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 programie działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof.*

W odniesieniu do konieczność uregulowania kwestii zarządzania ryzykiem – jest to wymogiem spełnienia warunkowości podstawowej 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.).

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. Głównym celem Programu jest znaczące ograniczenie liczby śmiertelnych ofiar katastrof oraz zminimalizowanie wpływu katastrof na ciągłość podstawowych procesów realizowanych przez państwo (w tym kluczowych usług

zapewniających ochronę życia i zdrowia obywateli oraz funkcjonowanie administracji i gospodarki).

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 (UNDRR) 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 cząstkowych 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 *Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem*. Zgodnie z Unijnym Mechanizmem Ochrony Ludności, streszczenia przekazuje się do dnia 31 grudnia 2020 r., a następne co trzy lata oraz jeśli zajdą ważne zmiany.

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 ujednolicenie terminów cyklów 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. Raport zostanie sporządzony na podstawie raportów cząstkowych do *Raportu o zagrożeniach bezpieczeństwa narodowego* wykonanych przez ministrów, kierowników urzędów centralnych oraz wojewodów. Jednostki samorządu terytorialnego nie mają obowiązku opracowywania raportów cząstkowych. Po przeprowadzeniu oceny ryzyka 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:

- ✓ cześć 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 Zrządzania 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 – istotną zmianą jest to, iż zostanie dokonany jej podział na taką , której zniszczenie lub zakłócenie będzie miało niekorzystny wpływ na:

- ✓ funkcjonowanie państwa i zaspokojenia potrzeb obywateli,
- ✓ lokalną społeczność danego województwa.

Projekt wskazuje na sposób wyłaniania i umieszczania w wykazie obiektów, instalacji, urządzeń lub usług z ich podziałem na „infrastrukturę krajową" oraz „infrastrukturę wojewódzką". W drugim przypadku natomiast kompetencje w zakresie wyłaniania i umieszczania wyłonionej infrastruktury w stosownych wykazach przypadną wojewodzie. Ochrona infrastruktury krytycznej nie może odbywać się z pominięciem czynnika ludzkiego.

Jednocześnie wyodrębniona do oddzielnego wykazu zostanie europejska infrastruktura krytyczna. Powstanie również wykaz, tzw. potencjalnej infrastruktury krytycznej – czyli wykaz obiektów, instalacji, urządzeń lub usług będących w fazie projektowania lub budowy, a mogących spełniać kryteria właściwe dla infrastruktury krytycznej istotnej dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

Planowane jest wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u wszystkich operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej we wszystkich systemach infrastruktury krytycznej będą wyznaczać osobę koordynująca działania na linii operator – organy administracji publicznej.

Projekt wprowadza ujednolicenie terminologii w obszarze szkoleń i ćwiczeń z zakresu zarządzania kryzysowego na poziomie ministra kierującego działem administracji rządowej oraz kierownika urzędu centralnego zadanie w postaci wskazania, iż mają oni możliwość 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.

II. Szczegółowe zmiany w ustawie o zarządzaniu kryzysowym.

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

Sytuacja kryzysowa

Definicja sytuacji kryzysowej zostanie ona uzupełniona o kwestie dotyczące dziedzictwa kulturowego. Projekt nowelizacji w definicji sytuacji kryzysowej uwzględnia postanowienia Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności, która w art. 2 określa, że „Ochrona zapewniana w ramach unijnego mechanizmu obejmuje przede wszystkim ludzi, lecz także środowisko naturalne i mienie, w tym dziedzictwo kulturowe, i chroni je przed wszystkimi rodzajami klęsk żywiołowych i katastrof spowodowanych przez człowieka, w tym następstwami ataków terrorystycznych…".

Ponadto Decyzja Parlamentu Europejskiego i Rady 2019/420 z dnia 13 marca 2019 r. zmieniająca Decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności rozszerzyła katalog zagrożeń jak też działań podejmowanych w sytuacji wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka. Brak regulacji dotyczących ochrony dziedzictwa kulturowego mógłby powodować, iż problematyka ta nie zostanie włączona do budowanego obecnie systemu przygotowań na zdarzenia nadzwyczajne, w szczególności w administracji publicznej różnych szczebli, między innymi poprzez podejmowane działania planistyczno-organizacyjne, szkoleniowe i kontrolne. Ponadto pozbawia instytucje kultury, w których zgromadzone są zbiory, a które stanowią dziedzictwo narodowe, z korzystania z zasobów ludzkich i sprzętowych, podmiotów wyspecjalizowanych w prowadzeniu akcji ratowniczych.

Za ujęciem tego obszaru w projektowanych zmianach przemawiają zarówno doświadczenia historyczne jak również olbrzymie straty w dziedzictwie kultury w wyniku klęsk żywiołowych w Rzeczypospolitej Polskiej, w tym w szczególności powodzi w 1997 r.

Uzupełnienie dotychczasowej treści definicji o wskazanie istoty zakłóceń funkcjonowania organów administracji publicznej 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.

Systemy infrastruktury krytycznej

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 ulegnie jedynie nazwa jednego z jedenastu systemów infrastruktury krytycznej. Zmiana dotyczy dodania w systemie zaopatrzenia w wodę kwestii odprowadzania ścieków. Kwestie zbiorowego zaopatrzenia w wodę są nierozerwalnie 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.

Ponadto w zakresie infrastruktury krytycznej – wprowadzono definicję operatora infrastruktury krytycznej. Tak jak obecnie będą to właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń lub usług infrastruktury krytycznej, które zostały ujęte w wykazie infrastruktury krytycznej.

Operator infrastruktury krytycznej

Wprowadzono do słowniczka pojęcie operatora infrastruktury krytycznej jako właściciela, posiadacza samoistnego lub posiadacza zależnego obiektu, instalacji, urządzenia lub usługi, które zostały ujęte w wykazie infrastruktury krytycznej.

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 na terytorium Rzeczypospolitej Polskiej.

Ryzyko

Mając na względzie konieczność zarządzania ryzykiem – projekt wprowadza szereg definicji odnoszących się do kwestii ryzyka, począwszy od zdefiniowania „ryzyka" jak również definicji „ryzyka dla infrastruktury krytycznej". Istotną różnicą między tymi pojęciami jest uwzględnianie w przypadku ryzyka dla infrastruktury krytycznej - kwestii podatności.

Redefiniowano pojęcie mapy ryzyka, ponadto wprowadza się pojęcia: matrycy, ryzyka, zarządzania ryzykiem, analizy ryzyka oraz szacowania ryzyka.

Moduł zadaniowy

Zdefiniowano, funkcjonujące już w praktyce, pojęcie modułu zadaniowego, jako zestawienia przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez wykonawcę wskazanego w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony podmiotów wskazanych w siatce bezpieczeństwa.

Plany

Słowniczek do projektu zostaje uzupełniony o definicję planów zarządzania kryzysowego, planów zarządzania ryzykiem oraz planów reagowania kryzysowego.

Zagrożenia hybrydowe/ zarządzanie sytuacją hybrydową

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 oraz informacyjne.

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 progu wojny.

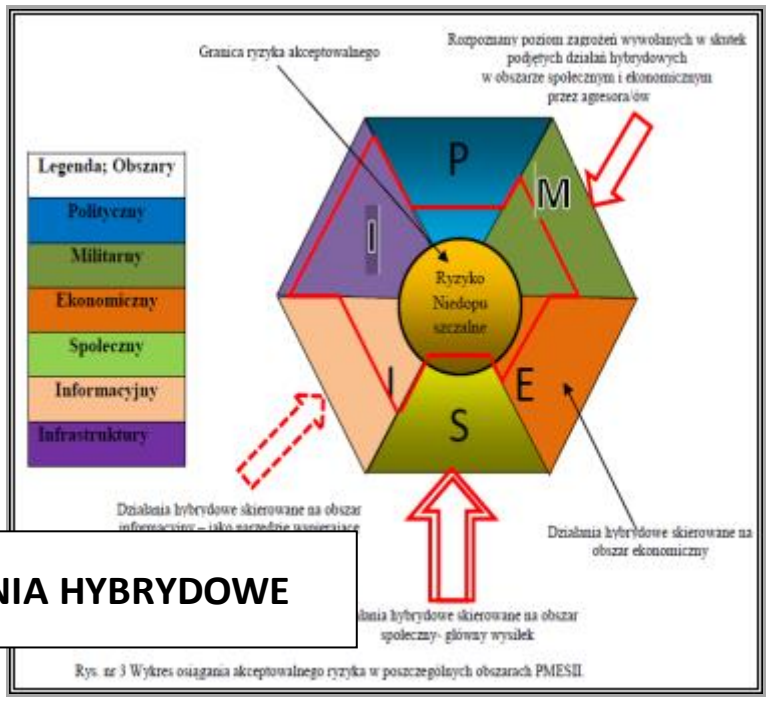
Najważniejszą rolę w przeciwdziałaniu zagrożeniom hybrydowym powinny odgrywać instytucje układu pozamilitarnego z obszaru ogniw ochronnych, gospodarczych, informacyjnych i systemu kierowania wspierane przez siły zbrojne, bowiem nie ma możliwości wyznaczenia dla całości działań hybrydowych podmiotu wiodącego. Ważną rolę odstraszającą 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 odstraszający 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.



Rys. nr 3 Wykres osiągania akceptowalnego ryzyka w poszczególnych obszarach PMESII

DZIAŁANIA HYBRYDOWE

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, 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].

Obok pojęcia zagrożenia hybrydowego – projekt wprowadza kwestie zarządzania sytuacją hybrydową, przez którą należy rozumieć prognozowanie, przeciwdziałanie i reagowanie na zagrożenia hybrydowe. Znajdzie ona odzwierciedlenie w zadaniach Rządowego Zespołu Zarządzania Kryzysowego.

2) *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.

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

- ✓ organizacyjne i techniczne możliwości wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego, zgodnie z art. 25 ustawy o zarządzaniu kryzysowym;
- ✓ organizacyjne i techniczne możliwości wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej oraz wojsk sojuszniczych w przypadku ich użycia przy realizacji zobowiązań sojuszniczych w ramach Organizacji Traktatu Północnoatlantyckiego na terytorium Rzeczypospolitej Polskiej;

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

3) *Art. 5 – zmiana porządkowa*

Propozycja zmierza do uchylenia regulacji dotyczących planów zarządzania kryzysowego w obecnej formie. Zostaną one ujęte w nowej formule w jednostkach redakcyjnych, tak aby zachować kolejność i korelacje Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów zarządzania kryzysowego;

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

Projekt przewiduje opracowywanie Raportu o zagrożeniach bezpieczeństwa narodowego (dalej „Raport") w celu dokonania oceny ryzyka wystąpienia zagrożeń oraz określenia celów strategicznych służących ograniczeniu ryzyka wystąpienia zagrożeń. Projekt wskazuje z jakich elementów będzie składał się Raport. Wskazuje również zadania w zakresie jego opracowywania, zarówno od strony podmiotów koordynujących, tj. dyrektora Centrum, Szefa ABW oraz Pełnomocnika ds. Cyberbezpieczeństwa, jak również ze strony podmiotów koordynowanych, tj. ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów.

Projektowana regulacja wskazuje, iż na potrzeby opracowania Raportu ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie opracowują tzw. raporty cząstkowe o zagrożeniach bezpieczeństwa narodowego, których elementy składowe zostały wskazane w projektowanej regulacji.

Projekt przewiduje, iż opracowanie raportów cząstkowych koordynuje Rządowe Centrum Bezpieczeństwa, z wyłączeniem części:

- ✓ dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Szef Agencji Bezpieczeństwa Wewnętrznego oraz
- ✓ dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, której opracowanie koordynuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

Na podstawie otrzymanych raportów cząstkowych Rządowe Centrum Bezpieczeństwa opracowuje Raport, z wyłączeniem części:

- ✓ dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, którą opracowuje Szef Agencji Bezpieczeństwa Wewnętrznego,

- ✓ dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, którą opracowuje Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.

Projekt wskazuje dyrektora Rządowego Centrum Bezpieczeństwa jako właściwego do przedkładania Raportu Radzie Ministrów co trzy lata (Rada Ministrów przyjmuje Raport w drodze uchwały);

5) *Ocena ryzyka oraz wnioski wynikające z Raportu*

Projekt wskazuje, iż ocena ryzyka wynikająca z Raportu oraz wnioski z Raportu są uwzględniane w planach zarządzania kryzysowego oraz w innych dokumentach opracowywanych w tym zakresie przez organy administracji publicznej w zakresie zarządzania kryzysowego.

Ponadto na podstawie Raportu Rządowe Centrum Bezpieczeństwa opracowuje streszczenie istotnych elementów krajowej oceny ryzyka, które dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Komisji Europejskiej.

Plany zarządzania ryzykiem

Projekt definiując plany zarządzania ryzykiem – wskazuje wspólne elementy tych planów. Plany zarządzania ryzykiem zawierają bowiem takie same elementy na wszystkich szczeblach zarządzania kryzysowego.

Plany zarządzania ryzykiem opracowują:

- ✓ Rządowe Centrum Bezpieczeństwa – Krajowy Plan Zarządzania Ryzykiem,
- ✓ ministrowie kierujący działami administracji rządowej – plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej,
- ✓ kierownicy urzędów centralnych – plany zarządzania ryzykiem kierowników urzędów centralnych,
- ✓ wojewodowie – wojewódzkie plany zarządzania ryzykiem,
- ✓ starostowie – powiatowe plany zarządzania ryzykiem,
- ✓ wójtowie (burmistrzowie, prezydenci miast) – gminne plany zarządzania ryzykiem.

W przypadku gminnych planów zarządzania ryzykiem - wójt (burmistrz, prezydent miasta) przekazuje je właściwemu miejscowo staroście. Natomiast powiatowy plan zarządzania ryzykiem starosta przekazuje właściwemu miejscowo wojewodzie.

Na szczeblu centralnym natomiast - Rządowe Centrum Bezpieczeństwa, uwzględniając plany zarządzania ryzykiem ministrów kierujących działami administracji

rządowej, kierowników urzędów centralnych oraz wojewodów, opracowuje Krajowy Plan Zarządzania Ryzykiem. Minister właściwy do spraw rozwoju regionalnego opiniuje Krajowy Plan Zarządzania Ryzykiem pod względem spójności z programami strukturalnymi.

Tak opracowany plan na szczeblu krajowym dyrektor Rządowego Centrum Bezpieczeństwa przedkłada Radzie Ministrów, która przyjmuje ten plan w drodze uchwały.

Plany reagowania kryzysowego

Projekt definiuje plany reagowania kryzysowego jako Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego. Projekt wskazuje elementy dla poszczególnych rodzajów planów, uwzględniając specyfikę każdego ze szczebli zarządzania kryzysowego.

Przez analogię do rozwiązań dotyczących planów zarządzania ryzykiem oraz uporządkowania treści przepisów projekt wskazuje, iż plany reagowania kryzysowego:

- ✓ Rządowe Centrum Bezpieczeństwa – Krajowy Plan Reagowania Kryzysowego,
- ✓ ministrowie kierujący działami administracji rządowej – plany reagowania kryzysowego ministrów kierujących działami administracji rządowej,
- ✓ kierownicy urzędów centralnych – plany reagowania kryzysowego kierowników urzędów centralnych,
- ✓ wojewodowie – wojewódzkie plany reagowania kryzysowego,
- ✓ starostowie – powiatowe plany zarządzania ryzykiem,
- ✓ wójtowie (burmistrzowie, prezydenci miast) – gminne plany reagowania kryzysowego.

W ww. kolejności wskazano również rodzaje planów reagowania kryzysowego wraz określeniem elementów charakterystycznych dla danego planu.

Novum zawartym w projekcie jest to, iż Krajowy Plan Reagowania Kryzysowego będzie opracowywany przez Rządowe Centrum Bezpieczeństwa, a dyrektor Rządowego Centrum Bezpieczeństwa będzie każdorazowo przedkładał ten plan Radzie Ministrów. Zakłada się, iż Rada Ministrów będzie przyjmować Krajowy Plan Reagowania Kryzysowego Rządowego w drodze uchwały.

Natomiast plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych będą uzgadniane z dyrektorem Rządowego Centrum Bezpieczeństwa i stanowić będą załączniki funkcjonalne do Krajowego Planu Reagowania Kryzysowego.

Projekt zawiera ponadto normę, która nakazuje Rządowemu Centrum Bezpieczeństwa opracowanie streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, w oparciu o treści Raportu oraz planów zarządzania kryzysowego. Opracowanie te dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Komisji Europejskiej;

6) *Narodowy Program Ochrony Infrastruktury Krytycznej*

W treści Narodowego Programu Ochrony Infrastruktury Krytycznej (dalej „NPOIK") znajdą odzwierciedlenie zmiany w obszarze infrastruktury krytycznej, m.in. zmiana nazewnictwa jednego z systemów w definicji infrastruktury krytycznej, podział infrastruktury krytycznej na dwa szczeble – krajowy oraz wojewódzki, jak również 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 miałoby niekorzystny wpływ na:

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

Projekt uwzględnia ww. zmiany nadające nowy kształt NPOIK-u. Zdefiniowano na nowo elementy NPOIK jak również sposób jego opracowywania. Wprowadzono w odniesieniu do NPOIK nowy, trzyletni okres planistyczny.

Wskazano również nowe brzmienie przepisu dotyczącego szczegółowych kryteriów wyłaniania infrastruktury krytycznej, co w założeniu ma pozwolić wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa, danego systemu lub lokalnej społeczności danego województwa oraz zaspokojenia potrzeb obywateli.

Projekt zawiera również normy, które określają sposób opracowywania NPOIK we współpracy we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych oraz wojewodami.

7) *Wyznaczanie infrastruktury krytycznej*

W nowym ujęciu przewiduje się funkcjonowanie następujących wykazów infrastruktury krytycznej, tj.

- ✓ wykazu krajowego - sporządzanego przez dyrektora RCB na podstawie kryteriów, o których mowa w NPOIK, we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy, obejmującego obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej z podziałem na poszczególne systemy;
- ✓ wykazu europejskiej infrastruktury krytycznej – sporządzanego przez dyrektora RCB, zawierającego 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;
- ✓ wykazu potencjalnej infrastruktury krytycznej – sporządzanego przez dyrektora Rządowego Centrum Bezpieczeństwa, we współpracy z ministrami kierującymi działami administracji rządowej i kierownikami urzędów centralnych odpowiedzialnymi za systemy, obejmującego obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej z podziałem na poszczególne systemy, będące w fazie projektowania lub budowy, mogące potencjalnie spełniać kryteria, o których mowa w NPOIK;
- ✓ wykazu wojewódzkiego – sporządzanego przez właściwego miejscowo wojewodę na podstawie szczegółowych kryteriów, o których mowa w NOPIK, obejmującego obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej z podziałem na systemy zlokalizowanej na terenie danego województwa.

Projekt przewiduje, iż dyrektor Rządowego Centrum Bezpieczeństwa opracowuje wyciągi z wykazu krajowego dotyczące obiektów, instalacji, urządzeń lub usług znajdujących się w danym systemie oraz przekazuje je ministrom kierującym działami administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system. Ponadto opracowuje wyciągi z wykazu krajowego dotyczące obiektów, instalacji,

urządzeń lub usług znajdujących się na obszarze danego województwa oraz przekazuje właściwemu wojewodzie.

O ujęciu w wykazie krajowym dyrektor RCB informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług jak również zatwierdza plany ochrony infrastruktury krytycznej ujęte w tym wykazie, po zasięgnięciu opinii ministra kierującego działem administracji rządowej i kierownika urzędu centralnego odpowiedzialnego za system.

W odniesieniu do wykazu potencjalnej infrastruktury krytycznej - obiekt, instalację, urządzenie lub usługę uznaje się za potencjalną infrastrukturę krytyczną w przypadku gdy z założeń projektowych wynika, że będzie ona kluczowa dla bezpieczeństwa państwa i jego obywateli oraz będzie służyć zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców oraz spełni kryteria, o których mowa w NOPIK. W celu wyznaczenia potencjalnej infrastruktury krytycznej dyrektor Rządowego Centrum Bezpieczeństwa prowadzi rozmowy z inwestorem lub operatorem infrastruktury krytycznej. Dyrektor Rządowego Centrum Bezpieczeństwa w rozmowach przedstawia stanowisko uzgodnione z ministrami i kierownikami urzędów centralnych odpowiedzialnych za systemy, których przedstawiciele mogą brać udział w rozmowach.

Na podstawie ustaleń będących wynikiem rozmów, dyrektor dokonuje ujęcia obiektu, instalacji, urządzenia lub usługi w wykazie potencjalnej infrastruktury krytycznej - dyrektor Rządowego Centrum Bezpieczeństwa powiadamia inwestora lub operatora infrastruktury krytycznej o ujęciu w wykazie potencjalnej infrastruktury krytycznej.

Dyrektor Rządowego Centrum Bezpieczeństwa, we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnymi za systemy przedstawia inwestorowi informacje oraz dokumenty, pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub realizacji przy realizacji inwestycji.

W odniesieniu do wojewody natomiast opracowuje on wyciągi z wykazu wojewódzkiego oraz przekazuje ministrom kierującym działami administracji rządowej i kierownikom urzędów centralnych odpowiedzialnym za dany system jak również przekazuje wykaz wojewódzki dyrektorowi Rządowego Centrum Bezpieczeństwa. Ponadto informuje właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji,

urządzeń lub usług o ujęciu w wykazie wojewódzkim oraz zatwierdza plany ochrony infrastruktury krytycznej ujętej w wykazie wojewódzkim.

W zakresie ochrony infrastruktury krytycznej projekt porządkuje czynności w zakresie zapewnienia jej ochrony przez operatorów infrastruktury krytycznej. Do zadań operatora infrastruktury krytycznej należy:

- ✓ opracowywanie i wdrażanie planów ochrony infrastruktury krytycznej oraz bieżące monitorowanie stopnia wdrożenia planów;
- ✓ sporządzanie i przekazywanie informacji w zakresie realizacji zadań dotyczących ochrony infrastruktury krytycznej na żądanie dyrektora Rządowego Centrum Bezpieczeństwa oraz właściwego ministra odpowiedzialnego za jeden z systemów albo właściwego kierownika urzędu centralnego odpowiedzialnego za jeden z systemów infrastruktury krytycznej albo właściwego terytorialnie wojewody;
- ✓ zapewnienie współpracy z organami administracji publicznej oraz dyrektorem Rządowego Centrum Bezpieczeństwa, przez przekazywanie i odbieranie informacji o:
    - o zdarzeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,
    - o spodziewanym lub zaobserwowanym zwiększeniu zapotrzebowania na usługi lub produkty dostarczane przez operatorów infrastruktury krytycznej,
    - o spodziewanych przerwach lub zakłóceniach w dostawach usług lub produktów dostarczanych przez operatorów infrastruktury krytycznej.

Operator infrastruktury krytycznej będzie sporządzał do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące ochrony infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. Raport o stanie ochrony infrastruktury krytycznej sporządza się m.in. z uwzględnieniem rozwiązań zawartych w planie ochrony infrastruktury krytycznej operatora, możliwości wystąpienia ryzyka zidentyfikowanego w planie ochrony infrastruktury krytycznej, incydentów i zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, które nie były uwzględnione w planie ochrony infrastruktury krytycznej, wyników

przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń zawartych w planie ochrony infrastruktury krytycznej.

Operator infrastruktury krytycznej przekazuje tak sporządzony raport o stanie ochrony infrastruktury krytycznej dyrektorowi Rządowego Centrum Bezpieczeństwa oraz właściwemu ministrowi odpowiedzialnemu za jeden z systemów albo właściwemu kierownikowi urzędu centralnego odpowiedzialnemu za jeden z systemów albo właściwemu terytorialnie wojewodzie.

W celu realizacji ww. obowiązków operator infrastruktury krytycznej wyznacza osobę koordynująca działania na linii operator – organy administracji publicznej, tj. koordynatora ochrony infrastruktury krytycznej.

Należy w tym miejscu 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 z.k. – 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 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:

- ✓ jest pracownikiem operatora infrastruktury krytycznej, albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej,
- ✓ 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,
- ✓ spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli co najmniej:
    - o „poufne” w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej „krajowego” operatora infrastruktury krytycznej, albo
    - o „zastrzeżone” w przypadku zajmowania stanowiska koordynatora w strukturze organizacyjnej „wojewódzkiego” operatora infrastruktury krytycznej.

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 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 administracje, 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.

Istotną zmianą w zakresie ochrony infrastruktury krytycznej jest wskazanie w materii ustawowej elementów planów ochrony infrastruktury krytycznej oraz wskazanie zasad ich uzgadniania i zatwierdzania. Regulacje ustawowe w tym zakresie uzupełnione będą aktem wykonawczym do ustawy, w którym Rada Ministrów określi wyłącznie sposób i tryb opracowania oraz zatwierdzania planów ochrony infrastruktury krytycznej;

8) *art. 6 ustawy z.k. – zmiany porządkowe*

Wprowadzenie regulacji doprecyzowujących zadania operatorów infrastruktury krytycznej w zakresie ich ochrony oraz wyznaczenie koordynatora spowodowało konieczność doprecyzowania przepisów art. 6 ustawy z.k. przez nadanie nowego brzmienia w ust. 1 pkt 5, co będzie czyniło przepisy aktu normatywnego czytelnymi oraz uchylenia ust. 5-7, m.in. wprowadzenie instytucji koordynatora powoduje konieczność uchylenia ust. 5a, który dotyczy wyznaczania osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej;

9) *Rządowy Zespół Zarządzania Kryzysowego*

Projekt przewiduje nowe zadanie dla Rządowego Zespołu Zarządzania Kryzysowego, tj. monitorowanie i rekomendowanie Radzie Ministrów działań dotyczących zarządzania sytuacją hybrydową.

10) *Dyrektor Rządowego Centrum Bezpieczeństwa/ Rządowe Centrum Bezpieczeństwa*

Zmiana o charakterze porządkowym i doprecyzowującym - projektowane zmiany w art. 10 ustawy z.k. polegają na wskazaniu, które zadania określone w ustawie z.k. realizuje bezpośrednio dyrektor Centrum, a które zadania Centrum - reprezentowane przez dyrektora;

11) *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 oraz koordynatora do spraw wdrażania Ramowego Programu Działań na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof;

12) *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 należeć będzie:

- ✓ 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 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 zarządzaniu 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 następującą:

- ✓ 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;

13) *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;

14) *Wojewoda - ćwiczenia*

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.

W celu uporządkowania przepisów - uchyla się zadania wojewody związane z zapobieganiem, przeciwdziałaniem i usuwaniem skutków zdarzeń o charakterze terrorystycznym oraz współpracy w tym zakresie z Szefem AB. 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.

Analogiczne rozwiązanie zastosowano w przypadku starosty oraz wójta, burmistrza i prezydenta miasta.

Ponadto doprecyzowano przepis wskazując, iż zatwierdzony wojewódzki plan zarządzania kryzysowego wojewoda przekazuje dyrektorowi Centrum;

15) *Starosta – ćwiczenia*

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.

16) *Wójt, burmistrz, prezydent miasta – ćwiczenia*

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;

17) *Art. 20b zmiana porządkowa*

W związku z wprowadzeniem definicji operatora infrastruktury krytycznej treść art. 20b ustawy z.k. została stosownie przeredagowana;

18) *„ALERT RCB”*

Wprowadza się przepis, który umożliwia niewysyłanie operatorowi 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 optymalizacje 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 wysyłać komunikaty 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 posiadaną informację o liczbie kart SIM użytkowników końcowych, do których komunikat został dostarczony. Operator przekazuje te dane z uwzględnieniem obszaru, na który komunikat został wysłany zgodnie z żądaniem dyrektora Centrum.

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;

19) *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 mogły być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem oraz reagowaniem w przypadku wystąpienia sytuacji kryzysowej, a także usuwaniem jej skutków i odtwarzaniem zasobów.

III. Zmiany w innych ustawach.

Zmiany w innych ustawach mają przede wszystkim charakter wynikowy, jak również dokonują poprawek w zakresie błędnych odniesień do ustawy o zrządzaniu kryzysowym w innych ustawach. W przypadku zmian w ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw energii (…) zmiany mają również charakter merytoryczny – są one powiązane tematycznie z projektowanymi zmianami, gdyż dotyczą tematyki ochrony infrastruktury krytycznej.

Art. 2 – zmiany w ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia doprecyzowują przepis art. 5 ust. 1 pkt 5 tej ustawy w zakresie zmiany odniesień zawartych w tym przepisie do nowej systematyki ustawy z.k. Obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi wchodzące w skład infrastruktury krytycznej ujęte w wykazach: krajowym, europejskim oraz wojewódzkim.

Art. 3 – zmiany w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu są zmianami wynikowymi dotyczące art. 5 w ust. 1 pkt 2a, art. 32a ust. 1 oraz art. 32aa ust. 1 zostały wprowadzone w związku ze zmianą systematyki ustawy z.k.

Art. 4 – zmiana w ustawie z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych w art. 89 w ust. 1 pkt 7d jest zmianą *stricte* wynikową – dostosowuje przepisy ustawy p.z.p. do nowej systematyki ustawy z.k.

Art. 5 – zmiana w ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich w art. 24 w ust. 5 ustawy o.ż.p.m. polega na usunięciu odwołań do nieistniejących przepisów art. 23 i 24 ustawy z.k. Pozostawia się natomiast, nadal aktualne odwołania do przepisów art. 21 i 25 ustawy z.k.

Art. 6 - zmiany 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 obejmują poniższe kwestie.

Zmiany w tytule ustawy oraz w art. 1 ust. 1 polegają na usunięciu odniesienia do grup kapitałowych i mają charakter stricte porządkowy. Uprawnienia przysługujące ministrowi właściwemu do spraw energii są realizowane w odniesieniu do poszczególnych spółek, prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujęte w jednolitym wykazie obiektów instalacji, urządzeń i usług, a nie w odniesieniu do grup kapitałowych, w skład których wchodzą te spółki. W obowiązujących przepisach brak jest regulacji pozwalających na powołanie pełnomocnika w grupie kapitałowej, mając na względzie fakt, że przepis, zgodnie z którym kandydat na pełnomocnika powinien być pracownikiem spółki (ustawa nie przesądza, której spółki, czy wszystkich spółek grupy kapitałowej, czy spółek posiadających obiekty infrastruktury krytycznej, czy wyłącznie spółki dominującej).

Proponowane zmiany w art. 1 w ust. 2 pkt 1 i 3 przewidują objęcie przepisami ustawy o szczególnych uprawnieniach mienia spółek – operatorów infrastruktury krytycznej – służących do dystrybucji energii elektrycznej i paliw gazowych. Umożliwi to przeciwdziałanie czynnościom tych przedsiębiorców będących operatorami systemów dystrybucyjnych w sektorze energii elektrycznej i paliw gazowych (których mienie zostało ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług stanowiących infrastrukturę krytyczną), stanowiącym zagrożenie dla infrastruktury krytycznej. Obecnie w wykazie obiektów infrastruktury krytycznej zostało ujęte mienie jednej spółki dystrybucyjnej służące do dystrybucji energii elektrycznej, natomiast mienie żadnego z podmiotów zajmujących się dystrybucją paliw gazowych nie jest aktualnie ujęte w tym wykazie. Nie można wykluczyć, że w przyszłości wykazem objęte zostanie mienie innych spółek – operatorów systemu dystrybucyjnego, jeśli zostanie ono uznane za istotne dla funkcjonowania systemu lub jego części.

Natomiast uchylenie pkt 5 w art. 2 ust. 2 sprowadza się do usunięcia z katalogu uchwał organu spółki tych, które mogą zostać objęte sprzeciwem ministra właściwego do spraw energii: uchwały o przyjęciu planu rzeczowo-finansowego, planu działalności inwestycyjnej i wieloletniego planu strategicznego z uwagi na fakt, że plany te mają charakter deklaratoryjny, zawierają zakładane kierunki rozwoju spółki, a uchwała organu spółki o przyjęciu takiego planu nie jest jednoznaczna z jego realizacją. Realizacja przyjętych założeń w odniesieniu do istotnych obszarów działalności spółki wymaga podjęcia przez jej organy odrębnych uchwał, które w przypadku, gdy stanowić będą rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności

infrastruktury krytycznej, mogą zostać objęte sprzeciwem ministra właściwego do spraw energii (o ile będą się one mieścić w katalogu czynności wymienionych w ustawie).

Zmiana proponowana w art. 2 w ust. 3 polega na wydłużeniu terminów, w których minister właściwy do spraw energii może zgłosić sprzeciw wobec określonych czynności spółki stanowiących rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej z 14 do 30 dni od dnia otrzymania informacji od pełnomocnika oraz z 30 do 45 dni od dnia ich dokonania. Przedmiotowa zmiana jest uzasadniona potrzebą uzyskania przez Ministra Energii czasu niezbędnego na dokonanie wszechstronnej, kompleksowej oceny planowanych przez spółkę czynności w kontekście zagrożenia dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Przyjęty w obowiązujących przepisach 14-dniowy termin na przeprowadzenie postępowania i wydanie decyzji administracyjnej często w skomplikowanych sprawach jest zbyt krótki. Ponadto proponuje się wydłużenie z 14 do 30 dni terminu na załatwienie sprawy w przypadku złożenia wniosku o ponowne rozpatrzenie sprawy.

W art. 5 natomiast ust. 4 otrzymuje brzmienie, w którym przewiduje się, iż pełnomocnik do spraw ochrony infrastruktury krytycznej może być koordynatorem do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5i ust.1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Zmiana w art. 6 ust. 3 ma na celu ujednolicenie, z wymogami określonymi w projektowanym art. 5e ust. 2 ustawy o zarządzaniu kryzysowym, zakresu informacji, które powinien zawierać raport o stanie ochrony infrastruktury krytycznej.

Art. 7 – zmiany w ustawie z dnia 29 października 2010 r. o rezerwach strategicznych w art. 8 w ust. 4 w pkt 1 jest zmianą wynikową, dostosowującą przepisy ustawy r.s. do nowej systematyki ustawy z.k.

Art. 8 – zmiana w ustawie z dnia 14 grudnia 2012 r. o odpadach (w art. 25 ust. 6i pkt 2) jest również zmianą wynikową, dostosowującą przepisy tej ustawy do nowej systematyki ustawy z.k.

Art. 9 – zmiany w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej w art. 4 w pkt 8 lit. b jest zmianą wynikową, dostosowującą przepisy tej ustawy do nowej systematyki ustawy z.k.

Art. 10 – zmiana w ustawie z dnia 7 lutego 2014 r. o udziale zagranicznych funkcjonariuszy lub pracowników we wspólnych operacjach lub wspólnych działaniach ratowniczych na

terytorium Rzeczypospolitej Polskiej w art. 4 ust. 4 ww. ustawy znajduje się błędne wskazanie odniesienia do pojęcia zdarzenia o charakterze terrorystycznym, wskazujące w tym zakresie ustawę z.k. zamiast ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych.

Art. 11 – zmiany w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w art. 4 w pkt 8 lit. b są zmianami wynikowymi dostosowującymi przepisy tej ustawy do nowej systematyki ustawy z.k.

IV. Przepisy przejściowe i końcowe.

Projekt przewiduje, iż streszczenie istotnych elementów krajowej oceny ryzyka, w brzmieniu nadanym niniejszą ustawą, zostanie sporządzone w terminie do dnia 31 grudnia 2020 r.

Streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w brzmieniu nadanym niniejszą ustawą, zostanie po raz pierwszy sporządzone w terminie do dnia 31 grudnia 2020 r.

Plany zarządzania ryzykiem w brzmieniu nadanym niniejszą ustawą zostaną sporządzone w terminie do dnia 8 sierpnia 2020 r. Plany sporządzone po raz pierwszy nie zawierają oceny osiągniętych efektów i wniosków z wdrożonych działań.

Plany reagowania kryzysowego w brzmieniu nadanym niniejszą ustawą, zostaną sporządzone w terminie 12 miesięcy od dnia sporządzenia planów zarządzania ryzykiem.

Plany zarządzania kryzysowego sporządzone i zatwierdzone na podstawie dotychczasowych przepisów, przed dniem wejścia w życie niniejszej ustawy, pozostają w mocy do czasu sporządzenia planów zarządzania ryzykiem oraz planów reagowania kryzysowego.

Kryteria wyłaniania infrastruktury krytycznej zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

Wykazy infrastruktury krytycznej, tj. krajowy, europejski oraz wojewódzki zostaną sporządzone w terminie 24 miesięcy od dnia wejścia w życie niniejszej ustawy.

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

Raport o stanie ochrony infrastruktury krytycznej, w brzmieniu nadanym niniejszą ustawą, sporządza się po raz pierwszy za rok 2020.

Operatorzy infrastruktury krytycznej zapewnią zdolność do ochrony informacji niejawnych w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

Projektowany przepis art. 26 ust. 4a ustawy z.k. będzie miał zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2021 r.

Przepisy wykonawcze dotyczące sporządzania Raportu o zagrożeniach bezpieczeństwa narodowego oraz planów ochrony infrastruktury krytycznej zachowują moc do czasu wejścia w życie nowych aktów wykonawczych jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie projektowanych rozwiązań.

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

Projekt ustawy jest zgodny z prawem Unii Europejskiej oraz nie zawiera norm technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039, z późn. zm.) i w związku z powyższym nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawienia instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu.