Bogdan Grenda[1]

Zagrożenia asymetryczne militarnej infrastruktury krytycznej — szanse i wyzwania w zakresie ochrony

Wstęp

Pojęcie „infrastruktura krytyczna" (IK) jest stosunkowo nowe. Zaczęto się nim posługiwać w Stanach Zjednoczonych i Kanadzie w latach 90. ubiegłego wieku. Mianem tym określano „systemy i instalacje niezbędne do funkcjonowania nowoczesnego społeczeństwa i administracji"[2]. Pojęcie infrastruktury krytycznej używane jest także w odniesieniu do obiektów militarnych, a ich ochrona stanowić musi ważną część planów obronnych.

Przykłady ostatnich konfliktów zbrojnych dowodzą, że podstawowym warunkiem osiągnięcia celu prowadzonych konfliktów jest zniszczenie elementów militarnej infrastruktury krytycznej w początkowym okresie wojny. Wyeliminowanie z walki lotnisk wojskowych, baz morskich, stanowisk dowodzenia itp. będzie miało istotne znaczenie dla trwałości i skuteczności działania całego systemu obronnego państwa. Jednym ze sposobów osiągnięcia tego celu jest niszczenie lub obezwładnienie kluczowych elementów

[1] Płk nawig. dr hab. inż. Bogdan Grenda — absolwent Wyższej Oficerskiej Szkoły Lotniczej w Dęblinie, ukończył studia podyplomowe dowódczo-sztabowe w Akademii Obrony Narodowej w Warszawie oraz logistykę na Uniwersytecie Ekonomicznym w Poznaniu. Doktor nauk wojskowych w specjalności siły powietrzne. Od 2010 r. zatrudniony w Akademii Sztuki Wojennej obecnie na stanowisku dziekana Wydziału Bezpieczeństwa Narodowego. Autor wielu artykułów i opracowań monograficznych w obszarze szeroko rozumianego bezpieczeństwa i obronności, w tym: *Wybrane problemy zarządzania kryzysowego w organizacji lotniczej, Komponenty Sił Powietrznych Rzeczypospolitej Polskiej w operacjach reagowania kryzysowego Unii Europejskiej, System walki Sił Powietrznych, Arena samobójców* i inne.

Kontakt z autorem za pośrednictwem redakcji.

[2] B. Cichoń, *System zarządzania kryzysowego w kontekście zapewnienia bezpieczeństwa publicznego* [w:] B. Kosowski, A. Włodarski (red.), *I Międzynarodowa konferencja naukowa. Wyzwania bezpieczeństwa cywilnego XXI wieku — inżynieria działań w obszarach nauki, badań i praktyki*, Warszawa 2007, s. 28.

infrastruktury obronnej państwa. Nie można zatem wykluczyć, że próby zakłócenia ich funkcjonowania podejmowane będą w każdym stanie gotowości obronnej państwa (pokoju, kryzysu i wojny), a zagrożenia mogą być generowane z następujących kierunków:

1) działalności wywiadowczej państw obcych — inwigilacja, sabotaż itp.;
2) organizacji terrorystycznych — porwania, dywersje, ataki bombowe itp.;
3) organizacji przestępczych — włamania do magazynów, wprowadzanie narkotyków na teren jednostek lotniczych, zabór uzbrojenia itp.;
4) miejscowej ludności lub cywilnych pracowników wojska — przejawiających chęć szybkiego wzbogacenia się poprzez oszustwa, kradzieże, włamania itp.;
5) bezpośredniego oddziaływania grup dywersyjnych, dywersyjno-rozpoznawczych, specjalnych przeciwnika na obiekty wojskowe;
6) ataku sił konwencjonalnych (naziemny, powietrzny i morski) przeciwnika.

Stąd też szczególnego znaczenia nabiera zapewnienie bezpieczeństwa zarówno całemu kompleksowi infrastruktury militarnej (sprzętowi wojskowemu, uzbrojenie, infrastrukturze wraz z systemami i podsystemami, układami i elementami), jak i stanowi osobowemu jednostki wojskowej. Jedną z dziedzin szeroko rozumianego bezpieczeństwa militarnej infrastruktury krytycznej jest ochrona. Pod pojęciem ochrony należy rozumieć zespół czynność (przedsięwzięć) uniemożliwiających skryte i podstępne przedostanie się na teren obiektu wojskowego osób niepowołanych, których zamiarem może być unicestwienie i neutralizacja personelu oraz sprzętu i techniki wojskowej. Celem ochrony jest zapewnienie porządku i bezpieczeństwa w rejonie obiektu, przeciwdziałanie aktom dywersji lub przejawom terroryzmu. Działania ochronne mają zapewnić skuteczną, bezpośrednią[3] i pośrednią ochronę[4] określonych obiektów oraz personelowi, mogącym stanowić przedmiot rozpoznania i ataków sił konwencjonalnych i dywersyjnych przeciwnika oraz ugrupowań terrorystycznych lub pospolitych grup przestępczych.

Dlatego też system ochrony militarnej infrastruktury krytycznej zabezpiecza ją przed wszelkimi zagrożeniami z zewnątrz i polega na sformułowaniu odpowiednich struktur organizacyjnych, opracowaniu procedur działania, wyposażeniu jednostki w techniczne środki ochrony itp. System ochrony każdego obiektu militarnego musi być nieustannie doskonalony, wciąż bowiem pojawiają się nowe zagrożenia, a potencjalny przeciwnik dysponuje coraz doskonalszymi środkami walki. W związku z powyższym celem artykułu jest ocena obecnie funkcjonującego systemu ochrony militarnej infrastruktury krytycznej oraz sformułowanie wniosków w zakresie jego poprawy.

[3] Ochroną bezpośrednią będziemy nazywać wszystkie te przedsięwzięcia i działania pododdziałów obrony naziemnej, podczas których następuje kontakt z przeciwnikiem usiłującym przerwać realizację standardowych zadań wykonywanych przez jednostkę.

[4] Ochroną pośrednią będziemy nazywali przedsięwzięcia mające zapobiegać spodziewanym oddziaływaniom przeciwnika.

Dokumenty normatywne

Problematykę związaną z ochroną militarnej infrastruktury krytycznej reguluje szereg dokumentów zarówno narodowych, jak i sojuszniczych. Szczególnie te drugie maja zastosowanie w przypadku realizacji zadań na rzecz państw obcych bazujących czasowo lub na stałe przebywających w Polsce. Podstawowymi dokumentami sojuszniczymi określającymi zadania i wymogi w zakresie ochrony wojsk są dyrektywy (np.: ACO Security Directive AD 70-1, ACO Forces Standards Vol. III — Standards for Air Forces), doktryny (np: Allied Joint Doctrine For Force Protection AJP 3.14) oraz zarzadzenia (np: NATO STANAG 2941, Zbiorowe metody ochrony, CM — Security within the North Atlantic Treaty Organisation — NATO) i inne.

Wśród dokumentów narodowych należy wyróżnić ustawy, rozporządzenia, regulaminy, decyzje, a w szczególności: ustawę o ochronie informacji niejawnych; ustawę o ochronie osób i mienia, instrukcję o ochronie obiektów wojskowych, regulamin ogólny Sił Zbrojnych RP, regulamin oddziałów wart cywilnych itp.

Na podstawie powyższych dokumentów na szczeblu jednostki wojskowej opracowuje się „Plan ochrony i obrony jednostki wojskowej", który określa zakres przedsięwzięć związanych z organizacją systemu ochrony jednostki wojskowej oraz sposoby minimalizacji skutków mogących wpłynąć na zdolność bojową i operacyjną lotniska. Innym dokumentem w tym obszarze działania jest „Instrukcja oficera dyżurnego jednostki wojskowej". Instrukcja ustala organizację służb dyżurnych w jednostce, wskazuje obiekty ochrony, sposób powiadamiania, sygnały alarmowe itp.

Wnioski i zalecenia

W każdej jednostce wojskowej istnieją ścisłe przepisy, które zawarte są w odpowiednich dokumentach zarówno w wewnętrznych strukturach prawnych sił zbrojnych, jak i krajowych oraz międzynarodowych przepisach. Specyfika funkcjonowania jednostki wojskowej wymusza konieczność dokładnego sprecyzowania norm i zasad, zarówno obowiązujących na jej terenie, jak i na terenach przyległych. Analiza dokumentów z obszaru ochrony jednostki wskazuje, że problematykę powyższą precyzją dwa dokumenty — „Plan ochrony i obrony jednostki wojskowej" opracowany na podstawie „Regulaminu ogólnego Sił Zbrojnych RP" oraz „Instrukcja oficera dyżurnego jednostki wojskowej ". Na podstawie analizy obu dokumentów można stwierdzić, że nie zawierają one szeregu istotnych z punktu widzenia ochrony militarnej infrastruktury krytycznej informacji, np. analizę zagrożeń, procedury działania służb ochrony, strefy ochrony itp. Dlatego też zasadne byłoby na szczeblu jednostki wojskowej opracować stałe procedury operacyjne. Dokument ten powinien zawierać takie informacje, jak: identyfikacja zagrożeń, strefy ochrony, procedury postępowania służb na wypadek zaistnienia sytuacji kryzysowej, organizację systemu ochrony

fizycznej i technicznej oraz rozmieszczenie tych elementów na terenie jednostki, zasady dostępu i kontroli dokumentów, wzory przepustek, organizację systemu łączności, wymogi dotyczące szkoleń i ćwiczeń itp. Innym ważnym dokumentem z punktu widzenia organizacji systemu ochrony, który należałoby opracować jest „Plan zabezpieczenia inżynieryjnego jednostki". Dokument ten powinien zawierać niezbędne informacje dotyczące rozbudowy infrastruktury inżynieryjnej jednostki wojskowej, w tym organizację elementów maskujących, fortyfikacyjnych np.: rozbudowę zapór drogowych i inżynieryjnych ograniczających ruch i dostęp na kierunkach szczególnie niebezpiecznych, ścian betonowych zabezpieczających sprzęt, stanowisk ogniowych oraz punktu kontrolnego, schronów przeciwodłamkowych dla personelu itp.

Charakterystyka militarnej infrastruktury krytycznej

W momencie wejścia do NATO i polskich aspiracji do członkostwa w Unii Europejskiej okazało się, że jednym z obszarów przyszłej integracji będzie również dostosowanie rozwiązań prawnych i terminologicznych do funkcjonujących w krajach członkowskich Unii Europejskich. Wśród wielu dotychczas nieznanych w naszym kraju pojęć pojawiły się nowe określenia, takie jak: zarządzanie kryzysowe (ang. *crisis management*) i infrastruktura krytyczna (ang. *critical infrastructure*). W praktyce okazało się, że oba te pojęcia są ze sobą bardzo silnie powiązane, ponieważ łączą je bezpośrednio zagadnienia bezpieczeństwa obywateli. Stały się one również podstawą do rozważań nad budowaniem skutecznych rozwiązań zapewniających swobodną i stabilną egzystencję współczesnych społeczeństw, zarówno na poziomie lokalnym, jak i krajowym czy międzynarodowym. Zdiagnozowano, że zmiany w tym obszarze w dużej mierze zależą od infrastruktury, którą rozumiano jako „urządzenia i instytucje usługowe niezbędne do należytego funkcjonowania społeczeństwa i produkcyjnych działów gospodarki"[5]. Z kolei określenie krytyczny definiowane jest jako „stanowiący przełom w czymś, rozstrzygający"[6]. Na podstawie analizy przedmiotu można stwierdzić, że dotychczas nie zdefiniowano pojęcia „militarna infrastruktura krytyczna", dlatego też punktem wyjścia do dalszych rozważań będzie „infrastruktura obronna kraju". Wśród elementów infrastruktury obronnej kraju wyróżnić można infrastrukturę wojskową. W *Słowniku terminów z zakresu bezpieczeństwa narodowego* zawarto definicję infrastruktury wojskowej — określonej ją w nim jako element infrastruktury obronnej

[5] M. Bańko (red.), *Wielki słownik wyrazów obcych*, Warszawa 2003, hasło: infrastruktura, s. 544.

[6] B. Dunaj (red.), *Słownik współczesnego języka polskiego*, tom 1, Warszawa 1999, hasło: krytyczny, s. 434. Natomiast w słowniku języka polskiego PWN słowo „krytyczny" zdefiniowano jako przełomowy, rozstrzygający, trudny, ciężki. Zob. M. Szymaczak (red.), *Słownik języka polskiego*, tom 1, Warszawa 1992, hasło: krytyczny, s. 1066.

obejmujący wszystkie stacjonarne (a w wyjątkowych wypadkach także ruchome) obiekty i urządzenia, które zgodnie ze swoim przeznaczeniem służą do zaspokajania potrzeb sił zbrojnych, a w szczególności dowodzenia, bytowania, szkolenia i przemieszczania wojsk[7]. W skład infrastruktury wojskowej wchodzą urządzenia i instytucje warunkujące działanie sił zbrojnych w czasie pokoju i wojny, takie jak: baza koszarowa, place ćwiczeń i strzelnice; systemy obsługi garnizonowej; system telekomunikacyjny; system transportowo-komunikacyjny; baza produkcyjna i technicznoremontowa; urządzenia radiotechniczne; lotniska; bazy morskie; obiekty służby zdrowia; składnice i magazyny; urządzenia inżynieryjno-obronne oraz jednostki wojskowe przeznaczone do ochrony i obrony oraz obsługi obiektów specjalnych[8].

Analizując powyższe, można przyjąć, że militarną infrastrukturą krytyczną są elementy infrastruktury obronnej, których działanie musi zostać zachowane w celu zapewnienia szeroko rozumianego bezpieczeństwa oraz najważniejszych usług w państwie. Stąd do kluczowych elementów militarnej infrastruktury krytycznej zaliczyć można: stanowiska dowodzenia, bazy lotnicze, bazy morskie, wyrzutnie rakiet i bazy logistyczne.

Baza lotnicza stanowi kompleks obiektów i zabudowań przeznaczonych do zabezpieczenia działań bojowych lotnictwa w różnych warunkach i porach doby. Do najważniejszych elementów bazy lotniczej zaliczyć można: statki powietrzne, lotnisko, składy paliwa i bomboskłady, schronohangary oraz stanowiska dowodzenia i systemy ubezpieczenia lotów. Maskowanie baz lotniczych jest bardzo trudne, dlatego współrzędne ich położenia, i prawdopodobnie także ich budowa, są dobrze znane przeciwnikowi już w okresie pokoju.

Baza morska to obszar na wybrzeżu morskim przeznaczony do bazowania marynarki wojennej obejmujący odpowiednio wyposażony i urządzony obszar wybrzeża morskiego z przylegającym do niego akwenem, służący do zabezpieczenia bojowej i codziennej działalności okrętów i jednostek marynarki wojennej. Bazę morską tworzą głównie porty wojenne — punkty bazowania (obecnie w Polsce — dwa) stanowią bazę marynarki wojennej. Stacjonują tu okręty, które w danym czasie nie wykonują żadnej misji na morzu. Zazwyczaj w porcie wojennym dokonuje się także drobnych napraw okrętów, dlatego też znajdują się tam miejsca i urządzenia do postoju okrętów, pobierania i uzupełniania zapasów amunicji, paliwa, żywności, wody słodkiej, umundurowania, urządzenia cumownicze (mola), falochrony, ukrycia dla okrętów, drogi dojazdowe, stacje elektryczne i wodociągowe, urządzenia do demagnetyzacji kadłubów okrętów wojennych i inne. Ponadto w skład bazy morskiej wchodzą odpowiednie siły i środki do jej obrony od strony morza, lądu i z powietrza.

[7] J. Kaczmarek, W. Łepkowski, B. Zdrodowski, *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 1996, s. 36.

[8] W. Ślemp, *Umocnienie terytorium jako element systemu obronnego Polski*, „Myśl Wojskowa" 1992, nr 5, s. 40.

Bazy logistyczne są zlokalizowane zazwyczaj w tylnej części obszaru działań w terenie zapewniającym ochronę i maskowanie, jednocześnie posiadającym odpowiednią liczbę dróg dowozu i ewakuacji.

Charakterystyczną cechą obiektów logistycznych jest to, że jest on mało odporny na oddziaływanie ogniowe. Szczególnie wrażliwe są składy amunicyjne oraz materiały pędne i smary (MPS), a także kolumny z dowożonym zaopatrzeniem.

Stanowisko dowodzenia to odpowiednio przygotowane i wyposażone oraz zajęte przez dowództwo (zazwyczaj dwie obsady operacyjne) miejsce, rejon, z którego dowódca dowodzi działaniami podległych mu wojsk. Stanowiska dowodzenia zajmują zazwyczaj dużą powierzchnię, na której rozmieszczona jest siła żywa (dowództwo, oficerowie sztabu, pododdziały obsługi) oraz środki kierowania i transportu. Zawsze jednak w jego strukturze występują trzy zasadnicze elementy: część operacyjna, węzeł łączności (telekomunikacyjny) i grupa zabezpieczenia, oddalone od siebie w odległości 100–500 m. Biorąc pod uwagę fakt, że wyeliminowanie SD powoduje naruszenie systemu kierowania wojskami, rażenie tego typu obiektów należeć będzie do celów priorytetowych przeciwnika.

Wnioski i zalecenia

Poszczególne elementy militarnej infrastruktury krytycznej usytuowane są w większości w kompleksach leśnych, co ułatwia ich znaczną penetrację i dostęp. Bazy lotnicze, morskie, stanowiska dowodzenia i inne rozumiane są jako kompleksy wojskowe i zgodnie z „Instrukcją o ochronie obiektów wojskowych" są zaliczone do najniższej kategorii ochrony (kategoria — IV), dlatego też główny wysiłek ochrony skupiony jest na obiektach wewnątrz tych obiektów zaliczonych do pierwszej kategorii ochrony.

Teren militarnej infrastruktury krytycznej jest ogrodzony i oświetlony, część jego budynków i pomieszczeń zabezpieczona jest instalacją sygnalizacji napadu i włamania, ochraniane budynki magazynowe i składy posiadają zabezpieczenia fizyczne zgodne z obowiązującymi przepisami. Na terenie obiektu znajduje się biuro przepustek i wartownia z centrum dozoru instalacji alarmowej. Takie usytuowanie obiektów i urządzeń stwarza konieczność organizacji systemu ochrony wewnątrz i na zewnątrz obiektu. Zasadne jest zatem dokonanie podziału na strefy ochrony różnych kategorii, czyli:

1) Strefę ochrony peryferyjnej — wydzielony obszar terenu poza ogrodzeniem zewnętrznym. W strefie tej nie instaluje się urządzeń i systemów alarmowych, natomiast powinno utrzymywać się pas o szerokości 25 m, wolny od wysokich zarośli, krzewów i traw, umożliwiający wgląd w teren przyległy.
2) Strefę ochrony zewnętrznej obwodowej — obszar terenu znajdujący się pomiędzy zewnętrznym i wewnętrznym ogrodzeniem obiektu. W strefie tej instaluje się zewnętrzne urządzenia i systemy alarmowe, oświetlenie, system łączności przewodowej dla sił ochronnych. W strefie ochrony zewnętrznej obwodowej należy stosować co najmniej dwa niezależnie działające systemy alarmowe, np.: system ogrodzeniowy i system

powierzchniowy, system ogrodzeniowy i system podziemny, dwa systemy powierzchniowe, w tym aktywne tory podczerwieni i bariery mikrofalowe, oraz inne kombinacje systemów.

3) Strefę ochrony zewnętrznej bezpośredniej — obszar terenu bezpośrednio przylegający do poszczególnych budynków. W strefie tej instalowane są zewnętrzne urządzenia i systemy alarmowe, które mogą współpracować z kamerami telewizyjnych systemów nadzoru. W strefie ochrony zewnętrznej bezpośredniej należy stosować pojedyncze systemy alarmowe — naziemne, podziemne lub ogrodzeniowe.
4) Strefę ochrony wewnętrznej — obszar wewnątrz magazynów, budynków wraz ze wszystkimi otworami okiennymi, drzwiowymi, wywietrznikami itp. W strefie tej instaluje się wewnętrzne urządzenia i systemy alarmowe. Można wykorzystywać w niej także kamery telewizyjnych systemów nadzoru współpracujące z wewnętrznymi urządzeniami alarmowymi oraz inne urządzenia wspomagające ochronę fizyczną tej strefy.

Zagrożenia dla militarnej infrastruktury krytycznej

Potencjalne zagrożenia dla militarnej infrastruktury krytycznej zaistnieć mogą w okresie pokoju, narastania sytuacji kryzysowej oraz podczas konfliktu militarnego. Najbardziej znany podział dotyczy zagrożeń zewnętrznych i wewnętrznych. Zagrożenia zewnętrzne dla ochranianego kompleksu militarnego mogą stanowić zorganizowane grupy przestępcze i terroryści, działający w sposób profesjonalny, przemyślany i zorganizowany oraz pojedynczy przestępcy. Mogą to również być przypadkowe osoby wykorzystujące nadarzającą się okazję, zaistniałą z powodu nieprawidłowego zabezpieczenia i nieprawidłowej ochrony mienia wojskowego lub osoby młodociane, które chcą zaimponować kolegom. Zagrożenia wywoływać też mogą byli żołnierze, znający system ochrony i miejsce składowania poszczególnych rodzajów sprzętu i środków bojowych, którzy w cywilu zeszli na drogę przestępczą. Pobliska ludność, która zamierza nielegalnie pozyskać np. sprzęt i materiały budowlane, siatkę ogrodzeniową, kable, paliwo itp. oraz osoby psychicznie niezrównoważone to kolejne potencjalne zagrożenia. Zagrożenia stwarzać także mogą obywatele państw obcych oraz regularne oddziały wojsk lądowych, sił powietrznych, marynarki wojennej oraz sił specjalnych przeciwnika w okresie poprzedzającym kryzys militarny i w trakcie jego trwania.

Zagrożenie wewnętrzne dla militarnej infrastruktury krytycznej mogą wynikać z działalności osób zatrudnionych na różnych stanowiskach w jednostce. Mogą być to zatem magazynierzy, którzy na skutek niegospodarności lub celowych działań spowodowali straty (ubytki) w przechowywanym mieniu i próbują nielegalnie je uzupełnić albo upozorować włamanie. Źródło zagrożeń stanowić mogą osoby zabezpieczające funkcjonowanie jednostki i mające dostęp do magazynów lub miejsc przechowywania mienia wojskowego. Nie można także bagatelizować osób angażowanych

do prac porządkowych na terenach technicznych, w magazynach lub innych miejscach przechowywania mienia oraz wartowników, pracowników ochrony i osób pełniących służby dyżurne. Wszystkie powyższe zagrożenia można zaliczyć do grupy zagrożeń asymetrycznych, które polegają przede wszystkim na strategii, na odniesieniu się do tych płaszczyzn u przeciwnika, w których państwo atakujące ma przewagę. W takich konfliktach odmiennie postrzegany jest również przeciwnik: przestaje być znany a staje się rozproszony, nieznany i w ten sposób niwelujący możliwość odwetu[9].

Wśród zagrożeń o charakterze zbrojnym należy wyróżnić:

— bezpośredni atak naziemny przeciwnika na jednostkę wojskową realizowany przez pododdziały specjalne, grupy dywersyjno-rozpoznawcze, pododdziały desantowo-szturmowe lub ugrupowania terrorystyczne;
— próby podłożenia materiałów wybuchowych w strefie jednostki wojskowej lub w niewielkiej odległości od niej z zamiarem oddziaływania na jej elementy;
— ostrzał artyleryjski lub rakietowy (ogień pośredni) jednostki wojskowej przy pomocy etatowych lub improwizowanych środków ogniowych (z zastosowaniem broni konwencjonalnej lub BMR);
— atak powietrzny przeciwnika — w ramach walki o zdobycie przewagi i panowania w powietrzu. Przeciwnik do niszczenia infrastruktury lotniskowej wykorzystywał będzie: bezzałogowe aparaty latające, śmigłowce, samoloty z konwencjonalnymi i jądrowymi środkami rażenia, strategiczne i taktyczne pociski balistyczne i aerodynamiczne (skrzydlate);
— porwania kluczowego personelu (np. dowództwa) w celu dezorganizacji pracy jednostki wojskowej oraz utrudnieniu realizacji zadań;
— katastrofy ekologiczne bezpośrednio wpływające na działalności jednostki wojskowej — spowodowane czynnikami zewnętrznymi lub oddziaływaniem przeciwnika.

Wnioski i zalecenia

Szybki rozwój technologiczny i ekonomiczny, zwiększający się zakres globalizacji, zanik tradycyjnych granic, to niektóre z wielu czynników powodujących wzrost zagrożeń bezpieczeństwa infrastruktury krytycznej cywilnej i wojskowej. Szczególnie niebezpiecznym zagrożeniem współczesnych czasów jest terroryzm, którego skutkiem mogą być zarówno choroby zakaźne, powodzie, skażenia środowiska, jak również zniszczenia obiektów budowlanych oraz urządzeń technicznych. Miejscem szczególnie podatnym na działania terrorystyczne stanowią urządzenia i obiekty militarnej infrastruktury krytycznej. Obiekty militarne mogą również być

[9] M. Madej, *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego — próba teoretycznej konceptualizacji* [w:] R. Kuźniar (red.), *Porządek międzynarodowy u progu XXI wieku*, Warszawa 2015, s. 54.

łatwym elementem oddziaływania grup przestępczych, służb specjalnych obcych państw, zorganizowanych grup militarnych itp. Różne też mogą być metody dezorganizacji funkcjonowania militarnej infrastruktury krytycznej np. sabotaż, ataki cybernetyczne i bombowe, potrwania itp. Generalnie można stwierdzić, że liczba czynników generujących zagrożenia wraz z rozwojem cywilizacyjnym stale wzrasta pomimo stosowania coraz doskonalszych systemów zabezpieczeń. Dlatego też w miarę jak pojawiają się nowe rodzaje zagrożeń powinno tworzyć się nowe lub doskonalić stare sposoby, metody i organizację zabezpieczania się przed nimi. Zatem w zakresie przeciwdziałania zagrożeniom militarnym i niemilitarnym system ochrony militarnej infrastruktury krytycznej powinien być przygotowany do realizacji następujących funkcji:

1) zbieranie — pozyskiwanie danych/informacji o zagrożeniach;
2) przechowywanie — gromadzenie danych, informacji i wiedzy o zagrożeniach w bazach danych;
3) analizowanie i przetwarzanie informacji;
4) dystrybucja informacji.

Zbieranie informacji o potencjalnych zagrożeniach dla bezpieczeństwa lotniska powinno odbywać się w sposób ciągły przy wykorzystaniu różnych źródeł informacji, począwszy od personelu militarnej infrastruktury krytycznej, pobliskiej ludności, a kończąc na służbach wojskowych i państwowych (np. Żandarmerii Wojskowej, Kontrwywiadzie i Wywiadzie Wojskowym, Policji, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej).

Gromadzenie informacji o zagrożeniach to konieczność, która pozwala na śledzenie zmian zachodzących w otoczeniu zewnętrznym i wewnętrznym militarnej infrastruktury krytycznej. Dane te powinny być gromadzone automatycznie (najczęściej poprzez specjalistyczne oprogramowanie pozwalające na zapis na dyskach twardych w postaci określonego sygnału użytecznego) lub też wprowadzane do banków danych ręcznie. Najważniejsze jest gromadzenie informacji wraz z opisem umożliwiającym ich szybkie odnalezienie (w przypadku konieczności ponownego wykorzystania) w systemie katalogowym.

Analiza i przetwarzanie informacji jest najtrudniejszą funkcją realizowaną w systemie ochrony. Dlatego też najistotniejszą kwestią jest dobór i profesjonalne przygotowanie personelu, który odpowiadałby za poddanie analizie i syntezie uzyskanych danych i opracowaniu ich w postaci zbiorczych zestawień. Informacje o zagrożeniach powinny być aktualizowane, kategoryzowane i selekcjonowane według ich przydatności. To na analizie zagrożeń powinno być oparte projektowanie systemu ochrony lotniska.

Dystrybucja informacji jest warunkiem niezbędnym do koordynacji działań w zakresie ochrony. Informacja o zagrożeniach powinna być dostarczona w odpowiednim czasie i formie do odpowiednich odbiorców (wewnętrznych — komórki organizacyjne bazy lotniczej oraz zewnętrznych — np. do przełożonego, podwładnego oraz ogniw pozamilitarnych). Dystrybucja zależeć będzie w ogromnej mierze od sprawności posiadanych kanałów informacyjnych.

Ochrona militarnej infrastruktury krytycznej

System ochrony militarnej infrastruktury krytycznej składa się z dwóch zasadniczych elementów: ochrony fizycznej i technicznych środków wspomagających ochronę obiektów. Ochronę fizyczną organizuje się na podstawie systemu służb dyżurnych oraz oddziałów wart cywilnych bądź specjalistycznie uzbrojonych formacji ochronnych przedsiębiorców. Najważniejszą rolę w systemie służb dyżurnych pełni oficer dyżurny, który jest bezpośrednim wykonawcą decyzji dowódcy. Kieruje on działaniami podległych służb dyżurnych (np. dyżurnych pododdziałów, dyżurnego parku sprzętu technicznego) oraz sprawuje nadzór nad ochroną obiektów i sprzętu wojskowego. Jednostki wojskowe są chronione także przez Specjalistyczne Uzbrojone Formacje Ochronne (dalej jako SUFO) lub Oddziały Wart Cywilnych. Specjalistycznie Uzbrojone Formacje Ochronne tworzone są jako prywatne firmy przez osoby, które uzyskały koncesje na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia, posiadają pozwolenie na broń. Oddział Warty Cywilnej tworzy, na wniosek dowódcy jednostki wojskowej, właściwy dowódca rodzaju Sił Zbrojnych RP. Warunkiem utworzenia oddziału wart cywilnych jest wprowadzenie stosownych zmian do jej etatu oraz przydzielenie etatów kalkulacyjnych i środków na wynagrodzenia pracowników Do technicznych środków wspomagających ochronę zalicza się:

— Ogrodzenie — teren jednostki musi być wydzielony pojedynczym rzędem ogrodzenia o wysokości 2 m wykonanym z elementów betonowych, siatki stalowej, lub drutu kolczastego.
— Oświetlenie — powinno zapewniać oświetlenie obwodnic patrolowych w warunkach nocnych i ograniczonej widoczności w sposób ciągły oraz doraźnie na obwodnicach niepatrolowanych.
— Umocnienia inżynieryjne — wykorzystywane w ochronie obiektów typu zapory, punkty oporu, stanowiska ogniowe. Zapory inżynieryjne ustawia się w miejscach, gdzie występuje największe zagrożenie obiektu, np. bramy wjazdowe.
— Systemy łączności (przewodowe i bezprzewodowe) działające w każdych warunkach atmosferycznych i terenowych, zapewniające skuteczną łączność z dowódcą warty.
— Urządzenia alarmowe — w strefie ochrony zewnętrznej należy stosować co najmniej dwa niezależnie działające systemy alarmowe instalowane na ogrodzeniach wewnętrznych. Obiekty podlegające szczególnej ochronie (kategoria I) należy chronić urządzeniami klasy S, pozostałe urządzeniami klasy C (klasyfikacja zgodna z PN-93/E-08390).

Wnioski i zalecenia

Ochronę fizyczną militarnej infrastruktury krytycznej tworzy kadra zawodowa pełniąca służby dyżurne oraz osoby cywilne zatrudnione w prywatnych firmach ochroniarskich. Służbę dyżurną pełnią żołnierze

zawodowi, którzy przeszli podstawowe szkolenie wojskowe i potrafią posługiwać się bronią. Znają też specyfikę funkcjonowania jednostek wojskowych oraz zasady i procedury postępowania na wypadek sytuacji nadzwyczajnych. Z kolei formacje chroniące jednostki wojskowe (SUFO) wybierane są w przetargach i jak zauważyła posłanka Beata Kempa znacznie większy nacisk kładzie się na cenę świadczonych usług niż na ich jakość. Posłanka w interpelacji nr 5474 z 6 czerwca 2012 r. do ministra obrony narodowej w sprawie ochrony jednostek wojskowych przez cywilów wskazuje również na ich słabą kondycje psychofizyczna oraz braki w wyszkoleniu — „Zmęczeni ochroniarze, często nieumiejący nawet posługiwać się bronią, chronią najbardziej elitarne polskie jednostki wojskowe”[10].

Analizując powyższe, można wskazać kilka obszarów doskonalenia systemu ochrony fizycznej jednostek wojskowych. Po pierwsze — do zadań ochrony obiektów militarnej infrastruktury krytycznej można byłoby zaangażować kadrę Żandarmerii Wojskowej. Wraz z zaprzestaniem powszechnego poboru do wojska zniknął problem żołnierzy służby czynnej, tym samym Żandarmeria ma mniej obowiązków i zadań. Obecnie w tej formacji wojskowej służy około 2200 osób, które są przygotowane zarówno do realizacji zadań ochronny obiektów, osób, jak i zadań obronnych na czas wojny. Dlatego też, w mojej opinii, główne zadanie Żandarmerii sprowadzałoby się do zapewnienia ochrony dostępu do jednostek (wejść i wjazdów) oraz ochrony kluczowego personelu w sytuacji narastania kryzysu militarnego. Po drugie należałoby stworzyć wojskowy pododdział zawodowy w jednostce wojskowej, który przejąłby zadania SUFO związane z jej ochroną oraz obroną (w czasie wojny). Obecnie na czas wojny przewidziany jest do utworzenia pododdział ochrony i obrony, ale składał się on będzie wyłącznie z żołnierzy rezerwy, których wyszkolenie i przygotowanie do realizacji zadań na czas wojny pozostawia wiele do życzenia. Dlatego też racjonalnym rozwiązaniem byłoby stworzenie grupy ochrony i obrony, składającej się tylko z żołnierzy zawodowych. Do zadań grupy należałoby: prowadzenie rozpoznania zagrożeń i przeciwdziałanie im, zapewnienie ochrony personelowi, sprzętu i infrastrukturze, eliminacja skutków zagrożeń ze strony BMR, zabezpieczenie medyczne i przeciwpożarowe oraz rozbudowa inżynieryjna. Adekwatnie do realizowanych zadań należałoby stworzyć strukturę organizacyjną Grupy, która mogłaby składać się z czterech najważniejszych komórek: Zespołu Obrony Pasywnej, Zespołu Odzyskiwania Zdolności Operacyjnej, Zespołu Obrony Naziemnej oraz Pionu Pełnomocnika ds. Informacji Niejawnych.

Drugim elementem systemu ochrony jednostek wojskowych są techniczne środki wspomagające ochronę. Zasadniczą funkcją technicznego podsystemu ochrony jest tworzenie bezpiecznego otoczenia dla funkcjonujących podmiotów na terenie jednostki. Jest to osiągalne poprzez

[10] Interpelacja nr 5474 do ministra obrony narodowej w sprawie ochrony jednostek wojskowych przez cywilów, <http://www.sejm.gov.pl/Sejm7.nsf/InterpelacjaTresc.xsp?key=363347E1>, 24 lutego 2018 r.

odpowiednie funkcjonowanie systemu przepustowego i udzielanie uprawnień dostępu do poszczególnych stref ochrony. Ważna jest też właściwa organizacja systemu wykrywania i informowania o intruzach. Wszystkie te elementy musza być zintegrowane w jeden wspólny system zarządzany przez Centrum Nadzoru.

W szczególności, biorąc pod uwagę aktualne zagrożenia, jednostki wojskowe powinny być wyposażone w następujące grupy środków technicznych:

1) Wyposażenie ostrzegające i oświetlające, takie jak samoczynne czujniki naziemne (UGS) i oświetlenie, takie jak miny oświetlające naciągowe, oświetlacze rakietowe (naboje sygnalizacyjne), reflektory szerokostrumieniowe i szperacze zamontowane na wieżach strażniczych.
2) Przyrządy do prowadzenia obserwacji w warunkach ograniczonej widoczności. Pododdziały ochrony powinny posiadać odpowiedni sprzęt do prowadzenia obserwacji i walki w warunkach nocnych i ograniczonej widoczności. Przyrządy takie obejmują: lornetki luminescencyjne, gogle noktowizyjne oraz celowniki noktowizyjne aktywne.
3) Zapory inżynieryjne. W zakresie przeciwdziałania ruchowi wojsk, powstrzymujące lub opóźniające wtargnięcie przeciwnika, połączone z systemem obserwacji i ognia. Obejmują one zapory z drutu kolczastego/concetriny (zapory betonowe, budowle przenośne, kolczatki — przenośne przyrządy do przebijania opon pneumatycznych) oraz bloki kamienne i betonowe, a w czasie zagrożeń militarnych grupy min oświetlających.
4) System ochronny w postaci kontroli wejść i wjazdów, posterunków ochronnych właściwie chroniony przed skutkami ataku bronią konwencjonalną i środkami rażenia NBC. Na czas wojny właściwie zorganizowany system ochronno-obronny (punkt ochronno-obronne) ze stanowiskami ogniowymi posiadającymi pasy ognia i pola obserwacji.

Podsumowanie

Ochrona militarnej infrastruktury krytycznej, z uwagi na jej ważne znaczenie dla systemu obronnego państwa, przybiera w dzisiejszych czasach znaczenia priorytetowego. Wzrosło bowiem zagrożenie ze strony zorganizowanych grup przestępczych, mających na celu m.in. pozyskiwanie broni, amunicji i materiałów wybuchowych. Jednocześnie rozwinął się terroryzm, a opłacalnym celem ataków grup terrorystycznych mogą stać się obiekty wojskowe. Nie można również bagatelizować możliwość pojawienia się zagrożeń stricte militarnych. Dlatego też bezpieczeństwo obiektów wojskowych można zapewnić m.in. poprzez skuteczną ochronę, która zawsze zależała od możliwości wykrycia obecności intruza — jeszcze przed wejściem do stref szczególnie chronionych — i poinformowania o tym fakcie służb ochrony fizycznej. Z oceny funkcjonowania systemów ochrony obiektów wojskowych wynika, że najsłabszymi ich ogniwami nadal pozostają ludzie, którzy wyznaczani są do ochrony, a także wadliwie skonstruowane

systemy bezpieczeństwa. W celu poprawy poziomu ochrony militarnej infrastruktury krytycznej należałoby podjąć następujące działania:

1) opracować szczegółowe procedury operacyjne w zakresie ochrony jednostek;
2) na bieżąco prowadzić analizę zagrożeń zewnętrznych (szczególnie w aspekcie zagrożeń o charakterze terrorystycznym) oraz wewnętrznych oraz wdrażać praktycznie wnioski z niej wynikające;
3) doskonalić rozwiązania organizacyjne zwiększające skuteczność systemów ochrony (stworzyć nowe pododdziały, np. grupę ochrony i obrony) oraz zaangażować do ochrony jednostek lotniczych stan osobowy Żandarmerii Wojskowej;
4) sukcesywnie zwiększać instalację nowoczesnych, technicznych urządzeń wspomagających ochronę, zarówno mechanicznych, jak i elektronicznych;
5) wyposażać jednostki wojskowe w nowoczesne środki łączności radiotelefonicznej i urządzenia sygnalizacji napadu oraz środki transportowe dla wart i służb;
6) prowadzić cykliczne szkolenia z zakresu ochrony obiektów i mienia wojskowego znacznej wartości z osobami odpowiedzialnymi za organizacje i realizację tych zamierzeń oraz administratorami systemów alarmowych z zakresu kontroli pracy i konserwacji urządzeń;
7) rozwijać współpracę z organami Żandarmerii Wojskowej, Policji i Wojskowych Służb Informacyjnych w zakresie wymiany informacji o zagrożeniach oraz podejmować działania w przypadku naruszenia systemu ochrony.

Słowa kluczowe: zagrożenia, obiekt militarny, infrastruktura krytyczna, system ochrony

Keywords: threats, military installations, critical infrastructure, protection system

Streszczenie: Zagrożenia asymetryczne to działania podmiotów, przede wszystkim pozapaństwowych, które dla osiągnięcia swoich celów wykorzystują niekonwencjonalne środki i techniki walki. Taki sposób działania może być przede wszystkim ukierunkowany na obezwładnienie lub zniszczenie infrastruktury krytycznej państwa, w tym elementów kluczowych związanych z systemem obronnym państwa. Dlatego też w artykule dokonano identyfikacji militarnej infrastruktury krytycznej, przybliżono dokumenty formalno-prawne z obszaru ochrony, ustalono też zagrożenia dla militarnej infrastruktury krytycznej oraz zaproponowano budowę systemu jej ochrony.

Summary: Asymmetric threats are actions of, predominantly non-state, actors, employing unconventional weapons and techniques to achieve their objectives. Such activities may be primarily aimed at degrading or destroying critical infrastructure of a targeted state, including key elements related to its national defence system. Therefore, the article identifies the elements of military critical infrastructure and potential threats, introduces formal and legal documents pertaining to the field of protection, and proposes the design of a military infrastructure protection system.