Dariusz Góralski

Artykuł 12a znowelizowanej ustawy o zarządzaniu kryzysowym – nowa odpowiedzialność ABW

W roku 2009 Sejm znowelizował ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, porządkując szereg kwestii związanych nie tylko z wąsko rozumianym tytułem ustawy, ale również dotyczących m.in. ochrony infrastruktury krytycznej i zwalczania zagrożeń asymetrycznych[1]. W tym właśnie obszarze mieści się również artykuł 12a wspomnianej ustawy, będący w trakcie prac sejmowych tematem wielu polemik. Nie tylko precyzuje on dotychczasowe uprawnienia Szefa Agencji Bezpieczeństwa Wewnętrznego (jako organu administracji) w zakresie przeciwdziałania zagrożeniom terrorystycznym, ale, co równie ważne, dodaje mu nowe obowiązki i odpowiedzialność wobec podmiotów gospodarczych w zakresie ich bezpieczeństwa. Oto zapisy tego artykułu:

1. Zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym są realizowane we współpracy z organami administracji rządowej właściwymi w tych sprawach, w szczególności z Szefem Agencji Bezpieczeństwa Wewnętrznego,
2. Organy administracji publicznej, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej są obowiązani niezwłocznie przekazywać Szefowi Agencji Bezpieczeństwa Wewnętrznego będące w ich posiadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym dla tej infrastruktury, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodnokanalizacyjnych, ciepłowniczych oraz teleinformatycznych, istotnych z punktu widzenia bezpieczeństwa państwa, a także działań, które mogą prowadzić do zagrożenia życia lub zdrowia ludzi, mienia w znacznych rozmiarach, dziedzictwa narodowego lub środowiska,
3. Szef Agencji Bezpieczeństwa Wewnętrznego, w przypadku podjęcia informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, może udzielać zaleceń organom i podmiotom zagrożonym tymi działaniami oraz przekazywać im niezbędne informacje służące przeciwdziałaniu zagrożeniom,
4. Szef Agencji Bezpieczeństwa Wewnętrznego o podjętych działaniach, o których mowa w ust. 3, informuje dyrektora Rządowego Centrum Bezpieczeństwa.

W trakcie wspomnianych prac nad nowelizacją opozycja ostrzegała, przywołując właśnie zapisy powyżej zacytowanego artykułu 12a, iż po raz kolejny administracja państwowa sięga po narzędzia władzy, by wymusić na właścicielach czy posiadaczach infrastruktury krytycznej (IK) właściwy poziom jej ochrony. Nic bardziej mylnego. Ustawa o zarządzaniu kryzysowym wprowadza nowe podejście, w którym interes państwowy zbiega się z interesem społecznym i prywatnym, by wspólnie chronić obiekty, urządzenia, systemy czy usługi, bez funkcjonowania których państwo nie mogło by wypełniać swoich obowiązków wobec obywateli.

[1] *Ustawa z dnia 17 lipca 2009 o zmianie ustawy o zarządzaniu kryzysowym*, Dz.U. z 2009 r., Nr 131, poz. 1076.

Ta nowatorska filozofia wyrażona zarówno w art. 12a, jak i w innych artykułach ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, umożliwia stworzenie warunków do wspomagania przez administrację publiczną instytucji i firm (często prywatnych) będących właścicielami lub posiadaczami IK. Pozwala również na wsparcie przez budżet państwa odbudowy IK, a także korzystania z możliwości ochrony ze strony służb państwowych, w tym Agencji Bezpieczeństwa Wewnętrznego.

Po raz chyba pierwszy ustawa zezwala, by informacje o zagrożeniach uzyskiwane czy posiadane przez państwową służbę specjalną (ABW) mogły być (po odpowiednim przetworzeniu) przekazywane podmiotom spoza administracji publicznej w formie ostrzeżeń czy rekomendacji.

Odpowiedzialność stron

Aby dokładniej zrozumieć nowatorskie podejście do tego zagadnienia skoncentrowane w artykule 12a, należy jego zapisy czytać łącznie z treścią art. 5b[2] tej samej ustawy, który powierza Dyrektorowi Rządowego Centrum Bezpieczeństwa opracowanie Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK). Podstawowe założenia treści NPOIK przedstawiają się następująco:

1. NPOIK ma być dokumentem, w którym rząd przedstawi swoją wizję ochrony zasadniczych dla funkcjonowania państwa składników infrastruktury. Ma wskazać cele, priorytety, wymagania oraz standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej.
2. W Programie zostaną wskazane organy i podmioty uczestniczące w OIK, organy odpowiedzialne za systemy IK (gospodarze systemów) oraz role, jakie pełnić będą w ramach funkcjonowania systemu OIK.

---

[2] *Ustawa z dnia 17 lipca 2009 o zmianie ustawy o zarządzaniu kryzysowym,* Dz.U. z 2009 r., Nr 131, poz. 1076, art. 5b:

1. „Rada Ministrów przyjmuje, w drodze uchwały, Narodowy Program Ochrony Infrastruktury Krytycznej, zwany dalej «programem», którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w szczególności w zakresie:
   1) zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej;
   2) przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną;
   3) reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej;
   4) odtwarzania infrastruktury krytycznej.
2. Program określa:
   1) narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej;
   2) ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2;
   3) szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.
3. Program przygotowuje dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy (...).
9. Rada Ministrów określi, w drodze rozporządzenia, sposób realizacji określonych w ustawie obowiązków i współpracy w zakresie programu przez organy administracji publicznej i służby odpowiedzialne za bezpieczeństwo narodowe z właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń i usług infrastruktury krytycznej oraz innymi organami i służbami publicznymi, biorąc pod uwagę konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa infrastruktury krytycznej".

3. Program będzie zawierał charakterystykę systemów IK wraz z metodyką oceny ryzyka dla tej infrastruktury, a także priorytety, jakimi kierować się powinni uczestnicy OIK.
4. W Programie wskazane zostaną kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokajania potrzeb obywateli.
5. Opisany zostanie sposób współpracy między sektorem publicznym i prywatnym w OIK na poziomach strategicznym i operacyjnym.
6. Przedstawiony zostanie model zwiększenia efektywności OIK poprzez większe zaangażowanie podmiotów prywatnych oraz budowę świadomości i wzajemnego zaufania pomiędzy uczestnikami OIK, a także udział w ćwiczeniach z zakresu OIK.
7. Wskazane zostaną najlepsze praktyki oraz standardy ochrony IK, a także projekty w zakresie badań i rozwoju w tym zakresie.

Jak wynika z powyższego, NPOIK ma być dokumentem, który wytyczy kierunek dążeń wszystkich uczestników ochrony infrastruktury krytycznej, przyczyniając się tym samym do ograniczenia działań związanych z IK w innych kierunkach. Program, rozumiany jako ciąg działań, będzie w ten sposób stanowić narzędzie i przewodnik do realizacji tego celu. Dążeniem autorów jest również to, by NPOIK zawierał w sobie inne dokumenty lub w maksymalnym stopniu był z nimi interoperacyjny (np. z Rządowym Programem Ochrony Cyberprzestrzeni RP na lata 2010 - 2015).

Wykonanie Programu polegać ma na:

1) realizacji wyznaczonych priorytetów oraz celów,
2) zapewnieniu warunków do doskonalenia ochrony i ciągłości funkcjonowania infrastruktury krytycznej,
3) przygotowaniu na sytuacje kryzysowe mogące być skutkiem zakłócenia funkcjonowania infrastruktury krytycznej lub niekorzystnie wpływające na tę infrastrukturę, będące wynikiem przeprowadzonej oceny ryzyka,
4) przygotowaniu do reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
5) zapewnieniu warunków do odtwarzania infrastruktury krytycznej,
6) przestrzeganiu standardów oraz wymagań w nim zawartych,
7) współpracy w realizacji Programu.

Zasadnicze znaczenie dla sukcesu koncepcji Programu będzie miała współpraca w jego realizacji. Współpraca ta ma polegać na utrzymywaniu kontaktów pomiędzy jego uczestnikami i dotyczyć w szczególności:

1) identyfikacji obszarów działań niezbędnych do podniesienia poziomu ochrony IK,
2) przekazywania operatorom IK informacji dotyczących zagrożeń wobec tej infrastruktury,
3) przekazywania przez operatorów IK informacji o zidentyfikowanych zagrożeniach dla zarządzanej przez nich infrastruktury,
4) przekazywania informacji o spodziewanym lub zaobserwowanym zwiększeniu zapotrzebowania na usługi lub produkty dostarczane przez operatorów IK,
5) przekazywanie informacji o spodziewanych przerwach lub zakłóceniach w dostawach usług lub produktów dostarczanych przez operatorów IK, przy wykorzystaniu tej infrastruktury,
6) wspierania działań podejmowanych przez operatorów IK w przypadku zniszczenia lub zakłócenia funkcjonowania tej infrastruktury,

7) udzielania wsparcia merytorycznego przez podmioty administracji publicznej w zakresie ochrony IK oraz w zakresie funkcjonowania wewnętrznych mechanizmów tej ochrony i zarządzania kryzysowego,
8) przygotowania i udziału w ćwiczeniach z zakresu ochrony infrastruktury krytycznej,
9) udziału w przygotowaniu i aktualizacji Programu.

Jak widać, ochrona IK to nie tylko stwarzanie i egzekwowanie określonych wymogów. W tym konkretnym przypadku zastosowane zostało zupełnie nowe podejście do relacji podmiotów właścicielskich z administracją publiczną. Najtrudniejsze dla twórców NPOIK będzie przełamanie (zmiana) wąskiego spojrzenia na ochronę infrastruktury krytycznej wśród jej uczestników oraz zaangażowanie i aktywny, oparty na partnerskich warunkach, udział administracji, a także prywatnych i państwowych operatorów infrastruktury krytycznej, w tworzenie systemu ochrony IK.

Dla jeszcze głębszego zrozumienia odmiennego podejścia (wyrażonego w przepisach ustawy o zarządzaniu kryzysowym) do zagadnienia bezpieczeństwa infrastruktury krytycznej należy spojrzeć, jakie wymagania stawiane są przed właścicielami (posiadaczami) obiektów, urządzeń czy usług stanowiących elementy infrastruktury krytycznej. W art. 6, w ustępach 1, 5 i 5a, wskazano obowiązki właścicieli, tj.:

1. Zadania z zakresu ochrony infrastruktury krytycznej obejmują:
   1) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej,
   2) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej,
   3) odtwarzanie infrastruktury krytycznej,
   4) współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony.
5. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia.

5a. Właściciele, posiadacze samoistni i zależni, o których mowa w ust. 5, mają obowiązek wyznaczyć, w terminie 30 dni od dnia otrzymania informacji, o której mowa w art. 5b ust. 7 pkt 4, osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej.

Porównajmy zakres i skalę tych obowiązków z zakresem wymagań stawianych przed administracją publiczną w odniesieniu do tej samej infrastruktury, wymienione w odpowiednich ustępach w cytowanym wyżej artykule 5b. Mówimy tu praktycznie tylko o szczeblu centralnym administracji.

Odpowiednio w kolejnych artykułach (tj. 14, 17 i 19) poszczególne szczeble administracji terenowej, od wojewody poczynając, mają w swe zadania wpisaną organizację i realizację działań związanych z ochroną infrastruktury krytycznej. Ponadto, w każdym z tych artykułów znalazły się również przepisy związane pośrednio z zagadnieniem ochrony infrastruktury krytycznej, a bezpośrednio z omawianą kwestią artykułu 12a. Mianowicie wojewoda, starosta, wójt, burmistrz i prezydent posiadają uprawnienia do zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terro-

rystycznym oraz współdziałania z Szefem Agencji Bezpieczeństwa Wewnętrznego w tym zakresie.

Klamrą spinającą na poziomie centralnym system zarządzania kryzysowego jest Rządowe Centrum Bezpieczeństwa[3], które poza zapewnieniem obsługi Rady Ministrów, Prezesa Rady Ministrów i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełnienia funkcji krajowego centrum zarządzania kryzysowego, wykonuje trzy istotne zadania[4] wynikające z art. 12a ustawy o zarządzeniu kryzysowym, a mianowicie:

- realizuje zadania z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym,
- współdziała z Szefem Agencji Bezpieczeństwa Wewnętrznego w tym zakresie,
- realizuje zadania planistyczne i programowe z zakresu ochrony infrastruktury krytycznej.

Filozofia współpracy

Z powyższego wyliczenia zadań i zestawień przepisów widać wyraźnie, że system ochrony infrastruktury krytycznej opisany w ustawie o zarządzaniu kryzysowym oparty jest na wspomaganiu przez administrację publiczną właścicieli oraz posiadaczy samoistnych i zależnych obiektów, a także instalacji lub urządzeń infrastruktury krytycznej. W nowelizacji ustawy o zarządzaniu kryzysowym ogólne pojęcie infrastruktury zbiega się w obszarze infrastruktury krytycznej z interesem Państwa, ale także z możliwościami i obowiązkami administracji w dziedzinie bezpieczeństwa. Z jednej strony są to możliwości prawne organów centralnych i wykonawcze szczebli lokalnych. Z drugiej, szczególnie w odniesieniu do zagrożeń ze strony ludzi, to świat służb, zwłaszcza specjalnych.

Właściciel czy posiadacz IK ma opracować plan ochrony, wdrożyć go i wyznaczyć osobę do kontaktów z administracją. Mówiąc ogólnie, całą resztę wykona administracja.

To administracja na swoim poziomie powinna ująć elementy IK w swoich planach zarządzania kryzysowego, dostosować siły i środki dla zapewnienia najlepszej ochrony, a w razie zdarzenia nadzwyczajnego, zgodnie z ustaloną hierarchią priorytetów, przystąpić do jej ratowania. W razie zniszczenia przedmiotowej infrastruktury administracja winna wspomóc jej właściciela czy posiadacza w usuwaniu skutków awarii, katastrofy oraz w przywracaniu stanu pierwotnego. Powinna również zapewnić przetestowanie przyjętych planów współpracy odpowiednich służb, inspekcji czy straży z właścicielem lub posiadaczem IK tak, by w razie zagrożenia profesjonalnie zareagować. Poza tym, poprzez mechanizm współpracy publiczno-prywatnej ma powstać w przyszłości, w oparciu o inicjatywy RCB, forum (fizyczne i logiczne) wymiany praktyk, bank pomysłów na zabezpieczenie IK, zasób porad eksperckich, a także przenie-

[3] Ta zupełnie nowa w polskim systemie administracji instytucja, będąca państwową jednostką budżetową podległą bezpośrednio Prezesowi Rady Ministrów, utworzona została w dniu 2 sierpnia 2008 r. na podstawie art. 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r., Nr 89, poz. 590).

[4] Art. 11 ust. 2 pkt pkt 10, 10a i 11 *Ustawy z dnia 17 lipca 2009 o zmianie ustawy o zarządzaniu kryzysowym*.

sienie niektórych rozwiązań biznesowych do działań administracji w celu polepszenia procedur i zwiększenia efektywności działania służb reagowania kryzysowego (zasada *pomóż nam sobie lepiej pomóc*). Dodatkowe instrumenty wsparcia dla właścicieli i posiadaczy IK, a także pola odpowiedzialności poszczególnych resortów na poziomie strategicznym, zostaną wskazane w sporządzanym przez RCB Narodowym Programie Ochrony Infrastruktury Krytycznej.

Reasumując, elementem łączącym wysiłki na rzecz ochrony IK oraz mającym stanowić pomoc dla operatorów IK i administracji ma być właśnie wymieniony wcześniej Narodowy Program Ochrony Infrastruktury Krytycznej, poprzez zawarcie w nim w sposób syntetyczny i kompleksowy wizji, celów i standardów ochrony IK oraz współpracy w realizacji tego zadania.

Przeciwdziałanie zagrożeniom o charakterze terrorystycznym

Mając jasno określoną relację obowiązków i odpowiedzialności poszczególnych uczestników procesu ochrony infrastruktury krytycznej należy skierować uwagę na przyczyny zagrożeń dla bezpieczeństwa IK, a w szerszym sensie – na specyficzne przyczyny powstawania sytuacji kryzysowych we współczesnym świecie.

Kryzysy, katastrofy czy klęski żywiołowe spowodowane czynnikami naturalnymi są dość dobrze opisane, a w większości posiadają przypisane im odpowiedzialne instytucje posiadające siły i środki do zapobiegania takim kryzysom lub minimalizowania ich skutków. W ostatnim dziesięcioleciu pojawił się jednak zupełnie nowy czynnik sprawczy, który może powodować podobne kryzysy. Jest to działanie o charakterze terrorystycznym.

Celowo używam tu zwrotu o charakterze terrorystycznym, gdyż polski kodeks karny nie posługuje się pojęciem terroru i terroryzmu. Używa jedynie pojęcia przestępstwa o charakterze terrorystycznym, które jest zagrożone karą pozbawienia wolności (art. 115 § 20). Czyn ten musi być popełniony w celu: poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej RP lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce RP, innego państwa lub organizacji międzynarodowej. Karalna jest także groźba popełnienia takiego czynu.

W kodeksie karnym można także odnaleźć najbardziej typowe przestępstwa, których podłoże może lub musi być terrorystyczne. Wymieniając najbardziej charakterystyczne, warto wspomnieć o zamachu na bezpieczeństwo powszechne, w tym zabójstwo z użyciem materiałów wybuchowych, sprowadzenie zdarzenia zagrażającego życiu lub zdrowiu wielu osób albo mieniu w wielkich rozmiarach (art. art. 148 i 163), wzięcie i przetrzymywanie zakładnika oraz każde inne przestępstwo spełniające normę art. 115 § 20.

Ustawa o zarządzaniu kryzysowym musiała objąć powyższe przyczyny sytuacji kryzysowych, stąd zadania wyznaczone wszystkim szczeblom administracji omówione na wstępie tego artykułu. Dzięki takiemu posunięciu udało się wypełnić kilka luk prawnych istniejących do tej pory w polskim ustawodawstwie. Po pierwsze, wprowadzono powszechny obowiązek informowania o zagrożeniach terrorystycznych. Po drugie, wprowadzono obowiązek planowego przeciwdziałania spodziewanym następstwom zdarzeń o charakterze terrorystycznym. Wreszcie po trzecie, przypisano te zadania odpowiednio organom administracji publicznej na wszystkich szczeblach.

Czyn o charakterze terrorystycznym może dotknąć praktycznie każdej dziedziny życia. Dlatego tak trudno jest wskazać jeden organ, który całościowo odpowiadałby za ten rodzaj zagrożeń. Stąd obszerny system łączący organy administracji publicznej działające w systemie zarządzania kryzysowego z Agencją Bezpieczeństwa Wewnętrznego.

Ustawa o zarządzaniu kryzysowym nie stara się rozdzielać i dochodzić, kiedy i jakie zdarzenia mogą wchodzić w zakres kompetencji poszczególnych organów. Nie inaczej jest z większym kryzysem obejmującym szereg zjawisk i skutków. Dlatego ustawodawca obciąża organy administracji publicznej obowiązkiem zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym. Ale, zgodnie z art. 6 ust. 5 ustawy, również właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury do czasu jej pełnego odtworzenia. Przez tę krótką dyspozycję na właścicieli nałożone zostały obowiązki związane z ochroną IK, w tym również przed zdarzeniami o charakterze terrorystycznym.

Konieczność współpracy z Szefem ABW w przedmiotowym zakresie w żadnym razie nie rozszerza jego uprawnień zawartych w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Z tego punktu widzenia, obowiązki organów administracji publicznej i właścicieli oraz posiadaczy samoistnych IK nie zwiększają uprawnień ABW, a wręcz zobowiązują tę instytucję do współpracy, współodpowiedzialności oraz dzielenia się swoją wiedzą i doświadczeniami. Art. 12a ust. 3 to zobowiązanie Szefa ABW do wzięcia na siebie odpowiedzialności za bezpieczeństwo IK, skuteczną prewencję oraz odpowiednio wczesne ostrzeżenie o możliwym zagrożeniu.

Tak zarysowana współpraca w sposób naturalny umożliwia realizację wszystkich czterech faz zarządzania kryzysowego, zaliczając zwalczanie terroryzmu do planu zarządzania kryzysowego, traktując przy tym wszystkich uczestników systemu na równi. Pozwala to właścicielom i posiadaczom IK działać spójnie z organami samorządu czy wojewodą, którzy, wykonując zadania z zakresu zarządzania kryzysowego, współpracują także z ABW. Wydaje się, że to korzystnie wpływa przede wszystkim na tworzone plany ochrony IK i plany zarządzania kryzysowego, które dzięki jednolitemu oglądowi zagrożeń terrorystycznych będą ze sobą współgrać.

Omówione przepisy i współzależności tworzą nową jakość. ABW dzięki ustawie o zarządzaniu kryzysowym znalazła się w gronie instytucji współdecydujących o przedsiębranych krokach w sytuacjach kryzysowych. Zasilana wiedzą od organów administracji oraz właścicieli i posiadaczy samoistnych IK, wykorzystując wiedzę zdobywaną w sposób tradycyjny, a także dzięki doświadczeniu i danym spływającym od służb partnerskich, ABW jest uprawniona (po przetworzeniu informacji) do przekazywania sygnałów, ostrzeżeń i rekomendacji dotyczących sytuacji newralgicznych.

Na podkreślenie zasługuje przy tym fakt często nie poruszany podczas dyskusji nad ustawą o zarządzaniu kryzysowym. Otóż, ustawa w sposób bezdyskusyjny daje Szefowi ABW możliwość dzielenia się posiadanymi informacjami z podmiotami gospodarczymi, co do tej pory było ograniczone do wybranych organów administracji.

Warto zauważyć, że ustawa nie nadaje ABW uprawnień władczych w stosunku do uczestników systemu zarządzania kryzysowego, nawet w odniesieniu do zdarzeń o podłożu terrorystycznym. Szef Agencji może organom i podmiotom zagrożonym tego typu działaniami udzielać zaleceń oraz przekazywać niezbędne informacje służą-

ce przeciwdziałaniu zagrożeniom, te jednak nie są zobowiązane do wykonywania żadnych poleceń ani nakazów ABW.

Zadania ABW w ustawie o zarządzaniu kryzysowym

W tym miejscu warto zestawić wymienione obowiązki administracji publicznej wyrażone w ustawie o zarządzaniu kryzysowym z zadaniami Agencji Bezpieczeństwa Wewnętrznego wynikającymi z *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*.

W art. 5 tej ustawy czytamy m.in.:

1. Do zadań ABW należy:
   1) rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa,
   2) rozpoznawanie, zapobieganie i wykrywanie przestępstw:
      a) szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa,
      b) godzących w podstawy ekonomiczne państwa oraz ściganie ich sprawców,
   4) uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego,
   5) podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych.

Rozpatrując treść art. 12a ust. 1 ustawy o zarządzaniu kryzysowym w odniesieniu do zagrożeń terrorystycznych, a także zadań własnych ABW – widzimy komplementarność ich zapisów. Art. 12a stanowi podsumowanie wspomnianych artykułów z ustawy o zarządzaniu kryzysowym (art. art. 11, 14, 17 i 19), odnoszących się do realizacji zadań z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym, a także realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Bardzo silnie trzeba podkreślić różnicę pomiędzy zadaniami własnymi ABW a zadaniami poszczególnych wojewodów, starostów, wójtów, burmistrzów i prezydentów w systemie zarządzania kryzysowego. Szef ABW ma na celu rozpoznać, zapobiec lub wykryć przestępstwo o charakterze terrorystycznym, ścigać jego sprawców, zwalczać wszystkie zagrożenia godzące w bezpieczeństwo państwa i porządek konstytucyjny. Wykonuje więc zadania ukierunkowane na przestępcę i przestępstwo, a nie na efekty działania przestępcy (terrorysty).

Wspomniane wyżej organy administracji publicznej mają natomiast za zadanie zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym. Zajmują się więc efektami działania przestępcy (terrorysty) w różnych fazach jego działalności. Obowiązkiem tych organów jest zapewnienie bezpieczeństwa ludziom i mieniu na podległym im obszarze. Organy te powinny ćwiczyć współdziałanie służb, ludności, sposób ostrzegania o zagrożeniach itp. Ponadto, powinny planować siły i środki na odtworzenie stanu fizycznego sprzed zdarzenia o charakterze terrorystycznym. Nie zajmują się zaś sprawcą wprost.

Taki podział zadań rodzi potrzebę współpracy. Bez wiedzy i pomocy ze strony Szefa ABW poszczególne organy nie będą mogły właściwie zabezpieczyć osób i mie-

nia, przećwiczyć wariantów zdarzeń wobec dynamicznie zmieniających się sposobów, form i metod działania terrorystów. Wreszcie, bez ABW nie jest możliwe właściwe odtworzenie stanu pierwotnego przy znacznych zniszczeniach (z uwagi na brak wiedzy o priorytetach terrorystów i konieczności hierarchizacji etapów przywracania stanu sprzed zdarzenia).

Zadania ABW w ustawie o zarządzaniu kryzysowym nie ograniczają się jednak do enigmatycznie zarysowanego współdziałania z RCB, ministrami, wojewodami, starostami, burmistrzami, wójtami czy prezydentami w przedmiotowym zakresie. Uprawnienia i obowiązki ABW są znacznie szersze.

Dodatkowe obowiązki Szefa ABW zostały ustalone w art. 5a:

1. Na potrzeby Krajowego Planu Zarządzania Kryzysowego, ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają *Raport o zagrożeniach bezpieczeństwa narodowego*, zwany dalej *Raportem*.
2. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego.

Szef ABW z mocy ustawy występuje w tym artykule jako sporządzający raport cząstkowy, ale także jako odpowiedzialny za koordynację przygotowania *Raportu* w części odnoszącej się do zagrożeń terrorystycznych na podstawie materiałów innych organów. Dzięki temu może w sposób komplementarny ocenić zawartość raportów innych organów, obiektywnie zweryfikować ich subiektywną ocenę zagrożeń, wybór scenariuszy zdarzeń czy ryzyko wystąpienia zdarzenia. Dzięki współpracy z RCB Szef ABW ma także możliwość zweryfikowania innych raportów cząstkowych, nie zawierających początkowo informacji dotyczących zagrożeń o charakterze terrorystycznym. Pozwala mu to zwracać się o uzupełnienie raportów gdy uzna, że takie zagrożenia występują, a są jedynie nie dostrzegane przez dany organ.

W tych warunkach sporządzenie przez Szefa ABW raportu dotyczącego zagrożeń terrorystycznych gwarantuje całościowe spojrzenie na problem i dostosowanie działalności różnych organów i służb do zagrożeń występujących w danym obszarze w celu przeciwdziałania zjawisku, skutecznego jego zwalczania i umożliwienia szybkiego odtworzenia sytuacji sprzed zdarzenia terrorystycznego.

Na zakończenie tych rozważań należy wspomnieć o ważnej inicjatywie podjętej przez RCB i ABW. By wzmocnić bieżącą współpracę w zakresie wymiany informacji, realizowaną przez RCB poprzez CAT ABW, Szef ABW i Dyrektor RCB podpisali w dniu 19 sierpnia 2010 r. *Porozumienie w sprawie ustalenia szczegółowego zakresu i sposobów współdziałania Rządowego Centrum Bezpieczeństwa i Agencji Bezpieczeństwa Wewnętrznego*. W § 1 Porozumienia zapisano:

1. „Współdziałanie Stron w sprawach zarządzania kryzysowego obejmuje następujące przedsięwzięcia:
   1) wymianę informacji, wzajemne udostępnianie materiałów, tworzenie wspólnych opracowań, uzgadnianie wspólnych stanowisk dotyczących:
      a) koordynacji przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego, w tym przekazanie przez Szefa Agencji Bezpieczeństwa Wewnętrznego dyrektorowi Rządowego Centrum Bezpieczeństwa ostatecznej wersji *Raportu* w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej,

b) monitorowania potencjalnych zagrożeń, możliwości ich wystąpienia lub rozwoju, w tym zagrożeń o charakterze terrorystycznym,
c) realizacji zadań w zakresie zapobiegania, przeciwdziałania, reagowania zgodnie z kompetencjami i usuwania skutków zdarzeń o charakterze terrorystycznym,
d) ochrony infrastruktury krytycznej,
e) opiniowania projektów dokumentów rządowych, w tym projektów aktów normatywnych i innych aktów prawnych,
f) opiniowania dokumentów innych niż wymienione w lit. e, związanych z realizacją ustawowych zadań Stron;

2) współpracę dotyczącą ochrony informacji niejawnych;
3) współpracę w organizowaniu, współorganizowaniu oraz opiniowaniu programów konferencji, szkoleń i narad poświęconych zarządzaniu kryzysowemu;
4) wymianę doświadczeń dotyczących wykonywania ustawowych zadań każdej ze Stron".

Porozumienie to porządkuje i wypełnia zakres współpracy na poziomie centralnym, umożliwiając sprawną realizację zapisów ustawowych i nie pozostawiając wątpliwości co do intencji i determinacji obu instytucji w budowaniu systemu zarządzania kryzysowego z uwzględnieniem zagrożeń o charakterze terrorystycznym.

Podsumowanie

Kluczem do sukcesu wzajemnej współpracy, dość precyzyjnie nakreślonej w kolejnych ustępach art. 12a, jest wzajemne zaufanie. Obie strony, w tym przypadku Agencja Bezpieczeństwa Wewnętrznego i podmioty gospodarcze, będą działały w newralgicznych obszarach. Z jednej strony tajemnica biznesu, pokazanie wrażliwości systemów czy procedur, z drugiej – przekazywanie rekomendacji i zaleceń na podstawie wiedzy służb specjalnych.

Co ważne, obie strony muszą przyjąć, że przy realizacji art. 12a nie ma mowy o żadnej pracy operacyjnej czy też nierówności którejś ze stron. W zakresie, w jakim jest to możliwe, wszystkie niezbędne informacje muszą być przekazywane zgodnie z art. 12a przez osoby wyznaczone do współpracy z administracją zgodnie z art. 6 ust. 5a przez właścicieli lub posiadaczy IK. Współpraca tych osób z ABW musi być przejrzysta i oparta na obowiązującym prawie.

Obok zaufania musi się również pojawić zaangażowanie w proces współpracy. Im więcej informacji, im częstsze (a więc i lepsze) kontakty, im więcej przypadków udoskonalania jakości i bezpieczeństwa systemów i procedur na podstawie zaleceń czy rekomendacji ABW, tym większe... zaufanie.

Jak widać, prezentowane rozwiązania oparte są na realizacji wspólnych celów i odpowiedzialności w relacjach administracji publicznej ze sferą de facto prywatną. Warto powtórzyć, że takie podejście nigdy dotąd nie było stosowane przy stanowieniu zależności pomiędzy państwem i jego administracją a światem biznesu. Dziwić jedynie może, że partnerskie relacje w zakresie bezpieczeństwa stały się możliwe w naszym kraju dopiero w obliczu i pod wpływem zagrożeń terrorystycznych.

ABSTRACT

Amendments from September 2009 to the Crisis Management Act hale introduced many New solutions to the whole Polish system. One of them is the necessity of cooperation between the public administration and the private sector in ensuring security to national critical infrastructure.

This trend can be seen in article 12a, which enables the exchange of information on threats to critical infrastructure between the owners, holders of critical infrastructure and the Internal Security Agency. For the first time such an institution has an obligation to inform institutions, often private about threats, but also give them advice and recommendation in order for them to better secure critical infrastructure.

All the information exchange should be conducted according to article 12a, by persons designated by owners, holders of critical infrastructure according to art 6(5a). This cooperation should be organized in a transparent, clear way according with current law.

Besides trust there also needs to be engagement in the cooperation process. The more information and the frequent (thus better) contacts, the more cases of improvements of quality and security of systems and procedures based on advice and recommendations of the Internal Security Agency the greater…the trust.