ZESZYTY NAUKOWE WSOWL

Nr 3 (161) 2011 ISSN 1731-8157

Agata TYBURSKA*

POLICJA A OCHRONA INFRASTRUKTURY KRYTYCZNEJ

„…Postęp ma jedną wadę:
od czasu do czasu eksploduje …"

Elias Canetti [1]

Policja jest instytucją identyfikowaną głównie jako podmiot odpowiedzialny za porządek publiczny i bezpieczeństwo obywateli. Zapewnienie odpowiedniego poziomu bezpieczeństwa w państwie wymaga nowego spojrzenia na rolę podmiotów działających w obszarze bezpieczeństwa, w tym również Policji. Konieczność ta wynika między innymi z nowych, dotychczas niespotykanych zagrożeń, które są wynikiem uzależnienia współczesnego człowieka od zdobyczy naukowo – technicznych. Sprawne funkcjonowanie systemów: energetycznego, paliwowego, transportowego i komunikacyjnego, finansów, ochrony zdrowia, czy też zapewniający ciągłość działania administracji publicznej - daje gwarancję nie tylko łatwiejszego życia ale stanowi również olbrzymie wyzwanie dla podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa w państwie. Nie podejmowanie stosownych działań w zakresie ochrony kluczowych elementów państwa może przerodzić się w niespotykane dotąd zagrożenia dla bezpieczeństwa obywateli i porządku publicznego. Dodatkowe zagrożenia wynikają także z powiązań pomiędzy elementami poszczególnych systemów, z których na co dzień nie zdajemy sobie sprawy. Zapewnienie odpowiedniej ochrony oraz określenie zadań stojących przed podmiotami działającymi w obszarach bezpieczeństwa stanowi wyzwanie nie tylko dla służb i straży ale również dla przedsiębiorców oraz administracji publicznej zaangażowanych w tworzenie przepisów prawa z zakresu ochrony infrastruktury krytycznej czy też wdrażających obowiązuje przepisy, wytyczne i procedury.

Słowa kluczowe: *bezpieczeństwo publiczne, porządek publiczny, zagrożenia bezpieczeństwa państwa, infrastruktura krytyczna, policja*

* dr Agata TYBURSKA – Instytut Służby Prewencyjnej Wydziału Bezpieczeństwa Wewnętrznego i Administracji Wyższej Szkoły Policji w Szczytnie

1 M. Wojdakowska, *Mała Księga Cytatów*, Printex, Białystok 2000.

WSTĘP

Zjawiska zachodzące w świecie na przełomie XX i XXI wieku wskazały na konieczność dokonania zmian w tradycyjnym pojmowaniu bezpieczeństwa państwa i jego obywateli. Dynamiczny rozwój naukowo – techniczny ostatnich lat, globalizacja, rozszerzanie się konsumpcyjnego stylu życia opartego na uzależnieniu współczesnego człowieka od elementów infrastruktury gospodarczej – to jedynie przykłady inicjujące zmiany w tradycyjnym klasyfikowaniu zagrożeń bezpieczeństwa państwa[2]. Piętno przeprowadzonych zamachów terrorystycznych, które przetoczyły się przez Stany Zjednoczone Ameryki oraz kraje Europy i Azji, wywołało zwiększenie obaw przed skutkami ataków szaleńców, jak również sprowokowało burzliwe dyskusje na temat zapewnienia odpowiedniego poziomu bezpieczeństwa i porządku. Racja stanu wskazuje między innymi na konieczność podjęcia szczególnych starań w zakresie ochrony infrastruktury kluczowej państwa. Zniszczenie, uszkodzenie czy awaria niekiedy niewielkiego elementu infrastruktury „wrażliwej" kraju może wywołać tzw. „efekt domina" i spowodować rozprzestrzenianie się skutków zaistniałej sytuacji kryzysowej na znaczne obszary kraju[3]. Skutki kryzysu mogą obejmować nie tylko kwestie finansowe, straty dla gospodarki państwa i biznesu. Nie zawsze zdajemy sobie sprawę, że ograniczenie możliwości dostępu do podstawowych dóbr, czy usług – będące efektem uszkodzenia, zniszczeń lub awarii elementu kluczowego danej infrastruktury może wywołać niezadowolenie i napięcia społeczne, skutkujące naruszeniami porządku publicznego[4] oraz sprzyjające poczuciu zagrożenia[5]. W skrajnych przypadkach zakłócenia prawidłowego funkcjonowania elementów infrastruktury krytycznej może również doprowadzić do utraty zdrowia lub życia dużej liczby osób.

Zagrożenia związane z utratą funkcji elementów kluczowych państwa inicjują rozważania i dyskusje ekspertów zajmujących się teorią bezpieczeństwa państwa. Problem zapewnienia odpowiedniej ochrony elementom kluczowym państwa dostrzegają również elity polityczne. Coraz częściej problem ten dostrzegają sami obywatele, domagając się zapewnienia odpowiedniego poziomu bezpieczeństwa. Oczekiwania obywateli są z reguły efektem lęków społecznych wynikających z aktywności grup terrorystycznych operujących na całym świecie oraz obrazu terroryzmu przedstawianego w środkach masowego przekazu[6].

---

[2] M. Ciecierski, *Nowe trendy w bezpieczeństwie – rozwój prywatnego sektora bezpieczeństwa*, [w:] *Wymiary bezpieczeństwa na progu XXI wieku*, pod red. A. Zaremba, B. Zapały, Adam Marszałek, Toruń 2010, s. 192 – 196, T. Szczurek, *Resort obrony narodowej w zarządzaniu kryzysowym w latach 1989 – 2009*, WAT, Warszawa 2009, s. 20 – 36.

[3] W. Pokruszyński, *Współczesne bezpieczeństwo narodowe*, Wyd. WSGE, Józefów 2009, s. 120 – 121.

[4] Szerzej na ten temat: J. Prońko, B. Wiśniewski, *Klasyfikacja zagrożeń*, [w:] *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, pod red. K. Liedel, J. Prońko, B. Wiśniewski, Wyższa Szkoła Administracji, Bielsko – Biała 2007, s. 14.

[5] W. Pokruszyński, *Uwarunkowania współczesnego bezpieczeństwa międzynarodowego*, WSPol., Szczytno 2006, s. 11 – 13, I. Dziubek, *Proaktywne wykorzystanie inicjatyw lokalnych na rzecz bezpieczeństwa i porządku publicznego w mieście Kaliszu*, [w:] *Bezpieczeństwo publiczne w przestrzeni miejskiej*, pod red. W. Fehler Arte, Biała Podlaska 2010, s. 94.

[6] T. R. Aleksandrowicz, *Medialne aspekty terroryzmu i walki z terroryzmem*, [w:] *Terroryzm w medialnym obrazie świata*, pod red. K. Riedel, St. Mocka Wydawnictwo TRIO, Warszawa 2010, s. 13 – 21.

Jednym z priorytetowych zadań administracji rządowej jest zagwarantowanie społeczeństwu odpowiedniego poziomu bezpieczeństwa[7]. Istotne zadania w zakresie zapewnienia bezpieczeństwa i porządku publicznego ma do spełnienia również administracja samorządowa[8]. Dlatego też projekty zmierzające do faktycznego podniesienia bezpieczeństwa inicjowane są najczęściej przez stronę rządową, angażując jednocześnie w swoje działania samorządy lokalne, służby, straże i inspekcje, przedsiębiorców oraz samych obywateli.

Powstałe rozwiązania dotyczące ochrony elementów kluczowych państwa są najczęściej efektem dotychczasowych doświadczeń, tzw. dobrych praktyk oraz wniosków wynikających z sytuacji kryzysowych, zaistniałych w innych państwach. Wiele rozwiązań dotyczących interpretacji pojęcia infrastruktury krytycznej oraz przedsięwzięć prowadzonych w zakresie organizacji skutecznej ochrony elementów kluczowych państwa zaczerpnięto z doświadczeń Stanów Zjednoczonych Ameryki po tragedii 11 września 2001 roku, a także wymagań stawianych przez Unię Europejską.

1. AKTY PRAWNE DOTYCZĄCE OCHRONY INFRASTRUKTURY KRYTYCZNEJ – POLSKA A DOŚWIADCZENIA AMERYKAŃSKIE I PROPONOWANE KIERUNKI DZIAŁAŃ W UNII EUROPEJSKIEJ

Jedne z cenniejszych doświadczeń dotyczących ochrony infrastruktury krytycznej zebrali Amerykanie. Chociaż prace poświęcone wyodrębnianiu i ochronie elementów krytycznych państwa zostały zintensyfikowane po zamachach 11 września 2001 roku, tym niemniej działania skierowane na poszukiwanie odpowiedniej metodologii, umożliwiającej wyodrębnienie elementów kluczowych państwa prowadzone były już w latach wcześniejszych[9]. Od tamtego czasu definiowanie pojęcia infrastruktury krytycznej oraz jej wyodrębnianie - wielokrotnie ewoluowało.

Jedno z istotnych unormowań pojawiło się 15 lipca 1996 roku. Było to zarządzenie 13010 prezydenta Billa Clintona, które oprócz powołania Prezydenckiej Komisji do Spraw Ochrony Infrastruktury Krytycznej (PCCIP), definiowało również samo pojęcie infrastruktury krytycznej państwa, określając ją jako *strukturę współzależnych sieci i systemów obejmującą, możliwe do zidentyfikowania gałęzie przemysłu, instytucje (obejmując ludzi i procedury) oraz zdolności dystrybucyjne, które zapewniają przepływ produktów i usług istotnych dla obrony i ekonomicznego bezpieczeństwa Stanów Zjednoczonych, sprawnego funkcjonowania administracji rządowej na wszystkich szczeblach oraz całego społeczeństwa*[10].

Zarządzenie to zwracało uwagę na fakt, iż kwalifikując elementy państwa jako krytyczne, należy uwzględniać wpływ zniszczenia, uszkodzenia (destrukcji) na obronność i bezpieczeństwo ekonomiczne państwa.

---

[7] R. Jakubczak, J. Flis, *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa 2006, s. 172 – 178.

[8] W. Kitler, *Samorząd terytorialny w obronie narodowej Rzeczpospolitej Polskiej,* AON, Warszawa 2005, s. 215 – 221.

[9] R. Radvanovsky, A. McDougall, *Critical Infrastructure. Homeland Security and Emergency Preparedness,* CRC Press, London, New York 2010, s. 289.

[10] *CRS Report for Kongres,* October 1, 2004, s. 5.

Z kolei wydana 22 maja 1998 roku Prezydencka Dyrektywa nr 63 (PDD-63), będąca już efektem pracy Prezydenckiej Komisji do spraw Ochrony Infrastruktury Krytycznej, wzbogaciła opracowany wcześniej katalog elementów krytycznych państwa (obejmujący telekomunikację, transport, system energii elektrycznej, magazynowanie oraz transport gazu i ropy naftowej, bankowość, system zaopatrzenia w wodę), zapewniający ciągłość działania rządu o nowy jej wymiar, jakim stała się cyberprzestrzeń[11]. Dyrektywa ta wskazała także główne federalne organy (agencje), które miały podjąć wysiłek w identyfikowaniu elementów krytycznych państwa oraz włączyć w prace nad ochroną infrastruktury krytycznej podmioty sektora prywatnego. Wskazała także na konieczność opracowania Krajowego Planu Infrastruktury Krytycznej[12].

Ataki dokonane przez zamachowców na wieże World Trade Center 11 września 2001 roku stały się przyczynkiem do opracowania i wydania nowego zarządzenia. Podpisane w październiku 2001 roku przez prezydenta Busha zarządzenie 13228 ustanowiło Biuro Ochrony Kraju oraz Radę Bezpieczeństwa Narodowego. Jednym z głównych celów powołanych do życia podmiotów była koordynacja działań mających na celu podniesienie poziomu ochrony[13]:

- elementów związanych z produkcją energii, jej transmisji, usług dystrybucyjnych i urządzeń technicznych;
- ważnych obiektów użyteczności publicznej;
- telekomunikacji;
- urządzeń produkujących, zużywających, magazynujących lub dysponujących materiałami nuklearnymi;
- publicznych lub prywatnych systemów informacyjnych;
- miejsc tzw. specjalnych wydarzeń gromadzących znaczną liczbę ludzi;
- transportu (łącznie z liniami kolejowymi, autostradami, portami oraz drogami wodnymi);
- lotnisk oraz lotnictwa cywilnego;
- żywca (inwentarza żywego), strategicznych obszarów obejmujących rolnictwo, systemy zaopatrujące w wodę i żywność.

Należy podkreślić, iż za prezydentury Georga W. Busha powstało najwięcej istotnych unormowań prawnych (Dyrektywy Prezydenckie – HSPD) mających na celu podniesienie poziomu ochrony zarówno infrastruktury kluczowej państwa, jak i samych obywateli[14]. Od października 2001 do stycznia 2009 roku powstało w sumie około 27 aktów prawnych[15]. Wśród nich niezwykle cennym z punktu widzenia organizacji

[11] *CRS Raport for …*, op. cit. s. 6.

[12] *CRS Raport for …*, op. cit. s. 7.

[13] *Raport for …*, op. cit. s. 8.

[14] Szerzej na ten temat: A. Tyburska, *Ochrona infrastruktury krytycznej a zapewnienie bezpieczeństwa i porządku publicznego*, [w:] A. Gałecki, M. Dalecka, T. Tabaczniuk, *Współczesne problemy bezpieczeństwa*, Oficyna Wydawnicza Uniwersytetu Zielonogórskiego, Zielona Góra 2010, s. 192 – 196.

[15] R. Radvanovsky, A. McDougall, *Critical Infrastructure. Homeland Security and Emergency Preparedness*, CRC Press, London, New York 2010, s, 289 – 293.

ochrony elementów kluczowych państwa była Prezydencka Dyrektywa nr 7 (HSPD-7), która weszła w życie 17 grudnia 2003 roku, a dotyczyła identyfikacji, priorytetów oraz ochrony infrastruktury krytycznej państwa. Dyrektywa ta podkreśla konieczność współpracy administracji rządowej z jednostkami sektora prywatnego, podaje również kierunek wyznaczania krajowej infrastruktury krytycznej.

Wyodrębnianie elementów infrastruktury krytycznej, tworzenie priorytetów w zakresie organizacji ich ochrony wymusiło konieczność opracowania metodyki identyfikowania i szacowania majątku kluczowego, a także identyfikowania zależności składników majątku z innymi systemami. Jednocześnie założono, że składniki majątku, funkcje, czy systemy działające w obrębie każdego sektora infrastruktury nie są w tym samym stopniu istotne. Należało zatem przyjąć odpowiednie priorytety dla wyznaczania i ochrony infrastruktury krytycznej. Ważnym stało się, aby przy wyznaczaniu infrastruktury krytycznej, brać pod uwagę takie elementy, jak funkcja czasu, ryzyka i zmian rynku.

Uwzględnienie tych funkcji wymaga jednocześnie systematycznego przeglądu opracowanych wcześniej wykazów oraz wprowadzania w nich niezbędnych aktualizacji. Jednocześnie, zgodnie z Prezydencką Dyrektywą Bezpieczeństwa (HSPD-7), szczególną ochroną należy otoczyć te elementy infrastruktury krytycznej, czy kluczowe środki, których zniszczenie, uszkodzenie lub awaria mogłyby wywołać katastrofalne skutki zdrowotne i masowe straty w ludziach porównywalne do tych po użyciu broni masowego rażenia. Przepisy dotyczące wyodrębniania i ochrony infrastruktury krytycznej obowiązujące w Stanach Zjednoczonych jako priorytetowe wskazują obszary obejmujące zdrowie i bezpieczeństwo obywateli.

Amerykańscy eksperci zwrócili również uwagę na trudności w opracowaniu uniwersalnej metodologii służącej do wyznaczania infrastruktury krytyczne w państwie[16]. Jednocześnie należy zadawać sobie sprawę z faktu, że niejasne i nieprecyzyjne kryteria wyznaczania infrastruktury krytycznej państwa (kluczowych środków) mogą wywołać błędne decyzje w zakresie przygotowywanej i prowadzonej polityki bezpieczeństwa. Strona rządowa w Stanach Zjednoczonych odpowiedzialna jest między innymi za tworzenie bazy infrastruktury krytycznej państwa, określanie słabych punktów, przeprowadzanie analizy zagrożeń, monitorowanie incydentów zaistniałych w wyznaczonych obszarach. Federalny rząd może także partycypować w kosztach ochrony elementów infrastruktury krytycznej nie tylko dla infrastruktury posiadanej i działającej na poziomie stanowym, czy lokalnym, ale również wspierać w tym zakresie prywatny sektor[17].

Również w Unii Europejskiej przywiązuje się szczególną wagę do właściwego zabezpieczenia zarówno krajowej, jak również europejskiej infrastruktury krytycznej. Przyjęta przez Radę Unii Europejskiej definicja pojęcia infrastruktura krytyczna oznacza *„zasoby rzeczowe, usługi, urządzenia informatyczne, sieci i aktywa infrastrukturalne, których zakłócenie lub zniszczenie miałoby znaczący wpływ na najważniejsze funkcje społeczne, w tym łańcuch dostaw, zdrowie, bezpieczeństwo,*

[16] *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, February, 2003, s. 33 – 34.

[17] *CRS Report for Kongres*, October 1, 2004, s. 16.

ochronę, pomyślność gospodarczą lub społeczną obywateli lub funkcjonowanie Wspólnoty lub należących do niej państw członkowskich"[18].

Europejska Strategia Bezpieczeństwa, określając rodzaje współczesnych zagrożeń, wskazuje na konieczność opracowania i przyjęcia odpowiedniego systemu pozwalającego nie tylko na właściwy, szybki obieg informacji oraz koordynację działań pomiędzy państwami w zakresie ochrony najważniejszych obiektów (obszarów) *„infrastruktury krytycznej*", ale także ujednolicenia pojęć związanych z tym obszarem bezpieczeństwa państw członkowskich[19].

W czerwcu 2004 roku Rada Europejska zainicjowała przyjęcie przez Komisję Komunikatu *„Ochrona infrastruktury krytycznej w walce z terroryzmem*"[20]. W komunikacie tym przedstawiono wnioski dotyczące unowocześnienia europejskich systemów zapobiegania zamachom terrorystycznym ukierunkowanym na obiekty, obszary i urządzenia stanowiące infrastrukturę krytyczną państw członkowskich.

W grudniu 2005 roku Rada do spraw Wymiaru Sprawiedliwości i Spraw Wewnętrznych wskazała Komisji Europejskiej na konieczność przygotowania *Europejskiego Programu Ochrony Infrastruktury Krytycznej* (EPOIK), uwzględniającego interdyscyplinarne podejście do zagrożeń *infrastruktury krytycznej* ze szczególnym uwzględnieniem niebezpieczeństw wynikających z terroryzmu.

Europejski Program Ochrony Infrastruktury Krytycznej oparty został na sześciu podstawowych zasadach:

- pomocniczości;
- komplementarności;
- poufności;
- współpracy zainteresowanych stron;
- proporcjonalności;
- indywidualnego traktowania sektorów.

Uważa się również, że *Program* ten powinien uwzględniać wnioski z analizy indywidualnych potrzeb, wynikających ze specyfiki sektorów zaklasyfikowanych jako *„wrażliwe"*. Stąd też wyprowadzona została zasada indywidualnego traktowania poszczególnych sektorów stanowiących infrastrukturę krytyczną państw członkowskich.

---

[18] Art. 2 Decyzji Rady Unii Europejskiej z dnia 12 lutego 2007 roku ustanawiającej na lata 2007 – 2013 jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa", Dz.U.UE.L.07.58.1

[19] Dnia 12 grudnia 2003 roku, Rada Europejska przyjęła Europejska Strategię Bezpieczeństwa, Rezolucja Parlamentu Europejskiego w sprawie Europejskiej Strategii Bezpieczeństwa (2004/2167(INI)), pkt. 52, [online] [dostęp: 11.03.2008]. Dostępny w Internecie: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2005-0133+0+DOC+XML+V0//PL, Szerzej na ten temat: R. Zięba, *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej*, Wyd. akademickie i Profesjonalne, Warszawa 2007, s. 89 – 93.

[20] *Zielona Księga w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej*, Komisja Wspólnot Europejskich, pkt. 1, s. 2, [online] [dostęp: 11.03.2008]. Dostępny w Internecie: http://eur-ex.europa.eu/LexUriServ/site/pl/com/2005/com2005_0576pl01.pdf

Można zatem przyjąć, że celem podjęcia zintegrowanych działań wszystkich państw Unii Europejskiej w zakresie ochrony *infrastruktury krytycznej* stało się takie jej zaprojektowanie, aby wszelkiego rodzaju zakłócenia, ograniczenia i trudności w prawidłowym funkcjonowaniu elementów infrastruktury były krótkotrwałe, rzadkie, a ich usuniecie nieskomplikowane. Nie bez znaczenia jest także konieczność odpowiedniego geograficznego odizolowania miejsc, w których nastąpiło uszkodzenie (awaria) któregoś z elementów *infrastruktury krytycznej* dla zminimalizowania strat poniesionych przez państwa członkowskie oraz w trosce o życie i zdrowie obywateli.

Opracowanie koncepcji Europejskiego Programu Ochrony Infrastruktury Krytycznej poprzedzone zostało (listopad 2005 rok) przygotowaną przez Komisję *Zieloną Księgą w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej*, który to dokument wskazywał na konieczność opracowania, a następnie wdrożenia jednolitych standardów odnoszących się do sposobów opracowania i realizacji przyjętych koncepcji ochrony. Jednocześnie w dokumentach Unii Europejskiej podkreślane jest, że poprawa ochrony *infrastruktury krytycznej* w Europie może nastąpić poprzez wypracowanie wspólnych (obowiązujących wszystkie państwa UE), „ram regulacyjnych" dla poszczególnych krajów członkowskich[21]. Wspólne ramy odnoszące się do ochrony infrastruktury „wrażliwej", uwzględniałyby jednolite kryteria klasyfikowania (definiowania) obiektów, obszarów, czy urządzeń uznawanych za *krytyczne* w oparciu o *„wrażliwe"* sektory bezpieczeństwa państwa. Do najbardziej *„wrażliwych"* działów wymagających odpowiedniego poziomu ochrony ze strony państw członkowskich przyjmuje się sektory: energetyczny, informacyjno – komunikacyjny, finansowy, transportowy, przesyłowy, chemiczny i nuklearny, zaopatrywania w wodę, żywność, powiązane z przestrzenią kosmiczną i badaniami, bezpieczeństwa i porządku, administracji państwa, sił zbrojnych oraz ratownictwa medycznego[22].

Przyjęte w tym obszarze standardy Unii Europejskiej dotyczyłyby procedur określania i klasyfikowania obiektów, obszarów, urządzeń jako *krytycznych* z punktu widzenia transgranicznych skutków wywołanych ich niesprawnością. Do zadań państw członkowskich należałoby także wypracowanie jednolitych zasad obowiązujących przy ocenie potrzeb odnoszących się do podniesienia poziomu ochrony danego obiektu, obszaru lub urządzenia wytypowanego jako *krytyczny* z punktu widzenia bezpieczeństwa Wspólnoty.

Uwieńczeniem prac koncepcyjnych i przedsięwzięć realizowanych przez Radę Unii Europejskiej stała się wydana w grudniu 2008 roku Dyrektywa *w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej poprawy*[23]. W Dyrektywie tej znalazły się podstawowe definicje odnoszące się do wyznaczania tzw. *infrastruktur krytycznych*. Stąd też definicja infrastruktury krytycznej przyjęta przez Radę Europy w grudniu 2008 roku wskazuje, że

---

[21] Komunikat Komisji Wspólnot Europejskich w sprawie Europejskiego Programu Ochrony Infrastruktury krytycznej, Bruksela, dn. 12.12.2006 roku, [online] [dostęp: 15.02.2008]. Dostępny w Internecie: http://eur-lex.europa.eu/LexUriServ.do.

[22] Opracowano na podstawie: *Indicative List Of Critical Infrastructure Sectors, Zielona Księga*, op. cit. s. 26.

[23] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej poprawy, Dz.U.UE.L z dnia 23 grudnia 2008 roku.

należy przez nią rozumieć *składnik, system lub część infrastruktury zlokalizowanej na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji*[24]. Jednocześnie określono Europejską Infrastrukturę Krytyczną przyjmując, że jest to *infrastruktura krytyczna zlokalizowana na terytorium państw członkowskich, a jej zniszczenie lub zakłócenie w istotny sposób wpływałoby na co najmniej dwa państwa członkowskie*[25]. O znaczeniu tego oddziaływania decydowałyby tzw. kryteria przekrojowe, kryteria sektorowe oraz skutki wynikające z międzysektorowych współzależności z pozostałymi rodzajami infrastruktury. Jako kryteria przekrojowe przyjmowane są[26]:

- kryteria ofiar w ludziach rozumiane jako ewentualną liczbę ofiar śmiertelnych oraz rannych;
- kryterium skutków ekonomicznych odnoszone do wielkości poniesionych strat ekonomicznych, pogorszenia jakości towarów bądź usług czy też spodziewanych skutków zagrożenia środowiska;
- kryterium skutków społecznych wskazujące na poniesione cierpienia fizyczne, zakłócenia w funkcjonowaniu w życiu codziennym, brak możliwości zapewnienia podstawowych usług, a także oddziaływanie na opinię publiczną.

Na kryteria przekrojowe powinny zostać nałożone kryteria sektorowe odnoszące się do charakterystycznych cech poszczególnych sektorów Europejskiej Infrastruktury Krytycznej, zgodnie z przyjętym założeniem sektorowego podejścia do klasyfikowania elementów infrastruktury krytycznej. W unormowaniach Unii Europejskiej za podstawowe sektory ukierunkowujące wyznaczanie infrastruktur krytycznych uznano[27]:

- sektor energetyczny (energia elektryczna, ropa naftowa, gaz),
- sektor transportowy (transport drogowy, kolejowy, lotniczy, wodny śródlądowy, żegluga oceaniczna, żegluga morska bliskiego zasięgu, porty).

Zgodnie z zaleceniami Unii Europejskiej procedura typowania infrastruktury krytycznej powinna przebiegać w trzech etapach:

- I etap – rozpoznawanie kluczowych elementów infrastruktury państwa;
- II etap – przeprowadzenie analizy ryzyka (analiza słabych punktów elementów kluczowych, potencjalnych skutków zniszczenia, uszkodzenia bądź awarii);
- III etap – rozpoznanie, selekcję i ustalenie hierarchii ważności środków przeciwdziałania negatywnym skutkom oraz procedur, które powinny uwzględniać stałe środki bezpieczeństwa oraz zróżnicowane (podejmowane w zależności od aktualnego poziomu ryzyka czy rodzaju zagrożenia).

---

[24] Art.2 pkt.a) Dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 roku ..., op. cit.

[25] Art. 2, pkt. b) Dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 roku..., op. cit.

[26] Art. 3, ust. 2, pkt. a), b), c) Rady 2008/114/WE z dnia 8 grudnia 2008 roku

[27] Załącznik Nr 1, Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 roku..., op. cit.

W Polsce unormowania prawne dotyczące ochrony infrastruktury krytycznej są zarówno oparte na doświadczeniach Stanów Zjednoczonych, jak również dostosowane do wymagań Unii Europejskiej, która zobowiązała państwa członkowskie, aby proces rozpoznawania i wyznaczania Europejskiej Infrastruktury Krytycznej został zakończony przez wszystkie kraje członkowskie do 12 stycznia 2011 roku. Po tym terminie będą prowadzone regularne przeglądy tych elementów kluczowych państwa, które zostały wskazane jako krytyczne, również z punktu widzenia bezpieczeństwa wspólnotowego.

Ustawa o zarządzaniu kryzysowym jako infrastrukturę krytyczną wymienia[28] systemy, które odpowiadają za zaopatrzenie w energię i paliwa, łączność i sieć teleinformatyczną, finanse, zaopatrzenie w wodę i żywność, ochronę zdrowia, transport i komunikację, ratownictwo, zapewnienie ciągłości działania administracji publicznej, produkcję, składowanie, przechowywanie i stosowanie substancji chemicznych oraz promieniotwórczych (m.in. rurociągi przesyłowe substancji niebezpiecznych). Oczywiście ustawa wskazuje jedynie obszary wyznaczania konkretnych obiektów stanowiących infrastrukturę krytyczną państwa[29].

Istotnym problemem, na który zwraca uwagę ustawa to odpowiednia ochrona *infrastruktury krytycznej* przed atakami, awariami, czy też innymi zdarzeniami (w tym również zamachami, nieprzewidywalnymi działaniami sił natury, katastrofami itp.), które w jakikolwiek sposób mogłyby zakłócić jej prawidłowe funkcjonowanie. Stąd też mówiąc o ochronie *infrastruktury krytycznej*, należy uwzględniać działania ukierunkowane na zagwarantowanie funkcjonalności, ciągłości działań, integralności danej infrastruktury, a wszystko to w celu zapobieżenia różnego rodzaju zagrożeniom, ryzykom oraz słabym punktom charakterystycznym dla danego systemu, obiektu lub urządzenia[30]. Ważnym zadaniem związanym z ochroną istotnej infrastruktury jest również ograniczenie i neutralizacja skutków zniszczenia, awarii elementu (podmiotu), tworzącego dany system krytyczny oraz szybkie jego odtworzenie, tak aby zaistniały incydent nie wpłynął negatywnie na stan bezpieczeństwa obywateli.

Należy jednocześnie pamiętać, że ochrona infrastruktury krytycznej powinna mieć charakter kompleksowy, co oznacza uwzględnienie w organizacji ochrony następujących obszarów: ochrony fizycznej, ochrony technicznej, ochrony osobowej, ochrony teleinformatycznej, ochrony prawnej oraz pomoc w trakcie odbudowy ze strony rządowej[31]. Za podstawowy cel przygotowania *Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK)* przyjęto podniesienie poziomu zabezpieczenia systemów, obiektów i urządzeń stanowiących potencjał bezpieczeństwa naszego państwa. W osiągnięciu tego celu niezbędne jest zapewnienie optymalnych warunków do poprawy zabezpieczenia krajowej infrastruktury krytycznej.

Ustawodawca dodatkowo określił elementy *Narodowego Programu Ochrony Infrastruktury Krytycznej*, na które składają się nie tylko narodowe priorytety, cele, wymagania i standardy gwarantujące właściwe funkcjonowanie infrastruktury

---

[28] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. nr 89, poz. 590 z późn. zm.

[29] W. Skomra, *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, PRESSCOM Sp. z o.o., Wrocław 2010, s. 92.

[30] Ibidem, s. 93.

[31] M. Pyznar, *Narodowy Program Ochrony Infrastruktury Krytycznej*, za: W. Skora, *Zarządzanie kryzysowe*, op. cit., s. 95.

krytycznej, ale również szczegółowe kryteria umożliwiające wyznaczenie obiektów, instalacji, urządzeń i usług będących częścią składową odpowiednich systemów *infrastruktury krytycznej*.

Opracowane i przyjęte kryteria mają na celu wyznaczenie tych elementów infrastruktury krytycznej kraju, które zapewniają właściwe funkcjonowanie państwa oraz zaspokojenie podstawowych potrzeb społeczeństwa. Przyjęte kryteria opatrzone zostały klauzulą niejawności – co spowoduje, że podmioty wskazane jako infrastruktura krytyczna państwa dowiedzą się o tym fakcie dopiero po uzyskaniu informacji od uprawnionych w tym zakresie organów.

W opracowanym *Programie* wskazani zostaną także ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych, którzy ponoszą odpowiedzialność za systemy wytypowane jako elementy infrastruktury krytycznej państwa.

Z uwagi na znaczną „wrażliwość" informacji zawartych w *Narodowym Programie Ochrony Infrastruktury Krytycznej*, zakłada się przyjęcie stosownej klauzuli, gwarantującej ochronę zawartych w nim szczegółów.

Należy jednocześnie podkreślić, że ministrowie kierujących działami administracji rządowej oraz kierownicy urzędów centralnych mają możliwość opiniowania wykazu obiektów, instalacji i urządzeń wchodzących skład narodowej infrastruktury krytycznej, przygotowanego przez Dyrektora Rządowego Centrum Bezpieczeństwa[32].

Kolejnym zadaniem przypisanym Dyrektorowi RCB jest przygotowanie wyciągów z wykazu krajowej infrastruktury krytycznej i ich przekazanie: odpowiednio poszczególnym ministrom i kierownikom urzędów centralnych odpowiedzialnych za dany system oraz wojewodom posiadającym elementy infrastruktury krytycznej na terenie swoich województw. Istotnym obowiązkiem Dyrektora RCB jest także powiadomienie właścicieli, posiadaczy samoistnych i zależnych o umieszczeniu elementu, urządzenia lub obiektu, którym zarządzają w wykazie infrastruktury krytycznej państwa.

Z uwagi na konieczność uwzględniania problematyki ochrony infrastruktury krytycznej w wojewódzkich planach zarządzania kryzysowego, przyjmuje się możliwość przekazywania przez wojewodę niezbędnych informacji innym organom administracji publicznej, których zadania przewidują również działania na rzecz ochrony infrastruktury krytycznej danego województwa.

Za odpowiednią ochronę obiektów, instalacji, czy urządzeń infrastruktury krytycznej odpowiedzialni są właściciele oraz posiadacze samoistni i zależni tych elementów infrastruktury krytycznej. Do nich również należy obowiązek opracowania planów ochrony posiadanej infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie elementu infrastruktury krytycznej, aż do czasu jej odtworzenia. Obowiązkiem właścicieli (posiadaczy samoistnych i zależnych) jest także wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami, które wskazano jako

[32] Art. 12 ust. 2 c, pkt.3) Ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym, op. cit.

właściwe w zakresie ochrony infrastruktury krytycznej. Na spełnienie tego obowiązku ustawodawcza wyznaczył termin 30 dni od dnia otrzymania informacji o umieszczeniu danego obiektu, instalacji bądź urządzenia w wykazie infrastruktury krytycznej.

W znowelizowanej ustawie przyjmuje się, że opracowane (na podstawie innych przepisów) plany ochrony obiektów, instalacji, urządzeń, które znalazły się w wykazie infrastruktury krytycznej mogą być zaakceptowane pod warunkiem, iż odpowiadają przyjętym wymogom planu ochrony infrastruktury krytycznej[33]. Jednocześnie ustawodawca zaznacza, że sposób tworzenia, aktualizacji, a także strukturę opracowywanych planów ochrony infrastruktury krytycznej określi Rada Ministrów w stosownym rozporządzeniu.

Znowelizowana *ustawa o zarządzaniu kryzysowym* formułuje również zadania z zakresu ochrony infrastruktury krytycznej, do których należy[34]:

- gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
- opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
- odtwarzanie infrastruktury krytycznej;
- współpraca pomiędzy administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.

Warto jednocześnie podkreślić, że problematyka *infrastruktury krytycznej* państwa znajduje swoje odzwierciedlenie w opracowywanych planach zarządzania kryzysowego przygotowywanych zarówno na poziomie centralnym (Krajowy Plan Zarządzania Kryzysowego), jak również regionalnym (wojewódzkie palny zarządzania kryzysowego) i lokalnym (powiatowe czy gminne plany zarządzania kryzysowego).

W planie zarządzania kryzysowego – bez względu na jego poziom (zasięg) – umieszcza się charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia również w aspekcie infrastruktury krytycznej znajdującej się na danym obszarze. Jest w nim także wykaz obiektów, instalacji urządzeń infrastruktury krytycznej znajdujących się odpowiednio (w zależności od planu) na terenie danego województwa, powiatu czy gminy. Jako załączniki funkcjonalne planu głównego zamieszane powinny być również procedury realizacji zadań z zakresu zarządzania kryzysowego, w tym odnoszące się do chronionej infrastruktury krytycznej oraz wykazy infrastruktury krytycznej, znajdującej się - w zależności od poziomu planu – na terenie danego województwa, powiatu bądź gminy[35]. Załącznikami do planu są także informacje dotyczące priorytetów w zakresie ochrony i odtwarzania infrastruktury krytycznej.

Starania odnoszące się do właściwej ochrony *infrastruktury krytycznej* powinny obowiązywać na każdym poziomie organizacji bezpieczeństwa państwa. Stąd też plany zarządzania kryzysowego, opracowywane przez poszczególnych ministrów, obejmują

[33] Art. 6 ust. 6 Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, op. cit.

[34] Art. 6 ust.1 pkt. 1 – 5 Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, op. cit.

[35] Art. 5 ust.2 pkt. 1a, pkt. 3a oraz 3 k Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, op. cit.

analizę zagrożeń i ocenę możliwości ich wystąpienia uwzględniającą również problematykę infrastruktury krytycznej w zakresie ich odpowiedzialności za przypisane systemy. Zakłada się również, że sporządzane plany powinny zawierać szczegółowe informacje na temat sposobów i reakcji podejmowanych na powstałe zagrożenia (w tym także infrastruktury krytycznej) wraz ze wskazaniem przedsięwzięć zmierzających do likwidacji powstałych skutków. W planach powinny znaleźć się również zapisy dotyczące zasad realizacji zadań z zakresu ochrony infrastruktury krytycznej[36]. Plany zarządzania kryzysowego przygotowane przez poszczególnych ministrów są uzgadniane z Dyrektorem RCB i są włączane w formie załączników do Krajowego Planu Zarządzania Kryzysowego[37].

Z uwagi na znaczenie ochrony infrastruktury krytycznej w Polsce dla bezpieczeństwa europejskiego i analogicznie odpowiedniego zabezpieczenia tego typu obiektów (urządzeń) przez inne państwa, niezbędnym jest prowadzenie ścisłej współpracy międzynarodowej w tym obszarze z instytucjami Unii Europejskiej, krajami członkowskimi oraz Organizacjami Paktu Północnoatlantyckiego. Rządowe Centrum Bezpieczeństwa stanowi w tym przypadku punkt kontaktowy do wymiany informacji, przygotowywania wspólnych szkoleń, projektów itp. pomiędzy instytucjami Unii Europejskiej, Paktu Północnoatlantyckiego i organizacjami międzynarodowymi[38].

Zadania związane z ochroną infrastruktury krytycznej ciążące na właścicielach, zarządzających tego typu obiektami, instalacjami nie dotyczą jedynie przygotowania planu ochrony oraz zagwarantowania jej odpowiedniego poziomu. Do zadań, które na nich spoczywają należy także niezwłoczne przekazywanie Szefowi Agencji Bezpieczeństwa Wewnętrznego wszelkiego rodzaju informacji dotyczących zagrożeń terrorystycznych skierowanych na infrastrukturę krytyczną państwa. Informacje te są szczególnie ważne, gdy zagrożone są systemy i sieci energetyczne, wodnokanalizacyjne, ciepłownicze lub teleinformatyczne, a skutki przeprowadzonych zamachów mogą być niebezpieczne dla życia, zdrowia ludzi, mienia w znacznych rozmiarach, środowiska lub obiektów stanowiących dziedzictwo narodowe[39]. Obowiązek ten ciąży także na organach administracji publicznej.

W przypadku wpłynięcia tego typu informacji – Szef Agencji Bezpieczeństwa Wewnętrznego – w celu zapobieżenia sytuacji kryzysowej będącej następstwem zamachu terrorystycznego - ma prawo do udzielania stosowanych zaleceń zarówno właściwym organom administracji publicznej, jak również zagrożonym zamachami podmiotom[40].

2. ZADANIA POLICJI A PROBLEMATYKA OCHRONY INFRASTRUKTURY KRYTYCZNEJ

Szczególną misję w obszarze bezpieczeństwa państwa ma do wypełnienia Policja, będąca umundurowaną i uzbrojoną formacją odpowiedzialną za ochronę bezpieczeństwa

[36] Art. 12 ust. 2, pkt. 1), 2) i 4) Ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym, op. cit.

[37] Art. 12 ust. 2a Ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym, op. cit.

[38] Art. 11 ust. 2 pkt. 6) oraz 11) Ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym, op. cit. Wskazana współpraca dotyczy również współdziałania w zakresie zarządzania kryzysowego.

[39] Art. 12 a ust. 2 Ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym, op. cit.

[40] Art. 12 a, ust.3 Ustawy z dnia 26 kwietnia o zarządzaniu kryzysowym, op. cit.

ludzi oraz utrzymanie bezpieczeństwa i porządku w państwie[41]. Istota działania Policji opiera się na założeniu uwzględniającym podmiotową rolę społeczeństwa w kształtowaniu bezpieczeństwa w państwie.

W ramach zadań wykonywanych przez Policję[42] wymieniana jest ochrona życia, zdrowia oraz mienia przed bezprawnymi zamachami, a także ochrona bezpieczeństwa i porządku publicznego, ze szczególnym uwzględnieniem miejsc publicznych, w tym środków transportu publicznego i komunikacji publicznej.

Duża liczba ofiar śmiertelnych oraz rannych w wypadkach drogowych zaistniałych na terenie Polski wpłynęła na wskazanie obszaru bezpieczeństwa i porządku publicznego w ruchu drogowym jako jednego z priorytetowych zadań Policji. Ograniczenie liczby wypadków śmiertelnych jest jednym z wymagań Unii Europejskiej stawianych Polsce na najbliższe lata.

Poczucie bezpieczeństwa społeczności lokalnych w znacznej mierze zależy od działalności profilaktycznej prowadzonej na danym terenie. Doświadczenia zebrane w tym obszarze przez funkcjonariuszy Policji zdecydowanie potwierdzają tezę, że łatwiej i taniej jest zapobiegać niepożądanym zjawiskom aniżeli walczyć z konsekwencjami jakie ze sobą niosą. Z tego też względu policjanci uczestniczą w wielu przedsięwzięciach profilaktycznych, których celem jest eliminowanie (ograniczanie) zjawisk patologicznych, sprzyjających łamaniu norm prawnych. Jednym z zadań stawianych funkcjonariuszom Policji jest zatem inicjowanie i organizowanie działań ukierunkowanych na zapobieganie popełnianiu przestępstw i wykroczeń oraz innym zjawiskom kryminogennym. Wypełniając tak sformułowane zadanie, policjanci mają obowiązek współpracować z organami państwowymi, samorządowymi oraz organizacjami społecznymi. Wzbogacanie wiedzy, doskonalenie umiejętności w obszarze profilaktyki możliwe jest dzięki stałej współpracy polskiej Policji z policjami innych państw europejskich, angażowaniu się w projekty unijne ukierunkowane na działania zapobiegawcze, a także wizytom studyjnym i wymianie funkcjonariuszy zajmujących się problematyką nieletnich, zjawiskiem przemocy w rodzinie, budowaniem programów profilaktycznych, czy współpracą z samorządami i organizacjami pozarządowymi.

Jedną z najbardziej efektywnych, a jednocześnie oczekiwanych i akceptowanych społecznie form działań zapobiegawczych prowadzonych przez Policję jest wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców. W realizacji tego zadania Policja wspierana jest coraz częściej przez najnowsze osiągnięcia techniki, informatyki, inżynierii genetycznej itp. Doświadczenie uczy, że szybkie ujawnienie, ujęcie i ukaranie sprawcy czynu niezgodnego z prawem stanowi jedną z najlepszych metod zapobiegania. Świadomość wykrycia sprawcy, nieuchronność i dolegliwość kary stają się czytelnym sygnałem dla potencjalnych sprawców przestępstw i wykroczeń.

Policja zobowiązana jest również do kontroli przestrzegania przepisów porządkowych i administracyjnych dotyczących działalności publicznej, czy też obowiązujących w miejscach publicznych.

---

[41] Porównaj: A. Tyburska, *Kierowanie w Policji – wybrane zagadnienia w aspekcie bezpieczeństwa narodowego*, [w:] *Kierowanie bezpieczeństwem narodowym*, B. Zdrodowski, B. Wiśniewski AON, Warszawa 2008, s. 163 – 174.

[42] Ustawa z dnia 6 kwietnia 1990 roku o Policji, art.1, ust. 2, op. cit.

W trosce o utrzymanie wysokiego poziomu usług i przestrzegania norm prawa, Policja zobowiązana jest także do prowadzenia nadzoru nad strażami miejskimi i gminnymi oraz specjalistycznymi uzbrojonymi formacjami ochronnymi, które to - w głównej mierze - zajmują się ochroną obszarów, obiektów, urządzeń i transportów wymagających obowiązkowej ochrony z punktu widzenia interesu gospodarczego państwa, bezpieczeństwa publicznego oraz innych żywotnych interesów państwa.

Specyficzne zadania ciążą również na Policji w przypadku wystąpienia zagrożenia atakami terrorystycznymi[43], czy też wystąpienia (zagrożenia) konfliktu zbrojnego.

W momencie wejścia Polski do Unii Europejskiej oraz strefy państw Schengen, nowego znaczenia nabrało zadanie dotyczące współpracy polskiej Policji z policjami innych państw oraz gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych[44].

Istotną rolę w zapewnieniu odpowiedniej ochrony infrastruktury krytycznej spełnia obok wcześniej wspomnianych podmiotów również Policja. Charakter podejmowanych w tym obszarze działań opiera się zarówno na działaniach planistycznych, jak i czysto operacyjnych, dotyczących realizacji określonych zadań wynikających z zaistniałej sytuacji kryzysowej, będącej efektem zniszczenia, uszkodzenia bądź awarii elementu kluczowego państwa.

Jednym z obowiązków właścicieli, osób zarządzających, czy operatorów elementów infrastruktury krytycznej jest sporządzanie planów ochrony dla wyznaczonego podmiotu kluczowego. Plany opracowywane są zgodnie z obowiązującymi wymaganiami i muszą zostać uzgodnione z komendantem wojewódzkim Policji, właściwym dla miejsca położenia elementu wyznaczonego jako krytyczny[45]. Ponadto zawartość planu wymaga od jego twórcy stałej współpracy z Policją, ponieważ należy uwzględnić w nim m.in. charakterystykę występujących zagrożeń, które nie zawsze związane będą z charakterem produkcji, czy świadczonych usług, ale mogą dotyczyć również zainteresowania określonym elementem krytycznym członków grup przestępczych czy zwykłych szaleńców. Tego typu informacjami dotyczącymi zagrożeń elementu krytycznego dysponują jednostki Policji.

Również w przypadku awarii, uszkodzenia lub zniszczenia elementu krytycznego przed Policją stają specyficzne zadania. Część z nich opracowana została

---

[43] Szerzej na ten temat; K. Jałoszyński, *Współczesny wymiar antyterroryzmu*, Wydawnictwo TRIO, Warszawa 2008. Porównaj też: Zarządzenie nr Pf 964/04 Komendanta Głównego Policji z dnia 9 września 2004 roku w sprawie określenia sposobu osiągania gotowości do przeciwdziałania zagrożeniom terrorystycznym, Zarządzenie Nr 845/Pf/2004 z dnia 29 lipca 2004 roku Komendanta Głównego Policji w sprawie organizacji pracy i zasad działania Policji w przypadku aktu terroru z użyciem materiałów wybuchowych oraz innych zdarzeń o charakterze terrorystycznym i ekstremistycznym, Decyzja Nr Z-69/03 z dnia 14 marca 2003 roku Komendanta Głównego Policji w sprawie zapewnienia bezpieczeństwa i porządku publicznego na obszarze RP w związku z potencjalnym zagrożeniem terrorystycznym wynikającym z działań militarnych.

[44] Szerzej na ten temat: Decyzja Nr 580 Komendanta Głównego Policji z dnia 17 sierpnia 2007 roku w sprawie procedur postępowania w związku z dokonywaniem sprawdzeń osób i przedmiotów w Systemie Informacyjnym Schengen, § 1.

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

na wypadek utraty funkcji przez elementy infrastruktury krytycznej państwa, których skutkiem bądź przyczyną może być chociażby katastrofa naturalna lub awaria techniczna. Sytuacje tego typu współwystępować będą zazwyczaj z sytuacją kryzysową. Zdarzenia o takim charakterze zobowiązują policjantów do podjęcia działań w ramach opracowanych procedur, wynikających z planów zarządzania kryzysowego.

W przypadku zaistnienia katastrofy naturalnej, czy awarii technicznej wyznaczono dla Policji określone obszary działania obejmujące[46]:

- alarmowanie i ostrzeganie,
- działania porządkowe,
- działania ratownicze,
- działania skierowane na przywracanie stanu przed wystąpieniem zagrożenia.

Wszelkie przedsięwzięcia prowadzone przez Policję w warunkach katastrof naturalnych i awarii technicznych realizowane są we wszystkich fazach reagowania kryzysowego, tzn. fazie zapobiegania, przygotowania, reagowania i odbudowy[47]. Należy jednocześnie pamiętać, że charakter i zakres szczegółowych zadań wykonywanych przez policjantów zależy bezpośrednio od konkretnej fazy związanej z zaistniałą katastrofą naturalną, czy awarią techniczną.

Każdy z określonych obszarów, wyznaczonych dla Policji, charakteryzuje konkretny katalog zadań. Dla zobrazowania ich specyfiki należy wskazać przykładowe zadania dla każdego z wymienionych obszarów. W ramach obszaru przypisanego alarmowaniu policjanci odpowiedzialni są chociażby za uzyskiwanie, przetwarzanie i przekazywanie informacji o zaistniałym zdarzeniu na potrzeby kierowania, dowodzenia i współdziałania, a także przekazywanie informacji i komunikatów o zagrożeniu poprzez policyjne systemy łączności oraz urządzenia rozgłoszeniowe.

W przypadku zadań porządkowych odpowiadają m.in. za ochronę pozostawionego mienia, identyfikację i prowadzenie wykazu ofiar, czy też umożliwienie swobodnego dojazdu i wyjazdu ekipom i jednostkom ratowniczym.

Prowadzone działania ratownicze wymagają od policjantów udzielania pomocy w ewakuacji osobom poszkodowanym, chorym i starszym, udzielania pierwszej pomocy przedlekarskiej oraz udziału w pracach zabezpieczających urządzenia techniczne.

Przywrócenie stanu sprzed awarii lub katastrofy wymaga od policjantów zaangażowania w ochronę miejsc dystrybucji środków pomocy humanitarnej, a także regulację ruchu osób i pojazdów.

Przy okazji rozważań dotyczących udziału Policji w ochronie infrastruktury krytycznej, warto przeanalizować problem skorzystania z jednego z podstawowych uprawnień, jakim jest użycie środków przymusu bezpośredniego. Wiadomym jest, że policjanci, wykonując określone czynności – oprócz innych przysługujących im

[46] Zarządzenie Nr 24/98 Komendanta Głównego Policji z dnia 10 listopada 1998 r. w sprawie realizacji przez policję zadań w warunkach katastrof naturalnych i awarii technicznych.

[47] Ibidem.

uprawnień - mają prawo użycia środków przymusu bezpośredniego oraz broni palnej[48]. Broń palna - w praktyce policyjnej – uznawana jest jako środek ostateczny i stosowany jedynie wówczas, gdy pozostałe środki przymusu bezpośredniego okazały się niewystarczające lub też ich użycie w danej sytuacji (okoliczności) byłoby niemożliwe.

Obowiązujące akty prawne wskazują na dziewięć przypadków uprawniających policjantów do użycia broni palnej. Jako czwarty z nich wymieniona jest sytuacja dopuszczająca użycie broni *w celu odparcia niebezpiecznego bezpośredniego, gwałtownego zamachu na obiekty i urządzenia ważne dla bezpieczeństwa lub obronności państwa, siedziby naczelnych organów władzy, naczelnych i centralnych organów administracji państwowej, wymiaru sprawiedliwości, obiekty gospodarki lub kultury narodowej, przedstawicielstwa dyplomatyczne i urzędy konsularne innych państw (organizacji międzynarodowych) oraz obiekty, które są strzeżone przez specjalistyczne uzbrojone formacje ochronne* [49].

Broni palnej mogą użyć policjanci również w bezpośrednim pościgu *za osobą wobec której istnieje uzasadnione podejrzenie wykonania (popełnienia) zamachu terrorystycznego, czy też umyślnego sprowadzenia niebezpieczeństwa powszechnego dla życia lub zdrowia ludzi*[50] oraz *w celu odparcia gwałtownego, bezpośredniego i bezprawnego zamachu na konwój ochraniający osoby, czy dokumenty zawierające wiadomości stanowiące tajemnicę państwową*[51].

Przytoczone zapisy to tylko przykłady odnoszące się do udziału polskiej Policji w obszarze ochrony obiektów *„wrażliwych”* państwa.

Zapisy te precyzują jednak katalog narzędzi, wraz z określeniem sytuacji pozwalających na ich zastosowanie w sytuacji zagrożenia tego typu obiektów. Równocześnie w sytuacji zagrożenia bezpieczeństwa publicznego, czy też zakłócenia porządku publicznego poprzez wywołanie niebezpieczeństwa powszechnego dla życia, zdrowia lub wolności obywateli, sprowadzenia bezpośredniego zagrożenia dla mienia w znacznych rozmiarach, czy też wywołania bezpośredniego zagrożenia dla:

- obiektów lub urządzeń ważnych dla bezpieczeństwa lub obronności państwa;
- siedzib naczelnych organów władzy, naczelnych i centralnych organów administracji państwowej albo wymiaru sprawiedliwości;
- obiektów gospodarki lub kultury narodowej;
- przedstawicielstw dyplomatycznych i konsularnych innych państw;
- przedstawicielstw organizacji międzynarodowych;
- obiektów dozorowanych przez SUFO.

Mogą zostać użyte uzbrojone oddziały i pododdziały Policji. Użycie tego typu sił może być również wykorzystane w sytuacji zagrożenia zamachem terrorystycznym

[48] Policjanci uprawnieni są do stosowana (według obowiązujących przepisów) takich środków przymusu, jak: fizyczne, techniczne i chemiczne środki służące do obezwładniania bądź konwojowania osób oraz do zatrzymywania pojazdów, pałki służbowe, wodne środki obezwładniające, psy i konie służbowe, pociski niepenetracyjne, miotane z broni palnej, Art. 16 ust. 1 pkt. 1 – 5 Ustawy o Policji, op. cit.

[49] Art. 17, ust. 1, pkt. 4 Ustawy o Policji, op. cit.

[50] Art. 17, ust. 1, pkt. 6 Ustawy o Policji, op. cit.

[51] Art. 17, ust. 1, pkt. 8 Ustawy o Policji, op. cit.

lub jego dokonania w stosunku do obiektów mających szczególne znaczenie dla bezpieczeństwa lub obronności państwa czy też zagrożenia życiu ludzi[52].

W takich przypadkach użycie uzbrojonych oddziałów lub pododdziałów Policji zarządza Prezes Rady Ministrów na wniosek Ministra Spraw Wewnętrznych i Administracji. Siły te mają za zadanie zapewnienie odpowiedniego poziomu bezpieczeństwa publicznego, odpowiadającego potrzebom obywateli lub przywrócenie zakłóconego porządku publicznego. Z uwagi na zmieniający się charakter zagrożeń, ich dynamikę, często nieprzewidywalny przebieg zdarzeń o dużym nasileniu agresji i przemocy – ustawodawca dopuszcza podejmowanie szybkich decyzji dotyczących użycia zwiększonych sił policyjnych. W sytuacjach nagłych, niecierpiących zwłoki decyzję o użyciu uzbrojonych oddziałów lub pododdziałów Policji podejmuje Minister Spraw Wewnętrznych i Administracji. Jego obowiązkiem jest jednak w takim przypadku niezwłoczne powiadomienie o fakcie użycia zwiększonych sił policyjnych Prezesa Rady Ministrów[53].

Zagrożenia skierowane na obiekty i urządzenia infrastruktury istotnej państwa, czy też wynikłe z planowanego lub przeprowadzonego zamachu terrorystycznego, mogą stwarzać równocześnie niebezpieczeństwo dla mienia w znacznych rozmiarach, życia i zdrowia wielu ludzi, a w konsekwencji doprowadzić do zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego w rozmiarach przekraczających możliwości ich sprawnego usunięcia jedynie siłami Policji.

W przypadku, kiedy użycie wzmocnionych sił policyjnych (uzbrojonych oddziałów lub pododdziałów) okazałoby się niewystarczające, istnieje możliwość wsparcia działań Policji przez oddziały i pododdziały Sił Zbrojnych Rzeczpospolitej. Możliwość użycia Sił Zbrojnych w takich przypadkach wymaga jednak postanowienia Prezydenta Rzeczpospolitej Polskiej, które to postanowienie wydawane jest na wniosek Prezesa Rady Ministrów.

W sytuacji, gdy zagrożenie bezpieczeństwa publicznego, czy też zakłócenie porządku publicznego ma charakter zamachu terrorystycznego[54] ukierunkowanego na obiekty mające szczególne znaczenie dla bezpieczeństwa lub obronności państwa, czy też skutkującego niebezpieczeństwem dla życia ludzi, a użyte (wzmocnione) siły policyjne są niewystarczające, pomoc Sił Zbrojnych może sprowadzać się do samodzielnego prowadzenia działań przez oddziały i pododdziały wojska, które będą ukierunkowane na przeciwdziałanie powstałym zagrożeniom.

W sytuacjach wskazujących na konieczność podejmowania szybkich kroków, w przypadkach niecierpiących zwłoki, decyzję o wsparciu Policji przez Siły Zbrojne może podjąć – na wniosek Ministra Spraw Wewnętrznych i Administracji - Minister Obrony Narodowej. Podejmując takie kroki - Minister Obrony Narodowej zobowiązany jest jednak do określenia zakresu oraz form pomocy niesionej Policji oraz niezwłocznego zawiadomienia o podjętej decyzji Prezydenta Rzeczpospolitej Polskiej. Prezydent zaś, po otrzymaniu decyzji o użyciu Sił Zbrojnych - wydaje postanowienie

[52] Art. 18 ust. 1, pkt. 3, 4 Ustawy o Policji, op. cit.

[53] Art. 18 ust. 1 i 2, Ustawa o Policji, op. cit.

[54] Ustawa posługuje się w tym przypadku sformułowaniem „zagrożenia przestępstwem o przestępstwem o charakterze terrorystycznym...", Art. 18, ust.1, pkt. 4, Ustawa o Policji, op. cit.

o zatwierdzeniu bądź też uchyleniu decyzji podjętej przez Ministra Obrony Narodowej[55].

Wspólne prowadzenie działań przez wzmocnione siły Policji oraz Siły zbrojne RP wymaga nie tylko przemyślanych procedur, odpowiedniego przeszkolenia policjantów i żołnierzy, ale również znajomości specyfiki działania obu tych podmiotów.

Należy jednocześnie podkreślić, że wskazane unormowania nie odnoszą się bezpośrednio do infrastruktury krytycznej państwa.

ZAKOŃCZENIE

Współczesny charakter zagrożeń wskazuje jednoznacznie, iż *„…przybywa dziedzin przedmiotowo wyodrębnianego bezpieczeństwa, a także coraz bardziej dostrzega się powiązania między różnymi jego składowymi oraz między jego wymiarami. Mając na myśli wielowymiarowość bezpieczeństwa, należy mieć na względzie: jego rozległy zakres w wymiarze przedmiotowym i przestrzennym, interdyscyplinarność w badaniach nad nim, ponadresortowość w zakresie praktycznych zadań państwa, relacje pomiędzy podmiotowymi wymiarami bezpieczeństwa, a także jego wymiar dynamiczny”*[56].

Tak sformułowana teza zmusza praktyków do ponownego przeanalizowania zadań ciążących zarówno na administracji rządowej, samorządach, jak i zaplanowanych do realizacji przez odpowiednie służby i straże, w tym również przypisane Policji.

Prawidłowość sformułowana w tych dwóch prostych, a zarazem niezwykle precyzyjnych zdaniach jeszcze przez wiele lat kierunkowała będzie działania podmiotów odpowiedzialnych za bezpieczeństwo państwa.

LITERATURA

1. Aleksandrowicz T. R., *Medialne aspekty terroryzmu i walki z terroryzmem*, [w:], Riedel K., Mocka St., *Terroryzm w medialnym obrazie świata*, Wydawnictwo TRIO, Warszawa 2010.
2. Ciecierski M., *Nowe trendy w bezpieczeństwie – rozwój prywatnego sektora bezpieczeństwa*, [w:], Zaremba A., Zapały B., *Wymiary bezpieczeństwa na progu XXI wieku*, Adam Marszałek, Toruń 2010.
3. Dziubek I., *Proaktywne wykorzystanie inicjatyw lokalnych na rzecz bezpieczeństwa i porządku publicznego w mieście Kaliszu*, [w:] *Bezpieczeństwo publiczne w przestrzeni miejskiej*, pod red. Fehler W., Arte, Biała Podlaska 2010.
4. Jałoszyński K., *Współczesny wymiar antyterroryzmu*, Wydawnictwo TRIO, Warszawa 2008.
5. Jakubczak R., Flis J., *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Bellona, Warszawa 2006.

[55] Art. 18 ust. 3, 4, 5, 6 Ustawy o Policji, op. cit.

[56] J. Stańczyk, *Polska wobec współczesnych wyzwań rozwoju i bezpieczeństwa*, [w:] W. Guzicki, D. Guzicka, *Polska i świat wobec wyzwań współczesności. Aspekty polityczne, ekonomiczne formalnoprawne*, Adam Marszałek, Warszawa 2008, s. 113.

6. Kitler W., *Samorząd terytorialny w obronie narodowej Rzeczpospolitej Polskiej*, AON, Warszawa 2005.
7. *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, February 2003.*
8. Pokruszyński W., *Uwarunkowania współczesnego bezpieczeństwa międzynarodowego*, WSPol., Szczytno 2006.
9. Pokruszyński W., *Współczesne bezpieczeństwo narodowe*, Wyd. WSGE, Józefów 2009.
10. Prońko J., Wiśniewski B., *Klasyfikacja zagrożeń*, [w:] *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, pod red. Liedel K, Prońko J., Wiśniewski B., Wyższa Szkoła Administracji, Bielsko – Biała 2007.
11. Radvanovsky R., McDougall A., *Critical Infrastructure. Homeland Security and Emergency Preparedness*, CRC Press, London, New York 2010.
12. Wojdakowska M., *Mała Księga Cytatów*, Printex, Białystok 2000.
13. Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik po nowelizacji ustawy*, PRESSCOM Sp. z o.o., Wrocław 2010.
14. Stańczyk J., *Polska wobec współczesnych wyzwań rozwoju i bezpieczeństwa*, [w:] *Polska i świat wobec wyzwań współczesności. Aspekty polityczne, ekonomiczne i formalnoprawne*, pod red. W. Guzicki, D. Guzicka Adam Marszałek, Warszawa 2008.
15. Szczurek T., *Resort obrony narodowej w zarządzaniu kryzysowym w latach 1989 – 2009*, WAT, Warszawa 2009.
16. Tyburska A., *Kierowanie w Policji – wybrane zagadnienia w aspekcie bezpieczeństwa narodowego*, [w:] *Kierowanie bezpieczeństwem narodowym*, Zdrodowski B., Wiśniewski B., AON, Warszawa 2008.
17. Tyburska A., *Ochrona infrastruktury krytycznej a zapewnienie bezpieczeństwa i porządku publicznego*, [w:] Gałecki A., Dalecka M., Tabaczniuk T., *Współczesne problemy bezpieczeństwa*, Oficyna Wydawnicza Uniwersytetu Zielonogórskiego, Zielona Góra 2010.

Akty prawne:

1. Konstytucja Rzeczpospolitej Polskiej, Ustawa z dnia 2 kwietnia 1997 roku (Dz.U.97.78.483).
2. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2007 r., Nr 43, poz.277).
3. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r., Nr 89, poz. 590 z późn. zm.).
4. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. Nr 83, poz. 542).
5. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. Nr 83 poz. 541).

6. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz.U. Nr 83, poz. 540).
7. Dyrektywa Rady 2008/114/WE, z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.U.UE L z dnia 23 grudnia 2008 r., Dz.U. UE.L.2008.345.75.).

Inne źródła:

1. Critical Infrastructure Protection, GAO-01-323, April 2001.
2. CRS Report for Kongres, October 1, 2004.
3. *Zielona Księga w sprawie Europejskiego Programu Ochrony Infrastruktury Krytycznej*, Komisja Wspólnot Europejskich, [online] [dostęp: 11.03.2008]. Dostępny w Internecie: http://eur-ex.europa.eu/LexUriServ/site/pl/com/2005/com2005_0576 pl01.pdf.

POLICE AND CRITICAL INFRASTRUCTURE PROTECTION

Summary

Police is an organization mainly identified as the authority responsible for public order and safety. Providing the country with the appropriate level of security requires a new look at the role of the authorities, including the police, involved in security matters. New, so far non-existing threats result from human dependence upon scientific and technological achievements. Efficient sectors such as energy, fuel, transportation, telecommunications, finance, health care, or any other sector ensuring continuity of public administration bodies, make our lives easier but at the same time pose a great threat to public order and safety. Additional threats result from interdependencies among elements of particular sectors, which we remain unaware of. The provision of relevant protective measures and identification of tasks assigned to the authorities involved in security pose a challenge not only to services and guards, but also to enterprises and public administration bodies involved in the development of regulations related to critical infrastructure protection as well as those which introduce regulations, guidelines or procedures.

Key words: *public safety, public order, threats to state security, critical infrastructure, police*

Artykuł recenzował: płk dr hab. Henryk SPUSTEK, prof. nadzw. WSOWL