze cyberbezpieczeństwa własnych systemów IT.

Te na pierwszy rzut oka trywialne spostrzeżenia wskazują na konieczność zmian w postrzeganiu problemów bezpieczeństwa, które nie były dotąd dostatecznie zauważane i na które nie reagowano we właściwy sposób.

Nowy paradygmat bezpieczeństwa energetycznego oparty na koncepcji zagrożeń i ryzyk systemowych oraz zarządzaniu odpornością

Koncepcja zagrożeń i ryzyk systemowych ma na celu uświadamianie złożoności interakcji czynników inicjujących oraz materialną, czasoprzestrzenną i społeczną nieograniczoność łańcuchów niebezpiecznych zdarzeń, które wpływają na całe układy, a nie tylko na poszczególne elementy.

Pod wpływem przykrych doświadczeń z wielkoobszarowymi awariami zasilania wzrasta świadomość zagrożeń i ryzyk systemowych, które pojawiają się nagle, przychodzą znikąd i wywołują kaskady zaburzeń zdolne pokonać wszelkie dotychczas stosowane warstwy zabezpieczeń. W przypadku infrastruktur tak newralgicznych i o tak krytycznym statusie zarządzanie kryzysowe – nazywane na obszarze cyberbezpieczeństwa obsługą incydentów – oraz uczenie się

na błędach nie wydają się jednak optymalną koncepcją bezpieczeństwa. Należy więc bacznie przyjrzeć się zagrożeniom systemowym specyficznym dla sektora energii, wynikającym z trudnych do przewidzenia synergii zwiększających prawdopodobieństwo wystąpienia niepożądanych zdarzeń lub dotkliwość ich konsekwencji. Punktem wyjścia badań nad zagrożeniami systemowymi (organicznymi, synergicznymi) winna być identyfikacja ogólnych, wspólnych wszystkim złożonym systemom czynników, które tworzą „żyzny grunt" dla tego typu zagrożeń:

- czynników strukturalnych, wynikających z właściwości złożonych systemów i skutkujących nieprzewidywalnością zachowań: synergii, nieliniowości, bezwładności, fazowości i progowości, histerezy, sztywności sprzężeń i utraty marginesów bezpieczeństwa, zwrotnych wzmocnień i zmiennej podatności na ryzyko;
- czynników społeczno-ekonomicznych, związanych z niekorzystnymi konstelacjami interesów, nieadekwatnymi modelami naukowego poznania (coraz węższa specjalizacja, dyscyplinowy redukcjonizm i nadmierna skłonność do fragmentaryzacji, zawyżone wymagania naukowej ścisłości – np. żądanie dowodów matematycznych lub eksperymentalnych potwierdzeń oraz metodyczny sceptycyzm nakazujący w razie wątpliwości co do istnienia jednoznacznych zależności przyczynowych ignorowanie takich wątpliwości), dynamiką zmian społecznych, akceleracją postępu technologicznego, wzrostem znaczenia innowacyjności jako głównego czynnika konkurencyjności skutkującym pochopnym wdrażaniem innowacji, zanim nauka w pełni rozpozna ich oddziaływania i zrozumie wynikające z nich niebezpieczeństwa, a także powstaniem wysokomarżowego przemysłu ryzyka, który tworzą m.in. operatorzy niebezpiecznych instalacji przemysłowych (m.in. reaktory atomowe, reaktory chemiczne, magazyny paliw itp.), firmy ubezpieczeniowe, producenci sprzętu ratowniczego, środków ochrony, leków, firmy specjalizujące się w likwidacji szkód i odbudowie zniszczeń oraz niezliczone rzesze podmiotów czerpiących zyski z nieszczęść spadających na innych[7];

[7] Przemysł, który profituje z zagrożeń, które sam wytwarza, nie tylko pozoruje prewencję zagrożeń, naprawdę nie eliminując ich przyczyn, ale niemal wszędzie może również liczyć na przychylność państwa, które opodatkowuje przepływy pieniężne w sektorze ryzyka. W interesie fiskalnym państwa nie jest wydawanie zakazów produkcji niebezpiecznych produktów w niebezpiecznych procesach z użyciem niebezpiecznych urządzeń, tym bardziej że państwowe organy nadzoru uzyskują dostęp do informacji o niebezpiecznych procesach, urządzeniach i produktach dopiero wtedy, kiedy proces rozwojowy jest zakończony i system

- czynników podmiotowych, związanych z błędami percepcyjnymi, błędami oszacowań, nieumyślnymi błędami oraz wpływem ludzkich decyzji na pojawianie się zagrożeń.

W centrum uwagi znajdą się najważniejsze wspólne cechy systemów technologicznych i organizacyjnych odpowiedzialne za normalną skłonność takich złożonych systemów do katastrof (Perrow, 1984; 2007) – strukturalną podatność na destabilizacje i zaburzenia, które za sprawą sieci powiązań szybko się rozprzestrzeniają i mogą tworzyć czasoprzestrzennie i społecznie nieograniczone łańcuchy lub kaskady zdarzeń szkodowych. Ze względu na strukturalne cechy systemów energetycznych niebezpieczne zdarzenia i sytuacje, które z powodu tajemniczych synergicznych współoddziaływań w skomplikowanych układach cechujących się złożonością interakcji i sztywnością sprzężeń oraz skłonnością do zachowań samoorganizacyjnych i działania bez człowieka wymykają się poznawczej i operacyjnej kontroli, utrudniając, a czasami nawet uniemożliwiając ochronę przed takimi zdarzeniami lub sytuacjami, należy uznać za coś najzupełniej normalnego.

W toku rozwoju cybernetyki wypracowano narzędzia analityczne zwiększające rozdzielczość obserwacji i opisu systemów pod kątem oddziaływań i konsekwencji ich złożoności oraz zróżnicowania, umożliwiające pomniejszanie tego, co duże, powiększanie tego, co małe i upraszczanie tego, co zbyt złożone (Büscher, 2011, s. 5). Redukcjonizm polegający na próbach zrozumienia, wyjaśniania lub przewidywania zachowań rozpatrywanego systemu poprzez jego elementaryzację (rozłożenie na pierwotne części składowe) bywa czasami użyteczny w przypadku niektórych prostych, elementarnych zagrożeń uwarunkowanych jednoczynnikowo, ale jest kontrproduktywny w przypadku większości zagrożeń złożonych, uwarunkowanych wieloczynnikowo, wynikających z synergii, koincydencji lub kumulacji wielu czynników sprawczych.

produkcyjny jest gotowy do normalnego rozruchu. Ponieważ przedsiębiorstwo poniosło już koszty inwestycyjne, które jak najszybciej chciałoby zamortyzować, zrozumiałe są opory firm przeciwko ewentualnym państwowym zakazom – przedsiębiorstwa żądają zniewalających dowodów potwierdzających niebezpieczeństwo produktu, procesu lub urządzenia, a takich dowodów – zwłaszcza w przypadku innowacyjnych procesów lub produktów – zwykle nie ma. Ze względu na przewlekłość postępowań administracyjnych i rozrost biurokracji organy państwa rzadko są więc w stanie zapobiegać katastrofom. Tę sytuację niezwykle trafnie zdiagnozował Martin Jänicke: „na problemy dnia dzisiejszego wytwarzane przez decyzje inwestycyjne przemysłu z wczoraj bazujące na innowacjach z przedwczoraj organy państwa zareagują jutro, a ich reakcja odniesie skutek pojutrze" (Jänicke, 1979, s. 32 i n.).

Integralnym elementem nowego paradygmatu bezpieczeństwa energetycznego opartego na koncepcji zagrożeń i ryzyk systemowych jest wzmacnianie odporności systemów na zaburzenia i destabilizacje, które w przypadku infrastruktur krytycznych wykluczających możliwość uczenia się na błędach jest z pewnością lepszą strategią bezpieczeństwa niż budowanie wyższych barier ochronnych lub gotowości do reagowania kryzysowego. Strategia bezpieczeństwa bazująca na zarządzaniu odpornością cyberfizycznych systemów energetycznych, rozumianą jako zdolność systemów do utrzymania usług w warunkach stresu lub zaburzeń (Gleich i in., 2017), jest wykonalna i pomaga lepiej przygotować systemy zasilania na nieprzewidywalne niebezpieczne zdarzenia.

Budowanie odporności systemów o krytycznym znaczeniu dla bezpieczeństwa nie może jednak ograniczać się do obowiązku operatorów, których działalności nadano – mniej lub bardziej arbitralnie – status usług kluczowych, związanego z terminowym zgłaszaniem incydentów z zakresu cyberbezpieczeństwa odpowiednim zespołom reagowania. Wydaje się, że Rada i Parlament Europejski zaczynają rozumieć konieczność zmiany kursu w polityce cyberbezpieczeństwa sektora energetycznego, o czym świadczą najnowsze zalecenia w sprawie cyberochrony systemów elektroenergetycznych, uznające za najistotniejsze priorytety:

(1) dostosowanie systemów bezpieczeństwa oraz systemów komunikacji (maszyna–maszyna, system zarządzania energią–system zarządzania dystrybucją) do wymogów czasu rzeczywistego, tj. reagowanie w ciągu milisekund oraz uwzględnianie ograniczeń czasu rzeczywistego w zarządzaniu środkami bezpieczeństwa;

(2) przeciwdziałanie efektom kaskadowym poprzez budowanie odporności, utrzymywanie jednolitych, odpowiadających wymogom krytyczności, standardów cyberbezpieczeństwa dla wszystkich komponentów, wzmacnianie ochrony węzłów krytycznych, wbudowywanie zapór ogniowych ograniczających rozprzestrzenianie się kaskad zaburzeń, utrzymywanie odpowiednich marginesów bezpieczeństwa oraz rozwijanie zdolności do wczesnego rozpoznania, wczesnego ostrzegania i skutecznego reagowania kryzysowego opartego na współpracy wszystkich interesariuszy i efektywnej wymianie informacji;

(3) bezpieczne połączenie starszych technologii i infrastruktur „analogowych" z nowszymi technologiami cyfrowymi oraz systemów obsługiwanych przez człowieka z najnowszymi rozwiązaniami z zakresu Internetu rzeczy,

bazujące przede wszystkim na systemach ochrony przed złośliwymi atakami z poziomu urządzeń lub aplikacji użytkownika, zdolnościach do automatycznego monitorowania i analizowania potencjalnie groźnych zdarzeń (np. nieudanych prób logowania), regularnych analizach ryzyka z podziałem na klasy aktywów, bieżących aktualizacjach sprzętu i oprogramowania do najnowszych wersji lub stosowania dodatkowych barier ochronnych w sytuacjach, gdy takie aktualizacje są niemożliwe (np. w przypadku produktów niewspieranych) oraz uzgadnianiu z dostawcami sprzętu, oprogramowań i usług szczegółowych wymogów cyberbezpieczeństwa i zakresów indywidualnej odpowiedzialności za skutki cyberataków lub incydentów (UE 2019). Zalecenia są z pewnością dobrym krokiem we właściwym kierunku, ale jest to dopiero pierwszy krok.

Obecna koncentracja uwagi organów państwa odpowiedzialnych za cyberbezpieczeństwo na działalności wyselekcjonowanych operatorów usług kluczowych grozi utratą z pola widzenia wielu „słabszych ogniw" wykluczonych z obiegu informacji i pozbawionych wsparcia, które stają się tym samym łatwym celem ataku i źródłem zaburzeń w opisanych wcześniej warunkach, mogą rozprzestrzeniać się wzdłuż łańcuchów sztywnych sprzężeń i powodować ogólnosystemowe awarie i wielkoobszarowe przerwy w zasilaniu krytycznie zagrażające bezpieczeństwu wszystkich systemów istotnych z punktu widzenia stabilności państwa, porządku publicznego oraz przetrwania ludności. Przeciwdziałanie takim krytycznym sytuacjom wymaga budowania partnerstwa dla cyberbezpieczeństwa – rozwiązań, które zachęcą wszystkie podmioty wchodzące w skład systemu elektroenergetycznego do zacieśnienia współpracy na rzecz bezpieczeństwa poprzez dzielenie się doświadczeniem i informacjami o zidentyfikowanych niebezpiecznych incydentach, o sprawdzonych, skutecznych sposobach reagowania („obsługi") i rozpoznanych mechanizmach powstawania zagrożeń i ryzyk systemowych – współpracy niezbędnej pomimo częstej rozbieżności, a nawet sprzeczności interesów tych podmiotów. Jeśli takie działania wymagają wspólnego zaplecza badawczego lub organizacyjnego, np. w formie ISAC (*Information Sharing and Analysis Center*), należy rozważyć ich subsydiowanie ze środków publicznych (Masera, 2010; Moore, 2010; Orwat, 2011, s. 51), niezależnie od tego, czy takie usługi będą miały charakter dobra publicznego, czy będą realizowane z wykorzystaniem komercyjnych centrów usług wspólnych.

Podsumowanie

Analizy zagrożeń, oceny podatności i szacunki dotyczące ryzyka ograniczające się jedynie do niezawodności pojedynczych komponentów systemu zaopatrzenia w energię elektryczną i zagrożeń elementarnych wydają się niewystarczającym standardem zarządzania bezpieczeństwem w przypadku infrastruktur o tak krytycznym statusie, który czyni całkowicie nieprzydatnymi koncepcje bezpieczeństwa bazujące na reagowaniu kryzysowym zorientowanym na skutki oraz uczeniu się metodą prób i błędów. Wysoka stawka bezpieczeństwa w przypadku infrastruktur elektroenergetycznych wymaga aktywnego, prewencyjnego podejścia do bezpieczeństwa – podejścia zorientowanego na przyczyny, bazującego na przezorności i uwzględniającego całościową, komplementarną perspektywę systemową w całej złożoności wzajemnych zależności, sprzężeń, krzyżowych interakcji i synergii między komponentami technologicznymi, środowiskiem przyrodniczym, strukturami społeczno-organizacyjnymi, determinizmami ekonomicznymi oraz działaniami regulacyjno-administracyjnymi. Takie szerokokątne spojrzenie na bezpieczeństwo pozwala zrozumieć przyczyny dysfunkcyjnych zachowań złożonych systemów, projektować bardziej adekwatne marginesy bezpieczeństwa, wbudowywać skuteczne mechanizmy ochrony, wcześnie rozpoznawać „słabe sygnały" zbliżających się zaburzeń i przygotowywać bardziej adekwatne scenariusze reagowania.

Bibliografia

Büscher, Ch. (2011). Systemic Risk as a Perspective for Interdisciplinary Risk Research. Introduction to the Thematic Focus. *Technikfolgenabschätzung – Theorie und Praxis, 20*(3), 4–12. DOI: https://doi.org/10.14512/tatup.20.3.4.

Cleeland, B. (2011). Contributing Factors to the Emergence of Systemic Risks. *Technikfolgenabschätzung – Theorie und Praxis, 20*(3), 13–21. DOI: https://doi.org/10.14512/tatup.20.3.13.

Dragos Inc. (2017). *Crashoverride. Analyzing of the Threat to Electric Grid Operations*. Dragos.com (version 2.20170613). Dostęp: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf [20.02.2020].

Dynes, S., Goetz, E., Freeman, M. (2008). Cyber Security: Are Economic Incentives Adequate? W: F. Goetz, S. Shenoi (Eds.), *Critical Infrastructure Protection* (International Federation for Information Processing, Vol. 253, pp. 15–27). Boston-New York: Springer Science + Businnes Media. DOI: https://doi.org/10.1007/978-0-387-75462-8_2.

Flick, T., Morehouse, J. (2011). *Securing the Smart Grid: Next Generation Power Grid Security*. Amsterdam, Boston, Heilderberg: Syngress/Elsevier Inc.

Gleich, A. von, Gößling-Reisemann, S., Stührmann, S., Woizeschke, P., Lutz-Kunisch, B. (2010). Resilienz als Leitkonzept. Vulnerabilitätalsanalytische Kategorie. W: K. Fichter, A. von Gleich, R. Pfriem, B. Siebenhüner (Eds.), *Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien*. (Berlichte Heft 1 'nordwest2050', pp. 13–49). Bremen-Oldenburg: Projektkonsortium nordwest2050. Dostęp: https://digital.zlb.de/viewer/rest/image/15348349/Bericht1_Theoriestudie.pdf/full/max/0/Bericht1_Theoriestudie.pdf [10.03.2020].

Hacken, H. (1982). *Synergetik. Eine Einfürung*. Berlin–Heidelberg–New York: Springer Verlag.

Helbing, D. (2010). *Systemic Risks in Society and Economics*. Zurich: International Risk Governance Council. DOI: http://doi.org/10.2139/ssrn.2413205.

Hellström, T. (2007). Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework. *Safety Science*, *45*(3), 415–430. DOI: https://doi.org/10.1016/j.ssci.2006.07.007.

Hellström, T. (2009). New Vistas for Technology and Risk Assessment? The OECD Programme on Emerging Systemic Risks and beyond. *Technology in Society, 31*(3), 325–331. DOI: https://doi.org/10.1016/j.techsoc.2009.06.002.

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

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

Kaufman, G.G., Scott, K.E. (2003). What is Systemic Risk, and do Bank Regulators Retardor Contribute to it? *The Independent Review*, *7*(3), 371–391. Dostęp: https://www.independent.org/pdf/tir/tir_07_3_scott.pdf [20.02.2020].

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (2017). Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. Dostęp: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-przyjeta-przez-rzad [10.02.2020].

Magnitskii, N.A. (2018). Bifurcation Theory of Dynamical Chaos. W: K.A.M. Al Naimee (Ed.), *Chaos Theory*. IntechOpen. DOI: http://doi.org/10.5772/intechopen.70987.

Masera, M. (2010). Governance: How to Deal with ICT Security in the Power Infrastructure? W: Z. Lukszo, G. Deconinck, M.P.C. Weijnen (Eds.), *Securing Electricity Supply in the Cyber Age. Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure* (Topics in Safety, Risk, Reliability and Quality, Vol. 15, pp. 111–127). Dordrecht: Springer. DOI: https://doi.org/10.1007/978-90-481-3594-3_6.

Mayntz, R. (2009). The Changing Governance of Large Technical Infrastructure Systems. W: R. Mayntz (ed.), *Über Governance. Institutionen und Prozesse politischer Regelung* (Schriften aus dem Max-Planck-Institut für Gesellschaftforschung, Band 62, s. 121–150). Frankfurt am Main: Campus Verlag.

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

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, *3*(3–4), 103–117. DOI: https://doi.org/10.1016/j.ijcip.2010.10.002.

NIST [National Institute of Standards and Technology Interagency]. (2014). *Guidelines for smart grid cybersecurity* (Vol. 1: Smart Grid cybersecurity strategy, architecture, and high-levelrequirements, Report 7628, Rev. 1). Gaithersburg: National Institute of Standards and Technology, U.S. Department of Commerce. DOI: https://doi.org/10.6028/NIST.IR.7628r1.

Orwat, C. (2011). Systemic Risks in the Electric Power Infrastructure? *Technikfolgenabschätzung – Theorie und Praxis, 20*(3) , 47-55. DOI: https://doi.org/10.14512/tatup.20.3.47.

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. DOI: https://doi.org/10.1111/j.1468-5973.1994.tb00046.x.

Perrow, Ch. (2007). *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters*. Princeton: Princeton University Press.

Renn, O., Keil, F. (2008). Systemische Risiken: Versuch einer Charakterisierung. *GAIA – Ecological Perspectives for Science and Society, 17*(4), 349–354. DOI: https://doi.org/10.14512/gaia.17.4.9.

Rossebo, J., Wolthuis, R., Fransen, F., Bjorkman, G., Medeiros, N. (2017). An Enhanced Risk-Assessment Methodology for Smart Grids. *Computer*, *50*(4), 62–71. DOI: https://doi.org/10.1109/MC.2017.106.

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

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. DOI: https://doi.org/10.1038/nature08227.

Sobczak, B. (2019, May 6). Experts Assess Damage After First Cyberattack On U.S. Grid. *E&E News*. Dostęp: https://www.eenews.net/stories/1060281821 [20.02.2020].

Styczynski, J., Beach-Westmoreland, N. (2019). *When The Lights Went Out. A Comprehensive Review of The 2015 Attacks On Ukrainian Critical Infrastructure.* Booz Allen Hamilton Inc. Dostęp: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf [20.02.2020].

Taleb, N.N. (2014). *Czarny łabędź. O skutkach nieprzewidywalnych zdarzeń* (tłum. O. Siara, T. Kasprowicz). Warszawa: Kurhaus Publishing Kurhaus Media.

Tervo, H., Wiander, T. (2010). Sweet Dreams and Rude Awakening – Critical Infrastructure's Focal IT-related Incidents. W: *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS-43)*. IEEE Computer Society. DOI: https://doi.org/10.1109/HICSS.2010.358.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M. P. 2019, poz. 1037).

Unia Europejska [UE]. (2019). *Zalecenie Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym* (nr C (2019) 2400) (Dz. Urz. Unii Europejskiej L 96/50 z 5.04.2019).

United States Government Accountability Office [US GAO]. (2011). *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*. (Report to Congressional Requesters No. GAO-11-117). Washington: United States Government Accountability Office. Dostęp: https://www.gao.gov/new.items/d11117.pdf [10.02.2020].

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560 ze zm.).

Vleuten van der, E., Lagendijk, V. (2010). Interpreting Transnational Infrastructure Vulnerability: European Blackout and the Historical Dynamics of Transnational Electricity Governance. *Energy Policy*, *38*(4), 2053–2062. DOI: https://doi.org/10.1016/j.enpol.2009.11.030.

Wagner-Döbler, R. (1989). *Das Dilemma der Technikkontrolle. Wirkungen der Technikentwicklung und Probleme der Technologiepolitik*. Berlin: Edition Sigma Verlag.

Wang, X., Chen, G. (2012). A chaotic system with only one stable equilibrium. *Communications in Nonlinear Science and Numerical Simulation*, *17*(3), 1264–1272. DOI: https://doi.org/10.1016/j.cnsns.2011.07.017.