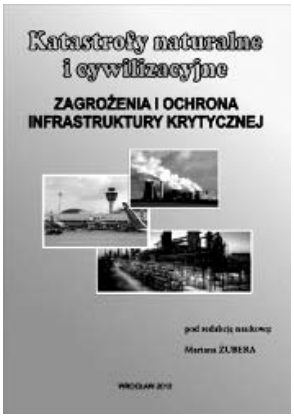
Andrzej Chodyński

"Katastrofy naturalne i cywilizacyjne : zagrożenia i ochrona infrastruktury krytycznej", red. Marian Żuber, Wrocław 2013 : [recenzja]

Bezpieczeństwo : teoria i praktyka : czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 8/3, 99-104

2014

BEZPIECZEŃSTWO 2014 nr 3 (XVI)
TEORIA I PRAKTYKA



Andrzej Chodyński*

Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej
pod redakcją naukową
Mariana Żubera

[Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki, Wrocław 2013, 240 s.]

Katastrofy są zjawiskiem związanym zarówno z działalnością człowieka, z postępem cywilizacyjnym, ale także ze zjawiskami naturalnymi. Problematyka ta stanowi w szczególności przedmiot zainteresowań bezpieczeństwa ekologicznego. Katastrofy naturalne, na przykład nietypowe zjawiska atmosferyczne mogą być powodowane również przez działalność człowieka. Najczęściej wiąże się je ze skutkami globalnego ocieplenia. Jako przykłady przytaczane są oddziaływania huraganów czy powodzi na kontynencie amerykańskim, których skutkiem jest zniszczeniem infrastruktury i wręcz fizyczna likwidacja podmiotów gospodarczych. W związku z tym coraz większą uwagę poświęca się tzw. kryzysom pozaekonomicznym, dotykającym tych podmiotów, jako skutek katastrof. Katastrofy cywilizacyjne mogą wiązać się z działaniami wojennymi czy aktami terrorystycznymi. Skutkiem katastrof jest zagrożenie dla życia ludzi, ale także wiążą się z zagrożeniem infrastruktury krytycznej. Zaletą recenzowanej książki jest podjęcie dyskusji na temat ochrony infrastruktury krytycznej, mając na uwadze istniejące rozwiązania prawne Polski i Unii Europejskiej. Na tym tle wskazano na występujące niedostatki i kierunki ewentualnych zmian. Książka składa się ze Wstępu i 18 rozdziałów. W publikacji podane szereg definicji, m.in. terroryzmu (B. Michailiuk). Zanalizowano różne dokumenty, głównie akty

* Profesor nadzw. doktor habilitowany, dyrektor Instytutu Rozwoju Organizacji i Zarządzania Ekologicznego na Wydziale Zarządzania i Komunikacji Społecznej Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego.

prawne (m.in. w rozdziale autorstwa A. Pęk i J. Żuber). Odniesiono się do wybranych aspektów metodologicznych w tym wykorzystanie sieci bezskalowych do analiz odporności infrastruktury krytycznej (A. Kowalczyk). W opracowaniu podniesiono kilka kluczowych zagadnień:

- scharakteryzowano infrastrukturę krytyczną i odniesiono się (na wybranych przykładach) do jej zagrożeń i ochrony;
- określono rolę Państwowej Straży Pożarnej (PSP);
- omówiono problemy ochrony infrastruktury energetycznej i podsystemu teleinformatycznego;
- odniesiono się do problemu ochrony infrastruktury komunikacyjnej;
- podniesiono temat ochrony infrastruktury wobec zagrożeń terrorystycznych;
- odniesiono się do programów narodowych i działalności administracji publicznej (na przykładzie sytuacji powodziowych);
- omówiono działania ludzi, jako pracowników ochrony;
- zanalizowano szczegółowe rozwiązania, np. systemy obserwacji czy geoinformacji obrazowej.

Poszczególne treści, związane z wymienionymi grupami tematycznymi, są umieszczone w różnych częściach wydawnictwa.

Infrastrukturę krytyczną z punktu widzenia ochrony formalnoprawnej zaprezentował S. Śladkowski. Autor ten wskazuje na podejście NATO i Unii Europejskiej, a także odnosi się do pojęcia infrastruktury krytycznej w Polsce, które jest zawarte w Ustawie o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku oraz jej nowelizacji z roku 2009. W ustawie tej podkreśla się że infrastruktura krytyczna to systemy i wchodzące w ich skład obiekty i usługi które są kluczowe dla bezpieczeństwu państwa, jej obywateli i służą zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji oraz przedsiębiorców. Analizy autora rozdziału wskazują, że w przypadku uszkodzenia lub zniszczenia elementów infrastruktury krytycznej następuje kryzys. Stan kryzysu oznacza m.in. realne zagrożenie dla funkcjonowania organizacji, państwa, narodu, czy struktury. Zwraca się uwagę na znaczenie kategoryzacji obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa. Wśród nich znajdują się obiekty o charakterze wytwórczym oraz związane z infrastrukturą transportową i łącznością. Podkreśla się także znaczenie obiektów (w tym należących do przedsiębiorców), których zniszczenie lub uszkodzenie może być groźne dla życia i zdrowia ludzi, środowiska i dziedzictwa narodowego. Uwypuklenie znaczenia obiektów prywatnych wynika z faktu, że to właśnie one stanowią większość infrastruktury krytycznej Unii Europejskiej. Śladkowski zwraca uwagę na zagrożenia naturalne i technologiczne, ale podkreśla równocześnie wzrost znaczenia zagrożeń terrorystycznych. W rozdziale podkreślono rolę współpracy administracji publicznej oraz sektora prywatnego, a także współpracy wewnątrz tych sektorów na rzecz ochrony infrastruktury krytycznej. Sądzę, że takie podejście wymaga nowego spojrzenia na zarządzanie na styku tych dwóch sektorów, z uwzględnieniem współczesnych poglądów wynikających z jednej strony z nowego zarządzania publicznego, ale również doświadczeń biznesu odnośnie funkcjonowania w ramach sieci międzyorganizacyjnych. Wskazano także na inicjatywy, związane z ochroną infrastruktury krytycznej w Polsce. Chciałbym zwrócić uwagę, że w działaniach tych w wyraźny sposób powinny znaleźć swoje miejsce zamierzenia związane z ciągłym doskonaleniem specjalistów (programy edukacyjne na

poziomie szkolnictwa wyższego, studia podyplomowe itd.) w zakresie ochrony infrastruktury krytycznej.

W jednym z dalszych rozdziałów P. Daniluk wymienia 11 podsystemów, do których odnosi się Narodowy Program Ochrony Infrastruktury Krytycznej z roku 2013: zaopatrzenia (dotyczy energii, surowców energetycznych i paliw), łączności, sieci teleinformatycznych, finansów, zaopatrzenia w żywość, zaopatrzenia w wodę, ochrony zdrowia, transportu, ratownictwa i ciągłości działania administracji publicznej. Jako ostatni wymienia się system (podsystem) obejmujący produkcję, składowanie, przechowywanie, a także stosowanie substancji chemicznych i promieniotwórczych. Obejmuje on także rurociągi substancji niebezpiecznych.

R. Radziejewski w swych rozważaniach analizuje infrastrukturę krytyczną z punktu widzenia polskiego prawodawstwa. Wychodzi z definicji bezpieczeństwa narodowego, zawartej w „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022". W dokumencie napisano, że „bezpieczeństwo infrastruktury krytycznej zaczyna mieć wymiar bezpieczeństwa narodowego". Autor zwraca m.in. uwagę na fakt, że ochrona infrastruktury krytycznej wiąże się z zapewnieniem ciągłości jej działania i szybkiego odtwarzania w przypadku awarii lub zniszczenia. Odnosząc się do infrastruktury organizacji, przedsiębiorstw dotykamy obszaru polityki ich bezpieczeństwa. Istnieje już odpowiednia ustawa uwzględniająca szczególne uprawnienia ministra właściwego do spraw Skarbu Państwa odnośnie infrastruktury krytycznej w spółkach lub grupach kapitałowych sektorów: energii elektrycznej, ropy naftowej oraz paliw gazowych. Autor odnosi się do opracowania Rządowego Centrum Bezpieczeństwa dotyczącego Narodowego Programu Ochrony Infrastruktury Krytycznej, podkreślając, że w załączniku dotyczącym dobrych praktyk i rekomendacji brak jest jednak kompletu zasad i informacji dotyczących infrastruktury krytycznej. W rozdziale zawarta jest sugestia szerszego wykorzystania, dla potrzeb ochrony infrastruktury krytycznej normy BS 25999 „Zarządzanie ciągłością działania". Wydaje się, że skorzystanie z tej normy może być rzeczywiście przydatne w praktyce zapewnienia bezpieczeństwa infrastruktury krytycznej.

M. Kopczewski, L. Pawelec i M. Tobolski odnoszą się do odporności infrastruktury krytycznej. Omawiają programy zapobiegania awariom przemysłowym i przygotowania działań po wystąpieniu awarii, w oparciu o zewnętrzne i wewnętrzne plany operacyjno-ratownicze. Przywołują dyrektywę Rady Unii Europejskiej z 9 grudnia 1996 (Seveso II – „W sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi"), która ma swoje odzwierciedlenie w polskim Prawie Ochrony Środowiska. Na tym tle zwracają uwagę, że gdy awaria wykracza poza teren zakładu to zewnętrzny plan operacyjno-ratowniczy przygotowuje PSP (komendant Wojewódzki PSP) i co warte podkreślenia – z możliwością udziału społeczeństwa, którego plan dotyczy. Chciałbym zwrócić w tym miejscu uwagę na fakt, że współpraca ze społecznościami lokalnymi będzie uwarunkowana m.in. stanem świadomości obywateli o występujących zagrożeniach. Autorzy podkreślają znaczenie tworzenie map ryzyka na poziomie infrastruktury lokalnej. Szczegółowo omawiają m.in. rolę straży miejskiej/gminnej, które sygnalizują konieczność interwencji w związku np. z występującymi awariami infrastruktury.

W kolejnym rozdziale rolę PSP w systemie ochrony infrastruktury krytycznej omawiają M. Kopczewski i M. Tobolski. Podkreślają, że władzom lokalnym powinny być

udostępniane wewnętrzne plany operacyjno-ratownicze dla zakładów o znaczeniu infrastruktury krytycznej, dla umożliwienia opracowania zewnętrznych planów operacyjno-ratowniczych. W uzgodnieniach planów zewnętrznych bierze udział PSP. Dyrektywa Seveso II nakłada obowiązek przekazywania społeczeństwu informacji o zagrożeniach i sposobach przeciwdziałania w sytuacjach zaistniałych wypadków. Informacje te powinny być przekazywane przez zarządzających zakładami i władze publiczne. Informacja może mieć charakter pasywny (o stałym dostępie, na życzenie społeczne) lub aktywny (o charakterze wyprzedzającym). Omówiono rolę PSP w świetle obowiązujących aktów prawnych w zakresie infrastruktury krytycznej odnośnie zewnętrznych i wewnętrznych planów operacyjno-ratowniczych, raportów bezpieczeństwa, kwalifikacji zakładów do grup zwiększonego lub dużego ryzyka, szczegółowego zakresu informacji udostępnianej do wiadomości publicznej i zgłaszania poważnych awarii. Chciałbym zwrócić uwagę, że komunikacja z różnymi podmiotami i reprezentantami społeczności (w tym lokalnej) może wykorzystywać dorobek teoretyczny i praktyczny związany ze współdziałaniem przedsiębiorstw z interesariuszami, dosyć szeroko omawiany w literaturze z zakresu nauk o zarządzaniu. PSP odpowiada za organizację Krajowego Sytemu Ratowniczo-Gaśniczego, który jest aktualnie przekształcany w Zintegrowany System Ratowniczy. PSP ma za zadanie nie tylko współdziałać ze wszystkimi służbami i podmiotami ratowniczymi, ale także z organizacjami pozarządowymi.

A. Biłozor i K. Szuniewicz odnoszą się do roli informacji przestrzennej w analizie zagrożeń. W szczególności omawiają możliwości wykorzystania geoinformacji obrazowej do oceny zagrożeń i ochrony infrastruktury krytycznej. Prezentowany jest m.in. informatyczny system ochrony przed nadzwyczajnymi zagrożeniami, w tym np. powodziowymi z wykorzystaniem ortofotomap. Podkreślono znaczenie tworzenia map zagrożeń i modeli potencjału kryzysowego miast. Z kolei K. Nowakowski, A. Wyrzykowski i M. Pająk prezentują, na przykładzie konkretnej gminy zagrożenia i ochronę infrastruktury krytycznej.

W kolejnym rozdziale M. Żuber i J. Miedziak odnoszą się do ochrony infrastruktury krytycznej wobec konieczności zapewnienia bezpieczeństwa energetycznego Państwa. W Ustawie Prawo energetyczne z 10 kwietnia 2007 roku podkreśla się, że bezpieczeństwo energetyczne Państwa, związane z pokryciem bieżącego i perspektywicznego zapotrzebowania na paliwa i energię realizuje się w sposób technicznie i ekonomicznie uzasadniony, z zachowaniem wymagań ochrony środowiska. Podstawę bezpieczeństwa energetycznego stanowi zatem pewność dostaw, konkurencyjność i spełnienie wymagań ochrony środowiska. Podkreślane jest znaczenie przedsiębiorstwa energetycznego, pełniącego funkcję operatora systemu przesyłowego oraz przedsiębiorstw będących operatorami systemów dystrybucyjnych. Autorzy zwracają uwagę, że infrastruktura krytyczna jest wrażliwa zarówno na oddziaływanie warunków naturalnych jak i oddziaływań celowych zarówno w czasie wojny, jak i pokoju. Zniszczenie lub uszkodzenie jednego elementu (obiektu) systemu wpływa na pozostałe. W opracowaniu podkreślono że ochrona infrastruktury krytycznej to proces, mający na celu zapewnienie funkcjonalności, ciągłości działań, ale również integralności tej struktury. Obejmuje on zadania dotyczące zapobiegania zagrożeniem, ograniczania ich skutków, zmniejszania podatności na zagrożenia ale także przywracanie właściwego funkcjonowania po zaistnieniu zakłóceń. Podkreślana jest konieczność

nieustannego doskonalenia. Chcę zwrócić uwagę, że koncepcja ciągłego doskonalenia ma mocne podstawy teoretyczne i praktyczne w naukach o zarządzaniu i celowe wydaje się szersze skorzystanie z tych doświadczeń na rzecz zapewnienia bezpieczeństwa infrastruktury krytycznej. Wydaje się także zasadne, aby doświadczenia z zakresu ciągłego doskonalenia dotyczącego infrastruktury krytycznej były wykorzystywane z kolei w zarządzaniu przedsiębiorstwami, które choć nie stanowią obiektów infrastruktury krytycznej, to narażone mogą być na różnego typu katastrofy, w tym naturalne. W rozdziale omawiane są zasady zawarte w Narodowym Programie Ochrony Infrastruktury Krytycznej (opracowanym przez Rządowe Centrum Bezpieczeństwa w 2013 roku), a więc: współodpowiedzialność, współpraca i zaufanie.

M. Kopczewski i P. Rowiński, w ramach problematyki bezpieczeństwa energetycznego omawiają zagadnienie zasobów gazowych jako elementu infrastruktury krytycznej. Analizują uwarunkowania międzynarodowe dostępności do gazu jako zasobu. Autorzy za cel opracowania stawiają analizę poziomu zagrożenia, która wynika z braku wspólnej polityki bezpieczeństwa gazowego Unii Europejskiej. Prezentują zachowania UE oraz podają ilościowe zestawienia związane ze zużyciem gazu i jego docelowym zapotrzebowaniem. Podkreślają, że stopień zagrożenia bezpieczeństwa gazowego poszczególnych państw Unii Europejskiej jest różny. Chcę podkreślić, że temat ten jest aktualny, a o jego aktualności przypominają perturbacje związane z potencjalnym lub rzeczywistym zagrożeniem dla ciągłości dostaw pomiędzy różnymi krajami.

W kolejnym rozdziale D. Olender odnosi się, na przykładzie gazoportu jako elementu infrastruktury krytycznej, do problematyki zagrożeń terrorystycznych Podkreślane jest, w ujęciu systemowym znaczenie rozpoznania, prewencji, zwalczania i likwidacji skutków ataków terrorystycznych. Uwypuklana została rola kształtowania odpowiedniej świadomości społecznej wobec zagrożeń kryzysowych i współpracy międzynarodowej.

P. Daniluk odnosi się z kolei do podsystemu teleinformatycznego i łączności jako części infrastruktury krytycznej w związku z Narodowym Programem Ochrony Infrastruktury Krytycznej z 2013 roku. Zwraca uwagę że program ten jest kierowany do administracji publicznej, operatorów infrastruktury krytycznej, przedsiębiorców, środowiska naukowego i społeczeństwa. Według tego dokumentu na strukturę krytyczną składają się określone obiekty, urządzenia, instalacje i usługi. Infrastruktura krytyczna stanowi system, oparty na podsystemach o kluczowym znaczeniu dla bezpieczeństwa państwa oraz jego obywateli (możliwość ochrony w pierwszej kolejności dotyczy państwa) i także służy sprawnemu funkcjonowaniu administracji, instytucji i przedsiębiorców (w kolejności jak zostały wymienione, czyli pierwsza kolejność dotyczy organów administracji państwa, a ostatnia – przedsiębiorstw). W oparciu o Ustawę o zarządzaniu kryzysowym z 2007 roku i Narodowy Program Ochrony Infrastruktury Krytycznej z 2013 roku można wnioskować, jakie systemy (podsystemy) obejmuje infrastruktura krytyczna (jest ich 11). Autor zwraca uwagę, że nie zostały określone jednoznacznie kryteria dla podziału systemu infrastruktury krytycznej, przy wydzielaniu poszczególnych podsystemów, i proponuje kryteria: rynkowe, informacyjne, ekonomiczne, technologiczne i społeczne. W sposób bardziej szczegółowy autor odnosi się do dwóch spośród 11 podsystemów: łączności oraz systemów teleinformatycznych. Zgłasza szereg uwag, pytań i propozycji.

W kolejnym rozdziale Z. Pietras i W. Winter zwracają uwagę na zagrożenia infrastruktury drogowej jako elementu infrastruktury krytycznej, z punktu widzenia bezpieczeństwa ruchu drogowego, uwzględniając stan techniczny dróg. A. Kowalczyk odnosi się z kolei do odporności elementu infrastruktury krytycznej na przykładzie układu komunikacyjnego Uniwersytetu. Wykorzystano przy tym analizę sieci bezskalowej. W kolejnym rozdziale B. Michailiuk analizuje potencjalne zagrożenia kolejowej infrastruktury transportowej. Omawia zagrożenia związane z przewozem koleją środków toksycznych. Wynikają one z faktu, że w Polsce funkcjonuje ponad 500 zakładów używających w produkcji lub posiadających niebezpieczne, toksyczne środki przemysłowe. Zwraca uwagę, że obiektami działań terrorystycznych mogą być obiekty infrastruktury transportu. K. Chomiczewski podejmuje temat zagrożeń bioterrorystycznych w transporcie morskim, omawia czynniki zagrożenia terrorystycznego związane z żeglugą. Odnosi się do działań w zakresie bezpieczeństwa żeglugi. Podkreśla, że skuteczne przeciwdziałanie zagrożeniom bioterrorystycznym w transporcie morskim jest niezwykle trudne.

Ostatnie rozdziały opracowania dotyczą różnych kwestii szczegółowych, jednak dobrze wkomponowują się w całościowe spojrzenie na ochronę infrastruktury krytycznej. A. Pęk i J. Żuber odnoszą się do roli pracowników ochrony fizycznej w zabezpieczeniu obiektów infrastruktury krytycznej. Opierając się na analizie aktów prawnych, omawiają wymagania związane z kategoryzacją pracowników ochrony. Porównują różne akty normatywne (prawne) w Polsce (lata 1997–2007), w których występują terminy dotyczące szczególnie ważnej infrastruktury dla prawidłowego funkcjonowania państwa. K. Szwarc i P. Zaskórski omawiają rolę „chmury obliczeniowej", jako formy usług informacyjnych, dla poprawy ciągłości działania organizacji w tym w warunkach zagrożeń i kryzysów. Chmura umożliwia powszechny dostęp do współdzielonej puli zasobów obliczeniowych. Jest jednak możliwość ograniczenia dostępu jedynie dla określonej grupy odbiorców. Autorzy zwracają uwagę na konieczność ochrony zasobów informacyjnych (jako zasobu krytycznego) przed zagrożeniami, w szczególności w sytuacjach kryzysowych. Odnoszą się też do pojęcia bezpieczeństwa informacyjnego. G. Pietrek analizuje działania administracji państwowej wobec zagrożeń powodziowych, w oparciu o raport NIK z roku 2012. Omawia organizację ochrony przeciwpowodziowej w Polsce. P. Mądrzycki, D. Karczmarz i K. Butlewski, opisują z kolei stacjonarny system obserwacji terenu wykorzystywany w misjach, dla ochrony baz wojskowych.

Omawiana książka zawiera zbiór informacji i przemyśleń na temat ochrony infrastruktury krytycznej. Odnosi się do infrastruktury krytycznej jako całości, ale rozważa także zagrożenia dla poszczególnych jej elementów. Wskazuje, że powodzenie działań wiąże się nie tylko z koniecznością przygotowania odpowiednich aktów prawnych, przepisów czy procedur, ale wymaga współdziałania podmiotów z różnych sektorów: publicznego, społecznego i biznesu (przedsiębiorstw). Jest to wartościowa pozycja wydawnicza, inspirująca do dalszych przemyśleń i propozycji.