Zeszyty Naukowe AON nr 4 (105) 2016
ISSN 0867–2245

SYSTEMOWE WYMOGI BEZPIECZEŃSTWA

IDENTYFIKACJA INFRASTRUKTURY KRYTYCZNEJ I JEJ ZAGROŻEŃ

mjr mgr inż. Jacek MILEWSKI
Akademia Sztuki Wojennej

Streszczenie

Infrastruktura krytyczna, definiowana jako urządzenia, instytucje usługowe, a także inne dziedziny, które mają istotny wpływ na poczucie bezpieczeństwa obywateli i sprawne funkcjonowanie gospodarki państwa, nabrała nowego znaczenia na przestrzeni ostatnich lat. Doświadczenia ostatnich konfliktów zbrojnych i ataków terrorystycznych oraz analiza zdarzeń wywołanych przez siły natury wskazują jednoznacznie, że zakłócenie prawidłowego działania poszczególnych elementów infrastruktury krytycznej może mieć znaczący, negatywny wpływ na jej funkcjonowanie jako systemu. Szeroki zakres potencjalnych, ewoluujących zagrożeń wymusza szukanie nowych i skutecznych rozwiązań jej ochrony.

Słowa kluczowe: infrastruktura krytyczna, zagrożenia infrastruktury krytycznej

Wprowadzenie

Rozwój cywilizacyjny, którego jesteśmy zarówno świadkami, jak i uczestnikami, przyczynił się do wzrostu poczucia bezpieczeństwa człowieka. Postęp naukowo-techniczny w takich dziedzinach jak energetyka, łączność, transport, opieka zdrowotna czy edukacja z jednej strony zwiększa komfort życia, a więc i poczucie bezpieczeństwa, ale z drugiej, w przypadku wystąpienia zakłóceń w działaniu którejkolwiek z powyższych dziedzin (a także wielu innych), możemy zaobserwować, jak bardzo egzystencja człowieka jest zależna od tego, co na pierwszy rzut oka jest dla niego powszechnie dostępne i powszednie.

Powyższe dziedziny, przyczyniające się do poprawy warunków życia człowieka, możemy zakwalifikować do infrastruktury, która definiowana jest jako „urządzenia

i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki”[1].

Ponieważ niezakłócony byt i rozwój państwa zależy od stanu i sprawności określonej infrastruktury, powinna ona podlegać szczególnej ochronie i obronie. W Polsce, na mocy różnych aktów prawnych, istnieją różne definicje i podziały tejże infrastruktury. W różnych aktach prawnych jest ona określana jako:

- obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa[2];
- obszary, obiekty urządzenia i transporty podlegające obowiązkowej ochronie[3];
- infrastruktura krytyczna[4].

W krajach Unii Europejskiej przyjęto określenie infrastruktura krytyczna (ang. *critical infrastructure*)[5]. Ze względu na jej szczególne znaczenie dla prawidłowego funkcjonowania gospodarki państwa i społeczeństwa za cel niniejszego artykułu autor przyjął identyfikację infrastruktury krytycznej oraz zagrożeń, które mogą wywołać jej nieprawidłowe działanie.

Aby osiągnąć założony cel, sformułowany został problem badawczy o następującej treści: jaką infrastrukturę należy zaliczyć do infrastruktury krytycznej i jaki jest wpływ zagrożeń na obiekty i urządzenia zaliczane do tej infrastruktury?

Ponieważ zdefiniowanie pojęcia infrastruktury krytycznej jest zadaniem złożonym ze względu na różnorodność obiektów i usług wchodzących w jej skład i ich ciągłą ewolucję, a co za tym idzie różnorodność zagrożeń, które mogą spowodować zakłócenia w działaniu tej infrastruktury, występuje potrzeba określenia następujących problemów szczegółowych:

- W jaki sposób zdefiniowano pojęcie infrastruktury krytycznej w obowiązujących aktach prawnych – zarówno polskich, jak europejskich?
- Jakie obiekty i urządzenia zaliczane są do infrastruktury krytycznej?
- Jakie jest znaczenie infrastruktury krytycznej dla właściwego funkcjonowania państwa i jego obywateli?
- Jakie są podstawowe zagrożenia wywołujące zakłócenia w działaniu infrastruktury krytycznej?

Dotychczasowa wiedza uzupełniona i wzbogacona studiowaniem literatury przedmiotu pozwala na określenie prawdopodobnego rozwiązania głównego problemu naukowego. Zostało ono przestawione w postaci hipotezy roboczej o następującej treści:

1 M. Bańko (red.), *Wielki słownik wyrazów obcych PWN*, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 544.

2 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. 03.116.1090.

3 Zob. Ustawa z dnia 22 sierpnia 1997 roku o ochronie mienia i osób.

4 Zob. Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym.

5 Podstawowym, europejskim dokumentem normatywnym jest Dyrektywa Rady 2008/114/WE z dnia 8.12.2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.

Infrastruktura krytyczna, tworzona przez obiekty i urządzenia usługowe przeznaczone do zapewnienia właściwego funkcjonowania państwa i gospodarki, podlega nieustannym zmianom wynikającym z rozwoju cywilizacyjnego człowieka. W związku z tym nie sposób zdefiniować w sposób jednoznaczny i trwały charakter zagrożeń tejże infrastruktury. Można założyć, że będą one adekwatne do rozwoju infrastruktury. O ile człowiek nie ma wpływu na występowanie zagrożeń naturalnych, to może dążyć do zminimalizowania występowania zagrożeń technicznych i terrorystycznych[6].

Podczas rozwiązywania powyższych problemów posługiwano się zarówno metodami teoretycznymi, jak i praktycznymi. Do głównych metod teoretycznych należały analiza i synteza. Ponieważ przedmiot badań jest zbyt złożony, aby można było badać go w całości, zastosowano analizę. Synteza pozwoliła na połączenie w całość wyodrębnionych i zbadanych w toku analizy różnych elementów składowych związanych z infrastrukturą krytyczną i czynników jej zagrażających. Ponadto autor wykorzystał wiedzę zdobytą podczas ćwiczeń wojskowych, w trakcie których planowane było użycie wojsk obrony przeciwlotniczej Sił Powietrznych do osłony wybranych elementów infrastruktury krytycznej. Autor wchodził w skład obsady stanowiska dowodzenia Brygady Rakietowej Obrony Powietrznej.

Uwarunkowania prawne infrastruktury krytycznej

Uwzględniając fakt, że problem skutecznej ochrony infrastruktury krytycznej znalazł swoje odzwierciedlenie w obowiązującym ustawodawstwie, można stwierdzić, że konieczność ochrony infrastruktury (niezależnie od tego, jak byłaby ona nazwana) była zadaniem o wysokim priorytecie na długo przed przystąpieniem Polski do Unii Europejskiej i nadal takim pozostaje. Różnorodność kryteriów, według których infrastruktura jest klasyfikowana, powoduje, że wybrane obiekty można zakwalifikować do różnych kategorii (wynikających z wymienionych wcześniej aktów prawnych). Wynika z tego także niejednoznaczny podział kompetencji organów odpowiedzialnych za wytypowanie obiektów o krytycznym znaczeniu dla państwa oraz określenie strategicznych celów ich ochrony[7]. Nie należy zapominać, że część tej infrastruktury znajduje się w rękach prywatnych (systemy łączności, teleinformatyczne, transport). Wymaga to odpowiedniej współpracy między gestorami poszczególnych systemów i świadomości, że w przypadku wystąpienia zakłóceń i nieprawidłowości skutki mogą objąć nie tylko bezpośrednich użytkowników infrastruktury, ale też mieć charakter międzynarodowy.

6 Przyjęto podział zagrożeń przedstawiony przez W. Lidwę w publikacji *Ochrona infrastruktury krytycznej*, AON, Warszawa 2012, s. 20.

7 Zob. W. Lidwa, *Ochrona infrastruktury krytycznej*, wyd. cyt., s. 15.

Członkostwo naszego kraju w Unii Europejskiej wiąże się z utworzeniem nowych lub dostosowaniem istniejących narodowych rozwiązań prawnych i terminologicznych do odpowiadających im rozwiązań unijnych. W krajach Unii używa się pojęcia infrastruktury krytycznej i zakłada się, że zniszczenie lub zakłócenie prawidłowego działania elementów infrastruktury krytycznej w jednym kraju może mieć skutki międzynarodowe. Wychodząc naprzeciw tym rozwiązaniom, uchwalono ustawę z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym oraz ustawę z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym, które co prawda nie wprowadzają jednolitego nazewnictwa i klasyfikacji w zakresie infrastruktury krytycznej (nadal w polskim ustawodawstwie funkcjonują wspomniane pojęcia: obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa oraz obszary, obiekty urządzenia i transporty podlegające obowiązkowej ochronie), niemniej zbliżają rozwiązania narodowe do rozwiązań europejskich. Ustawa określa m.in. zasady kategoryzowania obiektów jako należących do infrastruktury krytycznej, sporządzania ich wykazów, a także kryteria zakwalifikowania obiektu jako należącego do europejskiej infrastruktury krytycznej[8].

Wyróżnia się dwa rodzaje kryteriów: sektorowe i przekrojowe.

Kryteria sektorowe są to przybliżone progi liczbowe, które charakteryzują parametry wchodzące w skład systemów infrastruktury krytycznej obiektów, urządzeń oraz instalacji lub funkcje realizowane przez te obiekty, urządzenia oraz instalacje, warunkujące identyfikację infrastruktury krytycznej.

Kryteria przekrojowe obejmują:

- kryterium ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych;
- kryterium skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia jakości towarów i usług;
- kryterium skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej, cierpień fizycznych osób i zakłócenia codziennego życia, w tym utraty podstawowych usług.

Wymienione kryteria mają charakter niejawny.

Charakterystyka infrastruktury krytycznej

W Rzeczypospolitej Polskiej infrastruktura krytyczna wchodzi w skład 11 systemów mających kluczowe znaczenie dla bezpieczeństwa państwa oraz jego obywateli. Służą one zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

8 Szczegółowe zasady, zgodnie z którymi infrastruktura krytyczna może być uznawana za potencjalną europejską infrastrukturę krytyczną, zawarte są w Ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, art. 6a.

Infrastruktura krytyczna obejmuje następujące systemy[9]:
- 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).

Zapewnienie obywatelom energii elektrycznej, cieplnej, jak również zaopatrzenie struktur państwa w paliwa gwarantuje właściwe funkcjonowanie gospodarki oraz społeczeństwa. Rosnące zapotrzebowanie gospodarki i społeczeństwa na energię sprawia, że system zaopatrzenia w energię, surowce energetyczne i paliwa jest systemem o szczególnym znaczeniu dla funkcjonowania państwa[10]. Sektor energii elektrycznej jest dziedziną przemysłu grupującą podmioty:
- wytwarzające energię elektryczną,
- operatorów sieci przesyłowej,
- operatorów sieci dystrybucyjnej,
- sprzedające energię elektryczną.

Dostęp i korzystanie z zalet energii elektrycznej wymaga sprawnego działania rozbudowanego układu urządzeń do jej wytwarzania, przesyłania i rozdziału. Ponieważ brak jest możliwości magazynowania energii elektrycznej, w każdym momencie ilość energii wytwarzanej w elektrowniach musi być równa energii zużywanej przez odbiorców. System elektroenergetyczny musi więc być zdolny do zmiany kierunków i ilości przesyłanej energii. Jest to możliwe dzięki licznym połączeniom między elektrowniami, stacjami elektroenergetycznymi oraz grupami odbiorców energii.

Najważniejsze zagrożenia systemu zaopatrzenia w żywność mogą wynikać z funkcjonowania takich systemów infrastruktury krytycznej jak:
- zaopatrzenie w energię, surowce energetyczne i paliwa,
- łączności,
- finansowy,
- zaopatrzenia w wodę,
- transportowy.

Należy jednak zaznaczyć, że zakłócenia w powyższych systemach inaczej będą wpływać na rolnictwo tradycyjne (drobnotowarowe), a inaczej na rolnictwo inten-

9 Narodowy Program Ochrony Infrastruktury Krytycznej, s. 3, http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf [dostęp 26.11.2016].
10 Tamże, s. 4–6.

sywne, zwane też wysokotowarowym lub uprzemysłowionym. Gospodarstwa tradycyjne, najczęściej rodzinne, są bardziej odporne na krótkotrwałe zawirowania w zakresie funkcjonowania któregoś z systemu infrastruktury krytycznej od gospodarstw towarowych[11].

Sektor gazu ziemnego to dziedzina przemysłu grupująca podmioty wydobywające gaz ziemny oraz zajmujące się jego przesyłem, magazynowaniem i dostarczaniem do odbiorców końcowych.

W Polsce gaz ziemny wydobywany jest głównie na Podkarpaciu i Zapadlisku Przedkarpackim, a także w Wielkopolsce oraz rejonie Drezdenka i Międzychodu. W Polsce wydobywany jest głównie gaz zaazotowany (L). W gospodarce wykorzystywany jest głównie gaz wysokometanowy (E), dlatego zmuszeni jesteśmy do importu tego surowca. Głównym eksporterem jest Rosja, skąd przesyłany jest on do Polski:

- gazociągiem orenburskim, biorącym początek w południowej części Uralu;
- gazociągiem Zorza Polarna (z okolic Wuktyłu, przez Kobryń i Brześć do Warszawy);
- gazociągiem jamalskim (z Półwyspu Jamał w zachodniej Syberii)[12].

Sektor ropy naftowej to dziedzina przemysłu grupująca podmioty wydobywające oraz dostarczające i magazynujące ropę naftową, jak również zajmujące się jej przetwarzaniem oraz wytwarzaniem, dostarczaniem i magazynowaniem paliw płynnych.

Głównym źródłem dostaw surowca do przerobu jest import. Ropa naftowa transportowana jest do Polski odcinkiem rurociągu „Przyjaźń" i magazynowana w specjalnych zbiornikach o dużej pojemności.

Infrastruktura do transportu ropy naftowej składa się z trzech zasadniczych odcinków rurociągów:

- Odcinek Wschodni rurociągu „Przyjaźń" łączy Bazę Zbiornikową w Adamowie zlokalizowaną przy granicy z Białorusią z Bazą Surowcową w Płocku. Odcinek ten osiąga przepustowość 50 mln ton ropy naftowej rocznie;
- Odcinek Zachodni rurociągu „Przyjaźń" łączy Bazę Surowcową w Płocku z bazą ropy naftowej zlokalizowaną w Schwedt. Tą częścią magistrali płynie surowiec dla dwóch niemieckich rafinerii: PCK Raffinerie GmbH Schwedt oraz TOTAL Raffinerie Mitteldeutschland GmbH w Spergau. Odcinek Zachodni rurociągu „Przyjaźń" osiąga wydajność 27 mln ton ropy naftowej rocznie;
- Rurociąg Pomorski łączy Bazę Surowcową w Płocku z Bazą Manipulacyjną w Gdańsku. Tędy płynie rosyjska ropa naftowa przeznaczona dla rafinerii w Gdańsku należącej do Grupy LOTOS SA oraz na eksport przez Naftoport. Rurociągiem Pomorskim można transportować surowiec w dwóch kierunkach. Na trasie Gdańsk–

11 Tamże, s. 56.
12 Tamże, s. 15.

Płock jego przepustowość wynosi ok. 30 mln ton ropy naftowej rocznie, zaś w przeciwnym kierunku rurociąg osiąga wydajność ok. 27 mln ton na rok[13].

Sektor energii cieplnej to dziedzina przemysłu grupująca podmioty:

- wytwarzające energię cieplną,
- operatorów cieplnych sieci dystrybucyjnych.

Całkowita moc cieplna zainstalowana u koncesjonowanych wytwórców ciepła i w przedsiębiorstwach ciepłowniczych w Polsce wynosi około 60 tys. MW (dane za rok 2012), na co składają się:

- elektrownie i elektrociepłownie zawodowe,
- elektrociepłownie i ciepłownie niezawodowe,
- przedsiębiorstwa produkcyjno-dystrybucyjne i ciepłownie zawodowe[14].

Podstawowym paliwem wykorzystywanym do produkcji ciepła jest węgiel kamienny, którego udział w produkcji ciepła stanowi ok. 75%. Obok węgla swój udział mają olej opałowy, gaz ziemny i energetyka odnawialna[15].

Systemy łączności zapewniają przekazywanie informacji i obejmują pocztę oraz telekomunikację, jak również radiofonię i telewizję. Telekomunikację definiujemy jako nadawanie, odbiór lub transmisję informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną.

Łączność ma w gospodarce decydujące znaczenie dla procesów biznesowych, zarządzania czy w relacjach administracja–obywatel, obywatel–administracja, a także między samymi obywatelami[16].

System finansowy[17] jest to zespół instytucji finansowych, których zadaniem jest gromadzenie, dzielenie i wydatkowanie zasobów pieniężnych państwa, oraz ogół norm prawnych regulujących te procesy. Sprawnie funkcjonujący system finansowy ma decydujące znaczenie dla sprawnego funkcjonowania państwa i społeczeństwa. Organem administracji publicznej sprawującym państwowy nadzór nad rynkiem finansowym w Polsce jest Komisja Nadzoru Finansowego (KNF).

System finansowy składa się z kilku segmentów:

- budżetowego,
- bankowego,
- ubezpieczeniowego,
- kapitałowego.

System zaopatrzenia w żywność[18] to dziedzina gospodarki, na którą składa się wytworzenie środków produkcyjnych (np. nawozów, paszy) i usług dla rolnictwa, produkcja i pozyskiwanie surowców żywnościowych (w rolnictwie, rybactwie,

13 Tamże, s. 20.
14 Tamże, s. 24.
15 Tamże, s. 25.
16 Tamże, s. 27.
17 Tamże, s. 37–41.
18 Tamże, s. 42–43.

leśnictwie, łowiectwie), skup surowców żywnościowych, ich przechowywanie i transport, przetwórstwo surowców żywnościowych, obrót towarowy produktami żywnościowymi (magazynowanie i przechowywanie żywności, handel hurtowy i detaliczny, eksport i import) oraz system bezpieczeństwa żywności obejmujący wszystkie składowe łańcucha zaopatrzenia w żywność.

Rybołówstwo[19] jako część systemu zaopatrzenia w żywność obejmuje następujące gałęzi gospodarki:

- rybactwo śródlądowe i rybołówstwo morskie,
- racjonalne gospodarowanie żywymi zasobami morza,
- gospodarkę rybną i organizację rynku rybnego,
- organizację producentów rybnych, związków organizacji producentów rybnych i organizacji międzybranżowych.

System zaopatrzenia w żywność, jako jeden z podstawowych filarów gospodarki narodowej, ma bezpośrednie przełożenie na bezpieczeństwo ekonomiczne państwa. Celem strategicznym tego systemu jest zapewnienie wyżywienia narodu przez utrzymanie możliwości produkcyjnych gospodarki żywnościowej zapewniających bezpieczeństwo żywnościowe, bezpieczeństwo żywności i pasz.

Bezpieczeństwo żywnościowe jest kolejną z podstawowych potrzeb społeczeństwa. Składa się na nie szereg czynników i jest to zagadnienie zdecydowanie bardziej skomplikowane niż wyprodukowanie wystarczającego wolumenu żywności. Istotne są także: dostęp do pożywienia ubogiej ludności, systemy rolnictwa, polityka rolna, międzynarodowa polityka handlowa, koszty żywności, różnorodność i bezpieczeństwo żywności, łańcuchy żywnościowe, dystrybucja, walory żywieniowe i kwestie zdrowotne. Istotnym elementem bezpieczeństwa żywnościowego jest zapewnienie społeczeństwu dostępu do dostatecznej ilości żywności.

Głównym elementem systemu zaopatrzenia w żywność jest produkcja i pozyskiwanie surowców żywnościowych. Obejmuje ona przede wszystkim sprawy dotyczące:

- produkcji roślinnej i ochrony roślin uprawnych,
- nasiennictwa, z wyłączeniem leśnego materiału rozmnożeniowego,
- produkcji zwierzęcej i hodowli zwierząt.

Polska posiada 74 wyznaczone porty, przystanie i miejsca wyładunku. Blisko połowa z nich to miejsca wyładunku położone na plażach. Zwykle są one słabo wyposażone i wymagają znaczących usprawnień i modernizacji[20].

W Polsce zlokalizowanych jest 11 portów morskich, w których funkcjonuje 74 km nabrzeży portowych, w tym 43 km nabrzeży przeładunkowych. Natomiast ruch statków morskich odbywa się w 17 portach. Pięcioma najważniejszymi portami jeżeli chodzi o ilość wyładowywanej ryby, ilość obsługiwanych kutrów rybackich i odpowiedni stan wyposażenia są: Kołobrzeg, Darłowo, Ustka, Władysławowo i Hel[21].

19 Tamże, s. 49.
20 Tamże, s. 51.
21 Tamże, s. 66.

Znaczenie infrastruktury krytycznej dla bezpieczeństwa państwa i obywateli

Określenie „infrastruktura krytyczna" po raz pierwszy zostało użyte w latach dziewięćdziesiątych XX wieku i miało związek z poważnymi awariami sieci energetycznej w Stanach Zjednoczonych, skutkującymi utrudnieniami funkcjonowania dla milionów obywateli. Awarie sieci energetycznej wpłynęły negatywnie na inne systemy i instalacje, które w efekcie rozwoju cywilizacyjnego ułatwiają życie i zwiększają poczucie bezpieczeństwa, natomiast w przypadku zakłócenia ich prawidłowego działania można zaobserwować, jak bardzo człowiek jest od nich uzależniony.

Bezpieczeństwo[22] możemy postrzegać zarówno jako stan[23], jak i jako proces**,** w którym stan bezpieczeństwa i jego organizacja podlegają dynamicznym zmianom, co wymusza ciągłą działalność jednostek, społeczności lokalnych, państw oraz organizacji międzynarodowych w tworzeniu pożądanego stanu bezpieczeństwa. Z powyższego wynika, że bezpieczeństwo nie jest nam dane raz na zawsze, wraz ze zmianą charakteru zagrożeń należy podejmować nowe czynności zmierzające do zapewnienia bezpieczeństwa. Zmiana istoty zagrożeń wymusza sukcesywne rozszerzanie zasobów tworzących infrastrukturę krytyczną. Zwiększenie liczby systemów i instalacji tworzących infrastrukturę krytyczną wymusiło opracowanie strategii jej ochrony zarówno w odniesieniu do infrastruktury europejskiej (na wniosek Rady Europejskiej w 2004 roku), jak i znajdującej się w krajach członkowskich Unii (podstawowymi aktami prawnymi z tej dziedziny w Polsce są: ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym oraz ustawa z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym).

Kolejnym etapem realizacji strategii ochrony infrastruktury krytycznej było utworzenie europejskiego oraz narodowego programu ochrony infrastruktury krytycznej, uwzględniającego wszystkie rodzaje zagrożeń, spowodowanych zarówno działalnością człowieka, jak i naturalnych, wywołanych działaniami sił natury, oraz technologicznych, ze szczególnym uwzględnieniem zagrożeń terrorystycznych. Stworzenie odpowiednich warunków do poprawy bezpieczeństwa infrastruktury krytycznej realizowane jest przede wszystkim przez:

- zapobieganie zakłóceniom funkcjonowania infrastruktury krytycznej,
- przygotowanie na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,
- reagowanie w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
- odtwarzanie infrastruktury krytycznej.

Do realizacji i koordynacji powyższych zadań powołano w dniu 2 sierpnia 2008 roku Rządowe Centrum Bezpieczeństwa (RCB), pełniące funkcję krajowego cen-

22 E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011, s. 13.
23 Stan niezagrożenia, spokoju, pewności, stan i poczucie pewności, stan wolności od zagrożeń, stan wolności od strachu lub ataku; tamże, s. 13.

trum zarządzania kryzysowego. RCB jest strukturą ponadresortową i podlega Prezesowi Rady Ministrów. Dyrektor RCB w uzgodnieniu z ministrami i kierownikami urzędów centralnych odpowiedzialnych za systemy zaliczane do infrastruktury krytycznej opracowuje Narodowy Program Ochrony Infrastruktury Krytycznej[24].

Kolejnym istotnym dokumentem jest jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na poszczególne systemy. Wykaz wyróżnia europejską infrastrukturę krytyczną zlokalizowaną na terenie Rzeczypospolitej Polskiej, a także na terenie innych państw członkowskich, o ile wymieniona infrastruktura mogłaby mieć wpływ na nasz kraj. W celu właściwej identyfikacji europejskiej infrastruktury krytycznej wymagana jest współpraca międzynarodowa państw członkowskich Unii. Ze względu na niejawny charakter wymienianych informacji musi cechować się ona wzajemnym zaufaniem oraz należytą ochroną przed ich ujawnieniem.

Zagrożenia infrastruktury krytycznej

Określenie „krytyczny" jest definiowane jako „stanowiący przełom w czymś, rozstrzygający". Uwzględniając powyższe definicje, można wysnuć wniosek, że do infrastruktury krytycznej zaliczamy te urządzenia i instytucje usługowe, które są niezbędne do należytego funkcjonowania społeczeństwa i gospodarki państwa, a zakłócenie ich prawidłowego działania będzie miało znaczny wpływ zarówno na społeczeństwo, gospodarkę, jak i powiązane z nimi inne elementy infrastruktury. Wynika to z systemowego charakteru infrastruktury krytycznej – nieprawidłowe działanie choćby jednego z elementów systemu będzie miało negatywny wpływ na powiązane z nim inne elementy.

Zagrożenia, które mogą wywołać sytuację kryzysową mającą wpływ na bezpieczeństwo i funkcjonowanie całego państwa lub jego poszczególnych regionów, można podzielić na następujące kategorie[25]:

- zagrożenia naturalne,
- zagrożenia techniczne,
- terroryzm.

Zagrożenia naturalne związane są z siłami natury. Najważniejsze z nich to:

- Powodzie – definiowane jako naturalne, zwykle obejmujące znaczny obszar zjawisko przyrodnicze, charakteryzujące się silnym działaniem destrukcyjnym zarówno na środowisko, jak i na obiekty, instalacje i urządzenia ważne dla bezpieczeństwa obywateli. Możemy wyróżnić powodzie: opadowe (letnie), roztopowe (zi-

24 Szczegółowe zasady sporządzania i aktualizacji Narodowego Programu Ochrony Infrastruktury Krytycznej przedstawione zostały w Ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, art. 5b, oraz Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej.

25 Por. W. Lidwa, *Ochrona infrastruktury krytycznej*, wyd. cyt., s. 20.

mowe) oraz sztormowe. Do najbardziej wrażliwych na falę powodziową systemów i obiektów infrastruktury krytycznej zaliczane są systemy zaopatrzenia w żywność i wodę, systemy transportowe oraz produkcji i składowania materiałów i substancji niebezpiecznych.

- Silne wiatry, których obszaru występowania nie sposób przewidzieć. Do najgroźniejszych następstw możemy zaliczyć: powalone drzewa, zerwanie trakcji energetycznej (skutkujące przerwami w dopływie prądu, utrudnieniami komunikacyjnymi), uszkodzenia budynków.
- Długotrwałe susze – mimo że skala ich występowania na terenie kraju nie wywołuje zagrożenia dla życia i zdrowia obywateli, może przynieść znaczne straty materialne, zarównano dla rolnictwa, jak i reszty społeczeństwa w przypadku zwiększenia cen żywności.
- Ruchy tektoniczne będące przyczyną 90% wszystkich trzęsień ziemi, rozumianych jako wstrząsy podziemne, oraz drgania powierzchni ziemi spowodowane przyczynami naturalnymi – procesami tektonicznymi, wybuchami wulkanów. Prawdopodobieństwo wystąpienia trzęsień ziemi na terenie Polski jest niewielkie, aczkolwiek odnotowywane są tego typu zdarzenia. Znaczna część z nich wywołana jest tąpnięciami, związanymi z osiadaniem wyrobisk górniczych (tzw. trzęsienia ziemi zapadowe).
- Oblodzenia i intensywne opady śniegu, powodujące zakłócenia transportu, gospodarki komunalno-energetycznej i łączności. Oprócz bezpośredniego zagrożenia dla zdrowia i życia ludzkiego (oblodzenia i zaspy na drogach i liniach kolejowych) niebezpieczne są także uszkodzenia energetycznych linii przesyłowych, spowodowanie zarówno nadmiernym ich oblodzeniem, jak i uszkodzeniami wywołanymi przez ośnieżone drzewa i gałęzie. Nie należy zapominać o lawinach śnieżnych, mimo że ryzyko ich wystąpienia obejmuje niewielki obszar kraju.
- Epidemie – pod tym słowem należy rozumieć choroby zakaźne, atakujące większą liczbę ludzi. Mogą one zarówno być wywołane nieprzestrzeganiem zasad higieny, jak i powstawać w następstwie zdarzeń katastroficznych takich jak powodzie lub susze.

Ponadto ustawa z dnia 18 kwietnia 2002 roku o stanie klęski żywiołowej wyróżnia pod pojęciem katastrofy naturalnej: wyładowania atmosferyczne, długotrwałe występowanie ekstremalnych temperatur, osuwiska ziemi, masowe występowanie szkodników, a także choroby roślin i zwierząt.

Do największych zagrożeń naturalnych infrastruktury krytycznej występujących na terenie Polski należy zaliczyć powodzie, silne wiatry oraz silne opady śniegu i deszczu. Nagły charakter powyższych zjawisk, który przybierały wielokrotnie na przestrzeni ostatnich lat, pozwala założyć, że tego typu zagrożenia mogą występować cyklicznie, w sposób niespodziewany. Dotychczasowe obserwacje pozwalają wysnuć wnioski, że ochrona infrastruktury krytycznej przed tego typu zagrożeniami jest trudnym zadaniem. Ze względu na charakter systemowy infrastruktury krytycznej brak jest możliwości przewidywania rozwoju sytuacji kryzysowych. Znakomi-

tym przykładem może być awaria zasilania (ang. *blackout*)[26], która miała miejsce w 2003 roku na terenie Stanów Zjednoczonych Ameryki Północnej oraz Kanady. Wskutek lokalnej awarii sieci energetycznej doszło do przerw w zasilaniu na terenie ośmiu stanów w USA, prowincji Ontario w Kanadzie, wyłączenia szesnastu elektrowni atomowych na terenie obu krajów oraz licznych zakłóceń w transporcie drogowym i lotniczym, dezorganizacji pracy wielu instytucji. W efekcie awarii trwającej trzy dni doszło do strat ocenianych na 4 do 6 mld dolarów. Dla porównania straty poniesione w wyniku przerwy w dostawie energii elektrycznej w Szczecinie, która nastąpiła 8 kwietnia 2008 roku, ocenia się na 55 mln zł w odniesieniu do firm i instytucji, a przez operatorów energii elektrycznej – na 60 mln zł[27].

Zagrożenia techniczne spowodowane są działalnością człowieka. Dotyczą one z reguły obywateli, ich mienia, środowiska oraz obiektów infrastruktury krytycznej i mogą być następstwem awarii dotyczących:

- obiektów przemysłowych, w efekcie czego może wystąpić uwolnienie toksycznych środków przemysłowych – TŚP, w postaci gazów, cieczy lub ciał stałych; uwolnienie materiałów promieniotwórczych oraz biologicznych;
- obiektów komunalnych, gdzie do najpoważniejszych należą: awarie energetyczne, wodociągowe, gazownicze i ciepłownicze;
- obiektów budowlanych, gdzie do najpoważniejszych zaliczymy zawalenia się budynków i budowli;
- urządzeń transportowych (zwłaszcza służących do przewozu ładunków niebezpiecznych), których zniszczenie lub uszkodzenie może wystąpić w następstwie wypadku drogowego, kolejowego, lotniczego, morskiego lub śródlądowego.

Zaangażowanie Polski na arenie międzynarodowej (udział pododdziałów Wojska Polskiego w misji w Iraku, Afganistanie, czy rola, jaką Polska odegrała i nadal odgrywa podczas ostatnich wydarzeń z udziałem Ukrainy) może skutkować nie tylko postrzeganiem naszego kraju jako sojusznika w walce o demokrację na rzecz innych państw, ale także jako potencjalnego celu dla terrorystów. Wynikające z tego możliwe zagrożenia terrorystyczne, których celem jest wywołanie strachu wśród społeczeństwa[28] oraz wywarcie presji na aparat władzy, stawiają nowe zadania dla organów międzynarodowych i państwowych odpowiedzialnych za zapewnienie bezpieczeństwa w tej dziedzinie[29]. Mimo że na terenie Polski nie wydarzyły się dotąd ataki terrorystyczne (tak jak to miało miejsce w innych europejskich miastach: ataki bombowe na hiszpańskie pociągi 11 marca 2004 roku czy zamach na londyńskie metro 7 lipca 2005 roku), nie należy zapominać, że działalność terrorystyczna nie

26 Zob. https://pl.wikipedia.org/wiki/Awaria_zasilania_w_USA_i_Kanadzie_w_2003 [dostęp 26.11.2016].

27 R. Radzijewski, *O infrastrukturze krytycznej krytycznie* [w:] M. Żuber (red. nauk.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej*, WSOWL, Wrocław 2013, s. 33.

28 *Terror* (łac.) – strach, przerażenie.

29 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014, p. 83.

musi ograniczać się do tego typu działań – może być realizowana choćby w cyberprzestrzeni. Najlepszym tego przykładem jest cyberatak na Estonię (2007), który nastąpił bezpośrednio po decyzji władz o usunięciu z centrum Tallina pomnika żołnierzy radzieckich. Celem ataku były m.in. strony internetowe: instytucji rządowych, serwisów informacyjnych i banków. W szczytowym momencie kryzysu nie działała łączność wykorzystująca telefony komórkowe, brakowało możliwości realizacji transakcji finansowych z wykorzystaniem kart płatniczych[30]. Cyberatak może być także uzupełnieniem działań zbrojnych, co można było zaobserwować w czasie konfliktu rosyjsko-gruzińskiego w 2008 roku.

Funkcjonowanie polskich stron internetowych także było zakłócane przez cyberataki. W sierpniu 2014 roku strona internetowa Prezydenta RP oraz Giełdy Papierów Wartościowych przestały funkcjonować, a do ataku przyznała się grupa *CyberBerkut*[31], żądając jednocześnie zaprzestania wspierania władz ukraińskich przez Polskę. O kolejny atak na stronę Giełdy Papierów Wartościowych, odnotowany 23 października 2014 roku, podejrzewani są przedstawiciele tzw. Państwa Islamskiego[32].

O randze postrzegania potencjalnych zagrożeń z cyberprzestrzeni może świadczyć to, że mają one swoje odzwierciedlenie w Strategii Bezpieczeństwa Narodowego RP oraz osobnym dokumencie – Rządowym Programie Ochrony Cyberprzestrzeni RP.

Wydarzenia, jakie miały miejsce w Stanach Zjednoczonych (ataki terrorystyczne na World Trade Center i Pentagon z użyciem porwanych samolotów pasażerskich), oraz doniesienia o udaremnieniu kolejnych porwań samolotów w celu wykonania samobójczych ataków terrorystycznych zwracają uwagę na terroryzm powietrzny i lotniczy[33]. Terroryzm powietrzny definiowany jako ogół zagrożeń generowanych przez terrorystów z przestrzeni powietrznej jest pojęciem szerszym niż terroryzm lotniczy, który można zdefiniować jako atak na statek powietrzny i osoby w nim przebywające lub atak przy użyciu statku powietrznego na ludność i obiekty istotne dla funkcjonowania państwa.

Użycie statku powietrznego do bezpośredniego ataku na obiekty infrastruktury krytycznej, mimo ewidentnych trudności związanych z porwaniem samolotu i obezwładnieniem załogi, wydaje się skutecznym sposobem zniszczenia lub zakłócenia funkcjonowania tych obiektów. Nie bez znaczenia jest, że statek powietrzny ma możliwość pokonać przeszkody nie do przebycia przy wykorzystaniu „narzędzi lądowych". Samoloty pasażerskie i transportowe ze względu na potencjalne zniszczenia, jakie mogą wywołać, znajdują się pod szczególną ochroną. Nie wolno zapo-

30 Zob. http://wiadomosci.onet.pl/ciekawostki/10-najgrozniejszych-cyberatakow/djx4j [dostęp 26.11.2016].

31 Zob. http://wiadomosci.dziennik.pl/polityka/artykuly/467084,cyberatak-na-prezydent-pl-i-gpw-pl-cyber-berkut-nazywa-nas-sponsorami-ukrainskiego-faszyzmu.html [dostęp 26.11.2016].

32 Zob. http://tvn24bis.pl/informacje,187/dzihadysci-zaatakowali-strone-warszawskiej-gieldy-wykradziono-dane-klientow-gpw,481008.html [dostęp 26.11.2016].

33 Por. K. Dobija., *Zintegrowany system obrony powietrznej w walce z terroryzmem lotniczym*, rozprawa doktorska, AON, Warszawa 2009, s. 34.

minać, że oprócz nich terroryści mogą użyć całego spektrum statków powietrznych, które mimo mniejszych gabarytów (i związanych z tym możliwości oddziaływania na obiekty infrastruktury krytycznej) nadal mogą wywołać znaczne straty. Zaliczamy do nich śmigłowce, małogabarytowe samoloty, mikroloty (samoloty ultralekkie), lotnie z napędem, paralotnie z napędem oraz zdobywające coraz większą popularność (ze względu na ułatwiony dostęp) bezzałogowe aparaty latające i modele samolotów sterowane radiowo. Niewielka zdolność transportu ładunków może być zrekompensowana liczbą użytych środków – tzw. taktyka roju.

W wielu obiektach infrastruktury krytycznej można wyróżnić elementy składowe, których zniszczenie bądź uszkodzenie może mieć decydujący wpływ na ich pracę, a przy uwzględnieniu wzajemnych powiązań obiektów – na pracę innych elementów infrastruktury. Na przykład w celu przerwania pracy elektrowni wystarczy przerwać pracę jednego z elementów przemiany energii (kocioł, turbina lub generator) bądź doprowadzić do zniszczenia chłodni kominowej. W przypadku portu morskiego będą to np. konstrukcje służące do załadunku bądź rozładunku towarów – urządzenia dźwigowe, a w przypadku portów paliwowych ropociągi i gazociągi.

Nie należy także zapominać o zagrożeniach militarnych. Można jednak założyć, że w dającej się przewidzieć perspektywie czasu wybuch konfliktu na dużą skalę jest mało prawdopodobny, a ryzyko zaangażowania Polski w konflikt o charakterze regionalnym lub lokalnym jest niewielkie[34].

Doświadczenia ostatnich lat dobitnie wskazują, że mimo kilku dekad względnego spokoju na kontynencie europejskim prawdopodobieństwo wystąpienia konfliktu zbrojnego nie zostało do końca zażegnane. Wydarzenia na terenie byłej Jugosławii, których nierzadko bezradnymi świadkami była społeczność międzynarodowa, a także konflikt rosyjsko-gruziński (2008) czy wydarzenia na Ukrainie (2014) – począwszy od aneksji Krymu, przez walki na terenie wschodniej Ukrainy, zmuszają do zadania sobie pytania: co jeszcze możemy zrobić, aby zapewnić sobie bezpieczeństwo?

Rozważając zagrożenia dla infrastruktury krytycznej, należy zauważyć, że ona sama także może stanowić zagrożenie dla osób i innej infrastruktury (nie krytycznej) znajdującej się w jej sąsiedztwie. W razie awarii spowodowanej siłami natury uszkodzenie zbiorników zawierających chemikalia bądź materiały pędne może doprowadzić do katastrofy ekologicznej. Atak terrorystyczny na obiekty infrastruktury krytycznej może pociągnąć za sobą wiele ofiar ludzkich oraz straty materialne. Dlatego planując ochronę infrastruktury krytycznej, nie należy kierować się kosztami tych przedsięwzięć, ale potencjalnymi kosztami zaniechań zapewnienia kompleksowej ochrony.

Mimo że ochrona infrastruktury krytycznej znalazła swoje odzwierciedlenie w obowiązującym ustawodawstwie, można dostrzec obszary, które wymagają jednoznacznych działań. Pierwszym z nich jest kwestia obowiązującej definicji, przedstawiona na początku niniejszego artykułu. Mnogość aktów prawnych odnoszących

34 Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 14

się do ochrony infrastruktury krytycznej (obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa bądź obszarów, obiektów, urządzeń i transportów podlegających obowiązkowej ochronie – zależnie od tego, który z wcześniej przytoczonych dokumentów rozpatrujemy) powoduje niepotrzebny zamęt, w wyniku którego ten sam obiekt może wymagać różnego rodzaju przedsięwzięć z zakresu ochrony.

Samo pojęcie ochrony także nie jest jednoznacznie sprecyzowane. Ustawa o zarządzaniu kryzysowym nakazuje realizację „wszelkich działań zmierzających do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej", nie precyzując ich jednak. Zgodnie z zapisami ustawy o ochronie osób i mienia, ochrona osób i mienia realizowana jest przy pomocy ochrony fizycznej i technicznych (elektronicznych i mechanicznych) środków ochrony. Natomiast obiektom „szczególnie ważnym dla bezpieczeństwa i obronności państwa" zgodnie z zapisami ustawy należy zapewnić bezpośrednią ochronę fizyczną oraz zabezpieczenia techniczne, a także działania obronne obejmujące w szczególności rozbudowę inżynieryjną terenu na podejściach i wewnątrz bronionego obiektu, system ognia broni palnej, powszechną obronę przeciwlotniczą oraz ochronę przed skażeniami[35].

Zakres ochrony infrastruktury krytycznej został sprecyzowany w opublikowanym w 2013 roku Narodowym Programie Ochrony Infrastruktury Krytycznej wydanym przez Rządowe Centrum Bezpieczeństwa. Zgodnie z zapisami wymienionego dokumentu ochrona infrastruktury krytycznej obejmuje ochronę: fizyczną, techniczną, osobową, teleinformatyczną, prawną oraz plany odbudowy. Jednocześnie w dokumencie zawarty został zapis, że „dokument nie zawiera kompletu zasad i informacji na temat ochrony infrastruktury krytycznej, może jednak posłużyć jako rozbudowana lista kontrolna tego, jak należy zorganizować system ochrony IK"[36].

Podsumowanie

Podsumowując rozważania zawarte w niniejszym artykule, można stwierdzić, że nie ma prostej i jednoznacznej odpowiedzi na pytanie, jak zapewnić właściwą i skuteczną ochronę infrastruktury krytycznej.

Przyczyn takiego stanu rzeczy jest wiele. Jednym z powodów jest mnogość podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa poszczególnych systemów i urządzeń. Są to podmioty państwowe i prywatne, a biorąc pod uwagę obiekty zaliczane do europejskiej infrastruktury krytycznej – także podmioty funkcjonujące w innych krajach. Brak jednolitych rozwiązań dotyczących współpracy może skutkować nieprawidłowościami, których przyczyną nie są zaniedbania i zaniechania, ale

35 R. Radzijewski, *O infrastrukturze krytycznej krytycznie*, wyd. cyt., s. 27.

36 Narodowy Program Ochrony Infrastruktury Krytycznej. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Warszawa 2015, s. 4.

właśnie brak jednolitych uwarunkowań prawnych. Różnice w klasyfikacji obiektów występujących na terenie Rzeczypospolitej Polskiej, wynikające z różnych aktów prawnych, sugerują, że należałoby zacząć od ujednolicenia narodowych przepisów, nie zapominając o zgodności z analogicznymi dokumentami Unii Europejskiej.

Rozwój technologiczny i cywilizacyjny wymusza zmiany w zakresie obiektów i urządzeń tworzących infrastrukturę krytyczną. Obejmują one zarówno funkcje pełnione przez obiekty i urządzenia, jak i konkretne rozwiązania techniczne. Te zmiany z kolei mają wpływ na charakter zagrożeń infrastruktury krytycznej. Zagrożenia terrorystyczne zależą od pomysłowości terrorystów, ich możliwości wynikających z użytych przez nich rozwiązań technicznych oraz możliwości finansowych. Zaawansowane rozwiązania techniczne zwiększają podatność na działania niekinetyczne – aby spowodować zakłócenia w działaniu wybranych elementów infrastruktury krytycznej, wystarczy komputer z dostępem do Internetu i odpowiednio umotywowana osoba.

Bibliografia

Dobija K., *Zintegrowany system obrony powietrznej w walce z terroryzmem lotniczym*, rozprawa doktorska, AON, Warszawa 2009.

Jakubczak R., Marczak J., Gąsiorek K., Jakubczak W., *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*, Warszawa 2008, ISBN 978-83-7523-048-2.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, Dz.U. 1997 nr 78, poz. 483.

Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej*, AON, Warszawa 2012.

Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Charakterystyka systemów infrastruktury krytycznej.

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa 2011.

Radzijewski R., *Infrastruktura a bezpieczeństwo*, „Zeszyty Naukowe AON" nr 3 (92) 2013.

Radzijewski R., *O infrastrukturze krytycznej krytycznie* [w:] M. Żuber (red. nauk.), *Katastrofy naturalne i cywilizacyjne. Zagrożenia i ochrona infrastruktury krytycznej*, WSOWL, Wrocław 2013.

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. 2003 nr 116, poz. 1090.

Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 roku w sprawie planów ochrony infrastruktury krytycznej, Dz.U. 2010 nr 83, poz. 542.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014.

Ustawa z dnia 18 kwietnia 2002 roku o stanie klęski żywiołowej, Dz.U. 2002 nr 62, poz. 558.

Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia, Dz.U. 1997 nr 114, poz. 740.

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, Dz.U. 2007 nr 89, poz. 590.

Ustawa z dnia 29 października 2010 roku o zmianie ustawy o zarządzaniu kryzysowym, Dz.U. 2010 nr 240, poz. 1600.

Wołejszo J., Jakubczak R. (red.), *Obronność. Teoria i praktyka*, Bellona, Warszawa 2013.

IDENTIFICATION OF CRITICAL INFRASTRUCTURE AND ITS THREATS

Abstract

The significance of critical infrastructure, which is defined as devices, service institutions, as well as other areas that have a pertinent meaning on the sense of security of the citizens and the efficient functioning of the national economy, has gained new importance in recent years. The lessons learned from recent military conflicts and terrorist attacks, as well as analysis of events caused by natural disasters clearly demonstrate that disruption of the regular functioning of the individual elements of critical infrastructure might have a negative impact on its functioning as a single system. A wide spectrum of possible evaluating threats trigger development of new and effective solutions for protecting the critical infrastructure.

Key words: critical infrastructure, critical infrastructure threats