

UZASADNIENIE

I. Wstęp.

Projektowane zmiany w założeniu zmierzają do wzmocnienia systemu zarządzania kryzysowego w szczególności w zakresie zarządzania ryzykiem i ochrony ludności z uwzględnieniem postanowień *Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności oraz Ramowego programu działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof.*

Ponadto rozwiązania, o których mowa w projekcie ustawy przewidują wzmocnienie kompetencji struktur rządowych i samorządowych w zakresie zarządzania sytuacją kryzysową lub możliwością jej wystąpienia. W tym przypadku wykorzystane zostały postulaty zawarte w treści dokumentu rządowego pt. *„Propozycje zmian legislacyjnych i innych działań wynikających z rekomendacji Międzyresortowego Zespołu do oceny funkcjonowania systemu ratownictwa i zarządzania kryzysowego (Zespół został utworzony na podstawie zarządzenia nr 101 Prezesa Rady Ministrów z dnia 4 września 2017 r. w sprawie Międzyresortowego Zespołu do oceny funkcjonowania systemu ratownictwa i zarządzania kryzysowego).*

W odniesieniu do konieczności uregulowania kwestii zarządzania ryzykiem – jest to wymogiem spełnienia warunkowości *ex ante* w kolejnej perspektywie finansowej UE na lata 2021–2027. Zadania w zakresie zarządzania ryzykiem zostały określone w postanowieniu *Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.* Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bezpośrednio powiązane z jednym z warunków podstawowych kolejnej perspektywy finansowej, który mówi o osiągnięciu *Skutecznych ram zarządzania ryzykiem.*

Wymogi te wprost wskazują na konieczność opracowania planu zarządzania ryzykiem, na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Należy wskazać na art. 6 ww. decyzji, zgodnie z którym państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej streszczenie istotnych elementów tych ocen (pierwsze udostępnienia miało mieć miejsce do dnia 22 grudnia 2015 r., a następne w cyklach trzyletnich).

Cele wynikające z Unijnego Mechanizmu Ochrony Ludności powiązane są z priorytetami określonymi podczas Trzeciej Światowej Konferencji ONZ, która odbyła się w 2015 r. w Sendai. Jednym z podstawowych wymogów przyjętego wówczas *Ramowego programu działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof* jest realizacja przedsięwzięć zgodnie z opracowanymi przez poszczególne państwa celami strategicznymi, zarówno na szczeblu centralnym, jak i lokalnym.

Zgodnie z obowiązującą od dnia 21 marca br. decyzją Parlamentu Europejskiego i Rady (UE) 2019/420 z dnia 13 marca 2019 r. zmieniającą decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności, wszystkie działania na rzecz skutecznego zapobiegania klęskom żywiołowym i katastrofom spowodowanym przez człowieka powinny być spójne z *Ramowym programem*. Unia Europejska odegrała wiodącą rolę w negocjacjach w sprawie *Ramowego programu*, a wiele jego zaleceń opiera się na istniejących politykach i programach UE w zakresie zarządzania ryzykiem katastrof. Ponadto Komisja Europejska opracowała w 2016 r. *Plan działania na rzecz realizacji Ramowego programu z Sendai na lata 2015-2030 w sprawie ograniczania ryzyka katastrof*, który ma przyczynić się do wdrożenia przez państwa członkowskie postanowień *Ramowego programu*.

Biuro Narodów Zjednoczonych ds. ograniczenia ryzyka katastrof (UNISDR) otrzymało zadanie wsparcia krajów członkowskich we wdrażaniu postanowień *Ramowego Programu*. Współpraca realizowana jest poprzez wyznaczone przez poszczególne kraje punkty kontaktowe.

Według obowiązujących w Polsce regulacji, ocena ryzyka aktualizowana jest w cyklu dwuletnim w *Raporcie o zagrożeniach bezpieczeństwa narodowego* oraz w raportach częściowych do *Raportu* sporządzanych przez ministrów, kierowników urzędów centralnych oraz wojewodów. Dokumenty te stanowią podstawę opracowywanego, również cyklicznie, *Krajowego Planu Zarządzania Kryzysowego* oraz planów zarządzania kryzysowego na wszystkich szczeblach administracji. Brak jest jednak prawnego uregulowania kompleksowego podejścia do kwestii zarządzania ryzykiem. Przede wszystkim nie istnieje obowiązek opracowywania planów zarządzania ryzykiem oraz dokumentów, których założeniem jest informowanie Komisji Europejskiej, przez cykliczne przedkładanie następujących dokumentów: *Streszczenia istotnych elementów krajowej oceny ryzyka* oraz *Krajowej oceny zdolności zarządzania ryzykiem*.

Konieczne jest wprowadzenie przepisów zobowiązujących podmioty zaangażowane w proces zarządzania ryzykiem do opracowania i aktualizowania dokumentów w tym zakresie, a także wdrażania *Ramowego programu działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof*. Wskazane jest dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim.

Proponuje się ujednoczenie terminów cykli planistycznych krajowych z unijnymi, gdyż obowiązujące przepisy krajowe przewidują cykl 2 letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne. Dostosowania do procesu oceny ryzyka wymaga także *Raport o zagrożeniach bezpieczeństwa narodowego*. Dokonanie korelacji między regulacjami krajowymi a unijnymi będzie odbywać się bez konieczności opracowywania od podstaw nowych dokumentów planistycznych, lecz z wykorzystaniem już opracowanych i funkcjonujących.

Tak więc *Raport o zagrożeniach bezpieczeństwa narodowego* w dalszym ciągu dotyczyć będzie oceny ryzyka. Po jej przeprowadzeniu i wskazaniu najistotniejszych zagrożeń dla bezpieczeństwa narodowego, konieczne jest określenie celów strategicznych służących ograniczeniu ryzyka ich wystąpienia, z wykorzystaniem istniejących zapisów oraz wniosków zawierających hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do ich osiągnięcia, z uwzględnieniem regionalnych lub lokalnych inicjatyw, czyli podejmowanych na obszarze województwa. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka, identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na przedsięwzięcia ograniczające ryzyko katastrof.

W przypadku planów zarządzania kryzysowego – opracowywane do tej pory plany zarządzania kryzysowego podzielone zostaną na plany zarządzania ryzykiem oraz plany reagowania kryzysowego, tj.

- ✓ plany zarządzania ryzykiem w odniesieniu do działań uczestników zarządzania kryzysowego w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do przejmowania nad nią kontroli,
- ✓ plany reagowania kryzysowego w odniesieniu do działań uczestników zarządzania kryzysowego w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków.

Ww. rozwiązania zostały już zapoczątkowane – ostatnia wersja *Krajowego planu zarządzania kryzysowego* z 2018 r. została podzielona na dwie części:

- ✓ część A odnoszącą się do zarządzania ryzykiem, czyli de facto dwóch pierwszych faz zarządzania kryzysowego: zapobiegania i przygotowania,
- ✓ część B, która dotyczyła reagowania i odbudowy.

Dokonany podział był pierwszym krokiem do ostatecznego rozdzielenia KPZK na osobne dokumenty. Krajowy Plan Zarządzania Ryzykiem w założeniu dotyczyć będzie przedsięwzięć mających na celu niedopuszczenie do sytuacji kryzysowej i przygotowanie struktur zarządzania kryzysowego na wypadek jej wystąpienia.

Informacje dotyczące szczegółowych przedsięwzięć, które do tej pory stanowiły część *Raportu o zagrożeniach bezpieczeństwa narodowego* oraz zadania i obowiązki uczestników zarządzania kryzysowego dla faz: zapobieganie i przygotowanie, które stanowiły część A *Krajowego Planu Zarządzania Kryzysowego*, zostaną przeniesione do planu zarządzania ryzykiem na szczeblu krajowym. Konieczna będzie analiza i uzupełnienie wymienionych przedsięwzięć, z uwzględnieniem elementu służącemu ich weryfikacji aby ustalić czy ich realizacja wpłynęła na ograniczenie ryzyka. Podobnie będzie wyglądać konstrukcja planów zarządzania ryzykiem na pozostałych szczeblach.

Przewiduje się wprowadzenie dla organów administracji rządowej obowiązku wdrażania *Ramowego Programu Działań na lata 2015-2030 na rzecz ograniczenia ryzyka katastrof* oraz pełnienie przez Rządowe Centrum Bezpieczeństwa funkcji krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych do spraw jego wdrażania.

W procesach oceny i zarządzania ryzykiem nie sposób nie uwzględniać zagrożeń dotyczących infrastruktury krytycznej. Dlatego też ujęcie zagrożeń jej dotyczących znajdzie odzwierciedlenie w planach zarządzania ryzykiem oraz planach reagowania kryzysowego.

Przewiduje się wzmocnienie ochrony infrastruktury krytycznej poprzez wdrożenie rozwiązań minimalizujących skutki zakłócenia jej funkcjonowania dla ludności – w tym z zastosowaniem narzędzi zarządzania ryzykiem przewidzianych w ww. zmianach. Charakterystyka zagrożeń dotyczących infrastruktury krytycznej zostanie uwzględniona w planach zarządzania ryzykiem oraz planach reagowania kryzysowego.

Ponadto w odniesieniu do zmian dotyczących infrastruktury krytycznej – zostanie dokonany jej podział na infrastrukturę krytyczną, której zniszczenie lub zakłócenie będzie miało niekorzystny wpływ na:

- ✓ funkcjonowanie państwa lub na dany system infrastruktury krytycznej,
- ✓ lokalną społeczność danego województwa.

W przypadku pierwszym sposób wyłaniania i umieszczania w wykazie pozostanie na dotychczasowych zasadach. W drugim przypadku natomiast kompetencje w zakresie wyłaniania i umieszczania wyłonionej infrastruktury w stosownych wykazach przypadną wojewodzie.

Ponadto przewiduje się wprowadzenie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego związanych z przeciwdziałaniem zagrożeniom dla infrastruktury krytycznej. Wprowadzenie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego związanych z przeciwdziałaniem zagrożeniom dla infrastruktury krytycznej stanowi istotną zmianę w dotychczasowym systemie ochrony infrastruktury krytycznej.

Po raz pierwszy przewiduje się kompleksowo określenie wymagań w trzech powiązanych ze sobą sferach bezpieczeństwa, tj. bezpieczeństwa osobowego, fizycznego i teleinformatycznego. Przewiduje się wprowadzenie upoważnienia ustawowego dla Rady Ministrów do wydania rozporządzenia dotyczącego minimalnych wymagań wobec operatorów infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego, co będzie punktem odniesienia dla operatorów infrastruktury krytycznej w zakresie możliwości zabezpieczania prowadzonej działalności, a co za tym idzie świadczenia niezakłóconych usług dla ludności.

Wdrażanie technicznych zabezpieczeń infrastruktury krytycznej nie może odbywać się z pominięciem czynnika ludzkiego. Planowane jest więc wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u wszystkich operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej we wszystkich systemach infrastruktury krytycznej będą wyznaczać osobę koordynującą działania na linii operator – organy administracji publicznej.

Zmiany w zakresie wzmocnienia kompetencji struktur rządowych i samorządowych w zakresie zarządzania sytuacją kryzysową lub możliwością jej wystąpienia znalazły odzwierciedlenie zarówno w aspekcie podmiotowym jak i przedmiotowym. Zarządzanie kryzysowe obejmie również działania w odniesieniu do zagrożeń poza terytorium Rzeczypospolitej Polskiej. W tego typu przypadkach, w sytuacjach niecierpiących zwłoki, zarządzanie kryzysowe sprawował będzie minister właściwy do spraw zagranicznych. Będzie to dotyczyć przypadków, w których skutki zdarzenia dotyczą obywateli polskich przebywających poza terytorium Rzeczypospolitej Polskiej lub dotyczą instytucji polskich albo polskiej infrastruktury mieszczących się poza terytorium Rzeczypospolitej Polskiej.

Przewiduje się zmianę formuły Rządowego Zespołu Zarządzania Kryzysowego z opiniodawczo-doradczej na wykonawczo-koordynacyjną działania w zakresie zarządzania kryzysowego na szczeblu centralnym. Nowy katalog kompetencji RZZK będzie umożliwiał maksymalnie skuteczną koordynację działań na szczeblu centralnym jak również wsparcie organów zarządzania kryzysowego niższego szczebla w przypadku wystąpienia lub możliwości wystąpienia sytuacji kryzysowej.

Wzmocnienie skuteczności koordynacji działań w przypadku wystąpienia lub możliwości wystąpienia klęski żywiołowej przewiduje się również na szczeblu województwa, powiatu i gminy przez możliwość tworzenia tzw. sztabów koordynacyjnych. Takie rozwiązania zapewnia formalno-prawne narzędzia pozwalające kreować rozwiązania w zakresie zabezpieczenia lokalnych społeczności w przypadku wystąpienia sytuacji kryzysowych. Sztaby mają być efektywnym narzędziem w zakresie przejmowania kontroli nad sytuacją kryzysową, usuwaniu jej skutków, w tym odtwarzaniu zasobów i usług świadczonych przez infrastrukturę krytyczną (zarządzanie sytuacją kryzysową).

W obszarze szkoleń i ćwiczeń z zakresu zarządzania kryzysowego wprowadza się na poziomie ministra kierującego działem administracji rządowej oraz kierownika urzędu centralnego zadanie w postaci zarządzania, organizacji i prowadzenia szkoleń i ćwiczeń z zakresu zarządzania kryzysowego – w odniesieniu do ćwiczeń krajowych, jak również udziału w ćwiczeniach międzynarodowych.

Na poziomie województwa, powiatu oraz gminy zunifikowano brzmienie przepisów dotyczących szkoleń i ćwiczeń, dając podstawy prawne do wspólnego uczestnictwa w ćwiczeniach na różnych szczeblach, stosownie do lokalnych lub krajowych potrzeb.

Wprowadza się nowe narzędzia wsparcia w sytuacjach kryzysowych, np.

- ✓ zapewnienie przez wojewodę – w przypadku zdarzenia masowego, w szczególności katastrofy w ruchu lotniczym, kolejowym lub morskim – dostępu do informacji członkom rodzin osób poszkodowanych w zdarzeniu w formie dedykowanego numeru kontaktowego;
- ✓ prowadzenie przez wójta burmistrza, prezydenta miasta wykazu szczególnych form udzielania pomocy dla lokalnej społeczności.

W celu zapewnienia odpowiedniej alokacji i wykorzystania środków finansowych na potrzeby zarządzania kryzysowego przewiduje się m.in. następujące rozwiązania:

- ✓ wskazanie, iż samorząd województwa może udzielać pomocy innym jednostkom samorządu terytorialnego w zakresie zapobiegania sytuacjom kryzysowym, przygotowania do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowania w przypadku wystąpienia sytuacji kryzysowych, usuwania ich skutków oraz przywracania sprawnego funkcjonowania organów administracji publicznej i infrastruktury krytycznej. Zakres udzielanej pomocy w danym roku budżetowym będzie określała uchwała sejmiku wojewódzkiego;
- ✓ doprecyzowuje się regulacje w zakresie finansowania z rezerwy celowej realizacji przedsięwzięć związanych z zapobieganiem sytuacjom kryzysowym, przygotowaniem oraz reagowaniem w przypadku ich wystąpienia, a także usuwaniem skutków i odtwarzaniem zasobów.

II. Szczegółowe zmiany.

1) Pojęcie zarządzania kryzysowego

Projekt definiuje zarządzanie kryzysowe, tak jak dotychczas, jako działalność administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym. Natomiast nowym elementem definicji jest minimalizacja ryzyka wystąpienia sytuacji kryzysowych oraz minimalizacja skutków wystąpienia takich sytuacji. Minimalizacja ryzyka wystąpienia sytuacji kryzysowej oparta jest na dwóch pierwszych fazach zarządzania kryzysowego, tj. zapobieganiu oraz przygotowywaniu, natomiast w odniesieniu do minimalizacji skutków mówimy o dwóch kolejnych fazach zarządzania kryzysowego, tj. reagowaniu oraz usuwaniu tychże skutków, w tym przywracaniu sprawnego funkcjonowania organów administracji publicznej i infrastruktury krytycznej.

Uzupełnienie dotychczasowej treści definicji o „przywracanie sprawnego funkcjonowania organów administracji publicznej i infrastruktury krytycznej” związane jest z faktem, iż przepisy ustawy o zarządzaniu kryzysowym przede wszystkim statuują oraz wskazują obowiązki i kompetencje organów administracji publicznej w ramach systemu zarządzania kryzysowego. Ich niezakłócona działalność jest gwarantem działań podejmowanych na rzecz szeroko rozumianej ochrony ludności. Per analogiam należy traktować ochronę infrastruktury krytycznej, co w tym przypadku jest gwarantem ciągłości świadczenia podstawowych usług dla ludności.

Projekt doprecyzowuje ogólną zasadę działania organów administracji publicznej w czasie wojny oraz po wprowadzeniu jednego ze stanów nadzwyczajnych, o których mowa w art. 228 ust. 1 Konstytucji Rzeczypospolitej Polskiej, wskazując, iż zarządzanie kryzysowe jest sprawowane w tym czasie z uwzględnieniem przepisów dotyczących czasu wojny oraz stanów nadzwyczajnych;

- 2) *Definicje (projektowane zmiany w słowniczku ustawy o zarządzaniu kryzysowym (art. 3 ustawy z.k.)*

Infrastruktura krytyczna

Infrastruktura krytyczna definiowana jest co do zasady jak dotychczas. To systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli, kluczowe dla funkcjonowania państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Zmianie ulegną jedynie nazwy trzech z jedenastu systemów infrastruktury krytycznej. Dokonane zostanie połączenie w jeden system – dwóch odrębnych dotychczas systemów: łączności oraz sieci teleinformatycznych. Połączenie systemów łączności oraz sieci teleinformatycznych jest niezbędne ze względu na dwa aspekty. Po pierwsze, dotychczasowo oba systemy posiadały dwóch różnych ministrów koordynujących tj. Ministra Infrastruktury i Budownictwa oraz Ministra Cyfryzacji. Obecnie, oba systemy koordynowane są przez ministra właściwego ds. informatyzacji oraz ministra właściwego ds. łączności – czyli w praktyce Ministra Cyfryzacji. Po drugie, mając na uwadze stosowane przez operatorów infrastruktury krytycznej w obu systemach

rozwiązania techniczne, podstawą w nich są systemy teleinformatyczne, w związku z czym, obecny podział jest sztuczny i mylący. Połączenie obu systemów pozwoli na efektywniejsze tworzenie wytycznych i zaleceń dla operatorów infrastruktury krytycznej z tych systemów, a ponadto, kryteria wyznaczania będą mogły być ujednolicone.

Druga z proponowanych zmian dotyczy dodania w systemie zaopatrzenia w wodę kwestii odprowadzania ścieków. Kwestie zbiorowego zaopatrzenia w wodę są nierozdzielnie związane z odprowadzaniem ścieków, co znajduje odzwierciedlenie w aktach rangi ustawowej, m.in. ustawie z dnia 4 września 1997 r. o działach administracji rządowej, gdzie w ramach działu gospodarka wodna wskazuje się sprawy określenia zasad i warunków zbiorowego zaopatrzenia w wodę przeznaczoną do spożycia przez ludzi oraz zbiorowego odprowadzania ścieków, czy też ustawie z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, w której określa się zasady działalności przedsiębiorstw wodociągowo – kanalizacyjnych, tworzenia warunków do zapewnienia ciągłości dostaw i odpowiedniej jakości wody oraz niezawodnego odprowadzania i oczyszczania ścieków.

Tym samym proponowana w projekcie nowa nazwa systemu „zaopatrzenia w wodę oraz odprowadzania ścieków” skorelowana jest z przyjętą w innych aktach terminologią.

Zagrożenia hybrydowe

Do materii ustawy wprowadza się pojęcia zagrożenia hybrydowego, przez które należy rozumieć zaplanowane i skoordynowane działania prowadzone przez podmioty państwowe lub niepaństwowe w sposób utrudniający przypisanie odpowiedzialności za nie sprawcy. Działanie te zmierzają do osiągnięcia celów politycznych i strategicznych oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora, takie jak polityczne, militarne, ekonomiczne, społeczne, prawne czy informacyjne, w tym z wykorzystaniem mniejszości narodowych, etnicznych i religijnych.

Hybrydowość niesie za sobą złożoność i wielopłaszczyznowość, a skutki działań mogą zaistnieć zarówno na terenie całego kraju, jak i na jego części. Działania te cechują się tym, że są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego jednoznaczne zidentyfikowanie prognozy wojny.

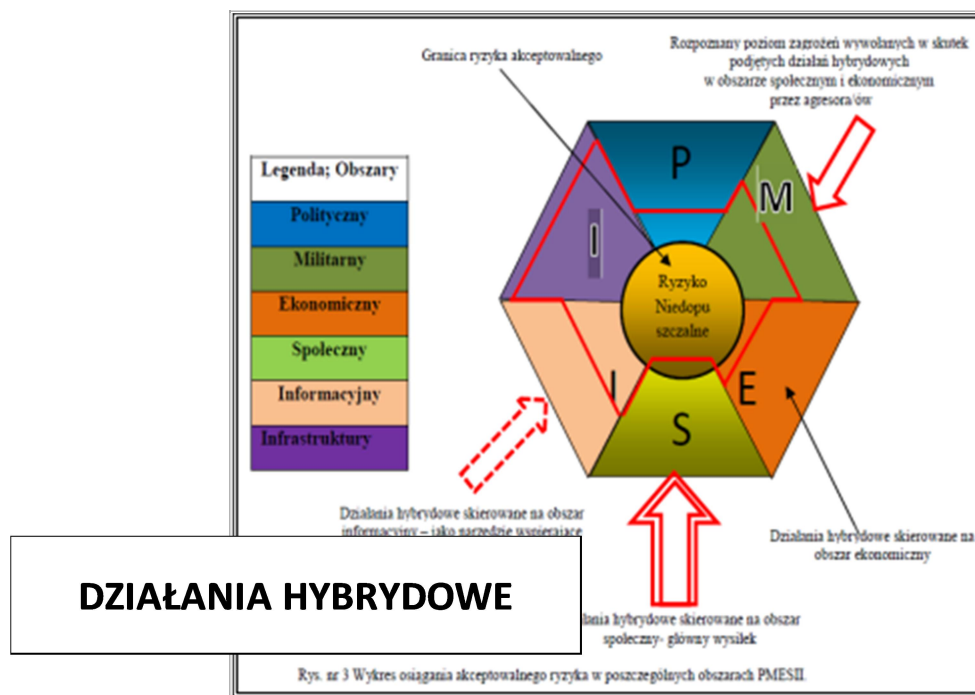
Najważniejszą rolę w przeciwdziałaniu zagrożeniom hybrydowym powinny odgrywać instytucje układu pozamilitarnego z obszaru ogniw ochronnych, gospodarczych, informacyjnych i systemu kierowania wspierane przez siły zbrojne, bowiem nie ma możliwości wyznaczenia dla całości działań hybrydowych podmiotu wiodącego. Ważną rolę odstraszącą odgrywają także siły zbrojne, które muszą mieć możliwość reagowania w sytuacji wystąpienia zagrożeń hybrydowych na wypadek niespodziewanej eskalacji kryzysu. Wojskowe środki używane w ramach działań hybrydowych mogą bowiem kamuflować przygotowania do faktycznego użycia sił zbrojnych (np. niezapowiedziane ćwiczenia militarne, którym towarzyszy duża koncentracja sił zbrojnych).

Skuteczną odpowiedzią na zagrożenia spowodowane działaniami hybrydowymi to ich wczesne rozpoznanie i efektywne reagowanie. Konieczne jest zrozumienie mechanizmów powstawania zagrożeń, a w konsekwencji oszacowanie ryzyka wystąpienia zagrożeń w warunkach normalnego funkcjonowania państwa. Niezbędna jest umiejętność szybkiego reagowania na pierwsze oznaki działań hybrydowych oraz elastyczna, efektywna i skoordynowana reakcja układu militarnego i pozamilitarnego. Podejście takie zapewni wypracowanie odpowiedniej strategii do przeciwdziałania zagrożeniom hybrydowym, a tym samym będzie miało także efekt odstraszący od dalszej eskalacji kryzysu.

Działania hybrydowe charakteryzują się tym, że mogą występować w poszczególnych obszarach PMESII^[1] lub w kilku równocześnie. Do przeprowadzenia skutecznych działań hybrydowych, muszą być zagwarantowane odpowiednie warunki dla powodzenia realizacji zakładanych celów. Dotychczasowe doświadczenia oraz te z przeszłości wskazują, iż obszar społeczny oraz ekonomiczny i informacyjny są najbardziej podatne na działania hybrydowe.

Potencjalny przeciwnik prowadząc działania w danym obszarze lub obszarach wybiera najbardziej podatne i najmniej odporne obszary.

^[1] PMESII – segmentacja środowiska bezpieczeństwa. Dzieli otoczenie na obszar: polityczny, militarny, ekonomiczny, społeczny, infrastruktury, informacyjny.



Powodzenie działań hybrydowych w wybranych obszarach – oddziałuje na pozostałe obszary zmniejszając ich odporność a zwiększając podatność. De facto w wyniku działań hybrydowych, każdy obszar PMESII może pośrednio zostać zaatakowany nawet bez konkretnej ingerencji agresora.

Należy zaznaczyć, że jedną z cech działań hybrydowych jest ich niska przewidywalność oraz możliwość utajnienia prawdziwych intencji przez potencjalnego przeciwnika zwłaszcza w fazie przygotowawczej.

Potencjalny przeciwnik dysponując szerokim wachlarzem możliwych narzędzi do zastosowania, znając najbardziej podatne obszary wykorzysta je w sposób jak najbardziej nieprzewidywalny, a scenariusz działań raz podjętych ulegnie modyfikacji i będzie skierowany na różne obszary w zależności od ich odporności i podjętych przeciwdziałań.

Do realizacji działań hybrydowych potencjalny agresor będzie używać różnych dostępnych przez siebie narzędzi (ataków terrorystycznych, organizacji przestępczych, cyberataku, dezinformacji, niekontrolowanej migracji, blokady gospodarczej i dyskryminacji gospodarczej, spekulacji finansowych, incydentów granicznych, niezapowiedzianych ćwiczeń przy granicy państwa, naruszeń granicy państwowej, nieporozumień na tle kulturalnym i religijnym, zakłóceń systemu zaopatrzenia, celowego manipulowania chorobami zakaźnymi wśród ludzi, jak np. wąglik i rozpowszechnienia

chorób zwierząt jak np.: afrykański pomór świń itp.) w zależności od celów i rozpoznanych obszarów PMESII danego podmiotu w szczególności do obszarów najbardziej podatnych.

Skutki zagrożenia zarówno dla ludności, gospodarki, mienia, infrastruktury czy środowiska będą zależały od rodzaju i skali zdarzeń. W zawiązku z tym należy się liczyć z możliwością paraliżu systemów finansowych, bankowych, telekomunikacyjnych, opieki zdrowotnej, zaopatrzenia w energię, paliwa, żywność i wodę, zakłócenia funkcjonowania struktur państwa, jego rozwoju gospodarczego, bezpieczeństwa przemysłowego w obszarach strategicznych gospodarki, dezinformacją, aż po bezpośrednie zagrożenie dla zdrowia i życia ludności oraz utratę suwerenności i integralności terytorialnej. W skrajnym przypadku działania hybrydowe mogą doprowadzić również do wystąpienia kryzysu polityczno-militarnego.

Wobec różnorodności możliwych zagrożeń, działania instytucji państwa powinny przebiegać według procedur przyjętych dla konkretnych zagrożeń, z uwzględnieniem złożoności poszczególnych scenariuszy^[2].

Planowanie cywilne

Pojęcie planowania cywilnego zostało przeredagowane tak aby w swojej treści zawierało aspekt planowania w zakresie wspierania operacji sojuszniczych prowadzonych w ramach Organizacji Traktatu Północnoatlantyckiego jak również planowania wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań związanych z zapobieganiem i zwalczaniem zagrożeń hybrydowych.

Ryzyko

Mając na względzie konieczność zarządzania ryzykiem – projekt wprowadza szereg definicji odnoszących się do kwestii ryzyka, a mianowicie mapę ryzyka – tj. mapę przedstawiającą obszar geograficzny objęty zasięgiem ryzyka, wraz ze wskazaniem jego poziomu. Obok nowego brzmienia mapy ryzyka, projekt definiuje pojęcie matrycy ryzyka, przez które należy rozumieć graficzny lub opisowy sposób przedstawienia poziomu ryzyka, jako kombinacji prawdopodobieństw wystąpienia zagrożeń oraz ich skutków.

^[2] Materiał opracowany we współpracy z ekspertami Centrum Doktryn i Szkolenia Sił Zbrojnych.

Obok modyfikacji obecnych definicji, projekt wprowadza również nowe pojęcia w tym zakresie, tj.

- ✓ zarządzanie ryzykiem, czyli cykl polegający na ocenie ryzyka, w tym identyfikowaniu zagrożeń, analizie ryzyka i jego szacowaniu, planowaniu i wdrażaniu działań minimalizujących ryzyko, osiągnięciu gotowości do reagowania na zdarzenia niekorzystne oraz okresowej ocenie osiągniętych efektów;
- ✓ szacowanie ryzyka rozumiane jako określenie poziomu akceptacji ryzyka z uwzględnieniem wyników analizy ryzyka oraz posiadanych sił i środków w zakresie organizacyjnym, technicznym i finansowym.

Zarządzanie sytuacją kryzysową

W związku z planowanym podziałem planów zarządzania kryzysowego na plany zarządzania ryzykiem oraz plany reagowania kryzysowego – konieczne stało się wprowadzenie pojęcia zarządzania sytuacją kryzysową.

Zarządzanie sytuacją kryzysową to realizacja działań, polegających na przejmowaniu kontroli nad sytuacją kryzysową, usuwaniu jej skutków, w tym odtwarzaniu zasobów i usług świadczonych przez infrastrukturę krytyczną. Tego typu działania znajdują odzwierciedlenie w planach reagowania kryzysowego.

Moduł zadaniowy

Zdefiniowano, funkcjonujące już w praktyce, pojęcie modułu zadaniowego. Moduł zadaniowy, będący istotnym elementem każdego planu reagowania kryzysowego, to uporządkowane zestawienie przedsięwzięć i zadań przewidzianych do wykonania w sytuacji kryzysowej, obejmujące działania w ramach kompetencji właściwego podmiotu, z wykorzystaniem własnych sił i środków, a także możliwym, zaplanowanym i uzgodnionym wsparciem ze strony innych podmiotów, w zakresie niezbędnym do efektywnego wykonania zadania.

Klęska żywiołowa/katastrofa

Dodatkowo słowniczek do ustawy uzupełnia się o definicje stosowane na użytek ustawy o zarządzaniu kryzysowym.

Przez klęskę żywiołową należy rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, środowiska naturalnego,

oraz dziedzictwa kulturowego lub funkcjonowanie infrastruktury krytycznej, której zwalczanie wymaga zaplanowanych i skoordynowanych działań. Definicja klęski żywiołowej znajduje zastosowanie w przypadku przesłanki wypłaty świadczeń odszkodowawczych, o których mowa w projektowanym art. 26b ustawy z.k. jak również celowości wykorzystania zasobów Centralnej Bazy Magazynowej, o której mowa w projektowanym art. 26c ustawy z.k.

Przez katastrofę rozumie się natomiast zdarzenie, spowodowane działaniem sił natury lub działalnością człowieka, mogące skutkować wystąpieniem sytuacji kryzysowej. Pojęcie katastrofy będzie wykorzystywane na potrzeby tworzenia Raportu o zagrożeniach bezpieczeństwa narodowego, gdyż jednym z jego elementów jest określenie celów strategicznych służących ograniczeniu ryzyka katastrof, z uwzględnieniem realizacji Ramowego Programu Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof. Ponadto jednym z elementów nowotworzonych planów zarządzania ryzykiem jest uporządkowana lista działań w zakresie organizacyjnym, technicznym i finansowym na rzecz ograniczenia ryzyka katastrof;

3) *Planowanie cywilne (zmiany w art. 4 ustawy z.k.)*

Projektowana zmiana brzmienia w art. 4 ustawy z.k. polega na uzupełnieniu katalogu zadań z zakresu planowania cywilnego o prowadzenie oceny ryzyka. Ponadto zmiany obejmują odniesienia do art. 5aa ust. 1, w którym po raz pierwszy w ustawie pojawiają się plany zarządzania kryzysowego w nowym ujęciu.

Dodatkowo przewiduje się uzupełnienie przesłanek niezbędnych do właściwej realizacji zadań z zakresu planowania cywilnego o:

- ✓ ochronę ludności przed skutkami zakłócenia funkcjonowania infrastruktury krytycznej;
- ✓ organizacyjne i techniczne możliwości wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego;
- ✓ organizacyjne i techniczne możliwości wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszników w przypadku ich użycia przy realizacji zobowiązań sojuszników w ramach Organizacji Traktatu Północnoatlantyckiego;

4) *Raport o zagrożeniach bezpieczeństwa narodowego/plany zarządzania ryzykiem/ plany reagowania kryzysowego*

Tak jak dotychczas ma to miejsce, tworzy się Raport o zagrożeniach bezpieczeństwa narodowego, którego celem jest ocena ryzyka wystąpienia zagrożeń oraz określenie celów strategicznych służących ich ograniczeniu. Co do systematyki ustawy dokonano zmiany w kolejności przepisów, wskazując najpierw Raport a dopiero następnie kwestie dotyczące planów. Uznano, iż Raport jako punkt odniesienia do kształtowania planów zarządzania ryzykiem powinien zostać ujęty w systematyce ustawy jako pierwszy.

Raport będzie zawierał następujące elementy:

- ✓ identyfikację i charakterystykę najważniejszych zagrożeń, z uwzględnieniem zagrożeń dla funkcjonowania infrastruktury krytycznej,
- ✓ analizę i szacowanie ryzyka związanego z zagrożeniami,
- ✓ mapy zagrożeń lub mapy ryzyka,
- ✓ matrycę ryzyka,
- ✓ określenie celów strategicznych służących ograniczeniu ryzyka katastrof, z uwzględnieniem realizacji Ramowego Programu Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof,
- ✓ wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych, z uwzględnieniem regionalnych lub lokalnych inicjatyw.

Tak jak dotychczas, na potrzeby opracowania Raportu ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają raporty cząstkowe o zagrożeniach bezpieczeństwa narodowego.

Bez zmian pozostaje kwestia koordynacji przygotowania Raportu, tj. za całość odpowiada dyrektor Rządowego Centrum Bezpieczeństwa, w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego, natomiast w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej – Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

Raport przedkładany jest Radzie Ministrów przez dyrektora Centrum nie rzadziej niż raz na trzy lata. Przedkładany Raport Rada Ministrów przyjmuje w drodze uchwały.

W celu sporządzania Raportu, w szczególności biorąc pod uwagę konieczność zapewnienia jednolitości sporządzania raportów częściowych będących materiałami wyjściowymi dla sporządzania Raportu, Rada Ministrów określi, w drodze rozporządzenia, sposób, tryb i terminy jego opracowywania.

Wynikająca z Raportu ocena ryzyka oraz wnioski zawierające hierarchicznie uporządkowaną listę przedsięwzięć niezbędnych do osiągnięcia celów strategicznych, z uwzględnieniem regionalnych lub lokalnych inicjatyw uwzględnia się w planach zarządzania ryzykiem, planach reagowania kryzysowego oraz innych, opracowywanych w zakresie swojej właściwości przez organy administracji publicznej dokumentach, w tym w strategiach, programach lub planach.

Ponadto na podstawie treści Raportu – dyrektor Centrum będzie sporządzał oraz udostępniał Komisji Europejskiej następujące dokumenty:

- ✓ Streszczenie istotnych elementów krajowej oceny ryzyka
- ✓ Krajową ocenę zdolności zarządzania ryzykiem;

5) Plany zarządzania kryzysowego

Zmodyfikowane pojęcie zarządzania kryzysowego znalazło odzwierciedlenie m.in. w obszarze tworzenia planów na potrzeby zarządzania kryzysowego.

Na potrzeby zarządzania kryzysowego tworzy się plany zarządzania ryzykiem oraz plany reagowania kryzysowego, które zbiorczo będą określane planami zarządzania kryzysowego.

W przypadku zarządzania ryzykiem, tworzone są następujące plany zarządzania ryzykiem:

- ✓ Krajowy Plan Zarządzania Ryzykiem,
- ✓ plany ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych,
- ✓ plany wojewódzkie,

- ✓ plany powiatowe i gminne.

Natomiast na potrzeby zarządzania sytuacją kryzysową, tworzy się Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego, zwane dalej „planami reagowania kryzysowego”.

W skład planów zarządzania ryzykiem wchodzi następujące elementy:

- ✓ charakterystyka zagrożeń, w tym dotyczących infrastruktury krytycznej, uwzględnionej w wykazie infrastruktury krytycznej,
- ✓ mapy ryzyka lub mapy zagrożeń,
- ✓ matryca ryzyka,
- ✓ zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do przejmowania nad nią kontroli,
- ✓ uporządkowana lista działań w zakresie organizacyjnym, technicznym i finansowym na rzecz ograniczenia ryzyka katastrof z uwzględnieniem:
 - hierarchii działań,
 - ram czasowych ich realizacji,
 - podmiotów wiodących oraz współpracujących przy ich wykonywaniu,
 - sposobów finansowania oraz wysokość nakładów finansowych,
 - oceny osiągniętych efektów i wniosków z wdrożonych działań.

W celu zapewnienia spójności treści planów zarządzania ryzykiem ministrów kierujących działami administracji rządowej – przewiduje się, iż plan zarządzania ryzykiem kierownika urzędu centralnego podległego lub nadzorowanego przez ministra jest zatwierdzany przez właściwego ministra i stanowi załącznik do planu zarządzania ryzykiem ministra.

Krajowy Plan Zarządzania Ryzykiem powinien być spójny z programami strukturalnymi. Dlatego też zmiany w ustawie przewidują, iż minister właściwy do spraw rozwoju regionalnego opiniuje Krajowy Plan Zarządzania Ryzykiem pod względem

spójności z tymi programami.

Krajowy Plan Zarządzania Ryzykiem jest przedkładany przez dyrektora Centrum Radzie Ministrów. Rada Ministrów przyjmuje tak przedłożony plan w drodze uchwały.

Załącznikami do Krajowego Planu Zarządzania Ryzykiem stają się plany zarządzania ryzykiem sporządzane przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych, po uprzednim ich uzgodnieniu z dyrektorem Centrum.

Natomiast w skład Krajowego Planu Reagowania Kryzysowego wchodzi następujące elementy:

- ✓ zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków,
- ✓ zasady współdziałania między uczestnikami, w tym wymiana informacji w relacjach krajowych i międzynarodowych,
- ✓ zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych, w tym oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej,
- ✓ tryb uruchamiania niezbędnych sił i środków,
- ✓ organizacja systemu monitorowania zagrożeń, ostrzegania i alarmowania,
- ✓ organizacja łączności,
- ✓ zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
- ✓ zasady oraz tryb oceniania i dokumentowania szkód,
- ✓ procedury uruchamiania rezerw strategicznych,
- ✓ procedury reagowania kryzysowego – Standardowe Procedury Operacyjne,
- ✓ priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej,
- ✓ wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie reagowania kryzysowego,
- ✓ uruchamianie i realizacja zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,

- ✓ wykaz katalogów i modułów zadaniowych.

Rada Ministrów przyjmuje, przedkładany przez dyrektora Centrum, Krajowy Plan Reagowania Kryzysowego w drodze uchwały.

Plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych są uzgadniane z dyrektorem Centrum i stanowią załączniki funkcjonalne do Krajowego Planu Reagowania Kryzysowego.

W skład planów reagowania kryzysowego ministrów i kierowników urzędów centralnych wchodzi następujące elementy:

- ✓ zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków,
- ✓ zadania w zakresie monitorowania zagrożeń i realizacji zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,
- ✓ przedsięwzięcia realizowane w ramach przypisanych katalogów i modułów zadaniowych,
- ✓ organizacja realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Plan reagowania kryzysowego kierownika urzędu centralnego podległego lub nadzorowanego przez ministra jest uzgadniany z właściwym ministrem i stanowi załącznik do planu reagowania kryzysowego ministra.

W skład wojewódzkich planów reagowania kryzysowego wchodzi następujące elementy:

- ✓ elementy, o których mowa w KPRK z wyłączeniem wykazu katalogu i modułów zadaniowych,
- ✓ zadania w zakresie monitorowania zagrożeń i realizacji zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,
- ✓ przedsięwzięcia realizowane w ramach przypisanych katalogów i modułów zadaniowych,
- ✓ zadania określone planami działań krótkoterminowych, o których mowa w art. 92 ustawy z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska,

- ✓ przedsięwzięcia minimalizujące skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności.

W skład powiatowych i gminnych planów reagowania kryzysowego wchodzi następujące elementy:

- ✓ elementy, o których mowa w KPRK z wyłączeniem wykazu katalogu i modułów zadaniowych,
- ✓ zadania w zakresie monitorowania zagrożeń i realizacji zadań stałego dyżuru w ramach podwyższania gotowości obronnej państwa,
- ✓ przedsięwzięcia realizowane w ramach przypisanych katalogów i modułów zadaniowych,
- ✓ przedsięwzięcia minimalizujące skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności.

Projekt przewiduje, iż plany zarządzania kryzysowego podlegają systematycznej aktualizacji, a cykl planowania nie może być dłuższy niż trzy lata.

Cykl planowania realizują właściwe organy administracji publicznej oraz podmioty przewidywane do realizacji przedsięwzięć określonych w planie zarządzania kryzysowego, w zakresie ich dotyczącym.

Plany zarządzania kryzysowego uzgadnia się z kierownikami jednostek organizacyjnych, w zakresie ich dotyczącym, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planie.

Plany postępowania na wypadek wystąpienia sytuacji kryzysowej, opracowane na podstawie innych przepisów stanowią załączniki do planu reagowania kryzysowego właściwego organu administracji publicznej;

6) *Narodowy Program Ochrony Infrastruktury Krytycznej*

W treści NPOIK znajdują odzwierciedlenie ogólne zmiany w obszarze infrastruktury krytycznej, m.in. zmiana nazewnictwa dwóch systemów w definicji infrastruktury krytycznej, podział infrastruktury krytycznej na dwa szczeble, opracowywanie i wdrażanie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego związanych z przeciwdziałaniem zagrożeniom dla

infrastruktury krytycznej oraz wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u wszystkich operatorów infrastruktury krytycznej.

Projekt przewiduje identyfikację oraz wyznaczanie infrastruktury krytycznej w zależności od przypadku, w którym jej zniszczenie lub zakłócenie miałyby niekorzystny wpływ na:

- ✓ funkcjonowanie państwa lub na dany system infrastruktury krytycznej,
- ✓ lokalną społeczność danego województwa.

NPOIK określać będzie więc nie tylko ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy ale również wojewodów – co znalazło odzwierciedlenie w nowym brzmieniu przepisów dotyczących elementów NPOIK. Ponadto wprowadza się nowy, trzyletni okres planistyczny.

Wyznaczanie infrastruktury krytycznej

Dyrektor Centrum sporządza na podstawie szczegółowych kryteriów we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, której zniszczenie lub zakłócenie miałyby niekorzystny wpływ na bezpieczeństwo państwa.

W wykazie wyróżnia się także europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską. Wykaz ma charakter niejawnny.

Dyrektor Centrum:

- ✓ sporządza na podstawie szczegółowych kryteriów we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy, jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, której zniszczenie lub zakłócenie miałyby niekorzystny wpływ na funkcjonowanie państwa lub na dany system. W wykazie wyróżnia się także europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii

Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską. Wykaz ma charakter niejawnny,

- ✓ opracowuje wyciągi z wykazu infrastruktury krytycznej, znajdującej się w danym systemie oraz przekazuje je ministrom kierującym działami administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system,
- ✓ opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się na terenie danego województwa oraz przekazuje właściwemu wojewodzie,
- ✓ informuje o ujęciu w wykazie obiektów, instalacji, urządzeń i usług – ich właścicieli, posiadaczy samoistnych i zależnych,
- ✓ zatwierdza plany ochrony infrastruktury krytycznej obiektów, instalacji, urządzeń i usług po zasięgnięciu opinii ministra kierującego działem administracji rządowej i kierownika urzędu centralnego odpowiedzialnego za system.

Wojewoda natomiast:

- ✓ sporządza na podstawie szczegółowych kryteriów jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, której zniszczenie lub zakłócenie miałyby niekorzystny wpływ na lokalną społeczność danego województwa. Wykaz ma charakter niejawnny,
- ✓ opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się w danym systemie oraz przekazuje ministrom kierującym działami administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system oraz dyrektorowi Centrum,
- ✓ informuje o ujęciu w wykazie operatorów infrastruktury krytycznej;
- ✓ zatwierdza plany ochrony infrastruktury krytycznej obiektów, instalacji, urządzeń i usług po zasięgnięciu opinii ministra kierującego działem administracji rządowej lub kierownika urzędu centralnego odpowiedzialnego za system.

Rada Ministrów określi, w drodze rozporządzenia, sposób realizacji określonych w ustawie obowiązków i współpracy w zakresie programu przez właściwe organy administracji publicznej z operatorami infrastruktury krytycznej, biorąc pod uwagę sprawne wyznaczanie infrastruktury krytycznej oraz zapewnienie jednolitego poziomu bezpieczeństwa infrastruktury krytycznej;

7) *Koordinator ochrony infrastruktury krytycznej*

Operatorzy infrastruktury krytycznej we wszystkich systemach wyznaczają osobę koordynującą działania na linii operator – organy administracji publicznej, tj. koordynatora ochrony infrastruktury krytycznej.

Należy przypomnieć jak od strony organizacyjno-prawnej wygląda stan faktyczny w zakresie osób funkcyjnych zajmujących się, ze strony operatorów infrastruktury krytycznej utrzymywaniem kontaktów z podmiotami państwowymi, właściwymi w zakresie ochrony infrastruktury krytycznej. Przepis art. 6 ust. 5a ustawy z.k. nakłada obowiązek wyznaczenie osoby do kontaktów. Jednakże regulacja ta nie jest w żaden sposób kompletna. Poza czynnością wyznaczenia osoby do kontaktów – brak jest przepisów, które wskazywałyby np. na zakres zadań takiej osoby czy też opisywałyby procedury z jej udziałem. Taki mechanizm nie pojawia się zarówno w ustawie z.k., jak i na poziomie aktów wykonawczych do ustawy o z.k.

Z jednej strony mamy bowiem do czynienia z celowym wyodrębnieniem osoby do wykonywania określonych funkcji, z drugiej strony jednak brak jest wskazania szczegółowych wymagań i obowiązków. Można więc przyjąć, iż jeden operator infrastruktury krytycznej wyznaczy osobę odpowiednio przygotowaną i zajmującą w strukturze organizacyjnej miejsce gwarantujące poprawne i efektywne wykonywanie powierzonych czynności. W innych przypadkach natomiast może to być osoba, wyznaczona wyłącznie w celu wypełnienia obowiązku zawartego w przepisach, w rzeczywistości jednak nieposiadająca realnych narzędzi realizacji powierzonych zadań.

Dotychczasowa praktyka wskazuje na ogromne zróżnicowanie zarówno przygotowania do pełnienia obowiązków jak i ich faktycznej realizacji. Dlatego też rozwiązaniem, mającym być efektywnie działającym narzędziem systemowym w zakresie ochrony infrastruktury krytycznej, a nie jedynie „skrzynką kontaktową”, jest dokonanie instytucjonalizacji osoby do utrzymywania kontaktów, tj. zastąpienie jej funkcją „koordynatora ochrony infrastruktury krytycznej”, któremu jednocześnie zostaną przyznane stosowne kompetencje.

Mając na względzie, iż w obecnym stanie prawnym operatorzy infrastruktury krytycznej mają obowiązek zapewnienia współpracy z administracją publiczną w zakresie ochrony infrastruktury krytycznej czy też wyznaczania osób do utrzymywania kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej –

proponowane rozwiązania, w założeniu stanowią więc usprawnienie rozwiązań w tym zakresie, z wykorzystaniem funkcjonujących już, choć nie do końca efektywnych rozwiązań.

Projekt zmian dotyczy powoływania koordynatorów ochrony infrastruktury krytycznej we wszystkich systemach infrastruktury krytycznej, o których mowa w art. 3 pkt 2 ustawy o zarządzaniu kryzysowym – co jest analogią do obecnie wyznaczonych osób kontaktowych, funkcjonujących u operatorów infrastruktury krytycznej.

W projekcie wskazuje się sposób powoływania koordynatora przez operatora infrastruktury krytycznej, w oparciu o określone kryteria, sposób umiejscowienia koordynatora w strukturze organizacyjnej operatora infrastruktury krytycznej, jak również wskazuje się zadania koordynatora oraz rozwiązania zapewniające ciągłość jego działania i umożliwiające wykonywanie przez niego zadań. Proponowane rozwiązania mają na celu zagwarantowanie efektywnego wykonywania zadań przez koordynatora.

Projekt w zakresie instytucji koordynatora przewiduje następujące propozycje (projektowane art. 5c – 5f).

Projekt przewiduje, iż operator infrastruktury krytycznej wyznacza, w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie koordynatora ochrony infrastruktury krytycznej

Kryteria wyboru koordynatora zostały ustalone w następujący sposób – koordynatorem może być osoba, która:

- ✓ posiada obywatelstwo polskie,
- ✓ posiada wykształcenie wyższe,
- ✓ korzysta z pełni praw publicznych,
- ✓ posiada odpowiednią wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem organizacji, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej,
- ✓ nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe,
- ✓ daje rękojmię zachowania tajemnicy w rozumieniu przepisów ustawy o ochronie informacji niejawnych.

Projekt wskazuje na bezpośrednie podporządkowanie koordynatora organowi zarządzającemu operatora infrastruktury krytycznej. Takie umiejscowienie w strukturze organizacyjnej operatora jest gwarancją prawidłowej i efektywnej realizacji zadań powierzonych koordynatorowi. Bezpośredni dostęp do organu zarządzającego jest konieczny np. ze względu na czynności koordynujące opracowywanie i wdrażanie planów ochrony infrastruktury krytycznej. Czynności związane z realizacją tego zadania wiążą się np. z procesem zbierania danych w ramach struktury organizacyjnej operatora w określonym przedziale czasowym w trakcie sporządzania planów jak również określonych działań w trakcie ich wdrażania – co wymaga wydawania dyspozycji określonym strukturom organizacyjnym operatora.

Operator infrastruktury krytycznej ma obowiązek niezwłocznego informowania o wyznaczeniu pełnomocnika dyrektora Centrum oraz ministra odpowiedzialnego za dany system infrastruktury krytycznej albo kierownika urzędu centralnego za dany system infrastruktury krytycznej, albo właściwego wojewodę.

Projekt określa ponadto zadania koordynatora oraz mechanizmy, które mają zapewnić kwestie organizacyjne i techniczne realizacji tych zadań, wskazując na rolę, jaką ma pełnić, będący pracownikiem operatora, koordynator - tj. rolę koordynującą realizację przedsięwzięć prowadzonych przez operatora infrastruktury krytycznej w zakresie ochrony jego obiektów, instalacji, urządzeń i usług ujętych w jednolitym wykazie infrastruktury krytycznej.

Projekt przewiduje, iż do zadań koordynatora należy:

- ✓ koordynowanie opracowywania i wdrażania planów ochrony infrastruktury krytycznej,
- ✓ monitorowanie działalności operatora w zakresie ochrony infrastruktury krytycznej,
- ✓ utrzymywanie kontaktów z administracją publiczną właściwą w sprawach zarządzania kryzysowego, w tym dyrektorem Centrum, przez przekazywanie i odbieranie określonych kategorii informacji o:
 - zdarzenia zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,
 - spodziewanym lub zaobserwowanym zwiększeniu zapotrzebowania na usługi lub produkty dostarczane przez operatorów infrastruktury krytycznej,

- spodziewanych przerwach lub zakłóceniach w dostawach usług lub produktów dostarczanych przez operatorów infrastruktury krytycznej,
- ✓ sporządzanie i przekazywanie informacji, analiz i sprawozdań dotyczących infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz planów ciągłości działania i odtwarzania na żądanie dyrektora Centrum oraz:
 - właściwego ministra odpowiedzialnego za dany system infrastruktury krytycznej, albo
 - kierownika urzędu centralnego odpowiedzialnego za dany system infrastruktury krytycznej, albo
 - właściwego wojewody
- ✓ sporządzanie raportu o stanie ochrony infrastruktury krytycznej.

Projekt określa zasady sporządzania raportu o stanie ochrony infrastruktury krytycznej. Regulacja przewiduje, iż koordynator sporządza dla organu zarządzającego operatora infrastruktury krytycznej albo rady nadzorczej do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

Przyjęto, iż raport, jako dokument o charakterze sprawozdawczym powinien stanowić roczne podsumowanie realizacji działań podejmowanych w zakresie ochrony infrastruktury krytycznej w podziale na następujące zagadnienia:

- ✓ zapewnienie bezpieczeństwa fizycznego;
- ✓ zapewnienie bezpieczeństwa technicznego;
- ✓ zapewnienie bezpieczeństwa osobowego;
- ✓ zapewnienie bezpieczeństwa teleinformatycznego;
- ✓ zapewnienie bezpieczeństwa prawnego;
- ✓ plany ciągłości działania i odtwarzania.

Wskazane powyżej elementy raportu są spójne z terminologią zawartą w Narodowym Programie Ochrony Infrastruktury Krytycznej.

Raport o stanie ochrony infrastruktury krytycznej jest przekazywany dyrektorowi Centrum oraz:

- ✓ właściwemu ministrowi odpowiedzialnemu za dany system infrastruktury krytycznej, albo
- ✓ kierownikowi urzędu centralnego odpowiedzialnemu za dany system infrastruktury krytycznej, albo
- ✓ właściwemu wojewodzie.

Projekt do uprawnień koordynatora, które warunkują realizację jego zadań, zalicza:

- ✓ możliwość żądania udzielania niezbędnych informacji i wyjaśnień oraz udostępnienia dokumentów będących podstawą udzielanych informacji i wyjaśnień,
- ✓ możliwość wskazywania organowi zarządzającemu operatora infrastruktury krytycznej nieprawidłowości w zakresie ochrony jego obiektów, instalacji, urządzeń i usług oraz formułować zalecenia co do sposobu ich usunięcia.

Projekt przewiduje się, iż operator infrastruktury krytycznej zapewnia koordynatorowi organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do dokumentów i informacji.

Ponadto przewidziano, iż operator infrastruktury krytycznej w związku z realizacją przedsięwzięć w zakresie ochrony jego obiektów, instalacji, urządzeń i usług zapewnia zdolność do ochrony informacji niejawnych. Należy bowiem przyjąć, że informacje wrażliwe wytworzone w ramach opracowywania, uzgadniania oraz realizacji planów ochrony infrastruktury krytycznej oraz informacje wymieniane z właściwymi organami administracji publicznej o zidentyfikowanych zagrożeniach lub zakłóceniach infrastruktury krytycznej oraz podejmowanych działaniach w celu jej ochrony lub odtworzenia, powinny być klasyfikowane jako informacje niejawne. Regulacja, spójnie z duchem ustawy o ochronie informacji niejawnych pozostawia operatorom infrastruktury krytycznej decyzję w odniesieniu do sposobów zapewnienia ochrony informacji niejawnych, w zależności od poziomu niejawności wytwarzanych informacji.

Mając z kolei na uwadze przekazywane do operatorów infrastruktury krytycznej informacje niejawne, stwierdzić należy, iż z wieloletniej praktyki Centrum wynika, iż przekazywane operatorom informacje posiadają najczęściej klauzulę „Zastrzeżone”. Biorąc pod uwagę konieczność niewprowadzania nadmiernych obciążeń kosztowych, zarówno na operatorów infrastruktury krytycznej jak i na współpracującą z nimi administrację, nie jest konieczne wprowadzanie rozwiązań ponad wymagane dla klauzuli

„zastrzeżone”. W celu ułatwienia przetwarzania u operatorów infrastruktury krytycznej informacji niejawnych o klauzuli zastrzeżone oraz wymiany takich informacji z Centrum, Centrum jako gestor SNPI OPAL zachęca operatorów infrastruktury krytycznej do zaimplementowania takiego systemu u operatorów.

Jeżeli jednak podmioty administracji publicznej przewidują przekazywanie informacji niejawnych o wyższych klauzulach niż „Zastrzeżone”, możliwe jest przeprowadzanie postępowań sprawdzających wobec wybranych pracowników operatorów infrastruktury krytycznej do wyższych klauzul. Wnioskowanie o wyznaczenie takich osób do operatora powinno posiadać określenie klauzuli niejawności informacji, która będzie przesyłana z konkretnego urzędu. Ponadto wskazane jest odstąpienie od pobierania kosztów postępowania sprawdzającego, jako że jest ono prowadzone ze względu na uzasadniony wniosek administracji;

8) *Zadania z zakresu ochrony infrastruktury krytycznej*

Projekt przewiduje, iż zadania z zakresu ochrony infrastruktury krytycznej, o których mowa w art. 6 ustawy z.k. zostają uzupełnione o konieczność opracowywania i wdrażania minimalnych wymagań wobec operatorów infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego związanych z przeciwdziałaniem zagrożeniom dla infrastruktury krytycznej.

Aktem wykonawczym do ustawy z.k. w tym zakresie będzie rozporządzenie Rady Ministrów, które określi minimalne wymagania wobec operatorów infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego, mając na uwadze dobór odpowiednich środków związanych z przeciwdziałaniem zagrożeniom dla infrastruktury krytycznej.

Wprowadzenie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego i teleinformatycznego związanych z przeciwdziałaniem zagrożeniom dla infrastruktury krytycznej stanowi istotną zmianę w dotychczasowym systemie ochrony infrastruktury krytycznej. Po raz pierwszy określono kompleksowo wymagania w trzech powiązanych ze sobą sferach bezpieczeństwa i nadano im rangę aktu o charakterze powszechnie obowiązującym. Wprowadzenie w ustawie z.k. upoważnienia ustawowego do wydania minimalnych wymagań wobec operatorów infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa osobowego, fizycznego

i teleinformatycznego w formie rozporządzenia Rady Ministrów będzie punktem odniesienia dla operatorów infrastruktury krytycznej w zakresie możliwości zabezpieczania prowadzonej działalności.

Proponowane rozwiązania pozwolą ograniczyć podatność na możliwość wystąpienia incydentów o charakterze terrorystycznym oraz zwiększy potencjał reagowania na te incydenty, Wprowadzenie pakietu minimalnych wymagań wpłynie również na odporność systemów bezpieczeństwa infrastruktury krytycznej na innego rodzaju zagrożenia, w tym zagrożenia o charakterze hybrydowym, np. sabotaż.

Ponadto wprowadzenie definicji operatora infrastruktury krytycznej powoduje konieczność ujednolicenia siatki pojęciowej w ustawie z.k. Dlatego też konieczne stało się nadanie nowego brzmienia w art. 6 ust. 1 pkt 5 oraz ust. 5, gdyż będzie to czyniło przepisy akt normatywnego czytelnymi;

Konsekwencją wprowadzenia instytucji koordynatora jest uchylene w art. 6 ust. 5a, który dotyczy wyznaczania osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej;

9) *Infrastruktura krytyczna „w budowie”*

Projekt przewiduje, iż dyrektor Centrum we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy infrastruktury krytycznej oraz wojewodami, na bieżąco rozpoznaje obiekty budowlane, urządzenia, instalacje i usługi, będące w fazie projektowania lub budowy, mogące potencjalnie spełniać kryteria infrastruktury krytycznej.

W przypadku rozpoznania obiektów budowlanych, urządzeń, instalacji i usług potencjalnie mogących spełniać kryteria ministrowie kierującymi działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialni za systemy albo wojewodowie podejmują rozmowy z właścicielami, posiadaczami samoistnymi i zależnymi na temat możliwości potencjalnego ujęcia w wykazie infrastruktury krytycznej budowli, urządzeń, instalacji i usług będących w fazie projektowania lub budowy.

W przypadku ujęcia projektowanego lub budowanego obiektu budowlanego, urządzenia, instalacji i usługi w wykazie infrastruktury krytycznej ministrowie

kierującymi działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialni za systemy albo wojewodowie współpracują z operatorami infrastruktury krytycznej w zakresie zapewnienia zgodności fazy projektowej lub budowy z wymaganiami dotyczącymi infrastruktury krytycznej;

10) *Podmioty sprawujące zarządzanie kryzysowe*

Projekt przewiduje, iż zarządzanie kryzysowe sprawuje Rada Ministrów. Pominęto sformułowanie „na terenie Rzeczypospolitej Polskiej”, wskazując jednocześnie na możliwość działania poza granicami kraju.

Przewiduje się, iż w sytuacjach niecierpiących zwłoki zarządzanie kryzysowe sprawuje, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów:

- ✓ minister właściwy do spraw wewnętrznych;
- ✓ minister właściwy do spraw zagranicznych w przypadku gdy skutki zdarzenia dotyczą obywateli polskich przebywających za granicą Rzeczypospolitej Polskiej lub instytucji polskich albo polskiej infrastruktury mieszczących się poza granicami Rzeczypospolitej Polskiej.
- ✓ Minister Obrony Narodowej w przypadku spraw związanych z wypełnianiem zobowiązań sojuszniczych lub uruchamianiem zadań wynikających z Planu Reagowania Obronnego Rzeczypospolitej Polskiej;

Działania podejmowane przez ww. ministrów w sytuacjach niecierpiących zwłoki są realizowane w szczególności przez:

- ✓ uruchamianie przedsięwzięć i procedur zawartych w Krajowym Planie Zarządzania Kryzysowego,
- ✓ uruchamianie przedsięwzięć i procedur systemu zarządzania kryzysowego.

Ww. działania jak i inne podejmowane w sytuacjach niecierpiących zwłoki podlegają rozpatrzeniu na najbliższym posiedzeniu Rady Ministrów. Katalog ten stanowi jedynie wybór narzędzi do realizacji zadań, nie zamykając możliwości wyboru innych rozwiązań;

11) *Rządowy Zespół Zarządzania Kryzysowego*

Projekt przewiduje zmianę formuły Rządowego Zespołu Zarządzania Kryzysowego z opiniodawczo-doradczej na wykonawczo-koordynacyjną działania w zakresie zarządzania kryzysowego na szczeblu centralnym.

Skład Rządowy Zespół Zarządzania Kryzysowego

Projekt przewiduje, iż przy Radzie Ministrów działa Rządowy Zespół Zarządzania Kryzysowego (dalej "Zespół") właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego.

W skład Zespołu wchodzi:

- ✓ Prezes Rady Ministrów - przewodniczący;
- ✓ pozostali członkowie:
 - Minister Obrony Narodowej, minister właściwy do spraw wewnętrznych oraz minister właściwy do spraw zagranicznych - zastępcy przewodniczącego,
 - minister właściwy do spraw administracji publicznej,
 - Minister Koordynator Służb Specjalnych,
 - Szef Biura Bezpieczeństwa Narodowego,
 - dyrektor Centrum – sekretarz Zespołu.

W pracach Zespołu, na prawach członka, biorą udział wyznaczone przez przewodniczącego, w zależności od potrzeb, następujące organy administracji rządowej:

- ✓ ministrowie kierujący działami administracji rządowej niewymienionymi jako członkowie Zespołu,
- ✓ Główny Geodeta Kraju,
- ✓ Główny Inspektor Ochrony Środowiska,
- ✓ Główny Inspektor Sanitarny,
- ✓ Główny Lekarz Weterynarii,
- ✓ Komendant Główny Państwowej Straży Pożarnej,
- ✓ Komendant Główny Policji,
- ✓ Komendant Główny Straży Granicznej,

- ✓ Komendant Główny Żandarmerii Wojskowej,
- ✓ Komendant Służby Ochrony Państwa,
- ✓ Prezes Państwowej Agencji Atomistyki,
- ✓ Prezes Urzędu Lotnictwa Cywilnego,
- ✓ Szef Agencji Bezpieczeństwa Wewnętrznego,
- ✓ Szef Agencji Wywiadu,
- ✓ Szef Obrony Cywilnej Kraju,
- ✓ Szef Służby Kontrwywiadu Wojskowego,
- ✓ Szef Służby Wywiadu Wojskowego,
- ✓ Szef Sztabu Generalnego Wojska Polskiego,
- ✓ Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa.

Przewodniczący może zapraszać do udziału w pracach Zespołu, na prawach członka, inne osoby.

W przypadku nieobecności przewodniczącego, pracami Zespołu kieruje wyznaczony przez niego zastępca.

Członkowie Zespołu mogą wyznaczać do udziału w jego pracach swoich przedstawicieli:

- ✓ Prezes Rady Ministrów – Wiceprezesa Rady Ministrów albo sekretarza lub podsekretarza stanu w Kancelarii Prezesa Rady Ministrów;
- ✓ ministrowie - sekretarza lub podsekretarza stanu;
- ✓ Szef Biura Bezpieczeństwa Narodowego – swojego zastępcę;
- ✓ dyrektor Centrum – swojego zastępcę;
- ✓ organy wyznaczone przez przewodniczącego, w zależności od potrzeb, biorące udział w pracach Zespołu – swoich zastępców;
- ✓ Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa – upoważnionego przedstawiciela.

Do zadań Zespołu należy:

- ✓ zapewnienie koordynacji działań organów administracji rządowej w przypadku wystąpienia lub ryzyka wystąpienia sytuacji kryzysowej;
- ✓ podejmowanie decyzji o konieczności opracowania planu imprezy niebędącej imprezą masową, wraz ze wskazaniem podmiotu wiodącego w zakresie jego opracowania oraz podmiotów współpracujących;
- ✓ podejmowanie decyzji o doborze i uruchomieniu modułów zadaniowych, wobec zagrożeń, które nie zostały ujęte w Krajowym Planie Reagowania Kryzysowego;
- ✓ uruchamianie działań i procedur, o których mowa w Krajowym Planie Reagowania Kryzysowego;
- ✓ uruchamianie przedsięwzięć i procedur, o których mowa w art. 7 ust. 4;
- ✓ dokonywanie oceny stanu bezpieczeństwa kraju, w tym występujących lub potencjalnych zagrożeń;
- ✓ dysponowanie pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej, o których mowa w art. 25, do wykonywania zadań z zakresu zarządzania kryzysowego na terenie kraju;
- ✓ zapewnienie koordynacji działań organów administracji rządowej oraz Sił Zbrojnych Rzeczypospolitej Polskiej w przypadkach, o których mowa w art. 18 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2017 r. poz. 2067, z późn. zm.), art. 22 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, z późn. zm.) oraz art. 11b -11d ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2017 r. poz. 2365, z późn. zm.).

Zespół koordynuje realizację zadań, wynikających z Planu Reagowania Obronnego Rzeczypospolitej Polskiej, do czasu wprowadzenia stanu wojennego i uruchomienia systemu kierowania obroną państwa. Propozycje w tym zakresie były postulowane Radzie Ministrów we wnioskach z ćwiczeń zarządzania kryzysowego NATO-CMX.

Regulacja dotycząca zwiększenia uprawnień dla Rządowego Zespołu Zarządzania Kryzysowego do wypełnienia koordynacyjnej roli w uruchamianiu działań reagowania na narastający kryzys, aż do czasu uruchomienia systemu kierowania obroną państwa, wypełniłaby obecnie lukę prawną i pozwoliłaby na zbieranie i analizę informacji o zagrożeniach przez obecnie dobrze funkcjonujące mechanizmy.

Prezes Rady Ministrów określi, w drodze zarządzenia, organizację i tryb pracy Zespołu, z uwzględnieniem rozwiązań pozwalających na niezwłoczne zebranie się Zespołu i zapewnienie uzyskania pełnej informacji o zdarzeniach będących przedmiotem posiedzenia;

12) *Dyrektor Centrum/Sekretarz Zespołu*

W art. 10 ustawy z.k. przewiduje się uchylenie ust. 2a, w którym wskazano, iż dyrektor Centrum pełni funkcję sekretarza Zespołu. Jest to zmiana porządkowa, gdyż w propozycjach dotyczących nowej formuły Zespołu wskazano dyrektora Centrum jako członka tego Zespołu i jednocześnie jego sekretarza;

13) *Zadania Centrum*

W zadaniach Centrum doprecyzowany przepis, w którym wskazano, iż realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa odbywa się na rzecz Prezesa Rady Ministrów (realizacja zadań stałego dyżuru Prezesa Rady Ministrów w ramach gotowości obronnej państwa). Zmiany w obszarze tworzenia planów spowodowały uzupełnienie katalogu zadań o konieczność opracowywania i aktualizowania Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego.

Dodatkowo do nowych zadań należeć będzie uzgadnianie planów sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz przygotowywanie uruchamiania, w przypadku zaistnienia zagrożeń, procedur związanych z reagowaniem kryzysowym.

Nowe zadania w obszarze współpracy międzynarodowej powodują konieczność odzwierciedlenia w treści zadań. Dlatego też wskazano, iż do zadań Centrum należy:

- ✓ współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej, Organizacji Narodów Zjednoczonych oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej,

- ✓ pełnienie funkcji krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych do spraw wdrażania Ramowego Programu Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof;

14) *Zniesienie obowiązku informacyjnego Centrum*

Uchyła się art. 11a ustawy z.k. Zadanie to było implementacją dyrektywy Parlamentu Europejskiego i Rady w sprawie kompatybilności elektromagnetycznej¹. Pomimo podejmowanych prób nie udało się ustalić z Komisją Europejską okoliczności, w jakich Centrum miałyby ją informować o zastosowanych w Polsce środkach chroniących sieci telekomunikacyjne. W efekcie przytoczony zapis jest przykładem martwej litery prawa i wymaga usunięcia. Tym bardziej, że dyrektywa, która była źródłem cytowanego zapisu, wygasła z dniem 20 kwietnia 2016 r. Jej uchylenie wynika z uchwalenia nowej wersji dyrektywy Parlamentu Europejskiego i Rady w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej;²

15) *Realizacja przez ministrów i kierowników urzędów centralnych zadań dotyczących zarządzania kryzysowego*

Zmiany w zakresie zadań ministrów zostały skorelowane z ogólnymi zmianami dotyczącymi kwestii planowania. Do zadań ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych dotyczące zarządzania kryzysowego, realizowanych w zakresie swojej właściwości, należy:

- ✓ opracowywanie planów zarządzania kryzysowego (zarówno planów zarządzania kryzysowego jak i planów reagowania kryzysowego),
- ✓ organizowanie, prowadzenie i koordynacja szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz biorą udział w ćwiczeniach krajowych

¹ Dyrektywa 2004/108/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 2004 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do kompatybilności elektromagnetycznej oraz uchylająca dyrektywę 89/336/EWG (DzUrz UE L 390/24).

² Zob. szerzej: Dyrektywa 2014/30/UE Parlamentu Europejskiego i Rady z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (Dz. Urz. UE L 96/79).

i międzynarodowych (celem jest to sformalizowanie na szczeblu ministrów i kierowników urzędów centralnych możliwości zarówno organizowania, prowadzenia i koordynowania szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udziału w ćwiczeniach krajowego lub międzynarodowego z zakresu zarządzania kryzysowego, co w założeniu ma umożliwić doskonalenie umiejętności podejmowania bez zwłoki adekwatnych do sytuacji decyzji na szczeblu kierownictwa - tak jak ma to miejsce w przypadku wystąpienia realnej sytuacji kryzysowej),

- ✓ współpraca z operatorami infrastruktury krytycznej przy tworzeniu planów ochrony infrastruktury krytycznej oraz planu zarządzania kryzysowego (w szczególności w przypadku ministrów będących koordynatorami poszczególnych systemów infrastruktury krytycznej).

Redefiniowaniu uległy zadania zespołów zarządzania kryzysowego ministrów i kierowników – nowy katalog zadań zespołów zarządzania kryzysowego na tym szczeblu wygląda następująco:

- ✓ dokonywanie okresowej oceny ryzyka na potrzeby Raportu,
- ✓ dokonywanie okresowej oceny gotowości do reagowania w zakresie organizacyjnym, technicznym i finansowym,
- ✓ opiniowanie projektów planów zarządzania kryzysowego,
- ✓ opiniowanie wykazu infrastruktury krytycznej w ramach swoich właściwości,
- ✓ wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom;

16) *Wdrażanie Ramowego Programu Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof*

Dodanie art. 13a ma na celu realizację skutecznego wdrażania Ramowego Programu Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof – oprócz wskazania Centrum jako punktu kontaktowego, przewiduje się, iż ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie będą ten program wdrażać oraz przekazywać dyrektorowi Centrum, w wyznaczonym terminie,

raporty dotyczące wdrażania oraz inne informacje, niezbędne do realizacji zadań w tym zakresie przez Centrum;

17) *Zadania wojewody w sprawach zarządzania kryzysowego; wojewódzkie plany zarządzania kryzysowego; wojewódzki zespół zarządzania kryzysowego*

Jak wspomniano już wcześniej – na wszystkich szczeblach zarządzania przewiduje się wprowadzenie jednolitej terminologii w kwestii organizowania, prowadzenia i koordynacji szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udziału w ćwiczeniach krajowych i międzynarodowych. Tak samo sformułowany przepis będzie również funkcjonował na szczeblu wojewody.

Uchyła się zadanie wojewody polegające na zapobieganiu, przeciwdziałaniu i usuwaniu skutków zdarzeń o charakterze terrorystycznym. Zasady prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tychże działań znajdują się w ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452). Dlatego też uznano, iż wskazywanie zadań w tym zakresie w ustawie z.k. jest zbędne. Jest to zmiana o charakterze porządkowym. Pozostawiono natomiast przepis wskazujący na obowiązek współpracy organów zarządzania kryzysowego na wszystkich szczeblach z Szefem ABW w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym.

Dodatkowo wprowadza się instytucję tzw. sztabu koordynacyjnego, będącego formalno-prawnym narzędziem pozwalający kreować rozwiązania w zakresie zarówno przygotowania lokalnej społeczności na wypadek wystąpienia klęski żywiołowej jak i koordynacji usuwania skutków tych klęsk.

Wojewoda może tworzyć sztaby koordynacyjne złożone z:

- ✓ kierownika komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim,
- ✓ kierowników zespolonych służb, inspekcji i straży wojewódzkich,
- ✓ osób zatrudnionych w urzędzie wojewódzkim lub w jednostkach organizacyjnych służb, inspekcji i straży wojewódzkich,

- ✓ osób zatrudnionych w Państwowym Gospodarstwie Wodnym Wody Polskie oraz Instytucie Meteorologii i Gospodarki Wodnej,
- ✓ szefa wojewódzkiego sztabu wojskowego lub jego przedstawiciela,
- ✓ przedstawicieli samorządu województwa, wyznaczonych przez marszałka województwa,
- ✓ innych osób zaproszonych przez przewodniczącego.

Wojewoda wyznacza osobę kierującą sztabem koordynacyjnym oraz określa jego skład, zadania, tryb i miejsce pracy;

18) *Samorząd województwa*

Projekt przewiduje, iż samorząd województwa w ramach realizacji zadań, o których mowa w art. 8a ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2018 r., poz. 913), będzie mógł udzielać pomocy innym jednostkom samorządu terytorialnego w zakresie zapobiegania sytuacjom kryzysowym, przygotowania do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowania w przypadku wystąpienia sytuacji kryzysowych, usuwania ich skutków oraz przywracania sprawnego funkcjonowania organów administracji publicznej i infrastruktury krytycznej.

Zakres udzielanej pomocy w danym roku budżetowym każdorazowo będzie określała uchwała sejmiku wojewódzkiego;

19) *Wojewódzkie centrum zarządzania kryzysowego*

Katalog zadań wojewódzkiego centrum zarządzania kryzysowego uzupełnia się o zadanie zapewnienia obsługi numer kontaktowego ustanawianego przez wojewodę w przypadku zdarzenia masowego, w szczególności katastrofy w ruchu lotniczym, kolejowym lub morskim. Wojewoda – zgodnie z projektowanymi regulacjami – zapewnia bowiem dostęp do informacji członkom rodzin osób poszkodowanych w zdarzeniu w postaci dedykowanego zdarzeniu numeru kontaktowego;

20) *Zadania starosty w sprawach zarządzania kryzysowego; powiatowy zespół zarządzania kryzysowego*

W zakresie zadań starosty, podobnie jak na pozostałych szczeblach zarządzania kryzysowego, dokonano korelacji terminologii w zakresie organizowania, prowadzenia i koordynacji szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udziału (możliwości brania udziału) w ćwiczeniach krajowych i międzynarodowych.

Wprowadza się obowiązek informacyjny dla starosty. Powinien on informować wojewodę, co najmniej raz w roku, o stanie realizacji zadań z zakresu zarządzania kryzysowego na obszarze powiatu.

Sztaby koordynacyjne będą mogły być powoływane na szczeblu powiatu – na potrzeby realizacji zadań starosty. Starosta wyznacza osobę kierującą sztabem koordynacyjnym oraz określa jego skład, zadania, tryb i miejsce pracy;

21) *Powiatowe centra zarządzania kryzysowego*

Mając na względzie uzyskanie pełnej funkcjonalności powiatowego centrum zarządzania kryzysowego przewiduje się, iż centra te mają być obsługiwane przez pracowników starostwa powiatowego.

Aktualnie pczk funkcjonują najczęściej na bazie komend powiatowych (miejskich) Państwowej Straży Pożarnej, nieliczne pracują w systemie 24 - godzinnym. W wypadku wystąpienia sytuacji kryzysowej, aktualne usytuowanie i nieodokreślone zasady obsługi pczk utrudniają lub wręcz uniemożliwiają wykonywanie przez starostę i zarząd powiatu zadań z zakresu zarządzania kryzysowego.

Proponowane rozwiązania pozwalają na uzyskanie jednoznacznego określenia usytuowania i zasad funkcjonowania pczk a co za tym idzie zapewnienie rozwiązań organizacyjnych niezbędnych dla zapewnienia ciągłości działania;

22) *Zadania wójta, burmistrza, prezydenta miasta w sprawach zarządzania kryzysowego; gminne (miejskie) centra zarządzania kryzysowego*

Analogicznie do ww. rozwiązań – na poziomie wójta, burmistrza i prezydenta miasta należy organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu

zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych.

Uchyła się zadanie wójta, burmistrza, prezydenta miasta polegające na zapobieganiu, przeciwdziałaniu i usuwaniu skutków zdarzeń o charakterze terrorystycznym. Zasady prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tychże działań znajdują się w ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452). Dlatego też uznano, iż wskazywanie zadań w tym zakresie w ustawie z.k. jest zbędne. Jest to zmiana o charakterze porządkowym. Pozostawiono natomiast przepis wskazujący na obowiązek współpracy organów zarządzania kryzysowego na wszystkich szczeblach z Szefem ABW w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym.

Wprowadza się obowiązek sprawozdawczy polegający na informowaniu starosty co najmniej raz w roku o stanie realizacji zadań z zakresu zarządzania kryzysowego na obszarze gminy.

Analogicznie do ww. rozwiązań umożliwia się tworzenie przez wójta, burmistrza, prezydenta miasta sztabów koordynacyjnych. Wójt, burmistrz, prezydent miasta wyznacza osobę kierującą sztabem koordynacyjnym oraz określa jego skład, zadania, tryb i miejsce pracy;

23) *Gminne centra zarządzania kryzysowego*

Katalog zadań gminnego centrum zarządzania kryzysowego zostaje uzupełniony o prowadzenie wykazu szczególnych form udzielania pomocy dla lokalnej społeczności. Zadanie obejmuje realizację czynności stricte obsługowych, m.in. obsługę przyjmowanych wniosków czy też aktualizację prowadzonego w gminie wykazu.

Ponadto w celu realizacji zadań z zakresu zarządzania kryzysowego wójt, burmistrz, prezydent miasta zapewnia całodobowy punkt kontaktowy. Tak jak dotychczas możliwe jest utworzenie gminnego (miejskiego) centrum zarządzania kryzysowego;

24) „ALERT RCB”

Wprowadza się przepis umożliwiający operatorom możliwości podjęcia decyzji ograniczającej wysyłanie komunikatu do kart SIM zainstalowanych i wykorzystywanych w urządzeniach telemetrycznych, np. miernikach, lokalizatorach GPS i innych urządzeniach przesyłających na odległość dane pomiarowe.

Powszechne jest bowiem gromadzenie danych, pozwalających na skuteczniejsze ich wykorzystywanie i w rezultacie optymalizację procesów, w jakich są one wykorzystywane. Telemetria znajduje zastosowanie w procesach, które na bieżąco kontrolują dane dotyczące funkcjonowania elementów systemów wielu przedsiębiorstw. Zastosowanie systemów z kartami SIM (telemetrycznymi) umożliwia na bieżąco otrzymywanie informacji o działaniu poszczególnych systemów. Dostęp do bieżących danych, obrazujących działanie poszczególnych elementów, pozwala na dokonywanie stosownych zmian w zachodzących procesach w czasie rzeczywistym. Ponadto w przypadku awarii jakiegoś elementu systemu – osoby odpowiedzialne otrzymują o tym informację – mogą więc natychmiast podjąć stosowne działania naprawcze.

Innym przykładem jest system lokalizacji GPS za pomocą kart SIM (telemetrycznych). Znajduje on zastosowanie zarówno w monitorowaniu transportu drogowego jak i w zdalnym określaniu lokalizacji pojazdów. Stosowanie takiego rozwiązania przynosi korzyść w postaci stałego monitoringu pojazdów i zdolności optymalizowania ich tras. Możliwe jest również monitorowanie parametrów funkcjonowania tych pojazdów, np. poziomu paliwa, prędkości z jakimi się poruszają, czy też liczby przejechanych kilometrów.

Powyżej wskazano tylko dwa przykłady używania kart SIM operatorów, na które nie ma potrzeby wysyłania ALERT-ów RCB. Projekt przewiduje, iż operator, stosownie do swoich możliwości technicznych, może podjąć decyzję o niewysyłaniu komunikatu do użytkownika końcowego, jeżeli będzie to karta SIM znajdującą się w urządzeniu telemetrycznym.

Takie rozwiązanie pozwoli ograniczyć liczbę wysyłanych komunikatów przede wszystkim do osób fizycznych na zagrożonym obszarze.

Ponadto proponuje się aby operator, po wysłaniu komunikatu, niezwłocznie przekazywał dyrektorowi Centrum informację o liczbie kart SIM użytkowników końcowych, do których komunikat został wysłany oraz informację o liczbie kart SIM użytkowników końcowych, do których komunikat został dostarczony.

Operator przekazując ww. dane powinien powiązać je z obszarem na który komunikat został wysłany. Dane liczbowo – obszarowe pozyskiwane w ten sposób są danymi niezbędnymi do budowania mapy ze wskazaniem zagrożenia, obszaru objętego zagrożeniem oraz szacunkową liczbą osób, które mogą być dotknięte skutkami tychże zagrożeń.

Pozyskiwane w ten sposób dane pozwolą również na ocenę skuteczności tego systemu oraz wskazanie ewentualnych kierunków jego dalszego rozwoju;

25) *Narzędzia wsparcia działań w zakresie zarządzania kryzysowego*

Imprezy masowe

Przewiduje się, iż w przypadku organizacji imprezy niebędącej imprezą masową w rozumieniu przepisów ustawy z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych, a stwarzającej możliwość wystąpienia sytuacji kryzysowej, zwaną dalej opracowuje się ramowy plan zabezpieczenia tego typu imprezy.

Uzupełnieniem regulacji ustawowych jest akt wykonawczy w postaci rozporządzenia Rady Ministrów, która określi w drodze rozporządzenia elementy ramowego planu zabezpieczenia imprezy, mając na względzie niezakłócony przebieg imprezy oraz bezpieczeństwo osób biorących w niej udział.

Celem jest zapewnienie właściwego zabezpieczenia tego typu imprez, które wymagają zaplanowania działań z zakresu ratownictwa i zarządzania kryzysowego ze względu na bezpieczeństwo uczestników.

Obecnie, w przypadku organizacji imprezy niebędącej imprezą masową w rozumieniu ustawowym, rozwiązania przyjmowane często ad hoc nie regulują w należyty sposób obowiązku organizatora imprezy w zakresie realizacji zadań planistycznych, podjętych na właściwym poziomie merytorycznym, z odpowiednim wyprzedzeniem, we współpracy z organami i służbami właściwymi w sprawach zapewnienia bezpieczeństwa i porządku publicznego oraz w sprawach zarządzania kryzysowego.

Proponowane rozwiązania pomogą właściwym organom, służbom i podmiotom optymalnie zaplanować działania, mające zapewnić bezpieczeństwo i porządek publiczny podczas tego typu imprez.

Zdarzenie masowe

W przypadku zdarzenia masowego, w szczególności katastrofy w ruchu lotniczym, kolejowym lub morskim, wojewoda zapewnia dostęp do informacji członkom rodzin osób poszkodowanych w zdarzeniu.

W celu zapewnienia dostępu do informacji wojewoda udostępnia na stronie podmiotowej Biuletynu Informacji Publicznej urzędu wojewódzkiego, dedykowany zdarzeniu, numer kontaktowy. Obsługę tego numeru zapewnia wojewódzkie centrum zarządzania kryzysowego.

Szczególne formy udzielania pomocy dla lokalnej społeczności

Na potrzeby zarządzania sytuacją kryzysową wójt, burmistrz, prezydent miasta określa szczególne formy udzielania pomocy dla lokalnej społeczności.

W takim przypadku wójt, burmistrz, prezydent miasta sporządza wykaz szczególnych form udzielania pomocy dla lokalnej społeczności oraz informuje, w sposób w zwyczajowo przyjęty, mieszkańców o możliwości ujęcia w tym wykazie.

Ujęcie w wykazie następuje na wniosek osoby wymagającej wsparcia lub jej opiekuna prawnego. Obsługę wykazu zapewnia powiatowe centrum zarządzania kryzysowego;

26) *Koordynowanie wsparcia SZ RP*

Doprecyzowano kwestię włączania Sił Zbrojnych RP do realizacji zadań z zakresu zarządzania kryzysowego. Koordynowanie udziału oddziałów Sił Zbrojnych w realizacji tych zadań, w zależności od obszaru występowania zagrożeń, zapewniają odpowiednio właściwe terytorialnie organy zarządzania kryzysowego:

- ✓ wojewoda,
- ✓ starosta,
- ✓ wójt, burmistrz, prezydent miasta;

Koordynowanie powierza się również - w przypadku działań ratowniczych - strażakowi kierującemu akcją ratowniczą.

Koordynowanie obejmuje przedsięwzięcia mające na celu sprawne włączenie oddziałów Sił Zbrojnych do realizacji zadań, z uwzględnieniem czasu i miejsca ich

użycia oraz sposobu współdziałania z innymi podmiotami. Zadania przewidziane dla Sił Zbrojnych RP ww. organy oraz funkcjonariusz Państwowej Straży Pożarnej kierujący akcją ratowniczą przekazują wyłącznie dowódcom pododdziałów lub oddziałów SZ RP;

27) Dysponowanie SZ RP w sytuacjach niecierpiących zwłoki

Projekt przewiduje, iż w sytuacjach niecierpiących zwłoki, Minister Obrony Narodowej, na wniosek ministra właściwego do spraw wewnętrznych, może przekazać do jego dyspozycji oddziały Sił Zbrojnych wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego oraz zwalczania zagrożeń hybrydowych.

Proponowana regulacja ma w założeniu zapewnić szybką ścieżkę decyzyjną w sytuacjach niecierpiących zwłoki, w zakresie zadysponowania i użycia SZ RP w realizacji zadań z zakresu zarządzania kryzysowego;

28) Alokacja środków finansowych na potrzeby zarządzania kryzysowego

Doprecyzowaniu ulega regulacja dotycząca dysponowania środkami finansowymi z rezerwy celowej na potrzeby zarządzania kryzysowego. Przewiduje się, iż środki finansowe z rezerwy celowej będą przeznaczane na realizację przedsięwzięć związanych z zapobieganiem sytuacjom kryzysowym, przygotowaniem oraz reagowaniem w przypadku ich wystąpienia, a także usuwaniem skutków i odtwarzaniem zasobów – w szczególności na wydatki związane z:

- ✓ zorganizowaniem własnego centrum zarządzania kryzysowego,
- ✓ przygotowaniem systemu ostrzegania i alarmowania ludności,
- ✓ organizacją szkoleń i ćwiczeń,
- ✓ wykrywaniem, monitorowaniem i oceną zagrożeń,
- ✓ utrzymaniem i odtwarzaniem niezbędnych zasobów materiałowych,
- ✓ podejmowaniem działań eliminujących zagrożenia,
- ✓ działaniami prowadzonymi w sytuacji kryzysowej,
- ✓ realizacją umów i porozumień wykorzystywanych na potrzeby działań w sytuacji kryzysowej,
- ✓ pokrycie kosztów wykorzystania sprzętu, usług, paliwa i części zamiennych wykorzystywanych w sytuacji kryzysowej,

- ✓ udzielaniem pomocy, w tym pomocy finansowej, innym jednostkom samorządu terytorialnego;

29) *Ochrona ludności*

Projekt przewiduje, iż rada gminy, powiatu i sejmik wojewódzki w formie uchwał określają sposób utrzymania niezbędnych zasobów pozwalających na utrzymanie realizacji zadań z zakresu zarządzania kryzysowego przez okres minimum 3 dni. Jednocześnie wskazano formy, w jakich można przygotować ww. zasoby, tj. przez:

- ✓ uzupełnienie istniejących magazynów przeciwpowodziowych o zasoby niezbędne do działania w innych sytuacjach kryzysowych niż powódzie,
- ✓ zawarcie umów pozwalających otrzymać niezbędne zasoby w sytuacji kryzysowej,
- ✓ utworzenie niezależnego magazynu.

Przewiduje się, iż osobom, które na wezwanie organów zarządzania kryzysowego włączyły się do ćwiczeń związanych z zarządzaniem kryzysowym lub do działań polegających na usuwaniu skutków zagrożenia lub klęski żywiołowej, i w czasie tych ćwiczeń lub działań uległy wypadkowi, oraz członkom rodziny osób zmarłych wskutek takiego wypadku, przysługują świadczenia odszkodowawcze w trybie i na zasadach wynikających z ustawy z dnia 30 października 2002 r. o zaopatrzeniu z tytułu wypadków lub chorób zawodowych powstałych w szczególnych okolicznościach.

Jako element wsparcia ochrony ludności ma poziomie centralnym przewiduje się utworzenie – na potrzeby ochrony ludności – w przypadku wystąpienia lub możliwości wystąpienia sytuacji kryzysowej, w tym spowodowanej klęską żywiołową tworzy się Centralną Bazę Magazynową (dalej „CBM”).

Konieczność utworzenia CBM została wskazana w dokumencie rządowym pt. „Strategia na rzecz odpowiedzialnego rozwoju do roku 2020 (z perspektywą do 2030 r.)”. W dokumencie tym (str. 362) wskazano jako projekt strategiczny utworzenie CBM – tj. centrum logistycznego na potrzeby ochrony ludności/obrony cywilnej, w oparciu o szkoły Państwowej Straży Pożarnej (Bydgoszcz, Częstochowa, Kraków). Celem utworzenia CBM „jest zapewnienie wsparcia ludności cywilnej w warunki do przeżycia zarówno w sytuacjach kryzysowych, klęsk żywiołowych, jak i podczas zagrożeń militarnych.”

W chwili obecnej konieczne jest uzupełnienie mechanizmu szybkiego i efektywnego wsparcia logistycznego na szczeblu centralnym. Obecnie na szczeblu centralnym niezbędne zasoby na sytuacje kryzysowe gromadzi Agencja Rezerw Materiałowych (dalej „ARM”) w ramach rezerw strategicznych. Rzeczywiste wydarzenia przy których próbowano wykorzystać sprzęt znajdujący się na stanie ARM, wykazało iż sprzęt ten jest nowy, niezarejestrowany i nie jest gotowy do użycia. Ponadto ARM nie zapewnia obsługi tego sprzętu, jak i dostarczenia tego sprzętu na miejsce. Proponowana CBM pozwoli wyszkolić obsługę sprzętu specjalistycznego, zapewni jego dostawy na miejsce działań oraz uzupełni zasoby wykorzystywane rutynowo przez służby oraz pozwoli przygotować zasoby do wykorzystania w razie potrzeby. CBM będzie też mogła stanowić podstawę wyposażenia niektórych specjalistycznych formacji obrony cywilnej (szczegółowe zasady wykorzystywania sprzętu CBM powinny być elementem Narodowego Programu Rozwoju Obrony Cywilnej).

CBM tworzy Komendant Główny PSP na bazie jednostek krajowego systemu ratowniczo – gaśniczego, o którym mowa w ustawie z dnia 24 sierpnia 1991r. o ochronie przeciwpożarowej (Dz. U. z 2018 r. poz. 620).

Do dysponowania zasobami CBM są uprawnieni:

- ✓ Rządowy Zespół Zarządzania Kryzysowego,
- ✓ minister właściwy do spraw wewnętrznych,
- ✓ wojewodowie,
- ✓ Komendant Główny PSP.

W celu włączenia informacji o zasobach CBM do baz danych tworzonych na potrzeby planów zarządzania kryzysowego, Komendant Główny PSP nie rzadziej niż co 6 miesięcy informuje wojewodów, ministra właściwego do spraw wewnętrznych oraz dyrektora Centrum o aktualnym stanie wyposażenia CBM.

Projekt przewiduje uzupełnienie regulacji ustawowych o upoważnienie dla ministra właściwego do spraw wewnętrznych do określenia w drodze rozporządzenia miejsca lokalizacji, normy wyposażenia, sposób zarządzania i administrowania obiektami oraz asortymentem CBM, biorąc pod uwagę czas dostarczenia niezbędnych zasobów do każdego województwa oraz rodzaje zagrożeń w nich występujących.

III. Zmiany w innych ustawach

Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej

W ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2018 r. poz. 1459, z późn. zm.) projekt wprowadza zmiany, które odnoszą się do kwestii poruszonych przez Najwyższą Izbę Kontroli w trakcie kontroli funkcjonowania Obrony Cywilnej. Kontrola wykazała bowiem, iż:

- ✓ Szef OCK nie ma wpływu na kształtowanie budżetu OC,
- ✓ żaden akt normatywny powszechnie obowiązujący nie wskazuje urzędu obsługującego Szefa OCK,
- ✓ wadliwie funkcjonuje planowanie zadań w ramach OC (wskazano kto zatwierdza plan krajowy OC, ale nie wskazano kto i jak go wykonuje).

Dodatkowo MSZ w swoim opracowaniu pt. II Raport o implementacji i upowszechnianiu międzynarodowego prawa humanitarnego w Rzeczypospolitej Polskiej (MSZ 2011) wskazuje na niezgodność sytuacji prawnej OC z Polsce z prawem międzynarodowym.

Niezgodność polega na tym, że organami OC są osoby odpowiedzialne za przygotowania obronne i działania obronne, podczas gdy Protokół II do konwencji Genewskich zakazuje personelowi OC wykonywania działań, które strona przeciwna mogłaby uznać za niekorzystne dla siebie.

Dlatego też zmiany w ustawie o powszechnym obowiązku obrony Rzeczypospolitej Polskiej przewidują, iż:

- ✓ Szefa Obrony Cywilnej Kraju w randze sekretarza albo podsekretarza stanu powołuje i odwołuje Prezes Rady Ministrów na wniosek ministra właściwego do spraw wewnętrznych. W efekcie Szef OCK jako członek kierownictwa resortu będzie miał wpływ na kształtowanie budżetu OC,
- ✓ Zastępcą Szefa Obrony Cywilnej Kraju jest Komendant Główny Państwowej Straży Pożarnej. Na wniosek Szefa Obrony Cywilnej Kraju uzgodniony z ministrem właściwym do spraw wewnętrznych, Prezes Rady Ministrów może powołać dodatkowo Zastępców Szefa Obrony Cywilnej Kraju,
- ✓ obsługę Szefa OCK oraz zastępców Szefa OCK zapewnia Komenda Główna Państwowej Straży Pożarnej. Wskazano tym samym jednoznacznie jednostkę organizacyjną zapewniającą obsługę Szefa OCK,

- ✓ dokonano rozdziału zadań OC realizowane w czasie pokoju w ramach przygotowania OC od kierowania formacjami OC w czasie konfliktu zbrojnego. Jako osoby kierujące formacjami OC wskazano odpowiednich komendantów PSP, którzy automatycznie będą wykluczeni z realizacji zadań obronnych. Dlatego też, zgodnie z propozycją, terenowymi organami obrony cywilnej są:
 - wojewoda – szef obrony cywilnej województwa,
 - starosta – szef obrony cywilnej powiatu,
 - wójt (odpowiednio burmistrz lub prezydent miasta) – szef obrony cywilnej gminy (miasta).”

Natomiast zastępcami szefów obrony cywilnej są odpowiednio:

- właściwy miejscowo komendant wojewódzki Państwowej Straży Pożarnej,
- właściwy miejscowo komendant powiatowy Państwowej Straży Pożarnej,
- osoba powołana przez wójta lub burmistrza (prezydenta miasta).

W razie ogłoszenia mobilizacji, w czasie stanu wojennego oraz w czasie wojny lub okupacji wskazany Zastępca Szefa Obrony Cywilnej Kraju, zastępca szefa obrony cywilnej województwa, zastępca szefa obrony cywilnej powiatu oraz zastępca szefa obrony cywilnej gminy (miasta) pełnią funkcje dowódców formacji OC na swoim terenie.

Przewiduje się wydanie rozporządzenia Rady Ministrów, która określi szczegółowy zakres działania Szefa Obrony Cywilnej Kraju oraz szefów obrony cywilnej województw, powiatów i gmin, dowódców formacji OC kraju, województwa, powiatu i gminy, jak również zasady i tryb kierowania oraz koordynowania przez nich przygotowań i realizacji przedsięwzięć obrony cywilnej.

Powyższe rozwiązania zmierzają do ustalenia czytelnych struktur zarządzania formacjami obrony cywilnej.

Ponadto projekt wskazuje na tworzenie formacji obrony cywilnej w oparciu o jednostki ochrony przeciwpożarowej, o których mowa w art. 15 ust. 1 i ust. 2-7 ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2019 r. poz. 730) oraz jednostki funkcjonujące w ramach systemu Państwowe Ratownictwo Medyczne, o których mowa w art. 32 ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. 2017 r. poz. 2195, z późn. zm.).

W przypadku jednostek ochrony przeciwpożarowej są to:

- ✓ jednostki organizacyjne Państwowej Straży Pożarnej,
- ✓ zakładowe straże pożarne,
- ✓ zakładowe służby ratownicze,
- ✓ gminne zawodowe straże pożarne,
- ✓ powiatowe (miejskie) zawodowe straże pożarne,
- ✓ terenowe służby ratownicze,
- ✓ ochotnicze straże pożarne,
- ✓ związek ochotniczych straży pożarnych,

Wyłączeniu podlegają jednostki organizacyjne Wojskowej Ochrony Przeciwpożarowej.

W przypadku jednostek systemu Państwowe Ratownictwo Medyczne są to:

- ✓ szpitalne oddziały ratunkowe,
- ✓ zespoły ratownictwa medycznego, w tym lotnicze zespoły ratownictwa, wchodzące w skład podmiotu leczniczego będącego samodzielnym publicznym zakładem opieki zdrowotnej albo jednostką budżetową, albo spółką kapitałową, w której co najmniej 51% udziałów albo akcji należy do Skarbu Państwa lub jednostki samorządu terytorialnego, na których świadczenia zawarto umowy o udzielanie świadczeń opieki zdrowotnej.

Projekt przewiduje, iż w odniesieniu do osób pełniących służbę lub zatrudnionych w ww. jednostkach podlegają oni reklamowaniu od służby wojskowej.

Projektują zmiany w ustawie o powszechnym obowiązku obrony Rzeczypospolitej Polskiej – dodano regulacje, które w zakładają korelację obiektów szczególnie ważnych dla bezpieczeństwa państwa z obiektami zapewniającymi sprawne funkcjonowanie organów administracji publicznej, instytucji i przedsiębiorców, co ma w założeniu umożliwić zapewnienie jednolitych rozwiązań w zakresie ich szczególnej ochrony.

W tym celu przewiduje się, iż Rada Ministrów określi obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa lub zapewnienia sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców, ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwość organów w tych sprawach, biorąc pod

uwagę obiekty, o których mowa art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tj. obiekty infrastruktury krytycznej).

Ustawa o szczególnych uprawnieniach ministra właściwego do spraw energii

W ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych wprowadza się normę, która przewiduje, iż pełnomocnik do spraw ochrony infrastruktury krytycznej może pełnić jednocześnie funkcję koordynatora ochrony infrastruktury krytycznej.

IV. Przepisy przejściowe i końcowe

Streszczenie (...) oraz Krajowa ocena ryzyka (...)

Projekt przewiduje, iż dokument, pt. „Streszczenie istotnych elementów krajowej oceny ryzyka”, w brzmieniu nadanym projektowaną ustawą zostanie po raz pierwszy sporządzony w terminie do dnia 22 grudnia 2021 r.

Natomiast dokument pt. „Krajowa ocena zdolności zarządzania ryzykiem”, w brzmieniu przewidzianym projektowaną ustawą zostanie sporządzona w terminie do dnia 8 sierpnia 2021 r.

Plany zarządzania kryzysowego

Plany zarządzania ryzykiem w brzmieniu przewidzianym niniejszym projektem ustawy zostaną sporządzone w terminie do dnia 8 sierpnia 2020 r. Plany sporządzane po raz pierwszy nie będą zawierać oceny osiągniętych efektów i wniosków z wdrożonych działań w zakresie organizacyjnym, technicznym i finansowym na rzecz ograniczenia ryzyka katastrof.

Plany reagowania kryzysowego w brzmieniu przewidzianym niniejszym projektem ustawy zostaną sporządzone w terminie 12 miesięcy od dnia sporządzenia planów zarządzania ryzykiem.

Do czasu sporządzenia ww. planów - plany zarządzania kryzysowego przygotowane przed dniem wejścia w życie ww. zmian, pozostają w mocy do czasu sporządzenia planów według nowego układu i z zachowaniem terminów przewidzianych w projektowanych rozwiązaniach.

Infrastruktura krytyczna

Przewiduje się, iż kryteria wyłaniania infrastruktury krytycznej uwzględniające regulacje zawarte w projekcie ustawy zostaną sporządzone w terminie 18 miesięcy od dnia wejścia w życie ustawy.

Wykazy infrastruktury krytycznej sporządzone na podstawie tych kryteriów zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie ustawy.

Operatorzy infrastruktury krytycznej wyznaczą po raz pierwszy koordynatorów do spraw ochrony infrastruktury krytycznej w terminie 30 dni od dnia wejścia w życie projektowanej ustawy.

Raporty o stanie ochrony infrastruktury krytycznej zostaną sporządzane są przez koordynatorów do spraw ochrony infrastruktury krytycznej po raz pierwszy w 2020 r.

Operatorzy infrastruktury krytycznej zapewnią zdolność do ochrony informacji niejawnych w terminie 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Regulacje dotyczące kwestii dotyczących finansowania zadań z zakresu zarządzania kryzysowego będą miały zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2020 r.

Akty wykonawcze

Przepisy wykonawcze dotyczące sporządzania Raportu o zagrożeniach bezpieczeństwa narodowego, sposobu wykonywania obowiązków wynikających z Narodowego Programu Ochrony infrastruktury Krytycznej oraz organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego zachowują moc do czasu wejścia w życie nowych aktów wykonawczych jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie projektowanych rozwiązań.

Wejście w życie projektowanych rozwiązań

Przewidziano 14 - dniowy termin wejścia w życie regulacji zawartych w projekcie ustawy.