Tomasz Długosz*

Nowa koncepcja polikryzysów w świetle dyrektywy 2022/2557 w sprawie odporności podmiotów krytycznych (dyrektywy CER)

Spis treści

I. Wprowadzenie
II. Pojęcie „polikryzysów”
III. Dyrektywa CER w sprawie odporności podmiotów krytycznych
IV. Wnioski

Streszczenie

Autor zajmuje się koncepcją polikryzysów, która może znaleźć zastosowanie przy zwiększaniu odporności tzw. podmiotów krytycznych i ochronie infrastruktury krytycznej. Dochodzi do wniosku, że jest to koncepcja, która zwraca uwagę na pewne ponadsystemowe zagrożenia i na reaktywność systemów społecznych na te zagrożenia. Jego zdaniem dyrektywa CER w sprawie odporności podmiotów krytycznych nakazuje w szerokim zakresie uwzględniać współzależności międzysystemowe, tworząc pole do wykorzystania koncepcji polikryzysów. Autor wyraża obawę, że możliwe uwikłanie ideologiczne koncepcji polikryzysów będzie prowadzić do nieproporcjonalnej ochrony infrastruktury krytycznej w stosunku do prawdziwych zagrożeń.

Słowa kluczowe: polikryzysy; infrastruktura krytyczna; podmioty krytyczne; usługi kluczowe; zarządzenie kryzysowe; sektor energetyki.

JEL: K32

I. Wprowadzenie

W grudniu 2022 r. przyjęto nową, dotyczącą ochrony infrastruktury krytycznej, dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (the Critical Entities Resilience Directive; dalej: dyrektywa CER)[1]. Prace nad nową dyrektywą trwały od dawna. W grudniu 2019 r. Komisja Europejska opublikowała projekt dyrektywy unijnej w sprawie odporności podmiotów krytycznych, który prezentował zmienione podejście do ochrony infrastruktury krytycznej, nawiązując

* Doktor habilitowany, adiunkt w Katedrze Publicznego Prawa Gospodarczego i Polityki Gospodarczej Uniwersytetu Jagiellońskiego w Krakowie; praktykujący radca prawny, specjalizuje się w publicznym prawie gospodarczym, prawie energetycznym i prawie sektorów infrastrukturalnych, członek Rady Naukowej przy Rzeczniku Małych i Średnich Przedsiębiorców. ORCID: 0000-0003-3174-1568; e-mail: t.dlugosz@uj.edu.pl.

Edition of that article was financed under Agreement Nr RCN/SP/0326/2021/1 with funds from the Ministry of Education and Science, allocated to the “Rozwoj czasopism naukowych” programme.

[1] Dz. U. UE. L. z 2022 r. Nr 333, str. 164.

© 2023 Authors. This is an open access article distributed under the Creative Commons BY 4.0 license (https://creativecommons.org/licenses/by/4.0/)

pojęciami i metodą regulacji do dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: dyrektywa NIS)[2]. Projekt zaprezentowano po przeprowadzeniu w 2019 r. pierwszej oceny dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (the European Critical Infrastructure Directive; dalej: dyrektywa ECI)[3]. Wtedy uznano, że zmienił się „kontekst" funkcjonowania infrastruktury krytycznej, że są nowe wyzwania, którym trzeba sprostać, w związku z rozwojem gospodarczym, społecznym, technologicznych, ale również zmianami środowiskowymi. Uznano, że dotychczasowy zakres ochrony infrastruktury krytycznej, który ogranicza się do sektorów energii i transportu jest niewystarczający, ponieważ nie pozwala na właściwe uwzględnienie międzysektorowych współzależności. Zdecydowano się na zmianę podejścia z myślą o zapewnieniu: lepszego uwzględniania różnego rodzaju ryzyk, lepszego zdefiniowania i uspójnienia ról i obowiązków podmiotów krytycznych. Dodatkowo Komisja ustaliła, że dyrektywa ECI została wdrożona nierównomierne w państwach członkowskich UE i że jej słabością jest to, że za punkt wyjścia przyjmuje się krajową infrastrukturę krytyczną, ponieważ utrudnia to zidentyfikowanie infrastruktury krytycznej o paneuropejskim znaczeniu ogólnoeuropejski, której przykładem są: europejski system nawigacyjny Galileo, system bezpieczeństwa powietrznej żeglugi Eurocontrol, a także połączone europejskie sieci przesyłu energii elektrycznej oraz gazu ziemnego[4].

Nowa dyrektywa CER zastąpi dyrektywę ECI i znacznie rozszerza zakres ochrony infrastruktury krytycznej, wprowadzając nową metodę jej ochrony. Założono w niej zwiększenie odporności pewnych kategorii podmiotów, które działają w wyróżnionych w dyrektywie sektorach, czyli w pewnych obszarach funkcjonowania społeczeństw, np. energii, transportu, bankowości administracji publicznej. Państwa członkowskie mają identyfikować tzw. podmioty krytyczne, które świadczą tzw. usługi kluczowe, do których z kolei zalicza się takie usługi, które odgrywają podstawową rolę w utrzymaniu niezbędnych funkcji społecznych, w tym niezbędnej działalności gospodarczej oraz funkcji związanych ze zdrowiem i bezpieczeństwem publicznym, ochroną środowiska (zob. definicję usługi kluczowej z art. 1 pkt 5 dyrektywy CER). Nowe prawo opiera się na idei zwiększania odporności podmiotów krytycznych w warunkach: współzależności między usługami kluczowymi, współzależności sektorów infrastruktury krytycznej (systemów społecznych, w ramach których funkcjonalnie organizuje się działania dla zaspokajania rozmaitych potrzeb społecznych[5]) oraz ogólnej zależności gospodarczej w ramach UE. W związku z tym ostatnim stwierdza się: „Współzależności te oznaczają, że jakiekolwiek zakłócenie usług kluczowych, nawet takie, które początkowo ogranicza się do jednego podmiotu lub jednego sektora, może wywołać efekt kaskadowy na szerszą skalę, potencjalnie prowadzący do daleko idącego i długoterminowego negatywnego wpływu na świadczenie usług na rynku wewnętrznym. Poważne kryzysy, takie jak pandemia COVID-19,

[2] Dz. U. UE. L. z 2016 r. Nr 194, str. 1.

[3] Dz. U. UE. L. z 2008 r. Nr 345, str. 75.

[4] Zob. Dokument roboczy służb Komisji z 23.07.2019 r. pt. Ocena dyrektywy Rady 2008/114 w sprawie identyfikacji i wyznaczania europejskiej infrastruktury krytycznej i oceny konieczności poprawy ochrony infrastruktury krytycznej, SWD(2019) 308 wersja ostateczna. Pozyskano z: https://home-affairs.ec.europa.eu/index_pl

[5] Takie rozumienie systemu społecznego koresponduje z rozumieniem społeczeństwa w tzw. ujęciu systemowym, zgodnie z którym społeczeństwo jest układem powiązanych funkcji, ról pozycji (statusów) (zob. Sztompka, 2002, s. 30–33).

uwidoczniają podatność naszych w coraz większym stopniu współzależnych społeczeństw na ryzyko o dużym wpływie i niskim prawdopodobieństwie" (motyw 5 dyrektywy CER).

Jest rzeczą ogólnie wiadomą, że postępująca urbanizacja zwiększa zależność ludzi od coraz bardziej skomplikowanej infrastruktury technicznej czy też od stechnicyzowanej infrastruktury społecznej, którą od niedawna zaczęto nazywać „krytyczną". Infrastruktura krytyczna ma szczególną zdolność wywoływania sytuacji kryzysowych, czyli do kumulowania zagrożeń, które ostatecznie mogą doprowadzić do kryzysu, czyli utraty stanu normalności i zakłócenia zasadniczych cech organizacji, układu czy systemu (stabilności, równowagi, sterowalności, efektywności itd.) (za: Więcek, 2010, s. 28)[6]. Dysfunkcja infrastruktury krytycznej często skutkuje efektem kaskadowym i przeniesieniem skutków na inne systemy czy sektory gospodarki[7]. Również powiązania między systemami infrastruktury krytycznej są dostrzegane od dawna, przy czym za wyjątkowo „krytyczny" uchodził zawsze sektor energetyczny, ponieważ wszystkie systemy zaspokajania podstawowych potrzeb społecznych są uzależnione od nieprzerwanych dostaw energii elektrycznej (Lauge, Hernantes i Sarriegi, 2015, s. 16–23). Natomiast ostatnio coraz większą wagę przywiązuje się do sieci informacyjnych czy systemów informatycznych. Zdano sobie sprawę, że transport, energia, zdrowie, telekomunikacja, finanse, bezpieczeństwo, obrona, a nawet przebieg tzw. procesów demokratycznych zależą w dzisiejszych społeczeństwach od takich sieci czy systemów, a cała gospodarka jest coraz bardziej powiązana w środowisku informatycznym[8]. Z pola widzenia nie traci się zarazem „krytycznego" uzależnienia samych sieci i systemów informacyjnych od zaopatrzenia w energię elektryczną[9]. Związek infrastruktury krytycznej z systemami informatycznymi przejawił się w tym, iż zarówno pojęcia, jak i metodę regulacji nowej dyrektywy CER wzorowano na rozwiązaniach wcześniej wprowadzonej dyrektywy 2016/1148 w sprawie cyberbezpieczeństwa (dalej: dyrektywa NIS). Dyrektywę CER wydano zaś wraz z nową dyrektywą unijną 2022/2555 w sprawie cyberbezpieczeństwa (tzw. dyrektywą NIS2)[10] oraz nowym prawem o cyfrowej odporności operacyjnej sektora finansowego (The Digital Operational Resilience Act, DORA)[11]. Dodać można, że tak strategia bezpieczeństwa UE na lata 2020–2025, jak i nowy program zwalczania terroryzmu z 2020 r., które przyjęła Komisja Europejska, podkreśliły znaczenie odporności infrastruktury krytycznej wobec zagrożeń cyfrowych[12]. Ochrona infrastruktury krytycznej została również ujęta w przedstawionej w grudniu 2020 r. unijnej strategii w cyberbezpieczeństwa[13].

[6] Kryzys ma cechować się utratą kontroli nad zdarzeniami, przy zwiększającej się niepewności i stopniu ryzyka, a także możliwością zaistnienia zmiany systemowej (nowego układu, struktur i funkcji w organizacji) (więcej Zieliński, 2017, s. 49–51).

[7] K. Szwarc mówi o „relacjach transsektorowych pomiędzy systemami", natomiast infrastrukturę krytyczną w ogóle charakteryzuje pojęciem „współzależności" (zob. Szwarc, 2016, s. 154). Z kolei N. Roubini, S. Mihm zauważają: „…kryzysy mają wiele podobieństw do pandemii: rozpoczynają się wybuchem choroby, która następnie rozprzestrzenia się coraz dalej od swojego epicentrum" (Roubini i Mihm, 2011, s. 27).

[8] W tym kontekście wyróżnia się fizyczne oraz informacyjne powiązania między sektorami (zob. np. Nowak, 2018, s. 175).

[9] Strategia UE w zakresie bezpieczeństwa cybernetycznego na dekadę cyfrową, JOIN(2020) 18 final, s. 1–2.

[10] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

[11] Na tzw. pakiet DORA składa się: dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2556 z dnia 14 grudnia 2022 r. w sprawie zmiany dyrektyw 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego (Dz. U. UE. L. z 2022 r. Nr 333, str. 153); rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. U. UE. L. z 2022 r. Nr 333, str. 1).

[12] Zob. Komunikat prasowy Komisji Europejskiej z 24 lipca 2020: EU Security Union Strategy: connecting the dots in a new security ecosystem. Pozyskano z: file:///C:/Users/Tomasz/Downloads/EU_Security_Union_Strategy__connecting_the_dots_in_a_new_security_ecosystem.pdf. Zob. też Kozioł, 2021.

[13] W grudniu 2020 r. Komisja Europejska i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili dokument pt. „Strategia UE w zakresie bezpieczeństwa cybernetycznego na dekadę cyfrową" (The EU's Cybersecurity Strategy for the Digital Decade), JOIN(2020) 18 final), którego głównym celem ma być ochrona „otwartego i globalnego internetu".

W przypadku infrastruktury krytycznej dysfunkcje, awarie czy inne zdarzenia destrukcyjne wywołują zagrożenia dla podstawowych funkcji społeczeństw i państw, czyli infrastruktura krytyczna wywołuje szczególne ryzyka. Ryzyko mierzy się prawdopodobieństwem wystąpienia zagrożenia oraz skutkami (konsekwencjami) wystąpienia zagrożeń, przy czym w przypadku infrastruktury krytyczniej wyżej wskazane zależności czy współzależności zwiększają zarówno skutki negatywnych zdarzeń (zagrożeń), jak i prawdopodobieństwo ich wystąpienia[14]. Powiązania między elementami i systemami infrastruktury krytycznej, a na gruncie nowej dyrektywy CER systemów funkcjonowania usług kluczowych, których niezbędnym elementem są podsystemy infrastruktury krytycznej[15] powodują ryzyko systemowe, a więc prawdopodobieństwa wystąpienia dysfunkcji całych układów powiązanych ze sobą elementów[16]. Zauważyć przy tym można, że w nowej dyrektywie CER nie eksponuje się ryzyka naruszenia podstawowych funkcji państwa, ale ryzyko naruszenia niezbędnych funkcji społecznych (zob. art. 2 pkt 5 dyrektywy CER).

Powyższa specyfika infrastruktury krytycznej oraz za jej pomocą świadczonych usług wpływa na sposób, w jaki analizuje się zagrożenia z nią związane. Wymusza ona systemowe analizy bezpieczeństwa, które – jak się przyjmuje w nauce – mają cechować się: ujmowaniem zjawisk, zabezpieczeń i obiektów zagrożeń jako systemu w całej jego złożoności, uwzględnianiem ogółu warunków, bliższego i dalszego otoczenia sytemu, szukaniem przyczyn, przekształceń wewnętrznym systemu, jego zdolności samosterowania, koordynacji i adaptacji do otoczenia[17]. W tych badaniach bierze się pod uwagę rozmaite zagrożenia i skutki: dla ludzi, mienia, ale także środowiska naturalnego i dziedzictwa kulturowego. W tym kontekście można zauważyć, że ostatnio w rozważaniach nad bezpieczeństwem i zarządzaniem ryzykiem pojawiła się koncepcja „polikryzysów". O polikryzysach wielokrotnie mówił przewodniczący Komisji Europejskiej Jean-Claude Juncker, gdy jeszcze przed wybuchem pandemii COVID-19 w 2018 r. opisywał sytuację Unii Europejskiej. Miał on wtedy na myśli wyjątkowe trudności, z jakimi przyszło się zmierzyć UE w swojej historii, wysyp trudnych sytuacji związanych z tzw. kryzysem finansowym, tzw. kryzysem migracyjnym oraz brexitem[18]. Obecnie o polikryzysach mówi się jednak również na gruncie nauk społecznych. Rozważmy, na czym właściwie polega ta koncepcja i czy nowa dyrektywa CER stwarza pole do jej wdrożenia czy rozwijania. Dyrektywa CER znaczenie rozszerza zakres ochrony infrastruktury krytycznej i zwraca uwagę na współzależności infrastrukturalne, sektorowe oraz międzysektorowe, a w związku z tym niejako zachęca do posługiwania się koncepcją polikryzysów. Koncepcja polikryzysów nie wydaje się być jednak czymś zupełnie nowym w badaniach nad rodzajami ryzyka. Natomiast dostrzec można pewne uwikłanie ideologiczne tej koncepcji, które może być źródłem obaw. Można mieć obawy, że będzie ona prowadzić do zastosowania nieproporcjonalnej względem zagrożeń ochrony bezpieczeństwa, co na płaszczyźnie prawnej przełoży się na zbyt daleko idące obowiązki podmiotów krytycznych.

[14] Narodowy Program Ochrony Infrastruktury Krytycznej 2020 przyjęty przez Radę Ministrów, s. 290. Pozyskano z: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej

[15] Zob. definicję infrastruktury krytycznej z art. 2 pkt. 4 dyrektywy CER.

[16] Wpływowi amerykańscy naukowcy George G. Kaufman i Keneneth E. Scott definiują ryzyko systemowe jako: *…the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, [as] evidenced by co-movements (correlations) among most or all parts* (Kaufman i Scott, 2003, s. 371–391).

[17] Tak P. Sienkiewicz, H. Świeboda, którzy mówią nawet o zmianie paradygmatu w badaniach nad zjawiskiem bezpieczeństwa i przejściu od holistyczno-systemowego ujęcia (2016, s. 50, 67). Na systemowe podjęcie problematyki ryzyka w ustawie z dn. 26.04.2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. 2023, poz. 122) zwraca z kolei uwagę R. Wróbel (2019, s. 61 i n.).

[18] Zob. przemówienie C. Junckera w dniu 21.06.2016 r. na dorocznym walnym zgromadzeniu Greckiej Federacji Przedsiębiorstw (SEV). Pozyskano z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_16_2293

II. Pojęcie „polikryzysu”

Wydaje się, że pojęcie „polikryzysu” wprowadzili do dyskursu znany francuski filozof i socjolog Edgar Morin oraz Anne Brigitte Kern w książce pt. „Ziemia – ojczyzna” z 1998 r., w której mówią oni o przeplatających się, nakładających kryzysach, które dotykają ludzkość. Autorzy ci zakładają, że mamy do czynienia z „inter-retro-akcjami” między różnymi problemami, różnymi kryzysami, zagrożeniami, odnoszącymi się do zdrowia, środowiska, sposobów życia, rozwoju, z problemami demograficznymi i cywilizacyjnymi, a w konsekwencji, że problemem są nie pojedyncze zagrożenie, lecz wiele problemów, kompleksowy ich związek – kompleks problemów, antagonizmów, kryzysów, niekontrolowanych procesów (polikryzys). Środkiem zaradczym ma być myślenie „zekologizowane”, które, zamiast izolować badany przedmiot, analizuje go w jego relacji „auto-eko-organizującej” z jego środowiskiem kulturowym, społecznym, ekonomicznym, politycznym i przyrodniczym (Morin i Kern, 1998, s. 125–126, 219). Koncepcja ta początkowo nie wzbudziła jakiegoś szczególnego zainteresowania, ale w 2013 r. południowoafrykański socjolog i teoretyk zrównoważonej transformacji Mark Swilling zaczął nazywać polikryzysem globalną sytuację związaną ze zmianami klimatu, rosnącymi nierównościami i kryzysami finansowymi. Zdefiniował on polikryzys jako „zagnieżdżony zestaw globalnie interaktywnych kryzysów społeczno-ekonomicznych, ekologicznych i kulturowo-instytucjonalnych, które wymykają się redukcji do jednej przyczyny” (za: Lawrence, Janzwood i Homer-Dixon, 2022). Mark Swilling podkreślał równoczesność kryzysów i powiązania między nimi, w sposób wyraźny zwrócił uwagę, że te powiązania tworzą złożone interakcje, które zwielokrotniają całkowity wpływ kryzysów na rzeczywistość. Z czasem terminem tym zaczęli posługiwać się również politycy, w tym również politycy unijni. Wspomniano już, że w 2016 r. ówczesny przewodniczący Komisji Europejskiej Jean-Claude Juncker mówił o polikryzysie, mając na myśl splot największych kryzysów o charakterze gospodarczym, finansowym i społecznym, z jakim borykała się Europa od czasów drugiej wojny światowej. W 2018 r. ogłosił on nawet, iż UE wyszła z „polikryzysu”, ponieważ – jak to wyjaśnił – „skończył się okres przechodzenia UE od kryzysu do kryzysu bez przebudzenia”[19]. W końcu polikryzysami zaczęli zajmować się naukowcy i analitycy. Gdy w 2019 r. naukowcy z kilku wpływowych ośrodków naukowych Europy mówili o politycznych problemach integracji unijnej („politycznych pułapkach”), to mówili ogólnie o polikryzysie, mając na myśli jednoczesne wystąpienie w Europie kryzysu zadłużeniowego państw południowej Europy, kryzysu uchodźczego, zapoczątkowanego przez wojnę domową w Syrii, brexit oraz wzrost skrajnie prawicowego autorytaryzmu (Zeitlina, Nicoliaand i Laffan, 2019, s. 963–976). W raporcie światowym z 2021 r., przygotowanym pod egidą UNESCO, pt. „Global Risks Perceptions Report 2021” nie ma jeszcze mowy o polikryzysie, jednak naukowcy z różnych stron świata dochodzą w nim do wniosku doniosłego z punktu widzenia nowej koncepcji, że zrozumienie wzajemnych powiązań między globalnymi rodzajami ryzyka, ich współzależności i sprzężeń zwrotnych jest kluczowym elementem poprawy ocen ryzyka i projektowania planów łagodzenia skutków kryzysów[20]. Na kanwie tych rozważań o globalnych zagrożeniach zaczęto posługiwać się pojęciem „polikryzysu”.

[19] Zob. przemówienie J.C. Junckera w dniu 22.02.2018 r. podczas sesji plenarnej otwierającej laboratorium Pomysłów 2018 pt. „Europa – powrót na właściwe tory” w Centrum Studiów nad Polityką Europejską. Pozyskano z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_1121

[20] *Understanding the interconnections between global risks – including building awareness of interdependencies and feedback loops – and which groupings of risk present the greatest threats, is thus a key part of improving risk assessment and discussing potential solutions, since strong interconnections need to be taken into account in mitigation planning* (Future Earth, Sustainability in the Digital Age, and International Science Council, 2021, s. 17).

Określenie to pojawiło się w raporcie Światowego Forum Ekonomicznego z 2023 r., w którym przez polikryzys rozumie się zbiór (klaster) powiązanych globalnych zagrożeń o nakładających się skutkach w taki sposób, iż ogólny skutek wykracza poza sumę skutków poszczególnych zagrożeń (Word Economic Forum, 2023, s. 57).

Wydaje się, że pośród naukowców jednym z najgorętszych orędowników nowego pojęcia i w związku z tym nowego kierunku badań jest Adam Tooze – historyk z Uniwersytetu Columbia w Stanach Zjednoczonych. Jego zdaniem świat jest pełen polikryzysów, które polegają na nakładaniu się efektów sytuacji kryzysowych. Naukowiec wyjaśnia: „w polikryzysie wstrząsy są różne, ale oddziałują na siebie tak, że całość jest nawet czymś więcej niż sumą części" (Tooze, 2022a). Po przedstawieniu skomplikowanego układu „napięć" w świecie (*stresses*) społecznych, gospodarczych, politycznych naukowiec ten wyjaśnił, że polikryzys to nie sytuacja, w której trzeba się mierzyć z wieloma kryzysami, ale sytuacja polegająca niejako na odwzorowaniu ryzyk, w których wszystkie te kryzysy stają się bardziej niebezpieczne[21]. Mówiąc o kryzysach, autor ten ma przy tym na myśli pewne subiektywnie wyróżnione zagrożenia, które mają potencjał do zmiany zasadniczych funkcji systemowych. Idąc dalej w tego rodzaju rozważaniach, badacze z kanadyjskiego centrum badawczego Cascade Institute – Michael Lawrence, Scott Janzwood i Thomas Homer-Dixon – przedstawili w 2022 r. prawdopodobnie najbardziej dotychczas rozwiniętą koncepcję polikryzysu, która według nich ma potencjał zapewnienia „niezbędnych i produktywnych ram" zrozumienia oraz rozwiązywania głównych problemów dzisiejszej ludzkości.

Michael Lawrence, Scott Janzwood i Thomas Homer-Dixon przez polikryzys rozumieją „uwikłanie przyczynowe" kryzysów (*causal entanglement of crises*), które pochodzą czy rozgrywają się w różnych miejscach oraz systemach. Za pomocą tego pojęcia chcą oni badać dynamikę i skutki połączonych zagrożeń czy sytuacji kryzysowych (*combined crises*), wychodząc z założenia, o którym już była mowa wyżej, że zagrożenia występujące w tym samym czasie, ale w odległych miejscach, oddziałują na siebie, wywołując szkody większe, niż gdyby te zagrożenia rozpatrywać w odosobnieniu. Dla tych badaczy zajmowanie się polikryzysami ma odgrywać podobną rolę do badania ryzyka systemowego, lecz różnica ma polegać na dostrzeganiu zagrożeń w innym miejscu. Koncepcje zarówno ryzyka systemowego, jak i polikryzysu wychodzą z obserwacji złożoności systemów społecznych i zakładają możliwość rozprzestrzeniania się problemów w ramach danego systemu i poza nim. Badanie różnych rodzajów ryzyk, w tym ryzyk systemowych, ma jednak dotyczyć możliwości wystąpienia szkód, negatywnych zdarzeń w przyszłości, a badanie polikryzysów ma wiązać się z odkrywaniem łańcuchów zdarzeń, w których już realizują się pewne zagrożenia czy też pewne niebezpieczeństwa już się aktywowały. Polikryzysy mają się przy tym odnosić do zagrożeń, które realizują się jednocześnie w wielu systemach społecznych i oddziałują na siebie, gdyż koncepcja polikryzysu ma służyć opisowi interakcji kryzysów pochodzących z różnych systemów. Na koniec zgodnie z nową koncepcją badanie polikryzysów ma koncentrować się na cechach samych systemów społecznych, które wywołują dodatkowe ryzyka i czyniąc je podatnymi na zagrożenia, wpływają na dynamikę procesów[22]. Mówiąc inaczej,

[21] *A polycrisis is not just a situation where you face multiple crises. It is a situation like that mapped in the risk matrix, where the whole is even more dangerous than the sum of the parts* (Tooze, 2022).

[22] *The polycrisis concept focusses on the organization of the system in such a way that the triggering event spreads in a rapid cascade of additional harms through this causal architecture* (Lawrence, Janzwood i Homer-Dixon, 2022, s. 7).

podejście polikryzysowe ma zwracać uwagę na właściwości zaangażowanych systemów, które są źródłem ponadsystemowych zagrożeń. Badanie ryzyka systemowego ma koncentrować się na możliwych scenariuszach rozwoju wydarzeń, natomiast badanie polikryzysów ma polegać na analizie zagrożeń w ramach „architektury" systemów, w których stwierdzamy zagrożenia[23]. Należy dodać, że omawiana koncepcja ma służyć analizie rozwoju zagrożeń o charakterze globalnym, które wpływają na planetę i ludzkość. Autorzy prezentowanej koncepcji są przy tym świadomi arbitralności wyboru „globalnych zagrożeń", niemniej jednak postulują odróżnienie polikryzysów występujących w skali globalnej od tych, które rozgrywają się w skali regionalnej, kontynentalnej, krajowej czy lokalnej (Lawrence, Janzwood i Homer-Dixon, 2022, s. 4).

Wydaje się, że w gruncie rzeczy wyróżnianie polikryzysów służy zwróceniu uwagi na pewne szczególne zagrożenia i ryzyko, których doniosłość jest ogólnoświatowa. Służy ona w istocie badaniu w kontekście tego rodzaju zagrożeń i ryzyka systemowego sprzężeń systemów społecznych[24]. Zwraca ona uwagę na sprzężenia tych systemów, które dodatkowo pogarszają sytuację, tzn. wpływają na skalę zagrożeń oraz dynamikę ich rozwoju. Nie wydaje się, by ta koncepcja wprowadzała jakąś gruntowną zmianę. W stosowanych ocenach ryzykiem uwzględnia się tzw. ryzyko zewnętrzne, możliwości wpływania na siebie zagrożeń pochodzących z różnych systemów czy sektorów. Dla tej koncepcji charakterystyczne jest może przypisanie szczególnej roli pewnych zagrożeniom, które traktuje się jako ogólnosystemowe, oraz identyfikowanie pewnych szczególnych ryzyk w związku z dostrzeganiem związków między różnymi systemami społecznymi i procesami, które w nich mają miejsce. Koncepcja ta może też wiązać się z uznaniem pewnej szczególnej reaktywności systemów społecznych na pewne bodźce, tzn. z dostrzeganiem wyjątkowego stosunku reakcji systemów społecznych na pewne bodźce. W świetle tych elementów nowej koncepcji można mieć wątpliwości czy nie doprowadzi ona do pewnego „zideologizowania" badań nad zagrożeniami i rodzajami ryzyka z nimi związanymi, czy nie zostanie użyta do promowania jakiegoś światopoglądu w obszarze zagrożeń dzisiejszego świata. Wydaje się, że istnieje takie niebezpieczeństwo, że posłuży ona ustalaniu związków tam, gdzie ich nie ma, że wiązać się ona będzie z przecenienia istotności pewnych bodźców czy reaktywności systemów[25], co negatywnie odbije się na przeprowadzanych ocenach ryzyka i decyzjach o zastosowaniu środków bezpieczeństwa.

Nie wydaje się również, aby płaszczyźnie obowiązujących przepisów nowa koncepcja wymagała jakiś zasadniczych zmian w sferze zarządzenia ryzykiem. Obecnie za podstawowy środek ochrony przed zagrożeniami uchodzi Unijny Mechanizm Ochrony Ludności, obowiązujący w UE i zapewniający współpracę ponadnarodową oraz koordynację ochrony przed różnego rodzaju zagrożeniami. Mechanizm wdraża decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności[26] i chroni się w ramach niego ludzi, mienie, ale również środowisko naturalne i dziedzictwo kulturowe przed „wszystkimi" rodzajami klęsk żywiołowych i katastrof spowodowanych przez człowieka, w tym

[23] *The difference between the study of systemic risk and polycrisis is the difference between the potential and the actual amidst a shared concern about cascading systems failures* (Lawrence, Janzwood i Homer-Dixon, 2022, s. 7).

[24] Więcej na temat sprzężeń według ogólnej teorii systemów zob. Mazur, 1976, s. 44 i n.

[25] Np. dojdzie do przeceniania wagi zmian klimatycznych. Na temat wątpliwości co do charakteru i wpływu ludzkości na zmiany klimatyczne zob. np. Przyborowska-Klimczak, 2010, s. 444.

[26] Dz. U. UE. L. z 2013 r. Nr 347, str. 924 z późn. zm.

przed klęskami i katastrofami technicznymi, zagrożeniami ekologicznymi, zanieczyszczeniem mórz, niestabilnymi warunkami hydrogeologicznymi (zob. art. 1 ust. 2 decyzji 1313/2013/UE). Oceny ryzyka w ramach tego mechanizmu mają uwzględniać transgraniczny, międzysektorowy, w tym infrastrukturalny, związany z wpływem na krajową i europejską infrastrukturę krytyczną, wymiar ryzyka[27].

III. Dyrektywa CER w sprawie odporności podmiotów krytycznych

Można się zastanawiać czy ten aspekt współzależności, sprzężeń systemów społecznych, który wywołuje dodatkowe ryzyko, został uwzględniony w nowej dyrektywie CER, a jeżeli tak, to w jakim zakresie. Dotychczasowa, jeszcze obowiązująca dyrektywa 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej (dyrektywa ECI) dotyczy dwóch sektorów: energetycznego i transportowego – skupia się na wyznaczeniu infrastruktury krytycznej właśnie w tych dwóch sektorach. Również ona zwraca jednak uwagę na współzależności infrastrukturalne i międzysektorowe, w szczególności biorąc je pod uwagę przy rozpoznawaniu europejskiej infrastruktury krytycznej (zob. art. 3 dyrektywy ECI). Nowa dyrektywa CER znacznie rozszerza zakres i sposób ochrony infrastruktury krytycznej, zwracając uwagę na różnego rodzaju współzależności w znacznie większym zakresie.

Nowa dyrektywa CER rozszerza zakres ochrony infrastruktury krytycznej, obejmując dziesięć następujących sektorów: energia, transport, bankowość, infrastruktura rynku finansowego, zdrowie, woda pitna, ścieki, infrastruktura cyfrowa, administracja publiczna oraz technologie kosmiczne. Podchodzi się w niej w sposób kompleksowy do wzmocnienia odporności tzw. podmiotów krytycznych (*critical entities*), tzn. dostawców usług kluczowych, których funkcjonowanie opiera się na wykorzystaniu środków technicznych i systemów logicznych, które nazywa się infrastrukturą krytyczną. W nowej dyrektywie tak rozumiana infrastruktura krytyczna jest elementem wyodrębnianych funkcjonalnie systemów świadczenia usługi kluczowej (zob. 1 pkt 4 dyrektywy CER). W nowym prawie postawiono sobie za cel „wzmocnienie odporności" wobec rozmaitych zagrożeń, w tym również związanych z klęskami żywiołowymi i zmianą klimatu (zob. motywy 3 dyrektywy CER) oraz związanych z funkcjonowania systemów praworządności (zob. pojęcie „incydentu" z art. 2 pkt 3 dyrektywy CER). Bierze się również pod uwagę rozmaite współzależności. W prawie tym wychodzi się z założenia współzależności między samą infrastrukturą, systemami świadczenia usług kluczowych (mówi się o „współzależnej sieci świadczenia usług wykorzystującej kluczową infrastrukturę w całej Unii w sektorach energii, transportu, bankowości, wody pitnej, ścieków, produkcji, przetwarzania i dystrybucji żywności, zdrowia, w sektorze kosmicznym, w sektorach infrastruktury rynku finansowego i infrastruktury cyfrowej, a także w zakresie niektórych aspektów sektora administracji publicznej", a także o współzależności usług kluczowych na całą gospodarkę i funkcjonowanie społeczeństw, w tym o współzależnościach transgranicznych) (zob. motyw 5 dyrektywy CER). Już w świetle tej krótkiej charakterystyki widać, że koncepcja polikryzysów może okazać się przydatna na gruncie ww. dyrektywy.

[27] Zawiadomienie Komisji pt. Wytyczne oceny zdolności zarządzania ryzykiem, Dz. U. UE C 216 z 2015, s. 8, pkt 4.1.

W związku z powyższym zwróćmy jednak uwagę na następujące rozwiązania dyrektywy CER. Po pierwsze, dyrektywa wprowadza wymóg przygotowania przez państwa członkowskie UE strategii w zakresie odporności podmiotów krytycznej – strategia służy określeniu celów i priorytetów zwiększenia ogólnej odporności podmiotów krytycznych i w niej mają być uwzględniane transgraniczne oraz międzysektorowe „zależności i współzależności" (art. 4 ust. 2 lit. a dyrektywy CER). Jak już o tym powiedziano we wprowadzeniu, będzie to miało znaczenie zwłaszcza w odniesieniu do infrastruktury energetycznej oraz informacyjno-informatycznej, ponieważ z tego rodzaju infrastrukturą wiążą się szczególnie duże ryzyka systemowego i pozasystemowego. Zauważmy dalej, że opracowując przedmiotową strategię wykorzystuje się „[…] istniejące strategie krajowe i sektorowe, plany lub podobne dokumenty, cele strategiczne i środki polityczne, o ile tylko służą one osiągnięciu i utrzymaniu wysokiego poziomu odporności po stronie podmiotów krytycznych". W ten sposób dokonuje się kompleksowego przeglądu systemów infrastruktury krytycznej, ich funkcjonalności, identyfikuje się zagrożenia i ryzyka, dokonuje przeglądu środków ochrony. Rozpoznaje się układ zależności funkcjonalnych oraz logicznych systemów, przekładających się ostatecznie na świadczenie usług kluczowych[28]. Po drugie, oceny ryzyka przeprowadzane przez państwa członkowskie mają uwzględniać rozmaite rodzaje ryzyka, w tym „spowodowane przez człowieka", o charakterze „międzysektorowym i transgranicznym," zagrożenia zdrowia publicznego i zagrożenia hybrydowe (zob. art. 5 ust. 1 ak. 2 dyrektywy CER). Z kolei na podstawie tych ocen ryzyka identyfikowane są podmioty krytyczne i wprowadzane środki ochrony. Te oceny ryzyka mają z kolei uwzględniać rodzaje ryzyka wynikające ze stopnia wzajemnej zależności między sektorami świadczenia usług kluczowych, w tym zależności od podmiotów znajdujących się w państwach trzecich, a w ramach tego wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego, czyli również jakieś pozasystemowe zagrożenia (art. 5 ust. 2 dyrektywy CER). Przeprowadzając takie oceny ryzyka, państwa członkowskie mają również brać pod uwagę oceny ryzyka opracowywane na gruncie przepisów sektorowych, a nadto kierować się ogólną oceną ryzyka przygotowaną w ramach Unijnego Mechanizmu Ochrony Ludności, w której wykorzystuje się aktualizowane na poziomie unijnym tzw. międzysektorowe zestawienia i mapy różnych rodzajów ryzyka wiążących się z klęskami żywiołowymi i katastrofami spowodowanymi przez człowieka (zob. art. 5 ust. 1 lit. c decyzji 2013/1313/UE). Po trzecie, oceny ryzyka przygotowywane przez same podmioty krytyczne mają być bardzo rozległe i obejmować wszystkie istotne naturalne i spowodowane przez człowieka czynniki ryzyka mogące prowadzić do incydentu, w tym także czynniki ryzyka o charakterze międzysektorowym lub transgranicznym, wypadki, klęski żywiołowe, stany zagrożenia zdrowia publicznego i zagrożenia hybrydowe, zagrożenia związane z konfliktem, przestępstwa terrorystyczne (art. 12 ust. 2 dyrektywy CER). Wyraźnie podkreślono, że takie oceny ryzyka mają uwzględniać stopień zależności innych sektorów (systemów świadczenia usługi kluczowej) od danej usługi kluczowej i odwrotnie, stopień zależności podmiotu krytycznego od usług kluczowych pochodzących od innych systemów, również tych pochodzących z innych państw.

[28] Interesująca jest z tego punktu widzenia obserwacja, że działania instytucji politycznych mogą być „katalizatorami" kryzysu. Jako przykład podaje się sytuację w Stanach Zjednoczonych w przededniu kryzysu finansowego lat 2007–2008, gdy polityka instytucji nadzoru finansowego „zachęcała" do stosowania innowacyjnych instrumentów finansowych i w ten sposób przyczyniła się do kryzysu (tak Roubini i Mihm, 2011, s. 53).

IV. Wnioski

Za modnym ostatnio terminem „polikryzys" kryje się idea ze sfery zarządzania ryzykiem, która w gruncie rzeczy zmierza do tego, aby zwrócić uwagę na pewne zagrożenia oraz ryzyka ogólnosystemowe przy założeniu szczególnej reaktywności systemów społecznych na pewne zagrożenia. Zakłada się pewne sprzężenia miedzy systemami społecznymi, które powodują, że zagrożenia czy sytuacje kryzysowego obecne w tych systemach są wzmacniane czy też zyskują dodatkową dynamikę rozwoju. Idea polikryzysu została już rozwinięta koncepcyjnie w nauce przez Michaela Lawrence'a, Scotta Janzwooda i Thomasa Homer-Dixona. Nie wydaje się jednak, żeby za tą koncepcją szła jakaś jakościowa zmiana w zarządzaniu ryzykiem. Od dawna już w analizach różnych rodzajów ryzyka uwzględnia się sprzężenia systemów, zagrożenia pozasystemowe, różne współzależności systemów infrastruktury krytycznej czy świadczenia usług kluczowych. Niemniej jednak nowa koncepcja w pewien sposób zmienia optykę spojrzenia na niektóre zagrożenia, zwraca uwagę na pewne bodźce i znaczenie cechy reaktywności systemów społecznych na bodźce.

Przepisy nowej dyrektywy CER w sprawie odporności podmiotów krytycznych wymagają uwzględniania bardzo rozległego zakresu zagrożeń, skutków, zależności od innych systemów infrastruktury krytycznej i systemów społecznych, w tym również związanych ze zmianami klimatu i praworządnością, a co za tym idzie stwarzają one pole do wykorzystania koncepcji polikryzysów. Niemniej jednak rodzi to pewne obawy, ponieważ wydaje się, że sama koncepcja polikryzysów może zostać „uwikłana" ideologicznie, a wtedy może pojawiać się niebezpieczeństwo przeprowadzania niewłaściwych ocen ryzyka i wprowadzenia nadmiernych, nieproporcjonalnych do zagrożeń środków ochrony.

Bibliografia

Future Earth, Sustainability in the Digital Age, and International Science Council. (2021). *Global Risks Perceptions Report 2021*. Future Earth Canada Hub. https://doi.org/10.5281/zenodo.5764288. Pozyskano z: https://futureearth.org/initiatives/other-initiatives/grp-2021report/

Kaufman, G.G. i Scott, K.E. (2003). What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It? *The Independent Review*, *7*(3), 371–391.

Kozioł, A. (2021). Nowy plan zwalczenia terroryzmu w UE. *Biuletyn PISM Polskiego Instytutu Spraw Międzynarodowych*, (33).

Lauge, A., Hernantes, J. i Sarriegi, J.M. (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, *8*. 16–23. Pozyskano z: https://www.sciencedirect.com

Lawrence, M., Janzwood, S. i Homer-Dixon, Th. (2022). What Is a Global Polycrisis? And how is it different from a systemic risk? *Siscussion Paper. Cascade Institute*. Pozyskano z: https://cascadeinstitute.org/technical-paper/what-is-a-global-polycrisis/

Lidwa, W., Krzeszowski, W. i Więcek, W. (2010). *Zarządzanie w sytuacjach kryzysowych*. Warszawa: Wydawnictwo Akademii Obrony Narodowej.

Mazur, M. (1976). *Cybernetyka i charakter*. Warszawa: Wyższa Szkoła Zarządzania i Przedsiębiorczości.

Morin, E. i Kern, A.B. (1998). *Ziemia – ojczyzna* (tłum. T. Jekielowa). Warszawa: Państwowy Instytut Wydawniczy.

Nowak, W. (2018). W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Przyborowska-Klimczak, A. (2010). Zagrożenia związane ze zmianami klimatycznymi i przeciwdziałanie ich negatywnym skutkom na forum międzynarodowym. W: J. Symonides (red.), *Świat wobec współczesnych wyzwań i zagrożeń*. Warszawa: Wydawnictwo Naukowe Scholar.

Roubini, N. i Mihm, S. (2011). *Ekonomia kryzysu* (tł. R. Mitoraj). Warszawa: Wolters Kluwer.

Sienkiewicz, P. i Świeboda, H. (2016). Zarys teoretycznych podstaw inżynierii systemów bezpieczeństwa. W: J. Gryz (red.), *Zarys teorii bezpieczeństwa państwa*. Warszawa: Wydawnictwo Akademii Obrony Narodowej.

Sztompka, P. (2002). *Socjologia, Analiza społeczeństwa*. Kraków: Znak.

Szwarc, K. (2016). Współzależność jako wyzwanie w aspekcie ochrony infrastruktury krytycznej. W: A. Chabasińska, Z. Czachór (red.), *Bezpieczeństwo narodowe Polski. Zagrożenia i determinanty zmian*. Warszawa: Difin.

Tooze, A. (2022). Chartbook #130 Defining polycrisis – from crisis pictures to the crisis matrix. Pozyskano z: https://adamtooze.substack.com/p/chartbook-130-defining-polycrisis

Tooze, A. (2022a). Welcome to the world of the polycrisis. *Financial Times*, 28 October. Pozyskano z: https://www.ft.com/content/498398e7-11b1-494b-9cd3-6d669dc3de33

Więcek, W. (2010). W: W. Lidwa, W. Krzeszowski i W. Więcek, *Zarządzanie w sytuacjach kryzysowych*. Warszawa: Wydawnictwo Akademii Obrony Narodowej.

Word Economic Forum. (2023). *The Global Risks, Report 2023. 18th Edition*. Pozyskano z: https://www.weforum.org/reports/global-risks-report-2023/

Wróbel, R. (2019). Zarządzanie ryzykiem na potrzeby systemu zarządzenia kryzysowego w Polsce w optyce wymagań Mechanizmu Ochrony Ludności. *Zeszyty Naukowe SGSP*, *69*(1).

Zeitlina, J., Nicoliaand, F. i Laffan, B. (2019). Introduction: the European Union beyond thepolycrisis? Integration and politicization in an age ofshifting cleavages. *Journal of European Public Policy*, *26*(7).

Zieliński, K.R. (2017). *Ochrona ludności. Zarządzanie kryzysowe*. Warszawa: Difin.