JOURNAL OF MODERN SCIENCE
TOM 3/52/2023
www.jomswsge.com

DOI: doi.org/10.13166/jms/174175

Agata Tyburska
Police Academy in Szczytno, Poland
Email: a.tyburska@wspol.edu.pl
ORCID: 0000-0002-3788-786X

BADANIA POWIĄZAŃ I ZALEŻNOŚCI SYSTEMÓW INFRASTRUKTURY KRYTYCZNEJ – PODSTAWĄ UODPARNIANIA INFRASTRUKTURY KRYTYCZNEJ PAŃSTWA I DUŻYCH AGLOMERACJI MIEJSKICH

RESEARCH ON THE RELATIONSHIPS AND DEPENDENCES OF CRITICAL INFRASTRUCTURE SYSTEMS – THE BASIS FOR IMPROVINGCRITICAL INFRASTRUCTURE OF THE STATE AND LARGE URBAN AGGLOMERATIONS

Abstract

Effective management of infrastructure development in large urban agglomerations requires diagnosing interdependencies occurring in the process of its

development. This specific interdependence, links between various types of infrastructure, not only favours the development of agglomerations, but also generates threats with unprecedented consequences for public safety and order. Damage to one element of urban infrastructure may adversely affect another element, which in turn may result not only in threats to the safety of people living in the agglomeration, but also in threats to the state. Therefore, the issue of making the key infrastructure of an urban agglomeration more resilient should be considered in the context of system connections of state infrastructure elements, as well as the criticality of its individual elements, nodes and key points. The aim of this article is to present the importance of the diagnosis of connections and dependencies between elements of the city (state) infrastructure in the process of determining the essential service and, consequently, the proper immunization of critical infrastructure. The main research method used in the course of the research was the critical analysis of literature, materials and procedures. The publications of both Polish and foreign researchers on the links and dependencies of the state infrastructure and the determination of key services were analysed. The conducted analysis indicates the need to conduct research in Poland on diagnosing dependencies in the developing infrastructure. This need results from the dynamic nature of threats and the emergence of new technologies that support the development of modern agglomerations and make the state more sensitive to other, so far undiagnosed threats.

Streszczenie

Skuteczne kierowanie rozwojem infrastruktury dużych aglomeracji miejskich wymaga diagnozowania współzależności występujących w procesie jej rozwoju. Ta swoista współzależność, powiązania różnych rodzajów infrastruktury, nie tylko sprzyja rozwojowi aglomeracji ale również generuje zagrożenia o niespotykanych dotąd skutkach dla bezpieczeństwa i porządku publicznego. Uszkodzenie jednego z elementów infrastruktury miejskiej może bowiem niekorzystnie oddziaływać na inny element, czego efektem mogą być nie tylko zagrożenia dla bezpieczeństwa ludzi zamieszkujących aglomerację, ale również skutkować zagrożeniami państwa. Dlatego też zagadnienie uodpornienia infrastruktury kluczowej aglomeracji miejskiej należy rozpatrywać w kontekście systemu i powiązań systemowych elementów infrastruktury państwa, a także krytyczności poszczególnych jej elementów, węzłów i punktów kluczowych. Niniejszy artykuł ma celu przedstawienie znaczenia diagnozy powiązań i zależności pomiędzy elementami infrastruktury miasta (państwa) w procesie wyznaczania usług kluczowych, a w konsekwencji właściwego diagnozowania infrastruktury

krytycznej i jej uodparniania. Główną metodą badawczą wykorzystywaną w trakcie prowadzonych badań była analiza krytyczna literatury, materiałów i procedur. Analizie poddawano publikacje zarówno polskich, jak i zagranicznych badaczy dotyczące powiązań i zależności infrastruktury państwa oraz wyznaczania usług kluczowych. Przeprowadzona analiza wskazuje na potrzebę prowadzenia w Polsce badań dotyczących diagnozowania zależności w rozwijającej się infrastrukturze. Potrzeba ta wynika z dynamicznego charakteru zagrożeń i pojawiania się coraz to nowych technologii, które wspierając rozwój współczesnych aglomeracji – uwrażliwiają państwo na inne, nieznane dotychczas niebezpieczeństwa.

Keywords: *essential services, critical infrastructure, connections, dependencies, security*

Słowa kluczowe: *usługi kluczowe, infrastruktura krytyczna, powiązania, zależności, bezpieczeństwo*

„Ludzie znają dziś cenę wszystkiego,
nie znając wartości niczego"
Oscar Wilde

Wprowadzenie

Nowoczesne technologie przyczyniły się nie tylko do usprawnienia gospodarki, ale również rozwoju infrastruktury państwa ułatwiającej człowiekowi codzienną egzystencję. Dobra i usługi kluczowe dostarczane przez podmioty, urządzenia, instalacje, sieci czy systemy infrastruktury państwa zapewniają nie tylko funkcjonowanie gospodarki, administracji publicznej, ale także codzienne potrzeby mieszkańców dużych aglomeracji miejskich, małych miasteczek, czy wiosek. Doświadczenia zgromadzone w wyniku analizy zaistniałych sytuacji kryzysowych jednoznacznie wskazują na uzależnienie współczesnych społeczeństw od *dóbr i usług niezbędnych do utrzymania żywotnych funkcji społecznych w tym łańcucha dostaw* (Nieuwenhuijs, Luiijf, Klawer, 2008, s. 206) zapewnianych przez infrastrukturę państwa, która z uwagi na jej kluczowe znaczenie dla życia, zdrowia oraz gospodarki państwa nosi miano infrastruktury krytycznej (Krotofil i in., 2014, s.29-45). Pamiętać jednak należy, że nie

każdy element, infrastruktury, który jest krytyczny dla aglomeracji miejskiej będzie równocześnie krytyczny z punktu widzenia państwa. Z tego też względu administracja publiczna powinna dołożyć należytej staranności do właściwego wyodrębnienie spośród miejskiej infrastruktury tych elementów, których niesprawność mogłaby zagrozić niezakłóconemu funkcjonowaniu aglomeracji i jej mieszkańców. Do istotnych zadań administracji należy zatem zidentyfikowanie tych wszystkich elementów gwarantujących sprawne funkcjonowanie państwa i społeczeństwa, które są najbardziej krytyczne spośród infrastruktury państwa (Setola, Theocharidou, 2016, s. 19). Wszelkiego rodzaju zdarzenia zakłócające funkcjonowanie kluczowej infrastruktury mogą bowiem skutkować przerwami w dostawach podstawowych dóbr, bądź pozbawieniem ludzi fundamentalnych dla życia usług. Powstające zakłócenia, niesprawności w tej wrażliwej części infrastruktury nabierają szczególnego znaczenia w przypadku dużych aglomeracji miejskich, tzw. *mega miast*, czy *miast globalnych*, czego niezaprzeczalnym przykładem są odnotowywane ataki wojsk rosyjskich na infrastrukturę dużych aglomeracji miejskich Ukrainy.

Niniejszy artykuł ma celu przedstawienie znaczenia właściwie przeprowadzonej diagnozy powiązań i zależności pomiędzy elementami infrastruktury państwa w procesie wyznaczania usług kluczowych, a w konsekwencji właściwego wyznaczania i skutecznego uodparniania infrastruktury krytycznej. Przedmiotem badań były w tym przypadku rozwiązania, programy, procedury i dobre praktyki dotyczące badania powiązań i zależności pomiędzy infrastrukturą państwa oraz wyznaczania infrastruktury krytycznej. Główną metodą badawczą wykorzystywaną w trakcie prowadzonych badań była analiza krytyczna literatury, dokumentów i procedur. Analizie poddawano publikacje i inne dokumenty zarówno polskich, jak i zagranicznych badaczy dotyczące diagnozowania powiązań i zależności w infrastrukturze państwa oraz wyznaczania usług kluczowych i zapewniających je elementów infrastruktury określanych jako infrastruktura krytyczna. W procesie badawczym zastosowano również takie metody, jak: analiza, synteza, abstrahowanie, porównanie oraz uogólnienie, a także metody charakterystyczne dla procesu wnioskowania: dedukcja, redukcja, indukcja i analogia.

Diagnoza powiązań i zależności jako element diagnozy usług kluczowych i wyznaczania infrastruktury krytycznej państwa

Różne sposoby definiowania pojęcia infrastruktura państwa przez badaczy problemu sprowadza się właściwie do wspólnej konkluzji, co do olbrzymiego znaczenie posiadanej infrastruktury dla rozwoju gospodarczego kraju, dbałości o posiadaną już infrastrukturę oraz troski o jej rozbudowę (Kaczmarski, 2010, s. 16). Warto jednocześnie podkreślić bezpośredni związek tego terminu z określeniem *aglomeracja* rozumianym w urbanistyce jako obszar o intensywnej zabudowie, charakteryzujący się dużym zagęszczeniem ludności (Najgebauer, 2009, s. 29–30). Z tego względu określenie, np. infrastruktury komunalnej obejmuje sieci transportowe (ulice, rzeki, kanały), energetyczne, gazowe, wodno-kanalizacyjne, kolejowe, ciepłownicze, tramwajowe, metro czy telekomunikacyjne.

Aby odpowiednio kierować rozwojem infrastruktury kraju, czy też dużych aglomeracji miejskich, niezwykle ważne jest dokładne poznanie współzależności występujących w procesie jej rozwoju (Hurst, Merabti, Fergus, 2014, s. 127-138). Ta swoista współzależność, powiązania różnych rodzajów infrastruktury (jej elementów), nie tylko sprzyja rozwojowi państw i funkcjonujących w ich obszarach dużych aglomeracji miejskich ale — co istotne — inicjuje coraz to nowe zagrożenia bezpieczeństwa ludzi (Kaczmarski, 2010, s. 17). Uszkodzenie czy awaria jednego z elementów infrastruktury kluczowej może bowiem niekorzystnie oddziaływać na inny jej element, czego efektem może być przerwanie łańcucha dostaw usługi kluczowej generujące nie tylko zagrożenia lokalne, dotyczące funkcjonowania miasta i jego mieszkańców, ale niejednokrotnie niekorzystnie wpływać na bezpieczeństwa państwa. Dlatego też problematykę bezpieczeństwa danej infrastruktury należy rozpatrywać w kontekście systemu i powiązań systemowych elementów infrastruktury państwa, a także krytyczności poszczególnych jej elementów, węzłów czy punktów kluczowych odpowiedzialnych za dostarczanie usług kluczowych (Radwanovsky, McDougall, 2009, s. 191-192; Nieuwenhuijs, Luiijf, Klaver, s. 206). Według holistycznego podejścia do teorii systemów – całość stanowi więcej aniżeli jedynie sumę dodanych do siebie elementów; suma pojedynczych elementów jest większa niż wartość zsumowanych, pojedynczych elementów (Skurzyńska – Sikora, 2008, s. 7).

Najczęściej *system* jest charakteryzowany jako zbiór wzajemnie powiązanych elementów, o zhierarchizowanej strukturze wewnętrznej. Każdy z systemów ma określone istotne cechy, które pozwalają na zdiagnozowanie i określenie punktów krytycznych i współzależności pomiędzy poszczególnymi elementami systemu (Piekarczyk, Zieniewicz, 2010, s. 36–37).

Literatura przedmiotu jako istotne cechy każdego *systemu* wymienia: elementy (każdy system składa się z części składowych); stosunki, zależności (elementy są ze sobą powiązane, łączą się ze sobą we wzajemnych relacjach); właściwości (każdy system, każdy jego element ma określone cechy charakterystyczne, które pozwalają m.in. na określenie punktów krytycznych) (Setola, Theocharidou, 2016, s. 21-22). Niezwykle istotną właściwością w badaniach nad systemami jest zrozumienie, że każdy z nich może być — w zależności od obszaru badań — jednocześnie systemem, jak również częścią innego systemu, czyli podsystemem (Palmer, Shenoi, 2007, s.217-218). Stąd też istotnym w badaniu systemów jest również podejście określone jako redukcjonizm — pogląd filozoficzny, zakładający, że wszelkie zjawiska i procesy, zachodzące w rzeczywistości, prawa nimi rządzące, dadzą się wyjaśnić na podstawie analizy zjawisk oraz procesów prostych, a także odpowiadających im praw. Zgodnie ze wskazaną teorią badanie całości należy rozpocząć od rozłożenia jej na poszczególne elementy (Radziszewska-Szczepaniak, 2016, s. 379).

Z tego też względu wyróżnia się takie pojęcia, jak *system*, *podsystem*, *system zewnętrzny*, *system wewnętrzny*, *nadsystem*, *supersystem*, *subsystem*. Niezwykle cenne w tym przypadku są wyniki badań naukowych, diagnozujące zależności pomiędzy elementami systemu, słabe strony danego systemu infrastruktury państwa, a także miejsca ich szczególnej wrażliwości (krytyczności). Szczególnie cenne są wyniki badań prowadzone w zakresie sterowania złożonymi i skomplikowanymi systemami, określane jako sterowanie kompleksami. W takim przypadku kompleks tworzyły będą systemy złożone z wielkiej liczby elementów wraz z towarzyszącymi im zależnościami i powiązaniami. Jak twierdzi Jiři Beneš: „kompleks to system, który tworzy wielka liczba elementów żywych albo nieożywionych. Elementami kompleksu mogą być np. cząsteczki, podzespoły czy też całe urządzenia techniczne (Beneš, 1979, s. 9-10).

Rozważając zatem problematykę sprawnie działającego łańcucha dostaw usług zdiagnozowanych jako kluczowe, a także ochrony infrastruktury,

która je zapewnia – należy postrzegać ją kompleksowo, najlepiej przez pryzmat powiązań i zależności pomiędzy obiektami, urządzeniami, instalacjami, kluczowymi usługami stanowiącymi dany system (Lewis, 2006, s. 71-87). Warto w tym miejscu podkreślić, że z reguły nie cały system (kompleks) stanowi infrastrukturę krytyczną. Najczęściej jest nią jedynie element, fragment, wycinek, punkt czy węzeł istotny z punktu widzenia wytwarzania, dostarczenia, przesyłu, odbioru, czy rozdziału dóbr określanych jako dobra i usługi kluczowe dla życia, zdrowia ludzi, sprawnego funkcjonowania państwa zarówno w czasie pokoju, kryzysu, jak również w sytuacji bezpośredniego zagrożenia konfliktem zbrojnym (Sullivant, 2007, s.41 – 42).

Istotnym elementem w procesie wyodrębniania infrastruktury krytycznej jest proces wyznaczania krytyczności elementów stanowiących dany system, co jest bezpośrednio związane z rolą jaką pełnią w wytworzeniu dobra czy usługi kluczowej i jej sprawnego dostarczeniu do odbiorców. Ogólnie przyjmowane jest, że infrastrukturę państwa charakteryzuje systemowa krytyczność, jeżeli ma ona szczególnie wysokie, wzajemnie zależne znaczenie ze względu na swoją pozycję strukturalną, funkcjonalną i techniczną w całym systemie (kompleksie) obszarów infrastruktur bazowych. Przykładem tego założenia może być infrastruktura zapewniająca dostęp do energii elektrycznej, informatyczna czy telekomunikacyjna, które ze względu na wielkość oraz siłę powiązań są szczególnie istotne, a długotrwałe awarie, obejmujące swym zasięgiem duży obszar państwa, mogłyby prowadzić – w skutek przerwania łańcucha dostaw – do poważnych zakłóceń społecznych procesów, gospodarki, jak również bezpieczeństwa i porządku publicznego szczególnie w dużych aglomeracjach miejskich. Stąd też jako krytyczny jest określany zarówno sektor infrastruktury państwa, którego zakłócenie powoduje istotne skutki dla społeczeństwa, jak również taką cechę można przypisać procesom gospodarczym w przedsiębiorstwie, jeżeli w czasie zaistniałych zakłóceń pojawiłoby się zagrożenie dla przedsiębiorstwa lub też funkcjonowania aglomeracji miejskich.

Należy przy tym podkreślić, że infrastruktura państwa, pozostaje we wzajemnej zależności logicznej, jeżeli stan każdej z nich zależy od stanu drugiej. Najczęściej ten rodzaj zależności wynika bezpośrednio z decyzji podejmowanych przez ludzi.

Oprócz korzyści wynikających z istniejących zależności podkreślane są także sytuacje zagrażające będące ich konsekwencją. Zaistniałe sytuacje kryzysowe pokazują, ze nieprawidłowe funkcjonowanie nawet jednego składnika może sprawić, że właściciele (zarządzający, operatorzy) mogą podejmować niewłaściwe decyzje wpływające negatywnie na działanie innego systemu bądź elementu krytycznego odpowiedzialnego za dostawę usługi kluczowej. Szczególny rodzaj powiązań został zdiagnozowany w sektorach związanych z infrastrukturą wytwarzającą energię elektryczną (Setola, Theocharidou, 2016, s. 20). Sektor ten także jest uzależniony od innej infrastruktury państwa ze względu na to, że wymaga chociażby paliw do uruchomienia generatorów, technologii informacyjnych do zarządzania systemami kontrolnymi i sterującymi czy też wody pozwalającej na chłodzenia niektórych urządzeń. Z kolei wszystkie wymienione elementy są uzależnione od sprawnego działania infrastruktury elektrycznej. Na fundamentalne znaczenie opracowania skutecznych metod diagnozowania zależności i współzależności pomiędzy elementami infrastruktury państwa zwracają uwagę holenderscy badacze podkreślając, że *zależność to związek pomiędzy dwoma dobrami, produktami lub usługami, w którym jeden produkt lub usługa jest niezbędna do pozyskania innego dobra, produktu bądź usługi* (Nieuwenhuijs, Luiijf, Klaver, s. 206). Prowadzone przez nich badania zależności i współzależności opierają się głównie na analizie systemowej.

Z kolei francuscy badacze problemu podkreślają, że funkcjonowanie infrastruktury krytycznej opiera się w dużej mierze na sprawnym działaniu systemów gromadzenia i przetwarzania danych gwarantowanych przez nowe technologie związane z systemami informatycznymi i łączności. Podobne opinie formułują również badacze z innych państw wysokorozwiniętych (Arnold, Butts, Thirunarayan, 2014). Są to ich zdaniem, systemy szczególnie wrażliwe i podatne na zakłócenia, szczególnie w przypadkach umyślnego działania tzw. ataków *złej woli*, ale także w sytuacji popełniania nieumyślnych błędów fizycznych, błędów interakcji lub błędów koncepcyjnych systemu (Cavallini, d'Alessandro, Volpe, Armenia i in., 2014, s. 141-151). Zdaniem Amine Baina z Institut National des Sciences Appliquées w Tuluzie, wzajemne zależności pomiędzy elementami infrastruktury krytycznej, krytycznej infrastruktury informatycznej i elementami krytycznej infrastruktury informacyjnej należącymi do poszczególnych infrastruktur krytycznych mogą wywołać zakłócenia

kaskadowe (Baina, 2009), a w konsekwencji doprowadzić do zaburzeń w łańcuchu dostaw zdiagnozowanych usług kluczowych. Zakłócenie kaskadowe występuje wówczas, kiedy zakłócenie funkcjonowania jednej infrastruktury powoduje zakłócenia w innych. Mogą też wywoływać zakłócenia nasilające się, które polegają na tym, że niewielkie zakłócenie w funkcjonowaniu jednej infrastruktury powoduje poważną awarię elementów z nią powiązanych i w konsekwencji nagłe przerwy w dostawie usługi kluczowej (Setola, Theocharidou, 2016, s. 24). Dodatkowo zjawiska wzajemnych zależności, a także potencjalnych awarii kaskadowych narastają wskutek otwarcia i rozregulowania rynków kontrolowanych dawniej przez monopol państwowy, a obecnie — w wyniku globalizacji — otwartych dla innych podmiotów (Baina, 2009).

Kolejnym problemem związanym z zapewnieniem ochrony infrastruktury krytycznej są jej znaczne rozmiary, obejmujące niekiedy bardzo duży obszarowo zasięg. Chodzi tu głównie o skalę i strukturę infrastruktury krytycznej, które powodują powstanie licznych słabych punktów, a tym samym dodatkowe zagrożenia.

Według Amine Baina wzajemne zależności pomiędzy elementami infrastruktury krytycznej mogą mieć charakter logiczny oraz fizyczny. Wskazany badacz zwraca uwagę na potrzebę rozpatrywania zależności pomiędzy elementami infrastruktury krytycznej uwzględniającej zmienne ekonomiczne, techniczne i społeczne danego środowiska. Podkreśla również znaczenie rodzaju sprzężenia (silne lub słabe) pomiędzy infrastrukturami, które może wpływać na zmienne operacyjne poszczególnych elementów infrastruktury i wywoływać kaskadowe bądź nasilające się zakłócenia. Wynika to z faktu, że ma ono wpływ na warunki funkcjonowania systemów, a przez to jednocześnie oddziałuje na rozwój potencjalnych zakłóceń.

Zgodnie z koncepcją Amine Baina są wyróżniane trzy rodzaje wzajemnych zależności występujących w infrastrukturze krytycznej (Baina, 2009). Pierwszy rodzaj zależności pojawia się w związkach pomiędzy infrastrukturą krytyczną a siecią elektryczną, która ją zaopatruje w energię niezbędną do funkcjonowania. Nawet niewielka awaria — przerwa choćby tylko na jednej linii doprowadzającej — w sieci transportu i dystrybucji elektryczności może doprowadzić do całkowitego zatrzymania pracy niektórych typów infrastruktury krytycznej, a tym samym przerwania łańcucha dostaw kluczowej usługi. Jeśli chodzi o drugi rodzaj zależności – to wynika on powszechnej informatyzacji

i rozwoju społeczeństwa informacyjnego. Zależność ta dotyczy głównie powiązań pomiędzy infrastrukturą krytyczną a przynależącą do niej krytyczną infrastrukturą informacyjną działającą w tzw. cyberprzestrzeni. Zagrożenia dla infrastruktury krytycznej potęguje fakt, że systemy te poprzez sieci łączności, informacyjno-komunikacyjne, oprogramowanie, sprzęt, Internet już same w sobie tworzą infrastrukturę wrażliwą na zakłócenia. Najmniejsze zakłócenie pracy spowodowane chociażby wadą techniczną, błędem ludzkim czy tzw. *złą wolą* na poziomie krytycznej infrastruktury informacyjnej może skutkować (poprzez awarie kaskadowe lub nasilające się) ogólną awarią globalnej infrastruktury krytycznej państwa. W przypadku trzeciego rodzaju zależności – wynika on z wzajemnej zależności pomiędzy krytyczną infrastrukturą informacyjną a siecią energii elektrycznej. Każda taka sieć zależy bowiem od własnego systemu informacyjno-łącznościowego, a zwłaszcza od jednego lub kilku systemów kontrolnych, które prowadzą swoisty *nadzór* nad funkcjonowaniem sieci, odpowiadają za gromadzenie wszelkich koniecznych informacji, a także wykonywanie różnych operacji mających na celu stałe dostosowanie działania sieci elektroenergetycznej do warunków wewnętrznych i zewnętrznych.

Z kolei Benoît Rozel określił cztery klasy wzajemnych zależności pomiędzy elementami infrastruktury państwa: fizyczną, cybernetyczną, geograficzną oraz logiczną (Rozel, 2009). Każda z tych czterech klas wzajemnych zależności ma własne cechy charakterystyczne, które nie wykluczają się wzajemnie. Zależność fizyczna występuje w przypadku, kiedy dwie infrastruktury pozostają we wzajemnej zależności fizycznej, a stan każdej z nich zależy od skutków działania drugiej. Jako przykład tego typu zależności wskazywana jest infrastruktura zasilania w wodę i dostarczająca energię elektryczną. Pierwsza z wymienionych infrastruktur nie może realizować przypisanych jej funkcji bez zapewnienia jej nieprzerwanych dostaw energii elektrycznej, dzięki której pracują pompy. Z kolei infrastruktura związana z wytwarzaniem energii elektrycznej wymaga zaopatrzenia w wodę pozwalające na niezbędne chłodzenie urządzeń.

Infrastruktura pozostaje w zależności cybernetycznej, jeśli jej stan zależy od informacji przekazywanych w cyberprzestrzeni. Ze względu na procesy informatyzacji i automatyzacji, jakie w ostatnich latach objęły prawie wszystkie rodzaje infrastruktur, elementy te działają w sytuacji silnej zależności cyber i stają się coraz częściej obiektem ataku (Kacała-Szwarczyńska, 2019, s. 171-172).

Zależność geograficzna występuje wówczas, kiedy określone wydarzenie o charakterze lokalnym (np. powódź, śnieżyca, oblodzenie, huragan, pożar, susza) przekracza wstępnie diagnozowany obszar. W takiej sytuacji wzajemna zależność może obejmować nawet więcej niż dwie infrastruktury.

Należy przy tym podkreślić, że infrastruktury państwa, pozostają we wzajemnej zależności logicznej, jeżeli stan każdej z nich zależy od stanu drugiej.

Benoît Rozel wskazuje również na cztery charakterystyczne cechy sprzężenia pomiędzy infrastrukturami: silne lub słabe; układ sprzężenia; liniowe lub złożone, a także dostosowujące się lub sztywne (Rozel, 2009). Według tego badacza silne sprzężenie odpowiada infrastrukturze w wysokim stopniu uzależnionej od innej. Zakłócenia wydolności mają w takim przypadku tendencję do szybkiego rozprzestrzeniania się za pomocą elementów infrastruktury sprzężonej. Słabe sprzężenie jest symptomem niewielkiego poziomu zależności i umożliwia funkcjonowanie poszczególnych elementów bez zasilania z zewnątrz jeszcze przez wiele lat od powstania zakłócenia.

Układ sprzężenia informuje z kolei, czy dwie infrastruktury są połączone bezpośrednio czy pośrednio poprzez inne. Sprzężenie pierwotne odpowiada połączeniu bezpośredniemu, sprzężenie wtórne zaś pośredniemu. Istotnymi cechami sprzężenia pomiędzy elementami infrastruktury krytycznej może być ich liniowy lub złożony charakter. Interakcje liniowe to takie, które zostały przewidziane na etapie koncepcji. Złożone interakcje powstają wówczas, kiedy nie zostały wcześniej przewidziane, a ich pojawienie się nie było oczekiwane. Interakcje złożone często nie są łatwe do szybkiego zaobserwowania i zrozumienia i dlatego są niezwykle trudne do wykrycia i zdiagnozowania. Najczęściej są diagnozowane w sytuacji przerwania łańcucha dostaw którejś z usług kluczowych i wynikających z tego faktu sytuacjach kryzysowych.

Z kolei sprzężenie dostosowujące się określa zdolność systemu do uczenia się na podstawie zdarzeń z przeszłości i przystosowania się do przyszłych wydarzeń. W przypadku systemu o sprzężeniu sztywnym pozostaje on niezmienny, co wskazuje, że będzie zachowywał się zawsze tak samo, niezależnie od wcześniejszych doświadczeń.

Istotnym obszarem związanym bezpośrednio z budowaniem sprawnie działającego łańcucha dostaw, a tym samym uodpornienia infrastruktury zdiagnozowanej jako krytyczna — zdaniem francuskich badaczy — jest zagadnienie

niewydolności systemu. Niewydolność systemu polega głównie na jego wrażliwości na usterki albo też częściowe lub całościowe niespełnianie oczekiwań pokładanych wobec systemu (Rozel,2009), co w konsekwencji prowadzić będzie do przypadków powstawania zakłóceń w dostawach usługi kluczowej.

Benoît Rozel wyróżnia także trzy podstawowe rodzaje niewydolności infrastruktury złożonej. Należą do niej (Rozel,2009):

1. niewydolność kaskadowa określana również mianem *eskalacji* lub *efektem domina*; niewydolność tego typu występuje w przypadku, kiedy jedna niewydolność pociąga za sobą kolejną;
2. niewydolność nasilająca — powstaje wówczas, gdy zachodzi interakcja pomiędzy dwiema infrastrukturami, powodująca wzrost utrudnień lub niedyspozycyjności;
3. niewydolność wspólna — oznacza jednoczesną niewydolność kilku elementów, wynikającą z zaistnienia identycznej przyczyny zewnętrznej; przyczyny te mają najczęściej charakter geograficzny czy też leżący poza organizacją.

Przygotowanie optymalnej ochrony infrastruktury krytycznej wymaga również zdiagnozowania tzw. słabych stron elementu krytycznego. Aby przeprowadzić badania wszystkich słabych stron i zagrożeń skierowanych na infrastrukturę krytyczną, Amine Baina proponuje rozróżnienie poszczególnych poziomów *słabości* poprzez diagnozę: słabych punktów samej infrastruktury krytycznej; słabych stron konkretnego urządzenia (np. sieci energii elektrycznej) oraz słabych strony dotyczących krytycznej infrastruktury informacyjnej działającej w cyberprzestrzeni, a tym samym potęgującej jej wrażliwość (Pham, 2006, s. 1-2). Prawidłowo przeprowadzona diagnoza usług kluczowych, analiza łańcucha dostaw umożliwiająca wyznaczenie infrastruktury krytycznej i optymalnie zaprogramowane wzmocnienie odporności wyznaczonej infrastruktury krytycznej – powinno uwzględniać słabe punkty i braki w systemie bezpieczeństwa, dążyć do szybkiego ich niwelowania oraz – co istotne – przygotowywać społeczeństwo do możliwych przerw w dostawach kluczowych usług. Niezbędnym zadaniem jest także zbudowanie przejrzystej polityki bezpieczeństwa warunkującej diagnozującej minimalne standardy gwarantujące optymalny poziom uodparniania infrastruktury krytycznej

państwa, zarządzania tego typu infrastrukturą a tym samym niezakłóconego rozwoju dużych aglomeracji miejskich przy zapewnieniu bezpiecznego życia ich mieszkańcom (Lee, 2009, s. 1-12).

W celu zapewnienia właściwej ochrony elementom infrastruktury krytycznej francuscy eksperci proponują budowanie modeli wzajemnych zależności pomiędzy składnikami infrastruktury zapewniającej niezakłóconą dostawę usług kluczowych. Skonstruowanie modelu zależności jest uznane za pierwszy etap działania, prowadzący do optymalnego uodpornienia infrastruktury uznanej za krytyczną nie tylko z punktu widzenia dużych aglomeracji miejskich ale również z uwagi na zapewnienie bezpiecznego i harmonijnego rozwoju państwa.

Wnioski

Zapewnienie społeczeństwu niezakłóconego łańcucha dostaw dóbr i usług kluczowych jest niezwykle złożonym zadaniem, wymagającym trafnej diagnozy infrastruktury uznanej za krytyczną, a następnie optymalnego jej uodporniania. Warunkiem poprawnie przeprowadzonej diagnozy jest uwzględnienie faktu, że infrastruktura państwa stanowi system wielu pomniejszych infrastruktur wzajemnie od siebie zależnych. Badacze problematyki uodparniania infrastruktury krytycznej wskazują na potrzebę prowadzenia systematycznych badań w zakresie diagnozowania zależności i słabych punktów w rozwijającej się infrastrukturze. Pozyskana w ten sposób wiedza umożliwi zintensyfikowanie działań ukierunkowanych na uodpornienie tych elementów, które rzeczywiście stanowią infrastrukturę krytyczną państwa (Arnold, Butts, Thirunarayan, 2014). Stąd też badanie zależności i współzależności pomiędzy elementami infrastruktury państwa jest nigdy nie kończącym się procesem. W celu optymalizacji prowadzonych działań diagnozujących wskazane związki i zależności – niezbędnym jest poszukiwanie coraz to nowych metod oraz technik badawczych. Dzięki zabiegom warunkującym niezakłóconą dostawę niezbędnych dóbr, produktów i usług kluczowych – zwiększone będzie nie tylko bezpieczeństwo mieszkańców, ale również zapewnione warunki do dynamicznego rozwój aglomeracji miejskich. Prawidłowo przeprowadzona

diagnoza powiązań i zależności elementów systemów i podsystemów pozwoli również na przygotowanie przedsiębiorców, administracji publicznej, służb ratowniczych, na wypadek zaistniałych sytuacji kryzysowych, a samych mieszkańców aglomeracji miejskich do właściwego przygotowania na wypadek wystąpienia niedoborów w dostawach niezbędnych do przeżycia produktów, dóbr i usług. Potrzeba budowania wiedzy w tym zakresie wynika z dynamicznego charakteru zagrożeń i adaptowania do codziennego użytku zdobyczy tzw. nowych technologii. Coraz powszechniejszy dostęp do nowych technologii, budowanie tzw. *inteligentnych miast* z jednej strony ułatwia mieszkańcom aglomeracji miejskich codzienną egzystencję, z drugiej zaś inicjuje niespotykane dotychczas niebezpieczeństwa nie tylko dla społeczności wielkomiejskich, ale również może doprowadzić do destabilizacji i dezorganizacji sytuacji w państwie. Skutki ataków na elementy infrastruktury krytycznej państwa łatwo zauważyć obserwując przebieg konfliktu rozgrywającego się obecnie na Ukrainie i ich znaczenie dla społeczności zamieszkującej atakowany przez Rosjan obszar dużych aglomeracjach miejskich Ukrainy.

References

Arnold, Ch., Butts, J., Thirunarayan, K. (2014). Detecting Integrity Attacks on Industrial Control systems. w : J. Butts, S. Shenoi (red.), *Critical Infrastructure Protection VIII*, Springer. Dostęp 20.05.2023 r. z https://www.researchgate.net/publication/309665457_Critical_Infrastructure_Protection_VIII_8th_IFIPWG1110_International_Conference_ICCIP_2014_Arlington_VA_USA_March_17-19_2014

Baina, A. (2009). *Contrôle d'Accès pour les Grandes Infrastructures Critiques: Application au réseau d'énergie électrique*, Institut National des Sciences Appliquées de Toulouse, 29 septembre, Toulouse. Dostęp 12.05.2023 r. z https://theses.hal.science/tel-00432841/file/these_amine_baina_2009_CNRS.pdf

Beneš, J. (1979). *Teoria systemów*, PWN.

Cavallini, S., d'Alessandro, C., Volpe, M., Armenia, S., Corlini, C., Brein, E., Assogna, P. (2014). *A system Dynamics Framework for Modeling Critical Infrastructure Resilience*. w: J. Butts, S. Shenoi (red.), *Critical Infrastructure Protection VIII*, Springer. Dostęp 20.05.2023 r. z https://link.springer.com/chapter/10.1007/978-3-662-45355-1_10

Grabowski, A., Głowacki, P., Poźniak, K., Kasprowicz, G., Zabołotny, W., Wawrzyniak, Z., Wojeński, A., Tyburska, A., Ajdukiewicz, Z., Struniawski, J., Iwański, J., Brawata, S., Szymajda, W., Markowski, P., Kotlik, M. , Mrozowski, P., Katewicz, E. (2020). *MESH concept for mobile distribution point architecture of ICT infrastructure*, Proc. SPIE 11581, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2020, 115810G (14 October 2020); doi: 10.1117/12.2580242 Event: Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2020, Wilga, Poland. Dostęp 20.05.2023 z https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11581/115810G/MESH-concept-for-mobile-distribution-point-architecture-of-ICT-infrastructure/10.1117/12.2580242.short?SSO=1.

Hurst, W., Merabti, M., Fergus, P. (2014). A Survey of Critical Infrastructure Security. w: J. Butts, S. Shenoi (red.) *Critical Infrastructure Protection VIII*. Dostęp: 20.05.2023 r. z https://inria.hal.science/hal-01386760/file/978-3-662-45355-1_9_Chapter.pdf

Palmer, Ch., Shenoi, S. (red.) (2009). *Critical Infrastructure Protection III*. Springer.

Kacała-Szwarczyńska, A. (2019). *Cyberatak w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych*, Tom 2/41/. Journal of Modern Science. Dostęp 25.05.2023 r. z https://www.jomswsge.com/pdf-111176-41626?filename=Cyberatak%20w%20swietle.pdf

Kaczmarski, M. (2010). *Bezpieczeństwo energetyczne Unii Europejskiej*. Wydawnictwa Akademickie i Profesjonalne.

Krotofil, M., Cardenas, A., Angrishi, K. (2014). *Timing of Cyber-Physicial Attacks on Process Control Systems*. w: J. Butts, S. Shenoi (red.), *Critical Infrastructure*

Protection VIII, Springer. Dostęp 20.05.2023 z https://www.researchgate.net/publication/309665457_Critical_Infrastructure_Protection_VIII_8th_IFIPWG1110_International_Conference_ICCIP_2014_Arlington_VA_USA_March_17-19_2014.

Lee, E. (2009). *Homeland Security and Private Sector Business. Corporations' Role in Critical Inftastructure Protection*. CRC Press.

Lewis, T. G. (2006), *Critical Infrastructure Protection in Homeland Security. Defending a networked nation*. WILEY-INTERSCIENCE, A JOHN Wiley&Sons.

Najgebauer, A. (red.) (2009). *Modele zagrożeń aglomeracji miejskiej wraz z systemem zarządzania kryzysowego na przykładzie miasta stołecznego* Warszawy. WAT.

Nieuwenhuijs, A., Luiijf, E., Klaver, M. (2008). *Modeling Dependencies in Critical Infrastructures*. w: M. Papa, S. Shenoi (red.), *Critical Infrastructure Protection II*, Springer. Dostęp 06.07.2023 r. z https://link.springer.com/chapter/10.1007/978-0-387-88523-0_15

Piekarczyk, A., Zieniewicz, K. (2010). *Myślenie sieciowe w teorii i praktyce*, PWE.

Pham, H. (2006), *System Software Realiability*, Springer. Dostęp 05.06.2023 z https://link.springer.com/book/10.1007/1-84628-295-0

Radvanovsky, R., McDougall, A. (2009). *Critical Infrastructure. Homeland Security and Emergency Preparedness*. Second Edition, CRC Press, Taylor & Francis Group.

Radziszewska-Szczepaniak, D. (2021). *Redukcjonizm antropologiczny i jego konsekwencje*, NURT SVDZ (2016). Dostęp: 01.09.2021 r. z https://bazhum.muzhp.pl/media/files/Nurt_SVD/Nurt_SVD-r2016-t50-n2_(140)/Nurt_SVD-r2016-t50-n2_(140)-s378-395/Nurt_SVD-r2016-t50-n2_(140)-s378-395.pdf

Rozel, B. (2009). *La sécurisation des infrastructures critiques: recherche d'une méthodologie d'identification des vulnérabilités et modélisation des interdépendances,* Institut Polytechnique de Grenoble, Grenoble. Dostęp 12.05.2023 r. z https://theses.hal.science/tel-00407661/preview/These.pdf

Setola, R., Theocharidan, M. (2016). *Modeling Dependencies Between Critical Infrastructures*. w: R. Setola, V. Rosato, E. Kynakides, E. Rome (red.), *Managing the Compexity of Critical Infrastructures. A Modelling and Simulation Approach*, Springer. Dostęp 25.06.2023r. z https://link.springer.com/book/10.1007/978-3-319-51043-9

Skurzyńska – Sikora, U. (2008). *Poprawa efektywności organizacji przy wykorzystaniu modelu PEMM*, 3. Organizacja i Zarządzanie, Dostęp: 01.09.2021 r. z https://mfiles.pl/pl/index.php/Holistyczne_podej%C5%9Bcie#cite_note-1

Sullivant, J. (2007). *Strategies for Protecting National Critical Infrastructure Assets. A Focus on Problem-Solving*. WILEY-INTERSCIENCE, A JOHN Wiley&Sons.