JERZY KOWALSKI

Podmiotowy i przedmiotowy wymiar ochrony infrastruktury krytycznej w aspekcie zagrożeń asymetrycznych

Infrastruktura krytyczna, systemy wchodzące w jej skład, ich charakterystyka i znaczenie dla bezpieczeństwa państwa

Infrastruktura – to urządzenia i instytucje usługowe, niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki[1]. Krytyczny – stanowiący przełom w czymś, rozstrzygający[2]. Analiza treści powyższych definicji pozwala stwierdzić, iż znaczenia te mają charakter systemowy, stanowiący uporządkowaną i połączoną całość.

W znaczeniu międzynarodowym europejska infrastruktura krytyczna zdefiniowana jest jako: infrastruktura krytyczna zlokalizowana na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie[3]. W znaczeniu narodowym infrastruktura krytyczna określana jest jako pojęcie: przez które należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz

[1] M. Bańka, *Wielki słownik wyrazów obcych PWN*, Warszawa 2003, s. 544.

[2] B. Dunaj, *Słownik współczesnego języka polskiego*, t. 1, Warszawa 1999, s. 434.

[3] Art. 2b Dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony.

służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[4].

Znaczenie infrastruktury krytycznej (systemów) dla funkcjonowania państwa obiektów, instalacji i usług ma zasadnicze znaczenie w kształtowaniu należnego poziomu bezpieczeństwa obywateli.

System zaopatrzenia w energię, surowce energetyczne i paliwa przeznaczony jest do: zapewnienie obywatelom energii elektrycznej i cieplnej, zaopatrzenie struktur państwa w paliwa zapewniając właściwe funkcjonowanie gospodarki oraz społeczeństwa. Jego infrastruktura zapewnia wydobycie węgla na potrzeby elektroenergetyki, wytwarzanie energii elektrycznej oraz jej dostarczenie odbiorcom indywidualnym i przemysłowi, umożliwia wydobycie, import i przetwarzanie surowej ropy naftowej. Zapewnia również wydobycie, import i dostarczanie gazu ziemnego odbiorcom w celu zagwarantowania użytkowania urządzeń grzewczych w gospodarstwach domowych oraz wytwarzanie dóbr materialnych opartych o te źródła energii. Składa się z sektorów: energii elektrycznej, gazu ziemnego, ropy naftowej oraz sektora energii cieplnej.

Kolejnym elementem krytycznym jest system łączności, którego zadaniem jest zapewnienie i przekazywanie informacji, poprzez pocztę oraz telekomunikację, jak również radiofonię i telewizję. System ten ma bezpośredni wpływ na takie procesy gospodarki jak: biznesowy, zarządzania, relacje administracja – obywatel i odwrotnie.

Trzecim systemem jest system sieci teleinformatycznych określony jako: zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

[4] Ustawa z dnia 26 kwietnia 2007r. o zarządzaniu kryzysowym (Dz. U. z 2007 r., nr 89, poz. 590 ze zm.).

System finansowy jako ogół norm prawnych oraz zespół instytucji finansowych, których zasadniczym zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa ma decydujące znaczenie dla sprawnego funkcjonowania państwa i społeczeństwa pod warunkiem, kiedy sam funkcjonuje właściwie. Składa się on z segmentów budżetowego, bankowego, ubezpieczeniowego i kapitałowego.

System zaopatrzenia w żywność stanowi dziedzinę gospodarki składającą się z podsystemów wytwarzania środków produkcyjnych, usług dla rolnictwa, produkcji i pozyskiwania surowców żywnościowych w takich obszarach jak rolnictwo, skup surowców żywnościowych, ich przechowywanie i transport, przetwórstwo surowców żywnościowych, obrót towarowy produktami żywnościowymi oraz system bezpieczeństwa żywności obejmujący wszystkie składowe łańcucha zaopatrzenia w żywność.

System zaopatrzenia w wodę stanowi powiązane ze sobą przedsiębiorstwa i urządzenia pobierające, uszlachetniające, dostarczające i oczyszczające wodę dla odbiorców indywidualnych oraz przemysłu. Wraz z rozwojem cywilizacyjnym oraz postępującą koncentracją ludności w aglomeracjach miejskich zaopatrzenie w wodę i odbiór ścieków w dzisiejszych czasach jest jedną z najistotniejszych usług zapewniających sprawne funkcjonowanie społeczności.

System ochrony zdrowia to nic innego jak zespół osób i instytucji, którego nadrzędnym celem jest zapewnienie opieki zdrowotnej ludności, a jego sprawne funkcjonowanie (wraz z systemem ratowniczym) jest gwarantem praw obywatela zapisanych w Konstytucji.

System ratowniczy swoją nazwę opiera na ratownictwie, przez które rozumiemy ogół środków i przedsięwzięć organizacyjnych podejmowanych w celu ratowania zdrowia i życia, mienia i środowiska, znajdującym się w niebezpieczeństwie oraz przewidywania, rozpoznawania i likwidacji skutków zdarzeń. W ramach Systemu Ratownictwa w Polsce funkcjonują: Krajowy System Ratowniczo-Gaśniczy; Państwowe Ratownictwo Medyczne; System

Powiadamiania Ratunkowego; Ratownictwo górskie; Ratownictwo morskie; Ratownictwo górnicze; Ratownictwo wodne; Krajowy System Wykrywania Skażeń i Alarmowania.

System produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych jest kolejnym systemem zaliczanym do infrastruktury krytycznej. W skład opisywanego systemu wchodzą m.in. obiekty jądrowe i źródła promieniowania jonizującego oraz rurociągi substancji niebezpiecznych[5].

Zaprezentowane systemy infrastruktury krytycznej są niewątpliwie kluczowymi z punktu widzenia funkcjonowania państwa obiektami i systemami, od sprawności których zależy ciągłość działania określonych instytucji użyteczności publicznej, w tym struktur sprawowania władzy. Owe obiekty i systemy można przyporządkować do czterech obszarów związanych z obronnością państwa; ochroną interesu gospodarczego państwa; bezpieczeństwem publicznym; ochroną innych ważnych interesów państwa.

W skład obszaru związanego z obronnością państwa zaliczyć należy zakłady prowadzące badania z zakresu prac konstrukcyjnych oraz produkujące na potrzeby obronności kraju oraz magazyny rezerw państwowych i zakłady produkcji specjalnej. Kolejny obszar stanowiący ochronę interesu gospodarczego państwa wiąże się z zapewnieniem bezpieczeństwa obiektom mającym związek z wydobyciem surowców mineralnych o znaczeniu strategicznym dla państwa, portom i lotniskom, bankom oraz zakładom wytwarzającym, przechowującym bądź transportującym znaczne ilości pieniędzy lub papierów wartościowych. Trzeci obszar, dotyczy bezpieczeństwa publicznego. Związany jest z ochroną zakładów, obiektów i urządzeń, zapewniających właściwe funkcjono-

[5] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej*, zał. nr 1 Charakterystyka systemów ochrony infrastruktury krytycznej, Warszawa 2013, s. 4.

wanie społeczeństwa a uszkodzenie ich bądź zniszczenie spowodowałoby ogromne konsekwencje dla życia i zdrowia obywateli oraz środowiska naturalnego. Z kolei do obiektów zapewniających ochronę innych ważnych interesów państwa zalicza się zakłady prowadzące unikalną produkcję gospodarczą, obiekty związane z dystrybucją informacji (telewizja, poczta, Internet), archiwa państwowe oraz obiekty związane z ochroną dziedzictwa narodowego.

Z powyższego wynika, iż infrastruktura krytyczna niewątpliwie stanowi kluczowe znaczenie dla istnienia państwa, oraz funkcjonującego w nim – zorganizowanego społeczeństwa. W wyniku zakłócenia jej funkcjonowania, państwo i jego instytucje narażone są na utratę zdolności do wykonywania podstawowych funkcji administracyjnych i usługowych co więcej może również utracić zdolność do sprawowania rzeczywistej kontroli nad całym swoim terytorium. Za przykład może posłużyć sytuacja jaka miała miejsce w stolicy Iraku po 2003 r., gdzie jeszcze kilka lat po amerykańskiej inwazji w wielu rejonach miasta nie przywrócono regularnych dostaw energii elektrycznej i wody co przełożyło się na negatywne nastroje lokalnej ludności a w konsekwencji na brak bezpieczeństwa w mieście[6]. Obecne wydarzenia na Ukrainie są kolejnym przykładem próby przejęcia kluczowych obiektów infrastruktury krytycznej wschodniej części państwa przez grupy ekstremistyczne.

Zagrożenia asymetryczne a infrastruktura krytyczna

Zagrożenie definiowane jest jako sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia[7].

[6] Www.bbn.gov.pl/download/1/8612/181-197KarolStec.pdf (23.11.2013).

[7] J. Kunikowski, *Słownik terminów z zakresu wiedzy i edukacji dla bezpieczeństwa* [w:] *Bezpieczeństwo człowieka i zbiorowości społecznych*, W. J. Maliszewski, Bydgoszcz 2005, s. 189.

Jednym z podziałów zagrożeń, na które warto zwrócić uwagę przedstawia prof. R Wróblewski, który dzieli zagrożenia na symetryczne i asymetryczne. Przy czym asymetria ta odnosi się głównie do przeciwstawności celów, środków i metod działania stron konfliktu. Innymi słowy występuje wtedy, gdy jedna ze stron nie jest w stanie przeciwstawić się drugiej w sposób symetryczny, wykorzystując te same lub podobne środki walki[8].

Na początku lat 90. pojawił się nowoczesny wymiar podejścia do zagrożeń tego typu. Dotyczył on głównie przyczyn i źródeł powstawania zagrożeń asymetrycznych, a w tym potencjalnego ryzyka generowania nowych konfliktów zbrojnych oraz perspektywicznych zagrożeń krótko i długofalowych. Tragiczne wydarzenia z 11 września 2001 roku oraz zamachy w teatrze na Dubrobce, w Madrycie, Biesłanie, Londynie czy ostatnio w Wołgogradzie pokazują, że prawdziwe bezpieczeństwo globalne nie istnieje i w najbliższym czasie podobne wydarzenia mogą się powtarzać, niekoniecznie przy użyciu tych samych środków.

Systemy łączności oraz systemy sieci teleinformatycznych stanowiące elementy infrastruktury krytycznej, określone zostały mianem przedmiotu najbardziej narażonego na ingerencję z zewnątrz. Wymienione systemy to nic innego jak tzw. nowe technologie, technologie informacyjne dające nowe możliwości w dziedzinie poszukiwania, gromadzenia, przetwarzania i wykorzystywania informacji.

Globalne środowisko społeczne funkcjonujące w sieci teleinformatycznej sprzyja powstawaniu nowych zagrożeń a także rozwojowi dawnych, wyniesionych niejako z „ery industrialnej". Do nich należy zaliczyć: zorganizowany terroryzm międzynarodowy; proliferację broni masowego rażenia; nowe rodzaje przestępczości związane z rozwojem technologii informacyjnych (infoterroryzm, cyberterroryzm); niekontrolowane operacje finansowe

[8] B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, s. 9–11.

(zwłaszcza w e-bankowości); wrażliwość krytycznej infrastruktury państwa (zwłaszcza na cyberataki); wrażliwość globalnego systemu gospodarczego; zagrożenia ekologiczne (degradacja ekosfery); zagrożenia informacyjne (degradacja infosfery); wzrost zasięgu społeczności „odrzuconych", marginalizowanych (trudności w asymilacji i integracji); wzrost bezrobocia (w tym strukturalnego); wymuszone masowe migracje; przestępczość transgraniczną; nowe choroby zakaźne; rozwój zasięgu fundamentalistów.

Różna jest waga i skala wymienionych zagrożeń, jedne są bezpośrednim skutkiem globalizacji, inne zaś – rozwoju technologii informacyjnych.

W literaturze polskiej przedmiotu E. Lichocki podaje, że cyberterroryzm to: „przemyślany, politycznie lub militarnie motywowany, atak albo groźba ataku na systemy teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia infrastruktury krytycznej państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących politycznomilitarnych działań.

Można stwierdzić, że w znaczeniu wąskim cyberterroryzm to działalność terrorystyczna w systemach teleinformatycznych ukierunkowana na zniszczenie lub modyfikację danych w tych systemach, skutkujących ofiarami śmiertelnymi a często i zniszczeniem mienia w znacznych rozmiarach. W szerszym znaczeniu jest to wszelka działalność terrorystyczna związana z cyberprzestrzenią (systemami teleinformatycznymi) włączając w to fizyczne ataki na systemy oraz aktywność propagandową. Działalność taka może na przykład przyczynić się do pozyskiwania informacji przydatnych w realizacji bardziej klasycznych akcji terrorystycznych w tym zamachów bombowych.

Szczególnie groźne może być zaatakowanie systemów informacyjnych związanych z infrastrukturą krytyczną państwa zarówno cywilną, jak i wojskową. W kontekście wojskowej infrastruktury krytycznej, dużym zagrożeniem jest zarówno możliwość zaatakowania systemów informacyjnych mających kluczowe znaczenie dla systemu dowodzenia, jak i systemu obrony powietrznej

państwa. Skutki potencjalnego ataku cyberterrorystów mogą być na razie szacowane tylko teoretycznie, jednak należy przypuszczać, że byłyby poważne. Jako przykład możliwości oddziaływania potencjalnych cyberterrorystów posłużyć mogą systemy komputerowe Pentagonu. Hackerzy włamują się do nich średnio 250 tysięcy razy rocznie. Skuteczność tego typu ataków wynosi 65%. Departament Obrony Stanów Zjednoczonych przeprowadził badania, w ramach których dokonano 8932 próby penetracji własnych systemów komputerowych. Powiodło się 88% prób, z tego tylko 320 włamań zostało wykrytych a jedynie 22 zostały zgłoszone przez system zabezpieczający.

W odróżnieniu od broni jądrowej, ofensywne środki walki informacyjnej są w zasięgu możliwości prawie każdego państwa i także aktorów niepaństwowych, w tym również organizacji terrorystycznych. Celem tej walki będzie rozpoznanie, a następnie obezwładnienie systemów komputerowych przeciwnika, tak aby nie był on zdolny do podejmowania jakiejkolwiek działań. Skoro więc systemy obrony większości rozwiniętych państw oparte są na systemach informatycznych, aby przeprowadzić skuteczny atak wystarczy sparaliżować lub zakłócić ich funkcjonowanie.

Podsumowując, można stwierdzić, że największym zagrożeniem w cyberprzestrzeni, rozumianej jako system powiązań internetowych jest cyberterroryzm. Jest on zjawiskiem niezwykle szkodliwym zarówno dla społeczeństwa i prawidłowego rozwoju działalności gospodarczej, jak również dla infrastruktury krytycznej państwa[9].

Podmiotowy i przedmiotowy wymiar ochrony infrastruktury krytycznej

Ochrona infrastruktury krytycznej jest zagadnieniem nowym, którego owocem jest uchwalona w 2007 roku Ustawa o zarządza-

[9] *Ibidem*, s. 59–70.

niu kryzysowym, w której systemowo określono zakres jej ochrony, zadania poszczególnych podmiotów wskazując również jej przedmiotowy zakres.

Przez ochronę infrastruktury krytycznej należy rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie[10]. Należy jednocześnie pamiętać, że ochrona infrastruktury krytycznej powinna mieć charakter kompleksowy, co oznacza uwzględnienie w organizacji ochrony następujących obszarów: ochrony fizycznej, technicznej, osobowej, teleinformatycznej, prawnej oraz pomoc strony rządowej w trakcie jej odbudowy.

Zgodnie z założeniami ustawy o zarządzaniu kryzysowym to właściciele oraz posiadacze samoistni i zależni elementów infrastruktury krytycznej odpowiadają za odpowiednią ochronę obiektów, obszarów, instalacji oraz urządzeń określonych jako infrastruktura krytyczna państwa. Do nich również należy obowiązek opracowania planów ochrony posiadanej infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych, zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie elementu infrastruktury krytycznej aż do czasu jej odtworzenia[11].

Zgodnie z powyższym, ciężar ochrony infrastruktury krytycznej spoczywa na jej operatorach. Jednak biorąc pod uwagę jej znaczenie dla funkcjonowania państwa, ustawodawca zadania z zakresu ochrony infrastruktury przypisał również podmiotom administracji publicznej. Niewyobrażalnym jest, by władze publiczne odmówiły pomocy poszkodowanym, pozostawiając ten pro-

[10] Http://rcb.gov.pl/?page_id=210 (17.11.2013).

[11] A. Tyburska, *Ochrona infrastruktury krytycznej zarys problematyki*, Szczytno 2012, s. 151.

blem wyłącznie operatorowi infrastruktury krytycznej. Pamiętając o potencjalnych skutkach awarii infrastruktury krytycznej dla ludzi, ich mienia, gospodarki narodowej czy środowiska, niezależnie, czy infrastruktura krytyczna jest w zarządzie administracji publicznej czy pozostaje całkowicie we władaniu podmiotów gospodarczych, spodziewane skutki awarii infrastruktury krytycznej powodują, że zadania z zakresu jej ochrony realizowane są na wszystkich szczeblach administracji państwa.

Zgodnie z założeniami ustawy o zarządzaniu kryzysowym Dyrektor Rządowego Centrum Bezpieczeństwa zobowiązany został do przygotowania w porozumieniu z właściwymi ministrami oraz kierownikami urzędów centralnych wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej. Po sporządzeniu wykazu dyrektor Rządowego Centrum Bezpieczeństwa przygotowuje wyciągi z dokumentu dla ministrów i kierowników urzędów centralnych odpowiedzialnych za poszczególne systemy infrastruktury krytycznej oraz dla wojewodów, na terenie których znajduje się dana infrastruktura. Informuje on również właścicieli i posiadaczy infrastruktury krytycznej o ujęciu jej we wspomnianym wykazie. Z kolei wojewodowie upoważnieni zostali przez ustawodawcę do poinformowania odpowiednich organów administracji publicznej o infrastrukturze znajdującej się na terenie danego województwa, z zastrzeżeniem, że informacja o infrastrukturze krytycznej przekazywana jest jedynie niezbędnym podmiotom.

Podsumowując, należy podkreślić wiodącą rolę Rządowego Centrum Bezpieczeństwa w kształtowaniu polityki bezpieczeństwa infrastruktury krytycznej państwa. Jednocześnie ochrona infrastruktury krytycznej jest zadaniem przypisanym zarządzającym (właścicielom) konkretnymi elementami infrastruktury, którzy są zobowiązani do opracowania i wdrożenia konkretnych rozwiązań uodporniających infrastrukturę tego typu na zagroże-

nia, rozwiązanie te odzwierciedlają w opracowanych planach ochrony infrastruktury krytycznej, które podlegają obowiązkowej aktualizacji w okrasach nie dłuższych niż dwa lata[12].

Ochrona infrastruktury krytycznej w swoim przedmiocie związana jest z racją stanu, co wskazuje na konieczność podjęcia szczególnych starań w zakresie ochrony kluczowej infrastruktury państwa. W związku z powyższym ważnym jest przedstawienie wybranych narzędzi potrzebnych do ochrony infrastruktury krytycznej, zwłaszcza tych elementów, które zapewniają ciągłość działania organów administracji publicznej oraz gwarantują bezpieczeństwo ludzi.

Regulacje dotyczące ochrony infrastruktury krytycznej znajdujące się w aktach prawnych obejmujących rożne dziedziny funkcjonowania państwa w swoich zapisach wskazują przedmiotowy wymiar ochrony infrastruktury krytycznej. Należą do nich:

Ustawa z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców[13]. Ustawa mówi o realizacji zadań na rzecz obronności państwa w zakresie mobilizacji gospodarki, militaryzacji, planowania operacyjnego, szkolenia obronnego.

Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia[14], która w kontekście infrastruktury krytycznej za ważne uznaje kategorie obszarów, obiektów, urządzeń i transportów podlegających obowiązkowej ochronie, ważnych dla obronności, interesu gospodarczego, bezpieczeństwa publicznego i innych ważnych interesów państwa.

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze[15]. Obejmuje treści dotyczące żeglugi powietrznej, naziemnej infrastruktury lotniskowej oraz statków powietrznych. Problematyka ochrony lotnic-

[12] A. Tyburska, *Ochrona*…, *op. cit.*, s. 157–158.
[13] Dz. U. nr 2001, nr 122, poz. 1320 ze zm.
[14] Dz. U. z 2005 r., nr 145, poz. 1221 ze zm.
[15] Dz. U. z 2013 r., poz. 1393 ze zm.

twa cywilnego przed aktami bezprawnej ingerencji, zagrażającymi bezpieczeństwu lotnictwa oraz osób i mienia zawarta została w odrębnych ustawach oraz umowach i przepisach międzynarodowych.

Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym[16] odnosi się do infrastruktury kolejowej, której część stanowi infrastrukturę krytyczną. Za istotną część infrastruktury kolejowej należy uznać zdefiniowane w ustawie linie kolejowe o znaczeniu państwowym, linie kolejowe o znaczeniu obronnym oraz wyłącznie obronnym.

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[17] reguluje zasady prowadzenia działalności świadczenia usług telekomunikacyjnych. Jako narzędzie ochrony infrastruktury krytycznej wymieniona ustawa jest istotna z kilku powodów. Definiuje przedsiębiorcę telekomunikacyjnego, co pozwala w wielu przypadkach kwalifikować zarządzane przez niego instalacje, obiekty i urządzenia jako wchodzące w skład systemu telekomunikacyjnego infrastruktury krytycznej. Nakłada również na operatorów określone obowiązki umożliwiające monitorowanie infrastruktury telekomunikacyjnej.

Ustawa z dnia 18 lipca 2001 r. Prawo wodne[18] kompleksowo reguluje zagadnienia gospodarki wodnej, zawiera m.in. unormowania dotyczące ścisłej ochrony i nadzoru określonych obszarów, istotnych z punktu widzenia dostarczania wody pitnej.

Ustawa z dnia 29 października 2010 r. o rezerwach strategicznych[19] wskazuje powód tworzenia rezerw strategicznych – w tym kontekście wymieniono m.in. zagrożenie dla bezpieczeństwa i obronności państwa, bezpieczeństwa i porządku publicznego, wsparcie realizacji zadań w zakresie bezpieczeństwa i obrony

[16] Dz. U. z 2013 r., poz. 1594 ze zm.
[17] Dz. U. z 2014 r., poz. 243 ze zm.
[18] Dz. U. z 2012 r., poz. 145 ze zm.
[19] Dz. U. nr 229, poz. 1496 ze zm.

państwa, odtworzenie infrastruktury krytycznej, złagodzenie zakłóceń w ciągłości dostaw służących funkcjonowaniu gospodarki i zaspokojeniu podstawowych potrzeb obywateli.

Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony[20], określa obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa. Obszerny katalog, zawierający dziewiętnaście kategorii obiektów, obejmuje m.in. obiekty formacji i służb, obiekty związane z wydobywaniem kopalin, telekomunikacyjne, magazyny rezerw państwowych, zapory wodne i urządzenia hydrotechniczne, elektrownie i obiekty elektroenergetyczne, a także obiekty podległe lub nadzorowane przez Ministra Obrony Narodowej.

Powyższa analiza dowodzi, że planowanie i realizacja zadań ochronnych prowadzone są od wielu lat, a ustawa o zarządzaniu kryzysowym stanowi podstawę prawną do kompleksowego zdefiniowania i wyodrębnienia takiej infrastruktury z rożnych sektorów społeczno-gospodarczych.

W obecnej sytuacji ochrona infrastruktury krytycznej staje się priorytetowym zadaniem podmiotów za nią odpowiedzialnych. W dzisiejszych czasach to właśnie elementy zaliczane do infrastruktury krytycznej będą w pierwszej kolejności narażone na różnego rodzaju zagrożenia. Przykładem są aktualne wydarzenia mające miejsce na Ukrainie, gdzie prorosyjskie grupy ekstremistyczne w pierwszej kolejności dążą do zajęcia obiektów administracji publicznej. Tworzą nowe struktury władzy przejmując w ten sposób wpływ nad mieszkańcami zamieszkującymi dany obszar administracyjny. W dalszych działaniach dążą do odizolowania terenu, którym są zainteresowani. Odizolowanie takie, może powstać w wyniku przejęcia, uszkodzenia lub zniszczenia m.in. mostu lub zapory wodnej, co prowadzi do powstania znacznych strat strony przeciwnej zakłócając jej właściwe funkcjonowanie. Innym

[20] Dz. U. nr 116, poz. 1090 ze zm.

przykładem może być przejęcie przez przeciwnika strategicznych obiektów ważnych dla obronności państwa. Przejęcie kontroli nad tak ważnymi obiektami często jest punktem zwrotnym każdego konfliktu, co w konsekwencji może doprowadzić do upadku państwa.

Odnosząc się do stanu obecnego w polskim systemie prawnym istnieją przepisy umożliwiające wdrożenie ochrony obiektów zaliczanych do infrastruktury krytycznej. Prowadzone są szkolenia personelu szczebla kierowniczego oraz wykonawczego praktycznie realizującego jej ochronę. Istnieją również, procedury postępowania wszystkich podmiotów, w tym: właścicieli, formacji ochrony, służb na wypadek wystąpienia zakłócenia pracy lub ataku na obiekty infrastruktury krytycznej. Mimo to, często dochodzi do zaniedbań jej ochrony. Nasuwa się pytanie, dlaczego takie sytuacje mają miejsce? Odpowiedzi jest wiele, wskazując chociażby błędy w budowaniu właściwego systemu ochrony technicznej i fizycznej, niewłaściwego współdziałania właścicieli infrastruktury krytycznej ze służbami i organami wspomagającymi jej ochronę.

Doświadczenie potwierdza, że najsłabszym elementem w zapewnieniu właściwej ochrony infrastruktury krytycznej jest człowiek. Osoba sprawująca bezpośrednią ochronę fizyczną lekceważąc sygnały wysyłane przez system ochrony fizycznej lub działając rutynowo doprowadza do dalszego rozwoju niekorzystnych zdarzeń, których konsekwencje mogą i często są zagrożeniem dla życia i zdrowia obywateli. Aby przeciwdziałać tego typu sytuacjom należy ukierunkować działania mające na celu eliminację takich niedociągnięć i zagrożeń. Jedną z sugestii wyłonionych na podstawie powyższych wniosków jest objęcie z góry nadzorem i ochroną obiektów infrastruktury krytycznej, poprzez przydzielenie ich właściwym ogniwom, co w konsekwencji zabezpieczy inne obiekty oraz ludzi przed ich separacją będącą wynikiem uszkodzenia np. mostu, zapory, elektrowni lub innych obiektów, których uszkodzenie doprowadzić może do podobnych skutków. Co więcej ochrona obiektów infrastruktury krytycznej przez wskazanie od-

powiedzialnego ogniwa zapewni funkcjonalność, ciągłość działań i integralność infrastruktury krytycznej, ograniczy i zneutralizuje skutki zagrożeń oraz doprowadzi do szybkiego odtworzenia jej funkcjonowania.