DOI: 10.34752/rj6d-jz98

Robert WÓDKIEWICZ [1]

ANALIZA OBOWIĄZUJĄCYCH UWARUNKOWAŃ PRAWNYCH DOTYCZĄCYCH UŻYCIA SIŁ ZBROJNYCH RP W SYTUACJACH KRYZYSOWYCH ORAZ OCHRONIE INFRASTRUKTURY KRYTYCZNEJ

Słowa kluczowe: *Siły Zbrojne RP, sytuacje kryzysowe, infrastruktura krytyczna*

STRESZCZENIE

W artykule przedstawiono analizę obowiązujących uwarunkowań prawnych dotyczących udziału Sił Zbrojnych Rzeczypospolitej Polskiej w realizacji zadań reagowania kryzysowego, strukturę systemu zarządzania kryzysowego w Wojsku Polskim oraz ochronę wojskowej infrastruktury krytycznej z uwzględnieniem zadań realizowanych przez osoby funkcyjne Sił Zbrojnych RP, a także zakres działań organów rządowych i samorządowych w ramach Narodowego Programu Ochrony Infrastruktury Krytycznej.

Wstęp

Pojęcie infrastruktury krytycznej jest terminem stosunkowo nowym, którego znaczenie w ciągu ostatnich lat nabrało dużego znaczenia. Przyczyną tego zjawiska jest wzrastające napięcie związane z możliwością wystąpienia ataków terrorystycznych, które mogą być skierowane nie tylko w stosunku do ludności cywilnej danego państwa, ale przede wszystkim w kierunku pozbawienia zdolności produkcyjnych infrastruktury krytycznej. Częściowe bądź całkowite zniszczenie infrastruktury krytycznej państwa spowoduje jego paraliż, prowadząc do pozbawienia społeczeństwa dostępu między innymi do energii, zaopatrzenia w wodę i żywność oraz np. utraty łączności w przypadku zniszczenia przekaźników sieci komórkowych.

Pod pojęciem infrastruktury krytycznej należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego

[1] Wydział Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej

obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[2].

Infrastruktura krytyczna jest nierozerwalnie związana z zarządzaniem kryzysowym, ponieważ w przypadku jej awarii, ataków na nią lub też innych zdarzeń powodujących zakłócenie jej działania, uruchamiane są odpowiednie procedury w ramach przedsięwzięć reagowania kryzysowego.

Wagę zagadnienia ochrony infrastruktury krytycznej podkreśla umieszczenie jej w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Mówi ona, że ochrona infrastruktury krytycznej jest obowiązkiem operatorów i właścicieli, którzy są wspierani przez potencjał administracji publicznej. Działania państwa polegają na ewentualnym uruchomieniu systemu zarządzania kryzysowego na wypadek zakłócenia funkcjonowania infrastruktury krytycznej[3].

Rola Sił Zbrojnych w realizacji zadań reagowania kryzysowego

Sił Zbrojne Rzeczypospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic[4]. I właśnie poprzez realizację zadania zapewnienia bezpieczeństwa należy rozumieć udział sił zbrojnych w minimalizacji zagrożeń kryzysowych oraz ochronie infrastruktury krytycznej w przypadku zaistnienia sytuacji jej zagrożenia.

Udział sił zbrojnych naszego kraju w realizacji zadań z zakresu reagowania kryzysowego regulują następujące akty prawne:

1. ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2017 r. poz. 1430);
2. ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2017 r. poz. 209);
3. ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2017 r. poz. 1897);
4. ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2017 r. poz. 1928).

Siły zbrojne RP stanowią ściśle zhierarchizowaną strukturę organizacyjną.

---

[2] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. z 2007 r. poz. 209 z późn. zm.), art. 3 pkt 2.

[3] *Strategia Bezpieczeństwa Narodowego RP*, Warszawa 2014, pkt 86.

[4] Ustawa z dnia 2 kwietnia 1997 r. *Konstytucja Rzeczypospolitej Polskiej* (Dz.U. z 1997 r. Nr 78 poz. 483 z późn. zm.), art. 26.

Zwierzchnikiem Sił Zbrojnych RP jest Prezydent Rzeczypospolitej Polskiej. W czasie pokoju sprawuje zwierzchnictwo nad Siłami Zbrojnymi RP za pośrednictwem Ministra Obrony Narodowej[5].

Trzon Sił Zbrojnych RP stanowi Dowództwo Generalne Rodzajów Sił Zbrojnych (DG RSZ), pod którego dowódcę podlegają Inspektoraty: Wojsk Lądowych, Sił Powietrznych, Marynarki Wojennej, Wojsk Specjalnych, Szkolenia oraz Rodzajów Wojsk. Dodatkowo pod DG RSZ podlega Inspektorat Wsparcia Sił Zbrojnych (IWsp SZ), który odpowiada między innymi za organizowanie i kierowanie systemem wsparcia logistycznego sił zbrojnych.

To jednostki podległe DG RSZ oraz IWsp SZ będą brały bezpośredni udział w minimalizacji skutków zagrożeń kryzysowych oraz ochronie potencjalnie zagrożonej infrastruktury krytycznej.

Istotną rolę w realizacji przedsięwzięć zarządzania kryzysowego odgrywają powołane stosunkowo niedawno Wojska Obrony Terytorialnej, które na mocy ustawy z dnia 16 listopada 2016 roku o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw, stały się piątym rodzajem wojsk Sił Zbrojnych RP[6].

Jednymi z zadań, które stoją przed Wojskami Obrony Terytorialnej są:

1. ochrona ludności przed skutkami klęsk żywiołowych, likwidacja ich skutków, ochrona mienia, akcje poszukiwawcze oraz ratowanie lub ochrona zdrowia i życia ludzkiego, a także udział w realizacji zadań z zakresu zarządzania kryzysowego;
2. współpraca z elementami systemu obronnego państwa, w tym szczególnie z wojewodami i organami samorządu terytorialnego[7].

W świetle wspomnianej ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, Siły Zbrojne RP mogą brać udział w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działaniach antyterrorystycznych i z zakresu ochrony mienia, akcjach poszukiwawczych oraz ratowania lub ochrony zdrowia i życia ludzkiego, oczyszczania terenów z materiałów wybuchowych i niebezpiecznych

[5] Tamże, art. 134.

[6] Ustawa z dnia 16 listopada 2016 r. *o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (Dz.U. z 2016 r. poz. 2138), art. 1 pkt 1 lit. a.

[7] http://mon.gov.pl/Obrona Terytorialna/Zadania WOT.

pochodzenia wojskowego oraz ich unieszkodliwianiu, a także w realizacji zadań z zarządzania kryzysowego[8].

Siły Zbrojne mogą być również użyte do przywrócenia normalnego funkcjonowania państwa w czasie obowiązywania stanu wyjątkowego. Nie może to jednak zakłócić ich zdolności do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej[9].

Rolę i miejsce Sił Zbrojnych w systemie zarządzania kryzysowego reguluje ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. W myśl jej zapisów użycie pododdziałów lub oddziałów wojskowych do wykonywania zadań miedzy innymi:

1. współudziału w monitorowaniu zagrożeń;
2. poszukiwawczo-ratowniczych;
3. współudziale w ochronie mienia pozostawionego na obszarze występowania zagrożeń;
4. usuwaniu skażeń promieniotwórczych;
5. likwidowaniu skażeń chemicznych oraz skażeń i zakażeń biologicznych odbywa się na wniosek wojewody do Ministra Obrony Narodowej[10].

Warunkiem użycia oddziałów i pododdziałów Sił Zbrojnych w sytuacji kryzysowej jest wystąpienie sytuacji, gdy użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające w opanowaniu sytuacji kryzysowej. Biorąc natomiast pod uwagę realizację zadań z zakresu zarządzania kryzysowego, udział w nich oddziałów sił zbrojnych jest możliwy, stosownie do ich przygotowania specjalistycznego, zgodnie z wojewódzkim planem zarządzania kryzysowego, który jest uzgodniony z właściwymi organami wskazanymi przez Ministra Obrony Narodowej[11].

Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 roku w sprawie określenia organów administracji rządowej, które tworzą centra zarządzania kryzysowego oraz sposobu ich funkcjonowania, zobligowało Ministerstwo Obrony Naro-

---

[8] Ustawa z dnia 16 listopada 2016 r. *o powszechnym obowiązku obrony Rzeczypospolitej Polskiej* (Dz.U. z 2017 r. poz. 1430), art. 3 ust. 2.

[9] Ustawa z dnia 21czerwca 2002 r. *ostanie wyjątkowym* (Dz.U. z 2017 r. poz. 1928), art. 11 ust. 1 i 2.

[10] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. z 2007 r. poz. 209 z późn. zm.), art. 14 ust. 2 pkt 4.

[11] Tamże, art. 25 ust. 1, 2, 3 i 4.

dowej do utworzenia Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej (CZK MON)[12].

Przedmiotowe centrum zostało powołane decyzją Nr 245/MON Ministra Obrony z dnia 7 lipca 2010 roku w sprawie utworzenia Centrum zarządzania Kryzysowego resortu obrony narodowej[13].

Z dniem 1 lutego 2014 roku, w związku z reformą systemu dowodzenia i kierowania funkcję CZK MON przejęło Dowództwo Operacyjne Rodzajów Sił Zbrojnych (DO RSZ). Biorąc pod uwagę aktualną strukturę organizacyjną DO RSZ, zagadnieniami zarządzania kryzysowego szczebla resortowego zajmuje się Połączone Centrum Operacyjne oraz wchodzące w jego skład oddziały:

1. planowania kryzysowego;
2. reagowania kryzysowego i współdziałania z układem pozamilitarnym.

Zgodnie z ustawą o zarządzaniu kryzysowym Minister Obrony Narodowej opracowuje plan zarządzania kryzysowego, w którym w szczególności uwzględnia:

1. analizę i ocenę możliwości wystąpienia zagrożeń, w tym dla infrastruktury krytycznej;
2. szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczania i likwidacji ich skutków;
3. organizację monitoringu zagrożeń i realizację zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa;
4. organizację realizacji zadań z zakresu ochrony infrastruktury krytycznej[14].

Plan zarządzania kryzysowego Ministerstwa Obrony Narodowej składa się z dziesięciu załączników, które odzwierciedlają ilość wydzielanych sił i środków do wsparcia ludności i władz samorządowych w przypadku wystąpienia sytuacji kryzysowych:

- Załącznik Nr 1 – Użycie Sił Zbrojnych RP w działaniach antyterrorystycznych i utrzymania porządku publicznego;

---

[12] Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. *w sprawie określenia organów administracji rządowej, które tworzą centra zarządzania kryzysowego* (Dz.U. z 2009 r. Nr 226 poz. 1810), § 2 ust. 1 pkt 1.

[13] Decyzja Nr 245/MON Ministra Obrony z dnia 7 lipca 2010 r. *w sprawie utworzenia Centrum Zarządzania Kryzysowego resortu obrony narodowej* (Dz.Urz. MON, Nr 14 z 2010 r. poz. 183).

[14] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. z 2007 r. poz. 209 z późn. zm.), art. 12 ust. 2.

- Załącznik Nr 2 – Użycie Sił Zbrojnych RP w izolacji obszaru zagrożenia oraz działaniach zabezpieczenia, ratowania życia i zdrowia oraz ewakuacji przy zagrożonych obiektach budowlanych i zabytkach;
- Załącznik Nr 3 – Użycie Sił Zbrojnych RP w akcjach o charakterze poszukiwawczo-ratowniczych;
- Załącznik Nr 4 – Użycie Sił Zbrojnych RP w sytuacjach wymagających użycia specjalistycznego sprzętu, a także oczyszczania terenu z przedmiotów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwianie;
- Załącznik Nr 5 – Użycie Sił Zbrojnych RP w monitorowaniu i ocenie skutków zagrożeń niemilitarnych;
- Załącznik Nr 6 – Użycie Sił Zbrojnych RP w likwidacji skażeń chemicznych i promieniotwórczych;
- Załącznik Nr 7 – Użycie Sił Zbrojnych RP w odbudowie oraz naprawach zniszczonej infrastruktury technicznej oraz zapewnieniu drożności szlaków komunikacyjnych;
- Załącznik Nr 8 – Użycie Sił Zbrojnych RP w działaniach przeciwepidemicznych, sanitarno-higienicznych, udzielaniu pomocy medycznej oraz likwidowaniu skażeń i zakażeń biologicznych;
- Załącznik Nr 9 – Użycie Sił Zbrojnych RP w ewakuacji ludności i mienia oraz ochronie terenu podczas zagrożeń niemilitarnych;
- Załącznik Nr 10 – Ochrona i zabezpieczenie obiektów infrastruktury krytycznej użytkowanych przez Ministerstwo Obrony Narodowej[15].

Ilość sił i środków wydzielonych i utrzymywanych w gotowości do użycia adekwatnie do zaistniałej sytuacji kryzysowej określona jest w „Planie użycia oddziałów i pododdziałów Sił Zbrojnych RP w przypadku wystąpienia sytuacji kryzysowych”[16].

Minister Obrony Narodowej realizując postanowienia art. 12 ust. 4 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, wydał zarządzenie Nr 6/MON Ministra Obrony narodowej z dnia 17 lutego 2016 roku w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego Ministra Obrony Narodowej.

---

[15] G. Sobolewski, *Metodyka opracowania planu zarządzania kryzysowego*, AON, Warszawa 2011, s. 55.

[16] Z. Piątek, *Procedury i przedsięwzięcia systemu reagowania kryzysowego*, AON, Warszawa 2006, s. 109.

Do najważniejszych zadań, które realizuje zespół należą:

1. Dokonywanie okresowej oceny zagrożeń na potrzeby Raportu[17];
2. Opiniowanie projektów planu zarządzania kryzysowego Ministerstwa Obrony Narodowej;
3. Wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom[18].

W skład zespołu wchodzą:

1. Przewodniczący – Minister Obrony Narodowej;
2. Zastępcy przewodniczącego – Sekretarz Stanu w Ministerstwie Obrony Narodowej, Dowódca Operacyjny Rodzajów Sił Zbrojnych;
3. Sekretarz – Zastępca Szefa Sztabu Ds. Operacyjnych Dowództwa Operacyjnego Rodzajów Sił Zbrojnych;
4. Członkowie – Szef Sztabu Generalnego Wojska Polskiego, Komendant Główny Żandarmerii Wojskowej, Szef Służby Kontrwywiadu Wojskowego, Szef Służby Wywiadu Wojskowego, Dowódca Garnizonu Warszawa, Rzecznik Prasowy Ministra Obrony Narodowej[19].

Zespół spełnia rolę organu opiniodawczo-doradczego Ministra Obrony Narodowej w sprawach realizacji zadań z zakresu zarządzania kryzysowego.

Siły zbrojne w realizacji zadań ochrony infrastruktury krytycznej

Zadania zarządzania kryzysowego Ministerstwa Obrony Narodowej z zakresu ochrony infrastruktury krytycznej reguluje decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 27 stycznia 2014 r. w sprawie podziału odpowiedzialności za realizację zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej[20].

---

[17] Raport o zagrożeniach bezpieczeństwa narodowego, Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. z 2007 r. poz. 209 z późn. zm.), art. 5a.

[18] Tamże, art. 12 ust. 2c.

[19] Zarządzenie Nr 6/MON Ministra Obrony Narodowej z dnia 17 lutego 2016 r. *w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego Ministra Obrony Narodowej* (Dz.Urz. MON z 2016 r. poz. 14), § 2.1.

[20] Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 27 stycznia 2014 r. *w sprawie podziału odpowiedzialności za realizacje zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej* (Dz.Urz. MON z 2014 r. poz. 33).

Zadania zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej realizowane w resorcie obrony narodowej obejmują:

1. Udział w przygotowaniu i realizacji Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK);
2. Udział w przygotowaniu jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, z podziałem na systemy;
3. Opracowanie planów ochrony infrastruktury krytycznej dla wojskowych obiektów, instalacji, urządzeń i usług ujętych w jednolitym wykazie;
4. Ochronę wojskowej infrastruktury krytycznej;
5. Przygotowanie Planu Zarządzania Kryzysowego resortu obrony narodowej w części dotyczącej wojskowej infrastruktury krytycznej;
6. Prowadzenie ewidencji i przetwarzanie informacji w zakresie wojskowej infrastruktury krytycznej[21].

Decyzją Nr 8/14/PI Podsekretarza Stanu w Ministerstwie Obrony Narodowej z dnia 7 lutego 2014 roku w sprawie wskazania realizatorów zadań zarządzania kryzysowego z zakresu ochrony wojskowej infrastruktury krytycznej, na odpowiedzialnego za realizację zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej w resorcie obrony narodowej wyznaczono Dyrektora Biura Infrastruktury Specjalnej.

Dyrektor Biura Infrastruktury Specjalnej:

1. Koordynuje w resorcie obrony narodowej przedsięwzięcia związane z ochroną wojskowej infrastruktury krytycznej;
2. W ramach przygotowania Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) uczestniczy w określeniu szczegółowych kryteriów pozwalających wyodrębnić wojskową infrastrukturę krytyczną, biorąc pod uwagę jej znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli;
3. W ramach przygotowania jednolitego wykazu[22]:
   - koordynuje w resorcie obrony narodowej proces typowania wojskowych obiektów, instalacji, urządzeń i usługo do ujęcia w jednolitym wykazie i kieruje uzgodnioną w resorcie obrony narodowej propozycję wojskowej

[21] Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 27 stycznia 2014 r. *w sprawie podziału odpowiedzialności za realizację zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej* (Dz.Urz. MON z 2014 r. poz. 33) pkt 2.

[22] Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. z 2007 r. poz. 209 z późn. zm.), art. 5b ust. 7 pkt 1.

infrastruktury krytycznej do ujęcia w krajowym wykazie infrastruktury krytycznej;
- uzgadnia z Dyrektorem Rządowego Centrum Bezpieczeństwa zasadność ujęcia wytypowanych obiektów, instalacji, urządzeń i usług w jednolitym wykazie;
- dokonuje weryfikacji obiektów wojskowych pod względem zasadności ich ujęcia w jednolitym wykazie;
- przygotowuje i aktualizuje informację o wojskowej infrastrukturze krytycznej;

4. Koordynuje proces opracowania planów ochrony wojskowej infrastruktury krytycznej przez operatorów oraz ich uzgadnianie z właściwym terytorialnie wojewodą, komendantem wojewódzkim Państwowej Straży Pożarnej, komendantem wojewódzkim Policji, dyrektorem regionalnego zarządu gospodarki wodnej, wojewódzkim inspektorem nadzoru budowlanego, wojewódzkim lekarzem weterynarii, państwowym wojewódzkim inspektorem sanitarnym, dyrektorem urzędu morskiego[23];
5. W ramach ochrony wojskowej infrastruktury krytycznej:
   - gromadzi i przetwarza informacje dotyczące zagrożeń dla wojskowej infrastruktury krytycznej;
   - przygotowuje wytyczne dla operatorów, uszczegóławiające sposób sporządzania planów ochrony infrastruktury krytycznej i ich aktualizacji;
   - sprawdza zgodność przygotowanych projektów planów ochrony wojskowej infrastruktury krytycznej z wytycznymi, o których mowa powyżej;
   - przygotowuje w miarę potrzeb, wytyczne w zakresie odtwarzania wojskowego infrastruktury krytycznej;
6. Współuczestniczy w opracowaniu Planu Zarządzania Kryzysowego resortu obrony narodowej, w części dotyczącej wojskowej infrastruktury krytycznej;
7. Prowadzi ewidencję i przetwarza informacje w zakresie wojskowej infrastruktury krytycznej;
8. Współpracuje z dyrektorem Rządowego Centrum Bezpieczeństwa oraz ministrami odpowiedzialnymi za systemy infrastruktury krytycznej, do których zaliczono obiekty wojskowej infrastruktury krytycznej[24].

---

[23] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. *w sprawie planów ochrony infrastruktury krytycznej* (Dz.U. z 2010 r., Nr 83, poz. 542), § 4.

[24] Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 27 stycznia 2014 r. *w sprawie podziału odpowiedzialności za realizację zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej* (Dz.Urz. MON z 2014 r. poz. 33), pkt 4.

Zgodnie z art. 5b ust. 1 ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, Rada Ministrów uchwałą Nr 210/2015 z dnia 2 listopada 2015 roku przyjęła NPOIK, określając w nim ministrów odpowiedzialnych za poszczególne systemy infrastruktury krytycznej. Uchwałą Nr 61/2016 z dnia 1 czerwca 2016 roku Rada Ministrów przyjęła uchwałę zmieniającą uchwałę w sprawie przyjęcia NPOIK. Aktualizacja NPOIK wynikała z konieczności dostosowania jego treści do zmian w strukturze działów administracji rządowej, wprowadzonych między innymi:

1. Ustawą z dnia 19 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 1960);
2. Ustawą z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 2281).

Celem NPOIK jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej. Wraz z innymi dokumentami programowymi składa się na cel nadrzędny, którym jest podniesienie bezpieczeństwa naszego kraju.

Infrastruktura krytyczna służy do zaspokojenia potrzeb wszystkich obywateli. Nadrzędnym jej celem jest utrzymanie ciągłości świadczenia usług kluczowych dla państwa. Główny wysiłek realizacji NPOIK spoczywa na Rządowym Centrum Bezpieczeństwa, ministrach odpowiedzialnych za systemy infrastruktury krytycznej oraz operatorach infrastruktury krytycznej (właściciel oraz posiadacz samoistny i zależny obiektów, instalacji, urządzeń i usług infrastruktury krytycznej[25]) wyszczególnionych w wykazie infrastruktury krytycznej.

Najlepszą wiedzę i warunki do ograniczenia zagrożeń dla infrastruktury krytycznej oraz zmniejszenia jej podatności na te zagrożenia, mają operatorzy infrastruktury krytycznej. Dlatego też zobowiązani są oni do:

1. przygotowania i wdrożenia, stosownie do przewidywanych zagrożeń planów ochrony infrastruktury krytycznej oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia;
2. wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej;
3. niezwłocznego przekazywania Szefowi Agencji Bezpieczeństwa Wewnętrznego informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej;
4. współpracy w tworzeniu i realizacji NPOIK.

---

[25] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. *w sprawie Narodowego Planu Ochrony Infrastruktury Krytycznej* (Dz.U. z 2010 r., Nr 83, poz. 541), § 1.

Systemy infrastruktury krytycznej różnią się między sobą charakterystyką funkcjonowania, uwarunkowaniami prawnymi oraz użytkownikami tych systemów. Dlatego NPOIK wskazuje ministrów odpowiedzialnych za poszczególne systemy. Odpowiedzialność ta polega w szczególności na:

1. wsparciu Rządowego Centrum Bezpieczeństwa w budowie systemu ochrony infrastruktury krytycznej;
2. współpracy z Rządowym Centrum Bezpieczeństwa i wsparciu w identyfikacji infrastruktury krytycznej oraz wdrażaniu i aktualizacji NPOIK;
3. inicjowaniu zmian aktów prawnych w celu ułatwienia i wsparcia wykonywania zadań z zakresu ochrony infrastruktury krytycznej;
4. dokonywaniu oceny ryzyka zakłócenia funkcjonowania systemu infrastruktury krytycznej, wywołanego zniszczeniem lub zakłóceniem funkcjonowania infrastruktury krytycznej;
5. współpracy z organami, w kompetencji których znajdują się sprawy dotyczące części składowych systemu infrastruktury krytycznej, nie będących bezpośrednio we właściwości koordynatora;
6. współpracy z innymi koordynatorami systemów infrastruktury krytycznej, w zakresie zależności między systemami infrastruktury krytycznej;
7. współpracy z operatorami infrastruktury krytycznej w zakresie jej ochrony, animowanie tej współpracy i jej podtrzymywanie;
8. wsparciu działań zmierzających do odtworzenia infrastruktury krytycznej;
9. inspirowaniu wdrażania nowoczesnych technik ochrony infrastruktury krytycznej[26].

Bardzo ważnym elementem, chociaż bezpośrednio niezaangażowanym w realizację zadań na rzecz ochrony infrastruktury krytycznej jest Prezydent Rzeczypospolitej Polskiej. Ze względu na posiadane kompetencje w obszarze bezpieczeństwa państwa, jest gwarantem zaangażowania władz państwa w proces poprawy poziomu bezpieczeństwa infrastruktury krytycznej, a co za tym idzie również całego państwa.

Prezydent RP bierze udział w NPOIK w zakresie swoich konstytucyjnych kompetencji obejmujących bezpieczeństwo narodowe i obronność. Wspiera również administrację rządową i samorządową w działaniach na rzecz ochrony infrastruktury krytycznej.

Rola Rady Ministrów jest równie znacząca. Przyjmuje ona w drodze uchwały NPOIK, a przez podległe jej organy i podmioty oraz Rządowy Zespół Reagowania Kryzysowego:

---

[26] Narodowy Program Ochrony Infrastruktury Krytycznej 2015 r.

1. czuwa nad przestrzeganiem zasad i wypełnieniem postanowień NPOIK;
2. wspiera i promuje działania na rzecz osiągnięcia celów NPOIK;
3. umożliwia uzyskanie środków finansowych na ochronę infrastruktury krytycznej, uwzględniając te zadania w budżecie państwa.

Istotną rolę w systemie ochrony infrastruktury krytycznej pełnią służby specjalne. Dysponują bowiem potencjałem ludzkim i technicznym, wystarczającym do zidentyfikowania potencjalnych zagrożeń infrastruktury krytycznej. Wymiana informacji o tych zagrożeniach z operatorami infrastruktury krytycznej i innymi podmiotami właściwymi w sprawach ochrony infrastruktury krytycznej (z zachowaniem przepisów o ochronie informacji niejawnych) jest priorytetem w procesie planowania ochrony infrastruktury krytycznej[27].

Szczególną rolę odgrywa Agencja Bezpieczeństwa Wewnętrznego (ABW), szefowi której organy administracji publicznej, właściciele i posiadacze obiektów, urządzeń infrastruktury krytycznej przekazują informacje dotyczące zagrożeń o charakterze terrorystycznym dla infrastruktury krytycznej. W przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze krytycznej, Szef ABW może wydawać polecenia organom administracji publicznej, właścicielom i posiadaczom obiektów, urządzeń infrastruktury krytycznej mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację oraz przekazywać im informacje niezbędne do tego celu[28].

Infrastruktura krytyczna zlokalizowana jest na terenie gmin, miast i powiatów, dlatego też starostowie, wójtowie, burmistrzowie i prezydenci miast odgrywają ważną rolę w zakresie ochrony ludności narażonej na potencjalne skutki zakłócenia funkcjonowania infrastruktury krytycznej oraz w zakresie ochrony infrastruktury krytycznej, umożliwiając jak najszybsze wsparcie jej operatorów.

Ich zadania obejmują w szczególności:

1. ujęcie w planach zarządzania kryzysowego zadań z zakresu ochrony infrastruktury krytycznej zlokalizowanej w obszarze ich właściwości[29];
2. określenie procedur reagowania na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej w obszarze właściwości;
3. ochrona ludności przed skutkami zakłócenia funkcjonowania infrastruktury krytycznej z wykorzystaniem zasobów własnych oraz operatora infrastruktury krytycznej.

---

[27] Narodowy Program Ochrony Infrastruktury Krytycznej 2015 r.

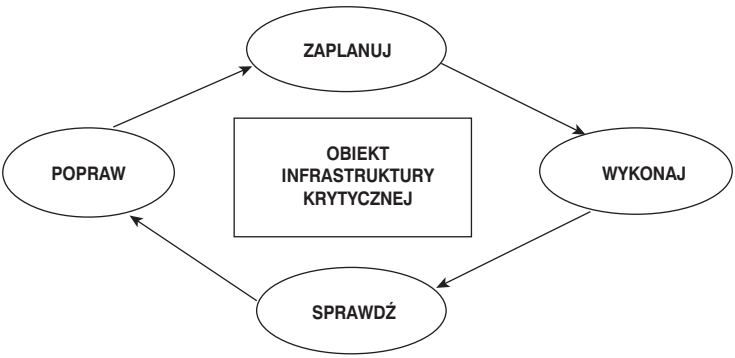
[28] Ustawa z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* (Dz.U. z 2016 r. poz. 904), art. 4.

[29] Narodowy Program Ochrony Infrastruktury Krytycznej 2015 r.

Co należy rozumieć pod pojęciem ochrony infrastruktury krytycznej? Jest to długofalowy, skomplikowany proces zapewnienia jej bezpieczeństwa. Składa się on z następujących etapów:

1. wskazanie zakresu, celów które należy osiągnąć w ramach ochrony infrastruktury krytycznej oraz adresatów tych działań;
2. identyfikacja krytycznych zasobów, funkcji oraz określenie sieci powiązań z innymi systemami infrastruktury krytycznej, w tym podmiotami i organami;
3. ocena ryzyka;
4. rozwój i wdrożenie systemu ochrony infrastruktury krytycznej, w tym opracowanie i akceptacja planów ochrony i odtwarzania infrastruktury krytycznej;
5. testowanie (przez ćwiczenia) i przegląd (przez audyt i samoocenę) systemu ochrony infrastruktury krytycznej oraz pomiar postępów na drodze do osiągnięcia celu;
6. doskonalenie rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów i pomiarów[30].

Konieczność nieustannego doskonalenia pozwala na ujęcie procesu ochrony infrastruktury krytycznej w cykl Deminga (rys. 1).



Rysunek 1. Obiekt infrastruktury krytycznej w cyklu Deminga

Źródło: NPOIK 2015.

Wersja popularna cyklu Deminga składa się z działań następujących po sobie w porządku logicznym: zaplanuj (wskaż zakres, cele do osiągnięcia w ramach

[30] Tamże.

ochrony infrastruktury krytycznej oraz adresatów), wykonaj (zidentyfikuj krytyczne zasoby, funkcje oraz zależności, dokonaj oceny ryzyka, wskaż priorytety działania, opracuj i wdróż system ochrony infrastruktury krytycznej), sprawdź (testuj i przeglądaj system ochrony infrastruktury krytycznej), popraw (doskonal, wprowadzając modyfikacje i korekty).

Kolejne powtórzenia cyklu przybliżają nas do osiągnięcia coraz to większego poziomu ochrony infrastruktury krytycznej. Staje się ona mniej podatna na wszelkiego rodzaju zagrożenia.

Wnioski

Złożoność obowiązujących przepisów prawnych oraz mnogość zadań nałożonych na osoby funkcyjne umocowane z racji swojej odpowiedzialności w systemach zarządzania kryzysowego oraz ochronie infrastruktury krytycznej mogą spowodować, że reakcja całego skomplikowanego systemu na wystąpienie zagrożenia nastąpi z dużym opóźnieniem, powodując często bardzo duże i nieodwracalne zniszczenia. Zbyt długa ścieżka legislacyjna pozwalająca na użycie pododdziałów sił zbrojnych w razie wystąpienia sytuacji kryzysowej o rozmiarach, których opanowanie przekracza możliwości użytych standardowo sił i środków. Właściwy terytorialnie wojewoda wnioskuje o ich użycie do Ministra Obrony Narodowej, co powoduje że tracony jest cenny czas, ponieważ pododdziały (po uzyskaniu formalnej zgody) mogą być kierowane niejednokrotnie z odległych o kilkadziesiąt kilometrów garnizonów. Dobrym rozwiązaniem byłoby umieszczenie w systemie reagowania kryzysowego powstałych i nowopowstających brygad obrony terytorialnej, które są i będą rozlokowane w każdym województwie. W znaczny sposób skróci to czas reakcji wyspecjalizowanych sił i środków na skutki sytuacji kryzysowej.

Bibliografia

1. Piątek Z., *Procedury i przedsięwzięcia systemu reagowania kryzysowego*, Akademia Obrony Narodowej, Warszawa 2006.
2. Sobolewski G., *Metodyka opracowania planu zarządzania kryzysowego*, Akademia Obrony Narodowej, Warszawa 2011.
3. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014.

Akty prawne

1. Ustawa z dnia 2 kwietnia 1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1997 r. Nr 78 poz. 483 z późn. zm.).
2. Ustawa z dnia 21 czerwca 2002 r. ostanie wyjątkowym (Dz.U. z 2017 r. poz. 1928).
3. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. poz. 209 z późn. zm.).
4. Ustawa z dnia 19 listopada 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 1960).
5. Ustawa z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 2281).
6. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. z 2016 r. poz. 904).
7. Ustawa z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 2138).
8. Ustawa z dnia 16 listopada 2016 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2017 r. poz. 1430).
9. Uchwała Rady Ministrów Nr 210/2015 z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej.
10. Uchwała Rady Ministrów Nr 61/2016 z dnia 1 czerwca 2016 r. zmieniająca uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej.
11. Rozporządzenie Rady Ministrów z dnia 15 grudnia 2009 r. w sprawie określenia organów administracji rządowej, które tworzą centra zarządzania kryzysowego (Dz.U. z 2009 r. Nr 226 poz. 1810).
12. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. z 2010 r., Nr 83, poz. 542).
13. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Planu Ochrony Infrastruktury Krytycznej (Dz.U. z 2010 r., Nr 83, poz. 541).
14. Zarządzenie Nr 6/MON Ministra Obrony Narodowej z dnia 17 lutego 2016 r. w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego Ministra Obrony Narodowej (Dz.Urz. MON z 2016 r. poz. 14).
15. Decyzja Nr 245/MON Ministra Obrony z dnia 7 lipca 2010 r. w sprawie utworzenia Centrum Zarządzania Kryzysowego resortu obrony narodowej (Dz.Urz. MON, Nr 14 z 2010 r. poz. 183).
16. Decyzja Nr 14/MON Ministra Obrony Narodowej z dnia 27 stycznia 2014 r. w sprawie podziału odpowiedzialności za realizację zadań zarządzania kryzysowego z zakresu ochrony infrastruktury krytycznej (Dz.Urz. MON z 2014 r. poz. 33).
17. Decyzja Nr 8/14/PI Podsekretarza Stanu w Ministerstwie Obrony Narodowej z dnia 7 lutego 2014 r. w sprawie wskazania realizatorów zadań zarządzania kryzysowego z zakresu ochrony wojskowej infrastruktury krytycznej.

Strony internetowe
1. http://mon.gov.pl/Obrona Terytorialna/Zadania WOT [dostęp: 15.12.2017].

ANALYSIS OF LEGAL CONDITIONS REGARDING THE PARTICIPATION OF THE ARMED FORCES IN THE IMPLEMENTATION OF CRISIS RESPONSE TASKS AND THE PROTECTION OF MILITARY CRITICAL INFRASTRUCTURE

***Keywords*:** *Polish Armed Forces, crisis situations, critical infrastrukture*

SUMMARY

The article presents the analysis of legal conditions regarding the participation of the Armed Forces of the Republic of Poland in the implementation of crisis response tasks, the structure of the crisis management system in the Polish Armed Forces and the protection of military critical infrastructure, including tasks carried out by officers of the Polish Armed Forces, as well as the range of government and local government actions as a part of the National Critical Infrastructure Protection Program.