mgr Izabela Juncewicz
doktorantka Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach

INFRASTRUKTURA KRYTYCZNA W ZARZĄDZANIU KRYZYSOWYM

We współczesnym świecie rozwój cywilizacyjny stworzył dobra ułatwiające życie, podnoszące jego standard oraz zwielokrotniające możliwości komunikacji. Równocześnie jednak nastąpiła eskalacja zagrożeń[1]. Obok zagrożeń naturalnych pojawiły się nowe problemy – efekty uboczne postępu technicznego, zagospodarowania przestrzeni i wykorzystywania coraz nowszych rozwiązań technologicznych[2].

Równocześnie postępująca globalizacja, wyrażająca się powszechnym dostępem do mediów, w tym szczególnie Internetu, oraz upowszechniająca się informatyzacja wszelkich dziedzin aktywności ludzkiej tworzą organizacjom terrorystycznym dogodne możliwości dotarcia do obiektów infrastruktury[3] krytycznej[4], i tym samym powodowania zagrożeń bezpieczeństwa państwa[5].

W przypadku części zagrożeń administracja samorządowa, organizacje i społeczeństwo radzą sobie z nimi. Mają jednak miejsce sytuacje, w których rutynowe działania nie są wystarczające. Obecnie bowiem zagrożenia są coraz częściej nieprzewidywalne i mogą mieć szeroki zasięg rażenia. Z tego względu konieczne jest wcześniejsze przygotowanie i organizacja działań, aby w przypadku wystąpienia zdarzenia móc jak najszybciej zareagować. Właśnie temu celowi służy zarządza-

[1] *Zagrożenie* – zdarzenie spowodowane przyczynami losowymi (naturalnymi) lub nielosowymi (celowymi), które wywiera negatywny wpływ na funkcjonowanie jednostki, grupy społecznej, organizacji, państwa lub powoduje niekorzystne (niebezpieczne) zmiany w ich strukturze i funkcjonowaniu, K. Ficoń, *Inżynieria zarządzania kryzysowego*, Bel Studio Sp. z o.o., Warszawa 2007, s. 76.

[2] K. Sienkiewicz-Małyjurek, F. R. Krynojewski, *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa 2010, s. 9.

[3] *Infrastruktura* oznacza urządzenia i instytucje usługowe (np. drogi, sieć telefoniczna lub wodociągowa), niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki, M. Bańka (red.), *Wielki Słownik Wyrazów Obcych PWN*, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 544.

[4] *Krytyczny* czyli przełomowy, rozstrzygający; trudny, ciężki moment, położenie, E. Sobol (red.), *Nowy Słownik Języka Polskiego PWN*, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 378. Przymiotnik *krytyczny* w odniesieniu do infrastruktury będzie wskazywać, oznaczać te jej elementy, których zakłócenia lub zniszczenie może spowodować kryzys. Z kolei *kryzys* oznacza, w sensie ogólnym, wybór, decydowanie, zmaganie się, walkę, w której konieczne jest działanie pod presją czasu, I. Kulik, *Analiza pojęć obiekt infrastruktury krytycznej, obiekt szczególnej ochrony i obiekt chroniony*, [w:] Z. Piątek, A. Letkiewicz (red.), *Terroryzm a infrastruktura krytyczna państwa – zewnętrznego kraju Unii Europejskiej*, Szczytno 2010, s. 56.

[5] Z. Piątek, A. Letkiewicz (red.), *Terroryzm a infrastruktura krytyczna* ..., s. 8.

nie kryzysowe[6], realizowane przez odpowiednie jednostki administracji rządowej i samorządowej[7].

Można zatem przyjąć, że brak możliwości całkowitego wyeliminowania zagrożeń naturalnych i cywilizacyjnych, towarzyszących rozwojowi ludzkości i w tym sensie ich nieuchronności, rodzi potrzebę zarządzania kryzysowego, rozumianego najogólniej jako działania (funkcje) kierownicze mające na celu radzenie sobie z sytuacjami kryzysowymi[8], które definiowane są jako *stan narastającej destabilizacji, niepewności i napięcia społecznego, stwarzający zagrożenie dla integralności terytorialnej, życia, zdrowia, mienia, dziedzictwa kulturowego, środowiska lub infrastruktury krytycznej*[9].

Należy również zwrócić uwagę na fakt, że zdobycze cywilizacji, od których zależy komfort życia społeczeństwa, tworzą jednocześnie tzw. sprzyjające okoliczności i warunki do powstania zakłóceń, a nawet potęgowania ich następstw. W tym kontekście możemy mówić także o podatności[10] społeczeństwa na zagrożenia i ich skutki, a czynnikami wzmagającymi tę podatność są[11]:

- zagęszczenie ludności (przemieszczenie ludności do miast i tworzenie wielkich aglomeracji oraz dużych skupisk wysokich budynków), w tym czasowa koncentracja w określonych obszarach i miejscach (biurowce, środki masowej komunikacji w godzinach pracy, miejsca imprez sportowych czy centra handlowe w okresach wzmożonych zakupów);
- uzależnienie ludności od dostaw usług, podnoszących jakość warunków bytowych (bieżąca woda, żywność, energia elektryczna, paliwa, łączność, komunikacja, transport itp.);
- rozbudowana infrastruktura, od której uzależnione są dostawy ww. usług;
- występowanie infrastruktury, która jednocześnie może stanowić źródło zagrożeń dla społeczeństwa (np. zakłady o dużym ryzyku wystąpienia poważnej awarii przemysłowej);
- wykorzystanie cyberprzestrzeni[12] w gospodarce, administracji oraz codziennym życiu obywateli;

---

[6] *Zarządzanie kryzysowe* to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej, *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm., art. 2.

[7] K. Sienkiewicz-Małyjurek, F. R. Krynojewski, *Zarządzanie kryzysowe* ..., s. 9.

[8] A. Zabłocka-Kluczka, *Próba oceny procesu zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego w Polsce*, ZN WSOWL Nr 3 (157), Wrocław 2010, s. 193.

[9] J. Walas-Trębacz, J. Ziarko, *Podstawy zarządzania kryzysowego. Część 2. Zarządzanie kryzysowe w przedsiębiorstwie*, Krakowskie Towarzystwo Edukacyjne Sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2011, s. 24.

[10] *Podatność* – cechy charakterystyczne zasobów, infrastruktury, systemów, społeczeństwa lub procesów, które czynią je wrażliwymi na zniszczenie, zakłócenie funkcjonowania, zmniejszenie potencjału lub efektywności działania oraz niewłaściwe wykorzystanie, w drodze wystąpienia klęsk żywiołowych, intencjonalnej działalności człowieka, awarii technicznych lub innych szkodliwych działań. Podatność określa jednocześnie trudności (wyzwania) w ochronie zasobów, infrastruktury, systemów, społeczeństwa lub procesów, W. Skroma, *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, Rządowe Centrum Bezpieczeństwa, s. 3.

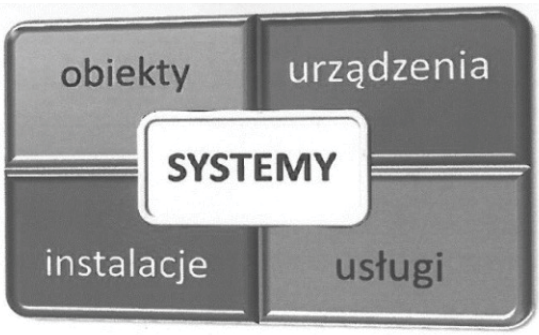
[11] W. Skroma, op. cit., s. 3-4.

[12] *Cyberprzestrzeń* – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci telein-

– niska świadomość zagrożonej ludności oraz nieadekwatne przygotowanie władz, społeczeństwa, infrastruktury do reagowania kryzysowego;
– niedostateczne i nieadekwatne wyposażenie służb odpowiedzialnych za reagowanie kryzysowe, w tym ograniczona możliwość, czy w ogóle brak możliwości ich wsparcia w przypadku wyczerpania posiadanych sił i środków.

Reasumując, można stwierdzić, że współcześnie, poczucie bezpieczeństwa kojarzy się nie tylko z brakiem zagrożeń zewnętrznych, ale głównie z zapewnieniem sprawności funkcjonowania szeroko pojętej infrastruktury państwa[13] zarówno w jej części technicznej (np. zakłady wytwórcze, energetyka, systemy łączności, teleinformatyczne, transport czy komunikacja), jak i społecznej (opieka zdrowotna, ratownictwo i ochrona ludności, edukacja itp.)[14].

Infrastruktura ta zdefiniowana została w *Ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym* jako infrastruktura krytyczna (rys. 1), czyli *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 służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców*[15].



Rys. 1. Infrastruktura krytyczna
Źródło: *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013, s. 14.

Regulacje prawne w zakresie infrastruktury krytycznej zawarte zostały zarówno w narodowych, europejskich, jak i natowskich dokumentach normatywnych. W naszym państwie ustawa o zmianie ustawy o zarządzaniu kryzysowym dokonuje implementacji do prawa polskiego dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infra-

formatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami, M. Huzarski, J. Wołejszo (red.), *Leksykon obronności Polska i Europa*, Bellona, Warszawa 2014, s. 44.

[13] *Infrastruktura państwa* – część infrastruktury obejmująca obiekty, urządzenia stałe i instytucje usługowe niezbędne do należytego funkcjonowania produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności kraju, *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2010, s. 48.

[14] W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, *Ochrona infrastruktury krytycznej*, AON, Warszawa 2012, s. 7.

[15] *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. z 2007 r. Nr 89, poz. 590, z późn. zm., art. 3, ust. 2.

struktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 2008.345.75).

W niniejszym opracowaniu pominięto jednak analizę przepisów unijnych i natowskich, skupiając się na specyfice krajowych rozwiązań w tym zakresie.

Zgodnie z ustawą o zarządzaniu kryzysowym infrastruktura krytyczna w Polsce obejmuje następujące systemy[16]:

– zaopatrzenia w energię, surowce energetyczne i paliwa,
– łączności,
– sieci teleinformatycznych,
– finansowe,
– zaopatrzenia w żywność,
– zaopatrzenia w wodę,
– ochrony zdrowia,
– transportowe,
– ratownicze,
– zapewniające ciągłość działania administracji publicznej,
– produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Dotychczasowe dociekania pozwalają stwierdzić, że obiektem infrastruktury krytycznej będą obiekty budowlane, urządzenia, instalacje, usługi funkcjonujące w ramach systemów (jak wyżej), których zniszczenie lub uszkodzenie może skutkować w krótkim czasie przerwaniem funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz będzie miało istotny wpływ na bezpieczeństwo wewnętrzne RP w wyniku utraty tych funkcji[17].

Dokonując pewnych uogólnień można zatem przyjąć, że infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (a w tych systemach obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa[18].

Analiza literatury i materiałów źródłowych, a także aktów prawnych dotyczących infrastruktury krytycznej, wykazała, że przed wprowadzeniem do terminologii związanej z zarządzaniem kryzysowym tego pojęcia, w naszym kraju funkcjonowały wcześniej określenia takie jak: obszary, obiekty, urządzenia i transporty podlegające obowiązkowej ochronie[19] oraz obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa[20].

[16] Ibidem.
[17] I. Kulik, op. cit., s. 56.
[18] Zob. www.rcb.gov.pl (dostęp: 05.07.2014 r.).
[19] Zob. Ustawa z dnia 22 sierpnia 1997 roku *o ochronie osób i mienia*, Dz. U. z 1997 r., Nr 114, poz. 740, z późn. zm.
[20] Zob. Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku *w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*, Dz. U. z 2003 r., Nr 116, poz. 1090.

Ustawa o ochronie osób i mienia z 22 sierpnia 1997 roku wymienia wiele obszarów, obiektów, urządzeń oraz transportów podlegających obowiązkowej ochronie. Zapisy w ustawie precyzują kryteria podziału wspomnianej infrastruktury i dzielą je na związane z obronnością państwa, ochroną interesu gospodarczego państwa, bezpieczeństwem publicznym oraz innymi ważnymi interesami państwa. Z kolei rozporządzenie z 24 czerwca 2003 roku *w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony* wskazuje na dwie kategorie obiektów. Zgodnie z wyżej wymienionym rozporządzeniem do pierwszej kategorii, związanej z potencjałem obronnym państwa, zaliczamy[21]:

- zakłady produkujące, remontujące i magazynujące uzbrojenie i sprzęt wojskowy oraz środki bojowe;
- zakłady prowadzące prace badawczo-rozwojowe lub konstruktorskie w dziedzinie bezpieczeństwa i obronności państwa;
- magazyny rezerw państwowych (w tym bazy i składy paliw płynnych, żywności, leków, materiałów sanitarnych);
- obiekty jednostek podległych Ministrowi Obrony Narodowej lub przez niego nadzorowane;
- obiekty infrastruktur transportu samochodowego, kolejowego, lotniczego, morskiego, wodnego śródlądowego, drogownictwa, kolejnictwa i łączności;
- ośrodki dokumentacji geodezyjnej i kartograficznej;
- zapory wodne;
- urządzenia hydrotechniczne;
- obiekty należące do jednostek organizacyjnych Agencji Wywiadu;
- obiekty Narodowego Banku Polskiego;
- obiekty Banku Gospodarstwa Krajowego;
- obiekty Polskiej Wytwórni Papierów Wartościowych oraz Mennicy Państwowej;
- obiekty, w których produkowane, stosowane lub magazynowane są materiały jądrowe czy też źródła i odpady promieniotwórcze;
- obiekty telekomunikacyjne służące nadawaniu programów radia publicznego i telewizji publicznej.

Do drugiej kategorii natomiast należą obiekty związane z właściwym funkcjonowaniem administracji publicznej oraz zapewnieniem odpowiedniego poziomu bezpieczeństwa i porządku publicznego, a mianowicie[22]:

- obiekty organów i jednostek organizacyjnych podległe ministrowi do spraw administracji publicznej oraz ministrowi do spraw wewnętrznych lub przez nich nadzorowane;

[21] Ibidem, § 2 pkt. 1-9.
[22] Ibidem, § 2 pkt. 10-19.

– obiekty jednostek organizacyjnych Agencji Bezpieczeństwa Wewnętrznego;
– obiekty Policji, Straży Granicznej i Państwowej Straży Pożarnej;
– obiekty będące we właściwości Ministra Sprawiedliwości, Służby Więziennej oraz jednostek organizacyjnych, które podlegają Ministrowi Sprawiedliwości bądź są przez niego nadzorowane;
– zakłady, których działalność ma bezpośredni związek z wydobywaniem kopalin podstawowych;
– obiekty, w których produkowane, stosowane lub magazynowane są materiały stwarzające szczególne zagrożenie pożarem lub wybuchem;
– obiekty, w których prowadzona jest działalność oparta na wykorzystywaniu toksycznych związków chemicznych i ich prekursorów, środków biologicznych, mikrobiologicznych, mikroorganizmów, toksyn i innych substancji powodujących zachorowania u ludzi lub zwierząt;
– elektrownie oraz inne obiekty elektroenergetyczne;
– inne obiekty znajdujące się we właściwości organów administracji rządowej lub też organów jednostek samorządu terytorialnego, formacji, instytucji państwowych, a także przedsiębiorców.

Nie należy zatem ustawy o zarządzaniu kryzysowym traktować jako pierwszego aktu prawnego odnoszącego się do kluczowych z punktu widzenia funkcjonowania państwa i społeczeństwa elementów infrastruktury. Z powyższego wynika bowiem, że planowanie i realizacja zadań ochronnych tzw. infrastruktury krytycznej prowadzone są w Polsce od wielu lat, a pojawienie się ustawy o zarządzaniu kryzysowym stanowi podstawę prawną do kompleksowego zdefiniowania i wyodrębnienia takiej infrastruktury z różnych sektorów społeczno-gospodarczych[23]. W ustawie tej zdefiniowana została również ochrona obiektów infrastruktury krytycznej, którą należy rozumieć jako *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*[24].

Z powyższego wynika, że aby skutecznie chronić infrastrukturę uznaną za krytyczną, należy zapewnić jej funkcjonalność w obliczu różnorodnych zagrożeń wynikających zarówno z działania sił natury (np. powodzie, pożary, huraganowe wiatry, niskie temperatury czy upały), jak i działalności człowieka (zaniedbań w terminowej obsłudze urządzeń, świadomym lub nieświadomym uszkodzeniu systemów i urządzeń)[25].

[23] K. Stec, *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, [w:] *Bezpieczeństwo Narodowe,* BBN, Warszawa 2011, nr 3, s. 196.
[24] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu* ..., art. 3, ust. 3.
[25] J. Wołejszo, R. Jakubczak (red.), *Obronność. Teoria i praktyka*, Bellona, Warszawa 2013, s. 476.

Jak wykazały badania problemu, w czasach coraz większego uzależnienia jednostek, narodów czy nawet państw od techniki, ochrona infrastruktury krytycznej nabiera nowego znaczenia, a zapisy dotyczące ochrony infrastruktury krytycznej zawarte w ustawie o zarządzaniu kryzysowym stały się dodatkowym impulsem do nowego spojrzenia na problematykę zapewnienia bezpieczeństwa wewnętrznego wobec jawiących się nowych jego zagrożeń[26].

Ochrona infrastruktury krytycznej powinna więc swoim zakresem obejmować[27]:

- gromadzenie i przetwarzanie informacji dotyczących infrastruktury krytycznej;
- opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożenia dla tej infrastruktury;
- odtwarzanie infrastruktury krytycznej;
- współpracę z administracją publiczną właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

Dotychczasowe wyniki badań upoważniają zatem do postawienia wniosku, że ochrona infrastruktury krytycznej to proces obejmujący znaczną liczbę obszarów zadaniowych i kompetencji oraz angażujący wiele zainteresowanych stron. Proces ten obejmuje wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej, zakłada również stopniowe dochodzenie do oczekiwanego rezultatu oraz nieustanne doskonalenie. Zadania w tym zakresie obejmują zapobieganie zagrożeniom i ograniczanie ich skutków, zmniejszanie podatności infrastruktury krytycznej na zagrożenia oraz szybkie przywrócenie jej prawidłowego funkcjonowania na wypadek wszelkich zdarzeń mogących je zakłócić[28].

Kolejną, bardzo istotną kwestią jest fakt, że w przeszłości elementy tworzące infrastrukturę krytyczną funkcjonowały jako niezależne lub też zależne w niewielkim stopniu systemy. Obecnie w dobie postępującej globalizacji i rozwoju technologicznego poszczególne jej obiekty są coraz bardziej współzależne nie tylko w wymiarze jednego państwa, ale i w skali regionalnej, europejskiej, a nawet światowej[29].

Dlatego też, z uwagi na to, że między poszczególnymi systemami oraz obiektami infrastruktury krytycznej występują ścisłe powiązania i zależności, istnieje potrzeba kompleksowego oraz holistycznego[30] podejścia do ochrony owych

[26] Por. W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, *Ochrona infrastruktury...,* s. 8.

[27] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu* ..., art. 6.

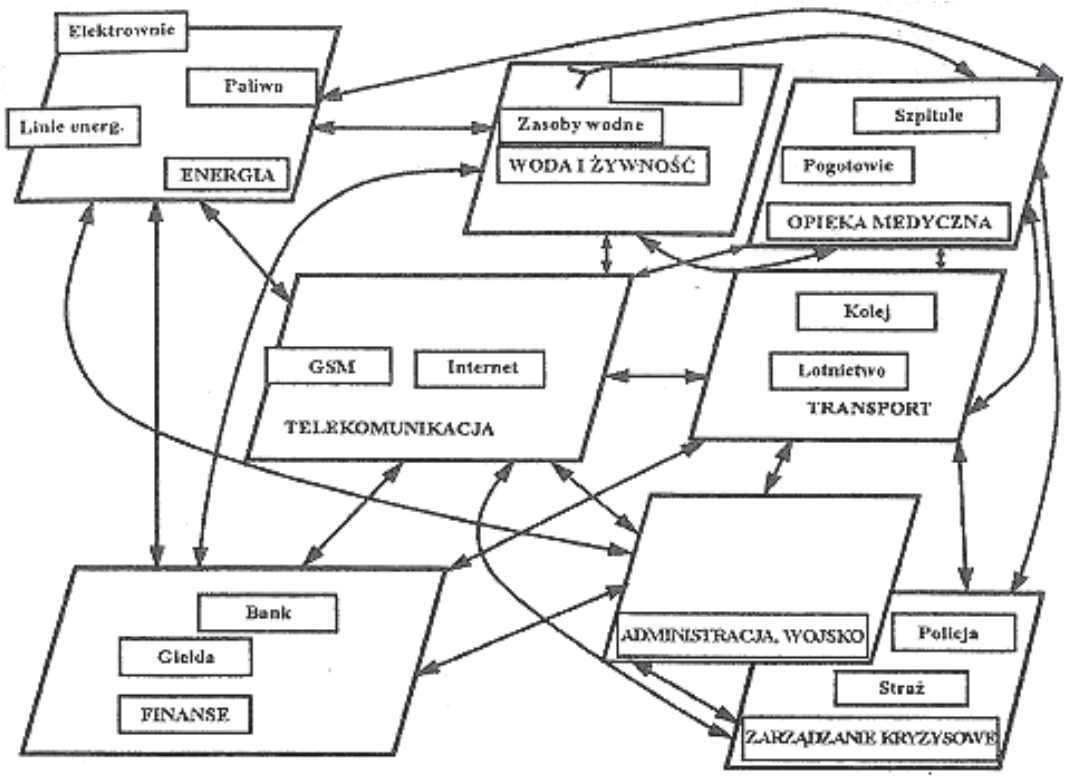
[28] *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013, s. 5.

[29] Zob. *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r., s. 24.

[30] prof. Piotr Sienkiewicz wymienia holizm i kompleksowość jako jedne z podstawowych cech konstytutywnych stylu zwanego ujęciem systemowym. *Holizm*, czyli rozpatrywanie zjawisk (obiektów, procesów, zdarzeń, itp.) jako całości. *Kompleksowość*, czyli ujawnianie różnorodności sprzężeń i relacji wewnętrznych rozpatrywanych zjawisk, Zob. P. Sienkiewicz (red.), *Metody badań nad bezpieczeństwem i obronnością*, AON, Warszawa 2010, s. 99-100.

systemów i obiektów[31]. Nie trudno bowiem zauważyć, że obecnie powiązania funkcjonalne (rys. 2) między niektórymi elementami, a nawet systemami tejże infrastruktury powodują, że przerwa w działaniu lub dysfunkcja jednego z nich może doprowadzić do zakłócenia funkcjonowania wielu innych systemów o skali i skutkach trudnych do przewidzenia, a jednocześnie mogących zagrozić zdrowiu lub życiu obywateli, nawet w skali międzynarodowej[32].

Można zatem przyjąć, że wzajemne zależności między różnymi rodzajami infrastruktury krytycznej są dodatkowym czynnikiem generującym zagrożenia. Najlepszym tego przykładem jest rola, jaką wśród różnych systemów omawianej infrastruktury odgrywają systemy zaopatrzenia w energię elektryczną, od której dostaw uzależnionych jest większość systemów infrastruktury krytycznej.



Rys. 2. Zależności między kluczowymi sektorami państwowymi
Źródło: W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, *Ochrona infrastruktury krytycznej*, AON, Warszawa 2012, s. 20.

Kluczowym dokumentem dla systemu ochrony infrastruktury krytycznej stał się Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), który został przyjęty 26 marca 2013 roku przez Radę Ministrów. W Programie zaproponowane zostało nowatorskie w naszym kraju – bezsankcyjne podejście do ochrony infrastruktury krytycznej. Zakłada ono współpracę, współodpowiedzialność

[31] W. Lidwa, W. Krzeszowski, W. Więcek, P. Kamiński, op. cit., s. 7.
[32] Ibidem, s. 19.

i wzajemne zaufanie przedsiębiorców – właścicieli infrastruktury krytycznej oraz administracji publicznej. Dokument przygotowano w Rządowym Centrum Bezpieczeństwa[33], a jego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w szczególności w zakresie: zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej; przygotowania na sytuacje kryzysowe, które mogą niekorzystnie wpłynąć na infrastrukturę krytyczną; reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz jej odtwarzania. Program ten adresowany jest przede wszystkim do administracji publicznej oraz operatorów infrastruktury krytycznej i określa[34]:

– narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej;
– ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy i obiekty omawianej infrastruktury;
– szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

Realizacja NPOIK wymaga zaangażowania wszystkich możliwych zainteresowanych stron, jednakże główny wysiłek spoczywa, zgodnie z posiadanymi kompetencjami, na Rządowym Centrum Bezpieczeństwa, ministrach i kierownikach urzędów centralnych oraz operatorach infrastruktury krytycznej, wyszczególnionych w wykazie infrastruktury krytycznej[35], który jest dokumentem niejawnym.

Ciekawą graficzną prezentację głównych podmiotów uczestniczących w procesie ochrony infrastruktury krytycznej oraz ich role przedstawia rys. 3. Natomiast podstawowe obowiązki tych podmiotów zawarte zostały w przywołanej już wcześniej ustawie o zarządzaniu kryzysowym.

Zatem powyższe treści prowadzą do wniosku, iż możemy wyróżnić przynajmniej cztery grupy podmiotów biorących udział w zarządzaniu ochroną infrastruktury krytycznej[36]:

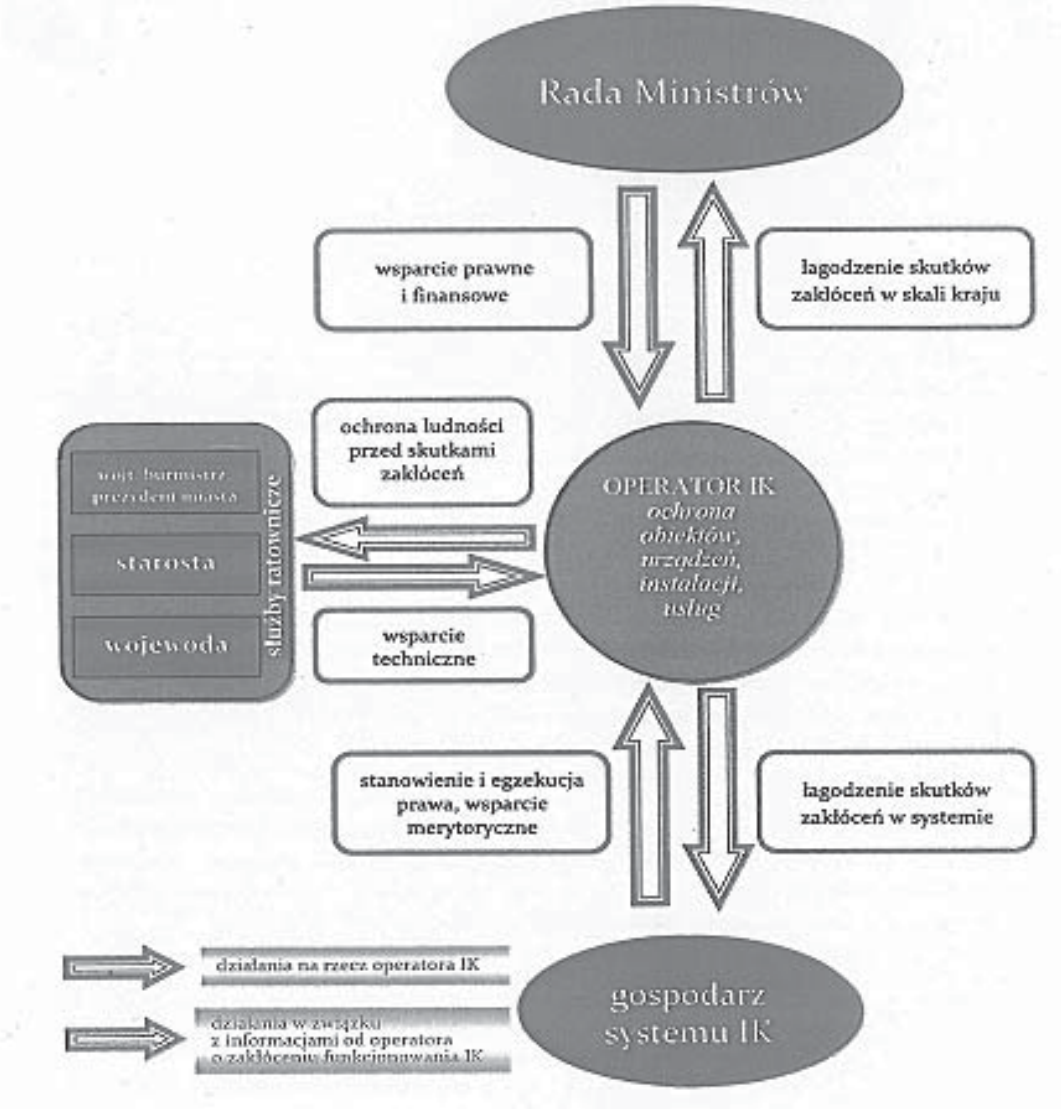
– ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie;
– Rządowe Centrum Bezpieczeństwa;
– centra zarządzania kryzysowego;
– właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej.

[33] *Rządowe Centrum Bezpieczeństwa* rozpoczęło działalność 2 sierpnia 2008 roku. Powstało na podstawie ustawy z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (art. 10) i rozporządzenia Prezesa Rady Ministrów z dnia 10 lipca 2008 r. *w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa*.

[34] Zob. www.rcb.gov.pl (dostęp: 05.07.2014 r.).

[35] *Narodowy Program Ochrony* ..., s. 13.

[36] Por. R. Radziejewski, *Podmioty wykonawcze w ochronie infrastruktury krytycznej*, [w:] G. Sobolewski, D. Majchrzak (red.), *Zarządzanie kryzysowe*, AON, Warszawa 2013, s. 137.



Rys. 3. Główne podmioty uczestniczące w procesie ochrony infrastruktury krytycznej i ich role
Źródło: *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013, s. 23.

Istotną rolę w systemie ochrony infrastruktury krytycznej pełnią ministrowie odpowiedzialni za poszczególne systemy tej infrastruktury (rys. 4), bowiem ich praca jest gwarancją zaangażowania najwyższych władz państwowych w proces budowy bezpieczeństwa państwa. Ponadto, należy wziąć pod uwagę fakt, że każdy system infrastruktury krytycznej posiada właściwą sobie charakterystykę funkcjonowania, uwarunkowania prawne oraz użytkowników. To powoduje, że każdy z tych systemów potrzebuje gospodarza posiadającego najlepszą wiedzę o danym systemie infrastruktury krytycznej, rozumiejącego jego budowę, a także potrzeby zaangażowanych podmiotów[37].

[37] *Narodowy Program Ochrony* ..., s. 15.

Rys. 4. Ministrowie odpowiedzialni za systemy infrastruktury krytycznej
Źródło: opracowanie własne na podstawie *Narodowego Programu Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013, s. 17.

Analiza literatury przedmiotu pozwala na przyjęcie stwierdzenia, że bardzo istotnym, wręcz kluczowym etapem procesu ochrony infrastruktury krytycznej jest jej identyfikacja. W tym celu Rządowe Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych, a także przy wsparciu przedsiębiorców prywatnych, opracowało kryteria identyfikacji infrastruktury krytycznej, które podzielono na dwie grupy[38]:

– kryteria systemowe – charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów;

[38] Ibidem, s. 11.

– kryteria przekrojowe – opisujące parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi. Kryteria te obejmują: ofiary w ludziach, skutki finansowe, konieczność ewakuacji, utratę usługi, czas odbudowy, efekt międzynarodowy oraz unikatowość.

Wszystkie kryteria identyfikacji infrastruktury krytycznej muszą oczywiście podlegać aktualizacji.

Konkludując, można zatem przyjąć, że ochrona infrastruktury krytycznej, której celem jest zapewnienie ciągłości działań tej infrastruktury, realizowana jest w następujących etapach[39]:

– przygotowanie wykazu infrastruktury krytycznej;
– analiza ryzyka zagrożeń dla tej infrastruktury;
– przygotowanie wykazu zasobów do ochrony infrastruktury krytycznej;
– wyznaczenie działań realizowanych w sytuacji zagrożenia;
– wyznaczenie działań odtwarzających infrastrukturę krytyczną;
– określenie kanałów komunikacji ze stronami trzecimi.

Uwzględniając powyższe treści, można zatem założyć z dużą dozą prawdopodobieństwa, iż współcześnie w dobie różnorodnych zagrożeń występujących na obszarze naszego państwa, rola infrastruktury krytycznej jest szczególnie ważna w zapewnieniu ciągłości pracy administracji publicznej, co z kolei przekłada się na właściwe funkcjonowanie poszczególnych gmin, powiatów i województw. Natomiast sprawność infrastruktury krytycznej zapewnia określony poziom i ciągłość dystrybucji usług, za które również ponosi odpowiedzialność administracja publiczna. Dotyczy to w szczególności transportu publicznego, usług medycznych, dostaw energii, czy też świadczenia usług związanych z ratowaniem ludzi i mienia. Właściwie utrzymana i funkcjonująca infrastruktura krytyczna pozwala także na efektywne wykorzystywanie posiadanych zasobów w razie nadzwyczajnych wydarzeń zakłócających normalne funkcjonowanie państwa czy też jego gospodarki. Jednocześnie należy zaznaczyć, że sprawność dużej części zasobów uznawanych za infrastrukturę krytyczną warunkuje także postęp technologiczny i rozwój gospodarczy[40].

Najogólniej można stwierdzić, że infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu struktur państwa i życiu jego obywateli. Dlatego też zapewnienie jej ochrony przed jakimikolwiek zagrożeniami jest jednym z priorytetowych zadań stojących przed administracją publiczną naszego państwa, która poza tym musi uwzględniać również problemy związane z ewentualnymi uszkodzeniami i zakłóceniami w jej funkcjonowaniu, by nie spowodowały one, a jeżeli już to tylko krótkotrwałe i jak najmniejsze, straty, które mogą ponieść nie tylko sami obywatele ale również gospodarka. Zatem problem ochrony infrastruktury krytycznej można uznać współcześnie za jeden z ważniejszych czynników rzutujących w sposób bezpośredni na zapewnienie bezpieczeństwa państwa i jego obywateli.

[39] K. Sienkiewicz-Małyjurek, F. R. Krynojewski, *Zarządzanie kryzysowe* ..., s. 36.
[40] Por. K. Stec, *Wybrane prawne narzędzia ochrony infrastruktury krytycznej* ..., s. 181.

Bibliografia

1. Bańka M. (red.), *Wielki Słownik Wyrazów Obcych PWN*, Wydawnictwo Naukowe PWN, Warszawa 2003.
2. Ficoń K., *Inżynieria zarządzania kryzysowego*, Bel Studio Sp. z o.o., Warszawa 2007.
3. Huzarski M., Wołejszo J. (red.), *Leksykon obronności Polska i Europa*, Bellona, Warszawa 2014.
4. Kulik I., *Analiza pojęć obiekt infrastruktury krytycznej, obiekt szczególnej ochrony i obiekt chroniony*, Szczytno 2010.
5. Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej*, AON, Warszawa 2012.
6. *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2013.
7. Piątek Z., Letkiewicz A. (red.), *Terroryzm a infrastruktura krytyczna państwa – zewnętrznego kraju Unii Europejskiej*, Szczytno 2010.
8. Radziejewski R., *Podmioty wykonawcze w ochronie infrastruktury krytycznej*, AON, Warszawa 2013.
9. *Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 roku w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony*, Dz. U. z 2003 r., Nr 116, poz. 1090.
10. Sienkiewicz P. (red.), *Metody badań nad bezpieczeństwem i obronnością*, AON, Warszawa 2010.
11. Sienkiewicz-Małyjurek K., Krynojewski F. R., *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa 2010.
12. Skroma W., *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, Rządowe Centrum Bezpieczeństwa.
13. *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2010.
14. Sobol E. (red.), *Nowy Słownik Języka Polskiego PWN*, Wydawnictwo Naukowe PWN, Warszawa 2002.
15. Sobolewski G., Majchrzak D. (red.), *Zarządzanie kryzysowe*, AON, Warszawa 2013.
16. Stec K., *Wybrane prawne narzędzia ochrony infrastruktury krytycznej w Polsce*, [w:] *Bezpieczeństwo Narodowe*, BBN, Warszawa 2011, nr 3.
17. *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r.
18. *Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia*, Dz. U. z 1997 r., Nr 114, poz. 740, z późn. zm.
19. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz. U. z 2007 r. Nr 89, poz. 590, z późn. zm.
20. Walas-Trębacz J., Ziarko J., *Podstawy zarządzania kryzysowego. Część 2. Zarządzanie kryzysowe w przedsiębiorstwie*, Krakowskie Towarzystwo Edukacyjne Sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2011.
21. Wołejszo J., Jakubczak R. (red.), *Obronność. Teoria i praktyka*, Bellona, Warszawa 2013.
22. www.rcb.gov.pl (dostęp: 05.07.2014 r.).
23. Zabłocka-Kluczka A., *Próba oceny procesu zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego w Polsce*, ZN WSOWL Nr 3 (157), Wrocław 2010.

Liczba znaków ze spacjami: 30 880