OCHRONA INFRASTRUKTURY KRYTYCZNEJ. GENEZA PROBLEMU

W artykule omówione zostały przyczyny i rys historyczny działań związanych z przygotowaniem do ochrony infrastruktury krytycznej, obejmującej m.in. systemy transportowe. Zakres tych przygotowań pokazano bardzo ogólnie w Stanach Zjednoczonych, które podobnie jak nasz kraj są członkiem NATO, a także w Europie i w Polsce.

WSTĘP

Z pojęciem zbliżonym do infrastruktury krytycznej spotykamy się już w starożytności w różnych państwach, na różnych kontynentach. Były to ważne elementy tych państw pozwalających na ich funkcjonowanie. Celem artykułu jest przybliżenie czytelnikowi powodów i kolejności działań wybranych administracji i organizacji krajów mających związki z Polską. Przedstawiono przyczyny i rys historyczny działań związanych z przygotowaniem do ochrony infrastruktury krytycznej w Stanach Zjednoczonych, w Europie i w Polsce. Z przyjętych oficjalnie dokumentów wynika, że infrastruktura krytyczna w większości państw dotyczy systemów i zasobów fizycznych lub wirtualnych, których niesprawność lub zniszczenie miałoby osłabiający wpływ na bezpieczeństwo tych państw i ich obywateli. Członkostwo Polski w Unii Europejskiej wymaga aby problematykę będącą treścią tego artykułu rozpatrywać głównie w ramach europejskiego programu ochrony infrastruktury krytycznej.

Infrastruktura, to „...podstawowe urządzenia i instytucje niezbędne do właściwego funkcjonowania zarówno działów gospodarki (infrastruktura techniczna), jak i społeczeństwa jako całości (infrastruktura społeczna, świadcząca usługi w dziedzinie prawa, bezpieczeństwa, oświaty, opieki zdrowotnej itd.)”. [4, s. 306].

Infrastruktura krytyczna jest terminem używanym w odniesieniu do zasobów mających podstawowe znaczenie dla funkcjonowania gospodarki, społeczeństwa i państwa. Jest pojęciem (często pod inną nazwą) tak starym jak stara jest cywilizacja na ziemi. Są to bardzo czułe, kluczowe punkty danego państwa, które pozwalają na jego istnienie, zapewniając minimum do jego funkcjonowania.

1. INFRASTRUKTURA KRYTYCZNA W PRZESZŁOŚCI

Z pojęciem zbliżonym do infrastruktury krytycznej spotykamy się już od wielu wieków w różnych państwach na różnych kontynentach. Dla Fenicjan były to porty i instalacje portowe wykorzystywane do działalności handlowej oraz budowy okrętów, zapewniających kontrolę morskich szlaków handlowych. W starożytnym Egipcie były to urządzenia irygacyjne związane z Nilem oraz magazyny na zboże. Dla starożytnych Rzymian infrastrukturą krytyczną były **drogi i akwedukty**. Drogi pozwalały na szybki transport żołnierzy i sprzętu wojskowego w zagrożone prowincje Imperium Romanum. Usprawniały też handel. Przez akwedukty płynęła woda dla ludności, co również jak na ówczesne czasy, było bardzo nowoczesnym rozwiązaniem technologicznym o niebanalnym znaczeniu sanitarnym dla funkcjonowania tego państwa. W starożytnej cywilizacji Chin infrastrukturą krytyczną był do dziś widoczny z kosmosu mur chiński. Zapewniał on bezpieczeństwo państwu środka przed dzikimi chor-

dami jeźdźców nękających jego ziemie. Mur skutecznie uniemożliwiał najazdy co ułatwiło rozwój gospodarczy, militarny i kulturowy. W Europie przykładem może być kolonialna Hiszpania, Portugalia, czy też Wielka Brytania. Dla Hiszpanii infrastrukturę krytyczną stanowiły kopalnie złota w Ameryce Południowej, **porty i flota**, która transportowała ten cenny surowiec do kraju. To wszystko, co było potrzebne do wydobycia i dystrybucji służąc gospodarce kraju. Dla Portugalii i Wielkiej Brytanii były to posiadłości zamorskie i **szlaki komunikacyjne** oraz porty umożliwiające transport różnych dóbr do metropolii.

W czasach współczesnych pojęcie infrastruktury krytycznej jest dużo szersze ze względu na postęp technologiczny, pojawienie się nowych zjawisk, itp. Wiele systemów infrastruktury krytycznej pozostaje jednak nie zmiennych do dziś. Problematyka związana z infrastrukturą krytyczną ujęta jest w wielu dokumentach normatywnych zarówno międzynarodowych, Unii Europejskiej, jak i w krajowych aktach o randze ustaw i rozporządzeń. Dokumentem międzynarodowym, który jako pierwszy wnosi w swej treści wkład do ochrony infrastruktury krytycznej są z pewnością protokoły dodatkowe do Konwencji Genewskich z 12 sierpnia 1947 r. W artykułach dotyczących ochrony budowli i urządzeń zawierających niebezpieczne siły ujęto zapis, że budowle te, a zwłaszcza zapory, groble i elektrownie atomowe, nie mogą być przedmiotem ataków, choćby stanowiły cele wojskowe, jeżeli takie ataki mogą spowodować wyzwolenie tych sił i w następstwie wywołać poważne straty wśród ludności cywilnej [5].

2. INFRASTRUKTURA KRYTYCZNA W STANACH ZJEDNOCZONYCH

Fakt uzależnienia społeczeństw od infrastruktury najlepiej oddają wydarzenia w Nowym Jorku z 13 lipca 1977 r. Tego dnia miała miejsce jedna z największych awarii linii energetycznych na świecie. Miasto (wówczas 12 milionów osób) na ponad dobę zostało pozbawione energii elektrycznej. W sparaliżowanym mieście wybuchły zamieszki i grabieże. Zrabowano i zniszczono 1616 sklepów. Wybuchło także ponad tysiąc pożarów w całym mieście. Pożary te były następstwem zamieszek co wyraźnie ukazują charakter zagrożeń infrastruktury krytycznej. Zjawiska te mają tendencje efektu domina, jedno w porę nie zneutralizowane zagrożenie może spowodować zmaterializowanie się zagrożeń o zupełnie innym charakterze, w zupełnie innym miejscu i czasie. Systemy wchodzące w skład infrastruktury krytycznej tworzą system naczyń połączonych. System finansowy państwa nie będzie działał poprawnie gdy zniszczony zostanie system teleinformatyczny, czy system łączności. W takim wypadku nie ma również mowy o poprawnym funkcjonowaniu systemu ochrony zdrowia. Zakłócenie pracy systemu zaopatrzenia w

energii, surowce energetyczne i paliwa wyklucza właściwie poprawne funkcjonowanie wszystkich innych systemów. Efekt domina przy poważnym uszkodzeniu jednego z systemów jest bardzo prawdopodobny. Straty w ofiarach ludzkich jak i te materialne jakie mogą być wywołane taką sytuacją będą ogromne [15].

Nazwą infrastruktura krytyczna zaczęto posługiwać się w Stanach Zjednoczonych i w Kanadzie w latach dziewięćdziesiątych XX w., kojarząc ją początkowo z przesyłem energii i usługami telekomunikacyjnymi. W 1996 r. w Stanach Zjednoczonych ustanowiono Prezydencką Komisję do spraw Ochrony Infrastruktury Krytycznej.

Określenie infrastruktura krytyczna (IK) po raz pierwszy pojawiły się w oficjalnych dokumentach państwowych w USA wraz z dyktywą prezydenta USA Bila Clintona z dnia 22 maja 1998 r. w sprawie ochrony infrastruktury krytycznej. Dyrektywa wskazywała na konieczność podejmowania działań w sprawie ochrony obiektów, systemów będących wrażliwymi na uderzenia potencjalnych przeciwników, a stanowiących niezbędne systemy dla prawidłowego funkcjonowania państwa [6].

Ukierunkowywała także na konieczność wzrostu wrażliwości Stanów Zjednoczonych na ewentualne ataki terrorystyczne, ze zwróceniem szczególnej uwagi na bezpieczeństwo infrastruktury krytycznej. Tego typu infrastrukturę zdefiniowano jako rzeczywiste i cybernetyczne systemy niezbędne do funkcjonowania gospodarki i państwa w minimalnym zakresie. Wśród tych systemów wymieniono m.in.: system telekomunikacyjny, energetyczny, **transportowy**, bankowy i finansowy. Podkreślono, iż w celu efektywnej ochrony infrastruktury krytycznej zachodzi konieczność ścisłej współpracy z sektorem prywatnym (wg danych Departamentu Bezpieczeństwa Narodowego USA, operatorami lub właścicielami około 85% infrastruktury krytycznej są podmioty prywatne) w ramach partnerstwa publiczno-prywatnego.

Podjęte działania w myśl ochrony infrastruktury krytycznej zostały zdominowane wydarzeniami z 11 września 2001 r. po zamachu terrorystycznym w Nowym Yorku. Wydarzenie to spowodowało wzmożenie i przyspieszenie prac celem wypracowania systemów mających na celu ochronę infrastruktury krytycznej. Od tego czasu zagadnienia ochrony infrastruktury krytycznej były systematycznie rozwijane, a Amerykanie stali się światowymi liderami w tej dziedzinie.

Obecnie infrastruktura krytyczna jest definiowana jako „systemy i zasoby fizyczne lub wirtualne, tak niezbędne dla Stanów Zjednoczonych, że niesprawność lub zniszczenie tych systemów i zasobów miałoby osłabiający wpływ na bezpieczeństwo, bezpieczeństwo gospodarki narodowej, narodową ochronę zdrowia lub każdą kombinację tych spraw”. Zidentyfikowano kilkanaście sektorów infrastruktury krytycznej i odpowiedzialnych za nie agend:

1. Rolnictwo i żywność – Departament Rolnictwa oraz Zdrowia.
2. Woda – Agencja Ochrony Środowiska.
3. Ochrona zdrowia – Departament Zdrowia i Opieki Społecznej.
4. Służby ratunkowe – Departament Bezpieczeństwa Krajowego.
5. Administracja – Departament Bezpieczeństwa Krajowego.
6. Przemysł obronny – Departament Obrony.
7. Informatyka i telekomunikacja – Departament Handlu.
8. Energia – Departament Energii.
9. **Transport – Departament Transportu.**
10. Banki i finanse – Departament Skarbu.
11. Chemia i materiały niebezpieczne – Departament Bezpieczeństwa Krajowego.
12. Poczta – Departament Bezpieczeństwa Krajowego.
13. Dziedzictwo narodowe - Departament Zasobów Wewnętrznych.

14. Krytyczna produkcja - Departament Bezpieczeństwa Krajowego.

Narodowy Plan Ochrony Infrastruktury (National Infrastructure Protection Plan) tworzy płaszczyznę integracji szerokiego spektrum wysiłków zmierzających do zwiększonej ochrony i odporności narodowej infrastruktury krytycznej i jej kluczowych zasobów [13].

3. INFRASTRUKTURA KRYTYCZNA W EUROPIE

Pierwsze inicjatywy w dziedzinie ochrony infrastruktur krytycznych poza Stanami Zjednoczonymi podjęte zostały pod koniec lat dziewięćdziesiątych XX w. także w Kanadzie, Australii, Wielkiej Brytanii, Szwajcarii, Szwecji, Norwegii, Finlandii i w szeregu innych krajach. W Europie, po zamachach terrorystycznych w Madrycie (11 marca 2004 r.) Rada Europejska (RE) – w czerwcu 2004 r. - wezwała do przygotowania ogólnej strategii ochrony infrastruktury krytycznej. Prace zostały ukierunkowane na usprawnienie systemów zapobiegania atakom terrorystycznym oraz podniesienia gotowości i zdolności do reagowania. Odpowiadając na ten apel, 20 października 2004 r. Komisja RE przyjęła Komunikat pod nazwą „Ochrona infrastruktury krytycznej w walce z terroryzmem”, zawierający propozycje sposobów usprawnienia europejskich systemów zapobiegania atakom terrorystycznym wymierzonym przeciwko infrastrukturze krytycznej, a także zwiększenia gotowości i zdolności reagowania na takie ataki.

W Komunikacie zaproponowano również przygotowanie nowych instrumentów – europejskiego programu ochrony infrastruktury krytycznej (EPOIK) oraz sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej (SOZIK). Sieć oprócz przesyłania informacji o prawdopodobnych zagrożeniach dla infrastruktury krytycznej, miała stworzyć możliwość wymiany informacji na temat najlepszych praktyk oraz środków zapewniających odpowiedni poziom bezpieczeństwa. Sieć miała stać się płaszczyzną wymiany informacji pomiędzy ekspertami krajów członkowskich, przedstawicielami Komisji oraz sektorem prywatnym.

17 listopada 2005 r. Komisja przyjęła „Zieloną księgę” w sprawie europejskiego programu ochrony infrastruktury krytycznej (The European Programme for Critical Infrastructure Protection - EPCIP) [7], w której przedstawiono założenia polityczne dotyczące opracowywania tego programu oraz sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej. Celem „Zielonej księgi” było uzyskanie opinii i komentarzy państw członkowskich na temat ochrony infrastruktury krytycznej, które następnie znalazły odzwierciedlenie w EPOIK. Zielona księga została udostępniona również przedstawicielom sektora prywatnego. Dzięki niej możliwe było uzyskanie opinii zainteresowanych stron między innymi w kwestiach definicji (czym jest infrastruktura krytyczna, europejska infrastruktura krytyczna, kwestia współzależności między poszczególnymi sektorami infrastruktury krytycznej) oraz zakresu i charakteru EPOIK.

Zaproponowano, aby wykaz elementów europejskiej infrastruktury krytycznej opierał się na tym, co zgłoszą państwa członkowskie. Uzyskane opinie podkreślały wartość dodaną wspólnotowego zbioru przepisów regulujących ochronę infrastruktury krytycznej. Uznano potrzebę zwiększenia zdolności w zakresie ochrony infrastruktury krytycznej w Europie oraz wsparcia działań na rzecz ograniczenia słabych punktów takiej infrastruktury. Podkreślono znaczenie podstawowych zasad pomocniczości, proporcjonalności, komplementarności oraz dialogu zainteresowanych stron. Program został sformułowany w Komunikacie Komisji Europejskiej EU COM (2006) 786 final.

W grudniu 2005 r. Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych wezwała Komisję do przygotowania wniosku dotyczącego europejskiego programu ochrony infrastruktury krytycznej i

zdecydowała, że program ten powinien opierać się na stosowaniu podejścia obejmującego wszystkie rodzaje ryzyka, traktując jednak przeciwdziałanie zagrożeniom terrorystycznym jako priorytet. Zgodnie z takim podejściem w procesie ochrony infrastruktury należy uwzględniać zagrożenia wywołane działalnością człowieka, zagrożenia technologiczne i katastrofy naturalne, największą uwagę poświęcając jednak zagrożeniom terrorystycznym.

W grudniu 2006 r. przyjęty został pakiet dotyczący polityki Unii w zakresie ochrony infrastruktur krytycznych, złożony z Komunikatu w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej (EIK, w angielskiej wersji dokumentu: European Critical Infrastructure (ECI) i Dyrektywy Rady [8]. Komunikat był pierwszą próbą całościowego uregulowania problemu na poziomie Unii Europejskiej, z uwzględnieniem tak ważnego elementu, jakim jest zaangażowanie sektora prywatnego. W Komunikacie określono, że celem EPOIK jest poprawa ochrony infrastruktury krytycznej w UE. Ma on zostać osiągnięty dzięki stworzeniu ram regulacyjnych. W komunikacie wskazano również, że UE powinna skupić się na wszelkich możliwych zagrożeniach dla infrastruktury krytycznej, ze szczególnym uwzględnieniem zagrożenia terroryzmem.

W kwietniu 2007 r. Rada przyjęła konkluzje w sprawie EPOIK, w których podkreśliła, że to państwa członkowskie ponoszą ostateczną odpowiedzialność za koordynację przygotowań do ochrony infrastruktury krytycznej znajdującej się na ich terytorium, a jednocześnie z zadowoleniem przyjęła starania Komisji na rzecz opracowania europejskiej procedury rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej (EIK) oraz oceny potrzeb w zakresie zwiększenia jej ochrony. Stanowiło to pierwszy krok w etapowym podejściu do rozpoznania i wyznaczenia EIK oraz do oceny potrzeb w zakresie poprawy ich ochrony.

Stwierdzono, że na terenie Wspólnoty znajduje się pewna liczba infrastruktur krytycznych, których zakłócenie lub zniszczenie miałyby istotne transgraniczne skutki. Tego typu EIK należy rozpoznać i wyznaczyć za pomocą wspólnej procedury. Sprawdzonym i skutecznym środkiem rozwiązywania kwestii związanych z transgraniczną infrastrukturą krytyczną są dwustronne programy współpracy państw członkowskich w dziedzinie ochrony infrastruktury krytycznej. EPOIK powinien opierać się na takiej właśnie współpracy. Informacje dotyczące wyznaczenia określonej infrastruktury jako EIK powinny zostać opatrzone klauzulą tajności na odpowiednim poziomie, zgodnie z obowiązującym prawodawstwem Wspólnoty i państwa członkowskiego.

Wspólnotowe podejście wymaga założenia pełnego zaangażowania sektora prywatnego z uwagi na bardzo istotny udział tego sektora w nadzorowaniu ryzyka, zarządzaniu ryzykiem, planowaniu ciągłości działania i w procesie przywracania stanu sprzed potencjalnej katastrofy. W przypadku sektora energetycznego i w szczególności metody wytwarzania i przesyłania energii elektrycznej, przygotowująca Dyrektywa może obejmować części elektrowni jądrowych zajmujące się przesyłaniem energii elektrycznej, bez elementów wyraźnie jądrowych, które są objęte odpowiednim prawodawstwem jądrowym, w tym traktatami i prawem wspólnotowym.

Dla wszystkich wyznaczonych EIK należy ustalić plany ochrony infrastruktury (POI) oraz powołać urzędnika łącznikowego ds. ochrony odpowiedzialnego za współpracę i komunikację z właściwymi krajowymi organami ds. ochrony infrastruktury krytycznej.

Skuteczne rozpoznanie ryzyka, zagrożeń i słabych punktów w poszczególnych sektorach wymaga komunikacji zarówno między właścicielami/operatorami EIK a państwami członkowskimi, jak i między państwami członkowskimi a Komisją. Każde państwo członkowskie powinno gromadzić informacje dotyczące EIK zlokalizowanej na swoim terytorium.

Należy także opracować wspólne metody rozpoznawania i klasyfikowania ryzyka, zagrożeń i słabych punktów związanych z poszczególnymi składnikami infrastruktury.

W celu utrzymania komunikacji, koordynacji i współpracy na poziomie krajowym i wspólnotowym, w każdym państwie członkowskim zaleca się utrzymanie punktów kontaktowych ds. ochrony EIK, które powinny koordynować sprawy związane z ochroną europejskiej infrastruktury krytycznej na terenie tego państwa, a także odpowiadać za współpracę w tym względzie z innymi państwami członkowskimi i Komisją.

Dla zachowania określonego stopnia poufności i bezpiecznej wymiany informacji informacje niejawne powinny podlegać ochronie zgodnie ze stosownym prawodawstwem wspólnotowym (m.in. rozporządzeniem WE nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji) i ustawodawstwem państw członkowskich.

Po intensywnych przygotowaniach w 2008 r. - ogłoszono Dyrektywę Rady Unii Europejskiej 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony [10]. Dyrektywa ustanawia procedurę rozpoznawania i wyznaczania elementów tej infrastruktury oraz wskazuje na zadania jakie winny być podjęte w zakresie poprawy jej obrony.

W Dyrektywie stwierdza się, że infrastruktura krytyczna „...oznacza składniki, systemy lub części infrastruktury zlokalizowane na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz którego zakłócenie lub zniszczenie miałyby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji (art. 2a). Europejska infrastruktura krytyczna dotyczy tylko dwóch systemów, a mianowicie systemu energii i **systemu transportu**. Wyznaczona infrastruktura krytyczna musi posiadać plan ochrony obejmujący identyfikację ważnych zasobów, analizę ryzyka opartą na scenariuszach głównych zagrożeń i słabościach zasobów oraz identyfikację, wybór i ustalenie priorytetów procedur i środków ochrony.

4. INFRASTRUKTURA KRYTYCZNA W POLSCE

W Polsce podjęte zostały działania nad prawnym rozwiązaniem ochrony obiektów mających najistotniejsze znaczenie dla bezpieczeństwa państwa i jego obywateli w ostatniej dekadzie XX w. Efektem tych działań jest Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia. Dokument ten określił, że obiekty podlegające obowiązkowej ochronie to obszary, obiekty, urządzenia i **środki transportu** ważne dla obronności, gospodarki i ochrony interesów państwa i bezpieczeństwa publicznego, które miały być obowiązkowo chronione przez specjalne, uzbrojone formacje lub odpowiednie zabezpieczenie techniczne. W ramach ochrony obowiązkowej, kierownik jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w ewidencji albo upoważniona przez niego osoba, zobowiązany zostaje do opracowania oraz uzgodnienia z właściwym terytorialnie komendantem wojewódzkim planu ochrony tych obszarów, obiektów i urządzeń.

Według informacji zawartych w referacie przedstawiciela Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego, w 2001 r. w Polsce rozpoczęto pewne wstępne działania zmierzające do stworzenia organizacyjnych ram dla koordynacji działań merytorycznych w dziedzinie zapewnienia bezpieczeństwa infrastruktur krytycznych kraju (realizowanych przez zarządy tych infrastruktur) [2]. W lutym 2001 r. odbyło się

spotkanie CERT Polska (Computer Emergency Response Team) z Biurem Bezpieczeństwa Łączności i Informatyki UOP. CERT Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. Natomiast UOP to nieistniejące już służby specjalne RP. Obecnie ich zadania przejęła Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu. Spotkanie dotyczyło reagowania na incydenty bezpieczeństwa. Po tej konferencji przeprowadzono jeszcze kilka innych, np. w listopadzie 2001 r. Konferencja SECURE'2001, gdzie zaprezentowano działania NATO w tym zakresie. Następnie w kwietniu 2002 r. przeprowadzono dyskusję podczas Konferencji „Bezpieczna Infrastruktura – Koordynacja działań w skali kraju”. Kolejne konferencje i spotkania uwydatniły brak uregulowań dotyczących relacji pomiędzy administracją publiczną odpowiedzialną za bezpieczeństwo obywateli, a właścicielami infrastruktury służącej do świadczenia różnego rodzaju usług. Dlatego świadomość negatywnych skutków w przypadku dużych awarii, np. elektrowni, doprowadziła do podjęcia próby prawnej regulacji tej kwestii. Zdecydowano, że państwo musi mieć prawo ingerencji w celu zapewnienia ciągłości pracy najważniejszych systemów: **komunikacyjnych**, finansowych, dostarczających energii i innych.

Z rozeznania, jakie można uzyskać z dostępnych publikacji, konferencji, itp. wynika, że w Polsce żadnych praktycznych prac, zwłaszcza prowadzonych na szerszą skalę, do 2002 r. nie podjęto.

Z „Kwestionariusza dotyczącego ochrony infrastruktury krytycznej w Polsce”, rozesłanego do organów administracji państwowej w wyniku ustaleń podjętych na posiedzeniu Zespołu ds. Kryzysowych w dniu 18 czerwca 2002 r., wynikały następujące wnioski:

- niepełne zrozumienie przez podmioty pojęcia „krytycznej infrastruktury państwa”;
- konieczność opracowania uregulowań prawnych;
- konieczność przygotowania szkoleń.

24 czerwca 2003 r. ukazało się Rozporządzenie Rady Ministrów [13], które określiło obszary, obiekty i urządzenia podlegające ochronie jako szczególnie ważne dla obronności i bezpieczeństwa państwa. W Rozporządzeniu tym do kategorii I zalicza się:

- zakłady zajmujące się produkcją, remontem, magazynowaniem sprzętu wojskowego i uzbrojenia oraz zakłady badawczo rozwojowe na potrzeby bezpieczeństwa i obronności;
- magazyny rezerw państwowych;
- obiekty jednostek podległych MON;
- **obiekty infrastruktury transportu samochodowego, kolejowego, wodnego, morskiego, lotniczego** oraz ośrodki dokumentacji geodezyjnej i kartograficznej;
- zapory wodne i inne urządzenia hydrotechniczne;
- obiekty Agencji Wywiadu
- obiekty NBP, BGK, Państwowej Wytwórni Papierów Wartościowych S.A. oraz Mennicy Państwowej S.A.;
- obiekty, w których produkuje się, stosuje lub magazynuje materiały jądrowe oraz źródła i odpady promieniotwórcze;
- obiekty telekomunikacyjne przeznaczone do nadawania programów radio i telewizji publicznej.

Do II kategorii obiektów wskazanych w Rozporządzeniu podlegających ochronie jako szczególnie ważne dla obronności i bezpieczeństwa państwa zostały zaliczone następujące obiekty, systemy i urządzenia:

- obiekty organów i jednostek podległych ministrowi do spraw administracji publicznej;
- obiekty jednostek podległych ministrowi właściwemu do spraw wewnętrznych;
- obiekty organizacyjne Agencji Bezpieczeństwa Wewnętrznego;
- obiekty policji, straży granicznej, straży pożarnej;

- obiekty znajdujące się we właściwościach ministra sprawiedliwości, służby więziennej;
- zakłady związane z wydobywaniem kopalin podstawowych;
- obiekty, które produkują, magazynują lub stosują materiały – szczególnie zagrożone wybuchem lub pożarem;
- obiekty, których działalność związana jest z wykorzystaniem toksycznych związków chemicznych, a także środków biologicznych mogących wywoływać choroby u ludzi i zwierząt;
- elektrownie i inne obiekty elektroenergetyczne;
- inne obiekty, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi, dziedzictwa narodowego, środowiska naturalnego i ich zniszczenie, uszkodzenie może spowodować zakłócenia funkcjonowania państwa.

Rozporządzenie na kilka lat przed wprowadzeniem w życie ustawy o zarządzaniu kryzysowym wskazuje na obiekty, urządzenia, systemy i budowle, które będą stanowić części składowe infrastruktury krytycznej.

9 lipca 2004 r. w obecności szefa ABW zostało podpisane porozumienie o współpracy NASK z Departamentem Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego. Zawarta umowa była wynikiem prowadzonych od kilku lat wspólnych działań ABW i zespołu CERT Polska działającego w ramach NASK. Głównym celem porozumienia był dalszy rozwój współpracy na rzecz ochrony krytycznej infrastruktury teleinformatycznej kraju, w ramach wspólnie prowadzonego projektu [3].

Próbę kompleksowego uregulowania trudnej kwestii zapewnienia ochrony, ciągłości funkcjonowania i zabezpieczenia przed zagrożeniami najważniejszych systemów w państwie poprzez nałożenie obowiązków na organy administracji publicznej i właścicieli podjęto w Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Z Ustawy wynika, że infrastruktura krytyczna to kluczowe elementy gospodarki narodowej, że spełnia ona kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. Urządzenia, instalacje, obiekty czy usługi wchodzące w skład infrastruktury krytycznej charakteryzują się następującymi cechami:

- długotrwały okres użytkowania i trudności związane z przystosowaniem urządzeń do nowych oczekiwań użytkowników,
- urządzenia infrastruktury charakteryzują się publicznym charakterem,
- obiekty, instalacje czy urządzenia lub usługi infrastruktury krytycznej koniecznie muszą być dostosowane do warunków miejscowych,
- infrastruktura spełnia funkcje usług podstawowych i wyspecjalizowanych,
- decydującą, bardzo ważną rolę w działaniu infrastruktury odgrywa człowiek, który zapewnia jej prawidłowe funkcjonowanie,
- infrastruktura charakteryzuje się służebnym charakterem nie istnieje sama dla siebie, świadczy usługi dla sfery przemysłowej lub konsumpcyjnej,
- konieczne jest tworzenie kompleksowo całych obiektów, infrastruktury nie można budować etapami,
- formy własności infrastruktury mogą być różne. Może ona należeć do państwa, być własnością korporacji lub być własnością komunalną albo osób prywatnych,
- infrastruktura krytyczna może mieć międzynarodowy charakter, ze względu na sieć powiązań i zależności np. sieci energetyczne, telekomunikacyjne i inne
- mając na uwadze obronność i bezpieczeństwo państwa elementy składowe infrastruktury krytycznej mają charakter informacji niejawnych i stanowią tajemnicę państwową czy wojskową[1].

W Polsce termin infrastruktura krytyczna używany jest przede wszystkim w odniesieniu do zasobów mających podstawowe znaczenie dla funkcjonowania państwa i jego obywateli. Pojęcie to oznacza obiekty fizyczne, systemy zaopatrzenia, technologie informacyjne i sieci informatyczne, które w wyniku zniszczenia, zakłócenia, uszkodzenia stają się niedostępne przez dłuższy okres, przez co mogą znacząco uderzać w społeczne lub ekonomiczne warunki społeczeństwa, lub wpływać na możliwości zapewnienia obrony i bezpieczeństwa narodowego. Inaczej mówiąc, infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (a w tych systemach obiekty, urządzenia bądź instalacje) niezbędne do funkcjonowania gospodarki i państwa. Infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka, infrastruktura krytyczna może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu, przez co zagrożone może być życie i mienie obywateli. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa.

Zgodnie ze znowelizowaną Ustawą o zarządzaniu kryzysowym, Infrastruktura krytyczna... są to „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” [11].

BIBLIOGRAFIA

1. Kosowski B., (red), Elementy ochrony infrastruktury krytycznej w zarządzaniu kryzysowym, Katowice 2014.
2. Kośla R., Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac, Referat na konferencji IT.FORUM - Secure 2002, Warszawa, 6-7 listopada 2002 (slajdy prezentacji dostępne w Internecie pod adresem Internetowym: http://www.cert.pl/PDF/Kosla_p.pdf).
3. Krasnodębski G., Zagrożenia krytycznej infrastruktury teleinformatycznej w dobie rozwoju społeczeństwa informatycznego, Zakład Zarządzania Kryzysowego AMW w Gdyni.
4. Leksykon naukowo-techniczny, WNT, Warszawa 1984.
5. Protokół dodatkowy I do Konwencji Genewskich z 12 sierpnia 1947 roku, art. 56 oraz Załącznik I Regulaminu dotyczącego identyfikacji art. 16, a także Protokół dodatkowy II do Konwencji Genewskich z 12 sierpnia 1947 roku, art.15.
6. Tryburska A., (red.), Ochrona infrastruktury krytycznej, Szczepiński 2010.
7. Zielona Księga w Sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej (Greek Paper on a European Programme for Critical Infrastructure Protection) COM (2005) 576, Komisja Wspólnot Europejskich, Bruksela, dnia 17.11.2005.
8. Dyrektywa Rady w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony (Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection), Wniosek, KOM (2006) 787 wersja ostateczna, 2006/0276 (CNS), Bruksela, dnia 12.12.2006. (http://eurlex.europa.eu/LexUriServ/site/pl/com/2006/com2006_0787pl01.pdf).
9. Dyrektywę Rady Unii Europejskiej 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznania wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dziennik Urzędowy Unii Europejskiej, 23.12.2008 r., L345/75-82.
10. Dziennik Urzędowy Unii Europejskiej, 23.12.2008 r., L345/75-82.
11. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz. U. z 2013 r. poz. 1166 (Dz. U. 2017.0.209).
12. Rozporządzeniem (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji.
13. Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz. U. 2003 Nr 116, poz. 1090).
14. http://pl.wikipedia.org/wiki/Infrastruktura_krytyczna (dostęp: 6.10.2017 r.).
15. <http://www.elektroda.pl/rtvforum/topic1716001.html> (dostęp: 6.10.2017 r.).

The critical infrastructure protection. The genesis

The concept of critical infrastructure was already known in a number of ancient civilizations across different continents. Critical infrastructure was considered vital, enabling civilization a proper functioning. The purpose of this article is to present reason and sequence of practice actions for selected Poland associated administrative offices and countries organizations. A cause and an historical overview of the preparation of the United States, European and Polish critical infrastructure protection was provided. According to the manuscripts, critical infrastructure of majority of nations concerns systems and physical or virtual resources, damage or destruction of which, impairing the national and citizen security. Polish European Union membership accession requires for this article to be examined regarding the European programme for Critical Infrastructure Protection.

Autor:

dr hab. Józef Sadowski prof. nadzw AP – Akademia Pomorska w Słupsku, Wydział Nauk o Zarządzaniu i Bezpieczeństwie, Katedra Zarządzania, adres e-mail: Jozef.sadowski@apsl.edu.pl

JEL: L99 DOI: 10.24136/atest.2018.259

Data zgłoszenia: 2018.05.29 Data akceptacji: 2018.06.15