RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 29 PAŹDZIERNIK – GRUDZIEŃ 2019

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz – Zastępca Dyrektora RCB

Martyna Olejnik-Kołodziej

Anna Zasadzińska-Baraniewska

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Krajowy system obrony przed BMR i CBRN – aspekty współpracy cywilno-wojskowej, planowania cywilnego i zarządzania kryzysowego

„Krajowy system obrony przed BMR i CBRN" – pod takim tytułem odbyło się 5 grudnia 2019 r. w Warszawie seminarium poświęcone obronie przed bronią i czynnikami masowego rażenia. Celem organizatorów przedsięwzięcia, a wśród nich Rządowego Centrum Bezpieczeństwa, było dokonanie analizy różnych aspektów obrony przed BMR i CBRN i sformułowanie diagnozy stanu obecnego tak, aby możliwe było wskazanie kierunków działań mających doprowadzić do udoskonalenia obecnych rozwiązań, a w efekcie do stworzenia kompleksowego, sprawnego i efektywnego systemu.

Współpraca cywilno-wojskowa w aspekcie obrony przed czynnikami masowego rażenia

Krzysztof Malesa
Rządowe Centrum Bezpieczeństwa

Rosnące znaczenie NATO jako organizacji wspierającej społeczność międzynarodową w walce z terroryzmem oraz znacząca intensyfikacja prac Sojuszu nad zwiększeniem odporności państw członkowskich na działania hybrydowe stawiają w nowym świetle kwestie współpracy cywilno-wojskowej. Współpraca ta jest kluczem do osiągnięcia odpowiedniego poziomu gotowości cywilnej państw członkowskich (Civil Preparedness) – na forum NATO rozumianej jako organizacyjna, logistyczna i techniczna gotowość do skorzystania w wyjątkowych wypadkach nawet z obrony kolektywnej na mocy art. 5 Traktatu Waszyngtońskiego. Z narodowego punktu widzenia gotowość cywilna przekłada się również na możliwość skutecznego zaangażowania połączonych zasobów cywilno-wojskowych do reagowania na sytuacje kryzysowe w czasie pokoju. Do takich potencjalnych zdarzeń z pewnością zaliczają się ataki z użyciem czynników masowego rażenia (CBRN).

Wydarzenia z Salisbury z marca 2018 roku, przypadki użycia broni chemicznej w Syrii oraz inne incydenty z użyciem czynników masowego rażenia (chociaż niekoniecznie na masową skalę) należy potraktować jako wyraźny sygnał ostrzegawczy, nakazujący powrócić do tych aspektów bezpieczeństwa narodowego, które zostały nieco zaniedbane po upadku Muru Berlińskiego. Potwierdzają to wyraźnie ustalenia szczytu Sojuszu Północnoatlantyckiego w Warszawie z lipca 2016 r., na którym państwa członkowskie przyjęły zobowiązanie do zwiększenia odporności w siedmiu uzgodnionych w NATO obszarach (Seven Baseline Requirements for Resilience). Jeden z nich obejmuje właśnie umiejętność reagowania na zdarzenia masowe, czyli m.in. z czynnikiem CBRN.

Efektywne reagowanie na zdarzenia z CBRN jest możliwe dopiero wówczas, gdy dane państwo – realizując zresztą zapisy art. 3 Traktatu Waszyngtońskiego – samo osiągnie pewien poziom odporności (Resilience) w tym obszarze – równocześnie niwelując podatności. Powinno się to odbyć z zaangażowaniem jak największej liczby interesariuszy (whole-society approach). Kluczowe na polskim gruncie wydaje się w związku z tym zapewnienie koordynacji działań na szczeblu Rady Ministrów, która zgodnie z ustawą o zarządzaniu kryzysowym sprawuje zarządzanie kryzysowe na terytorium RP. Pewne kwestie w tym zakresie reguluje Krajowy Plan Zarządzania Kryzysowego, daleko nam jednak jeszcze do osiągnięcia tak wysokiego poziomu zaangażowania wszystkich interesariuszy, jaki obserwujemy np. podczas ćwiczeń systemów obrony totalnej w państwach skandynawskich.

Biorąc pod uwagę wielowymiarowy charakter działań hybrydowych (zgodnie z definicją w Krajowym Planie Zarządzania Kryzysowego) oraz nieuniknione trudności z ich rozpoznaniem i atrybucją sprawcy, łatwo zrozumieć, dlaczego Rada Ministrów, przyjmując KPZK, przy zagrożeniu działaniami hybrydowymi nie wskazała podmiotu wiodącego. Nie można bowiem

a priori założyć, w jakim obszarze takie działania mogą wystąpić, a nawet trudno jednoznacznie stwierdzić, kiedy się zaczęły. W efekcie cała administracja – zarówno po stronie wojskowej, jak i cywilnej – powinna pozostawać w gotowości do reagowania na potencjalne zdarzenie. Dotyczy to w szczególności służb i urzędów obsługujących organy zaangażowane w ochronę infrastruktury krytycznej. Nieprzerwane, spójne zaangażowanie wszystkich uczestników – przedstawicieli sfery cywilnej, wojskowej oraz sektora prywatnego – nie jest wystarczająco zaakcentowane w Krajowym Systemie Wykrywania Skażeń i Alarmowania. Jest to system odpowiadający właściwie na potrzeby układu militarnego, chociaż podejmowane są próby nadania mu charakteru kompleksowego.

Jak się jednak zdaje, kompleksowe podejście do problematyki CBRN, połączone z wypracowaniem ogólnokrajowego cywilno-wojskowego systemu obrony przed bronią masowego rażenia, wymaga podjęcia prac od początku – z uwzględnieniem kwestii zarządzania kryzysowego, ochrony infrastruktury krytycznej i oczywiście, możliwości i oczekiwań wszystkich zainteresowanych, włączając w to zwłaszcza sektor prywatny.

W polskiej administracji, podzielonej pionowo na działy administracji rządowej (mające tendencję do autonomizacji i zamykania się w tzw. silosach) i poziomo na administrację rządową i samorządową (z konstytucyjnie gwarantowaną niezależnością od rządowej) nie będzie to jednak proste. Wspomniane podziały (do których należy doliczyć jeszcze sztywny podział na czas pokoju i wojny, determinujący możliwości wykorzystania potencjału militarnego RP) są głównym czynnikiem ryzyka, którym będzie trzeba efektywnie zarządzać. Z pewnością będzie to wymagać wsparcia i jednoznacznego komunikatu o akceptacji kierunku zmian ze szczebla politycznego.

Rola planowania cywilnego i zarządzania kryzysowego

Florian Naumczyk
Rządowe Centrum Bezpieczeństwa

Analizując rolę Rządowego Centrum Bezpieczeństwa w kontekście spraw dotyczących zagrożeń pochodzących od broni masowego rażenia (BMR) i środków chemicznych, biologicznych, radiacyjnych i nuklearnych (CBRN) oraz przeciwdziałania im, warto podkreślić, iż są to pojęcia ściśle powiązane. Dlatego w RCB operuje się najczęściej określeniem „CBRN" w odniesieniu do obu zagrożeń. Cechą wspólną BMR i CBRN jest bowiem oddziaływanie w masowej skali na ludzi, środowisko i infrastrukturę. Implikuje to konieczność wyprzedzającego planowania cywilnego, w tym przygotowania stosownych planów jako elementów zarządzania kryzysowego w kolejnych jego fazach, w celu zminimalizowania skutków oddziaływania CBRN. Tak właśnie definiowana jest rola RCB w myśl ustawy o zarządzaniu kryzysowym[1]. W ten sposób RCB wpisuje się w wysiłki służące poprawie odporności na zagrożenia CBRN i gotowości do reagowania możliwie szybko, sprawnie, w sposób skoordynowany, ale elastycznie – w zależności od danej sytuacji.

Rola RCB w odniesieniu do zagrożeń CBRN jest podwójna: pierwszym aspektem jest ich uwzględnienie w Krajowym Planie Zarządzania Kryzysowego (KPZK), drugim – współdziałanie z podmiotami cywilnymi i wojskowymi wykonującymi zadania na wypadek zdarzenia CBRN.

KPZK zawiera zadania organów centralnych w reagowaniu na wszystkie ujęte tam 19 zagrożeń, w tym te związane bezpośrednio z CBRN. Opisuje współdziałanie tych organów, a także odnosi się bezpośrednio do zaangażowania sił zbrojnych w przypadku zaistnienia któregokolwiek z zagrożeń w wielkiej skali. Sześć zagrożeń spośród ujętych w siatce bezpieczeństwa, czyli: epifitoza, epizootia, epidemia, skażenie chemiczne na lądzie i skażenie chemiczne na morzu oraz skażenie radiacyjne wywołane są środkami CBRN. W części A plan zawiera tabelę oszacowania ryzyka. W tabeli nr 1 zestawiono oszacowanie ryzyka dla zagrożeń CBRN w funkcji prawdopodobieństwa zaistnienia i potencjalnych skutków. Wartości i sposób zobrazowania wzięte zostały z aktualnego KPZK.

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2007 Nr 89 poz. 590, tj. Dz. U. z 2019 r. poz. 1398, art. 11, ust. 2).

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

PRAWDOPODOBIEŃSTWO ZDARZENIA						
	Bardzo prawdopodobne					
	Prawdopodobne			Epifitoza		
	Możliwe		Epifitoza B	Epidemia B		
	Rzadkie		Skażenie chemiczne C			
	Bardzo rzadkie			Skażenie radiacyjne RN		
		nieistotne	małe	średnie	duże	katastrofalne
	SKUTKI ZDARZENIA					

Wartość ryzyka:
– minimalne
– małe
– średnie
– duże
– ekstremalne

(na podstawie KPZK, cz. A, str. 6)

Tabela nr 1 – ocena ryzyka CBRN /na podstawie KPZK cz. A str. 6 – www.rcb.gov.pl.

Z KPZK powiązany jest Plan Współdziałania Krajowego Systemu Wykrywania Skażeń i Alarmowania (KSWSiA), ujmujący całościowo współpracę cywilno-wojskową na wypadek zdarzeń CBRN.

Rządowe Centrum Bezpieczeństwa uczestniczy bezpośrednio w uruchamianiu planu KSWSiA, jak i jego realizacji, prowadząc wymianę informacji z jednostkami organizacyjnymi systemu. Dyrektor RCB uczestniczy w przedsięwzięciach zapewniających koordynację w zakresie jednolitości i interoperacyjności funkcjonowania systemów wchodzących w jego skład. Ponadto RCB uczestniczy we współpracy z mediami w sytuacji kryzysowej, jak również przygotowuje pracowników biur prasowych różnych instytucji cywilnych do prowadzenia komunikacji w sytuacji kryzysowej (np. poprzez organizowanie ćwiczeń i szkoleń).

KSWSiA jest, z perspektywy RCB, wartościowym narzędziem, przy pomocy którego stopniowo, w miarę potrzeb, uruchamiane są zasoby i zdolności reagowania na zagrożenia CBRN przez różne podmioty cywilne oraz udzielane jest wsparcie przez siły zbrojne dla sfery cywilnej. KSWSiA jest – po działaniach służb ratowniczych (czyli pierwszych reagujących) – „drugą linią" obrony i likwidacji skutków użycia środków CBRN oraz służy budowaniu odporności na zagrożenia nimi spowodowane. Dzięki wspólnym cywilno-wojskowym treningom i ćwiczeniom powstaje interoperacyjność pomiędzy krajowymi podmiotami cywilnymi i wojskowymi. Niemniej KSWiA nie jest narzędziem zadawalającym, gdyż regulacje prawne[2] umożliwiają jego uruchomienie do działania po wprowadzeniu stanu nadzwyczajnego (lub w ramach ćwiczeń).

Istotnym ograniczeniem dla KSWSiA jest więc powiązanie jego uruchamiania ze stanami kwalifikowanymi. Taka sytuacja nie odpowiada aktualnym wyzwaniom w szczególności w odniesieniu do zagrożeń o charakterze hybrydowym, o czym RCB i współpracujące podmioty, zwłaszcza cywilne, przekonują się podczas ćwiczeń, w tym o charakterze strategicznym, organizowanych przez NATO. Niezbędna jest zatem nowelizacja wskazanych zapisów w rozporządzeniu Rady Ministrów, konstytuującym KSWSiA.

Kolejnym istotnym problemem jest przygotowanie systemowych rozwiązań na wypadek masowego (z bardzo dużą liczbą poszkodowanych) zdarzenia z użyciem środków CBRN. W szczególności dotyczy to przygotowań w obszarze pomocy medycznej poszkodowanym i infrastruktury do dekontaminacji poszkodowanych w miejscach i obiektach udzielania

[2] Rozporządzenie RM z dnia 7 stycznia 2013 r. w sprawie systemów wykrywania skażeń i powiadamianiu o ich wystąpieniu oraz właściwości organów w tych sprawach, § 3.1.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

pomocy medycznej. Chodzi przede wszystkim o infrastrukturę umożliwiającą dekontaminację poszkodowanych w razie nagłego zgłaszania się dużej liczby skażonych poszkodowanych do szpitali i placówek medycznych.

Wspomniany już hybrydowy charakter zagrożeń, do których można zaliczyć CBRN, wywoływanych (teoretycznie) zarówno przez aktorów państwowych, jak i niepaństwowych, implikuje konieczność zbierania w środowisku skażenia dowodów przestępstwa, pozwalających na dokonanie atrybucji takiego ataku. Tych kilka wymienionych istotnych wyzwań wskazuje, że wymogiem czasów, w których żyjemy, jest nie tylko podnoszenie odporności lecz także dokonanie zmian systemowych.

Blackout w Wielkiej Brytanii – analiza przypadku

Amelia Tomalska
Rządowe Centrum Bezpieczeństwa

Artykuł powstał na podstawie: https://www.nationalgrideso.com/information-about-great-britains-energy-system-and-electricity-system-operator-eso

Przerwa w dostawie prądu, która miała miejsce 9 sierpnia 2019 roku w Wielkiej Brytanii, uznawana jest za jedną z najpoważniejszych na terytorium Zjednoczonego Królestwa w ostatniej dekadzie. Konsekwencją tak poważnego incydentu było między innymi pozostawanie około 1,1 miliona mieszkańców bez prądu przez okres od 15 do 45 minut, przerwa w kursowaniu pociągów, a także brak zasilania w szpitalu w Ipswich oraz na lotnisku w Newcastle. W reakcji na zaistniałą sytuację brytyjski operator przesyłu i dystrybucji energii elektrycznej oraz gazu ziemnego, spółka National Grid, opublikował raport, w którym dokładnie przeanalizowano przebieg zdarzenia, starając się jak najbardziej szczegółowo odtworzyć sekwencję incydentów oraz ustalić przyczynę przerwy w dostawie prądu.

Sytuacja atmosferyczna 9 sierpnia, w dniu gdy doszło do blackoutu, nie odbiegała od normy. Brytyjski narodowy serwis meteorologiczny (National Weather Service) Met Office, wydał wprawdzie żółte (stopień niski) ostrzeżenia o możliwej złej pogodzie, w tym porywach wiatru i opadach deszczu, dla większości rejonów Anglii oraz Walii, ale nic nie wskazywało na jakiekolwiek anomalie pogodowe. Wkrótce jednak nastąpiło gwałtowne załamanie pogody, przynosząc intensywne opady deszczu oraz dużą liczbę wyładowań atmosferycznych. Według prognoz na ten dzień, przewidywany poziom zapotrzebowania na prąd w każdym sektorze był określony jako podobny do poprzedniego tygodnia. Około 30% produkcji energii elektrycznej pochodziło z wiatru, 30% z gazu, 20% z energii jądrowej, 10% z połączeń międzysystemowych i około 10% z wody (elektrowni szczytowo-pompowych), węgla i biomasy. O godzinie 16:52 piorun uderzył w linię przesyłową Eaton Socon – Wymondley o napięciu 400 kV. Systemy ochrony transmisji zadziałały natychmiastowo i linia powróciła do normalnego trybu funkcjonowania po około 20 sekundach. Jednakże niemal w tym samym czasie, co uderzenie pioruna, nastąpiło zredukowanie mocy w elektrowni gazowej Little Barford oraz elektrowni wiatrowej Hornsea. O godzinie 16:53 z powodu spadku produkcji energii przez obie elektrownie częstotliwość spadła do 49.1 Hz. W sytuacji, kiedy dochodzi do dużej zmiany częstotliwości, ESO (Electricity System Operator) posiada zasoby pozwalające na wytworzenie energii elektrycznej o mocy 1000 MW w określonym czasie. Tym razem jednak całkowity spadek generacji na skutek zakłóceń, szacowany na co najmniej 2000 MW, przerósł przygotowane na taki wypadek rezerwy, co spowodowało spadek częstotliwości do 48,8 Hz to jest poniżej limitu wartości operacyjnych. Skutkiem tego było uruchomienie systemu zabezpieczeń Low Frequency Demand Disconnection (LFDD), w wyniku którego automatycznie odłączonych od dostaw zostało 5%, czyli ok. 1,1 miliona odbiorców energii elektrycznej, aby chronić pozostałe 95% odbiorców oraz zapewnić bezpieczeństwo sieci w sposób kontrolowany i zgodny z parametrami ustanowionymi przez operatorów sieci dystrybucyjnych. O godzinie 16:57 częstotliwość została przywrócona, a system powrócił do normalnego, stabilnego stanu. O godzinie 17:06 operatorzy sieci dystrybucyjnych rozpoczęli podłączanie odłączonych wcześniej odbiorców. O godzinie 17:37 przywrócono dostawy energii elektrycznej do wszystkich użytkowników.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Wstępna analiza przebiegu i skutków zdarzenia pozwala na sformułowanie pierwszych wniosków. Sam fakt, że doszło do blackoutu na tak znaczną skalę wskazuje na niewystarczającą odporność (resilience) systemu energetycznego w Wielkiej Brytanii, a tym samym na potrzebę dogłębniejszej analizy systemu zapewnienia ciągłości działania. W raporcie, w ramach rekomendacji, znalazła się propozycja rewizji norm bezpieczeństwa (Security and Quality of Supply Standards), związanych z poziomem odporności w systemie elektroenergetycznym, co powinno zostać przeprowadzone w sposób ustrukturyzowany, aby zapewnić właściwe zbilansowanie ryzyka i kosztów.

Czasowe odcięcie od dostaw prądu szpitala i lotniska, unieruchomienie metra i pociągów nasuwa pytanie, dlaczego tak kluczowe obiekty nie miały zapewnionej wystarczającej ochrony. W raporcie zostało to odnotowane, a jedną z rekomendacji jest punkt odnoszący się do konieczności dokonania oceny, czy właściwe byłoby ustanowienie standardów dla infrastruktury i usług krytycznych (takich jak szpitale, transport, służby ratownicze), określających zakres zdarzeń i warunków w systemie elektroenergetycznym, dla których powinny być zaprojektowane wewnętrzne systemy, gwarantujące ciągłość funkcjonowania. Warto zauważyć, iż władze lotniska w Newcastle, również dotkniętego skutkami przerwy w zasilaniu, z własnej inicjatywy, zaraz po zdarzeniu, wystosowały wniosek do Northern Powergrid (Northeast) Limited o zaklasyfikowanie lotniska jako terenu chronionego (Protected Site) w ramach ESEC (Electricity Supply Emergency Code). Wniosek portu lotniczego został rozpatrzony pozytywnie.

W raporcie wskazano ponadto, że przeanalizowania wymaga ilość rezerw, które w dniu zdarzenia okazały się niewystarczające by pokryć deficyt. National Grid przyznał, iż istnieje potrzeba rewizji zasobów, z uwzględnieniem odpowiedniego zbilansowania kosztów zapewnienia dodatkowych rezerw w odniesieniu do prawdopodobieństwa wystąpienia podobnych zdarzeń w przyszłości. Zaznaczono, że mimo prognozowanej wysokości kosztów, z uwagi na bezpieczeństwo obywateli i infrastruktury, w tym infrastruktury krytycznej, taka inwestycja byłaby w dłuższej perspektywie opłacalna.

W ramach rekomendacji przedstawiono propozycję wspólnego wypracowania przez zainteresowane strony, w tym ESO (Electricity System Operator), BEIS (Department for Business, Energy and Industrial Strategy), Ofgem (Gas and Electricity Markets Authority), ENA (Energy Networks Association), zaktualizowanych uzgodnień i planów dotyczących komunikacji, na wypadek podobnej sytuacji w przyszłości. Podniesiono również aspekt komunikacji ze społeczeństwem oraz prowadzenia działań edukacyjnych, co ma doprowadzić do podniesienia świadomości obywateli i ograniczenia zachowań niepożądanych, w tym niepotrzebnej paniki. Wskazano także na wzrastające zapotrzebowanie na dostawy energii elektrycznej, związane m.in. z wykorzystaniem nowych technologii, a z drugiej strony na coraz większy udział odnawialnych źródeł energii, takich jak np. energia wiatrowa, w generacji mocy. Rosnące zapotrzebowanie na energię elektryczną, przy wykorzystaniu źródeł niegwarantujących ciągłości dostaw w połączeniu ze skutkami zjawisk pogodowych (będących m.in. efektem zmian klimatu), zwiększa poziom podatności, prawdopodobieństwa i tym samym ryzyka wystąpienia podobnych zdarzeń w przyszłości.

Zdarzenie, do którego doszło 9 sierpnia 2019 r. w Wielkiej Brytanii, zostało również omówione oraz poddane dyskusji na forum NATO w ramach grupy Industrial Resources and Communications Services.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Wdrażanie ramowego programu działań z SENDAI na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof

Beata Janowczyk
Rządowe Centrum Bezpieczeństwa

Z roku na rok obserwujemy wzrost częstotliwości występowania ekstremalnych zjawisk pogodowych. Każdego roku kilkadziesiąt tysięcy osób na świecie umiera wskutek katastrof. Ramowy program działań z Sendai na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof został przyjęty podczas Trzeciej Światowej Konferencji ONZ, która odbyła się w 2015 r. w Sendai w Japonii. Program jest odpowiedzią na coraz częściej występujące i przynoszące coraz większe straty klęski żywiołowe i katastrofy, zarówno naturalne, jak i związane z działalnością człowieka. Głównym jego celem jest znaczące ograniczenie liczby ofiar śmiertelnych 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. Unia Europejska odegrała wiodącą rolę w negocjacjach dotyczących przygotowania Programu działań z Sendai, a wiele jego zaleceń opiera się na istniejących politykach i programach UE w zakresie zarządzania ryzykiem. 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 Programu.

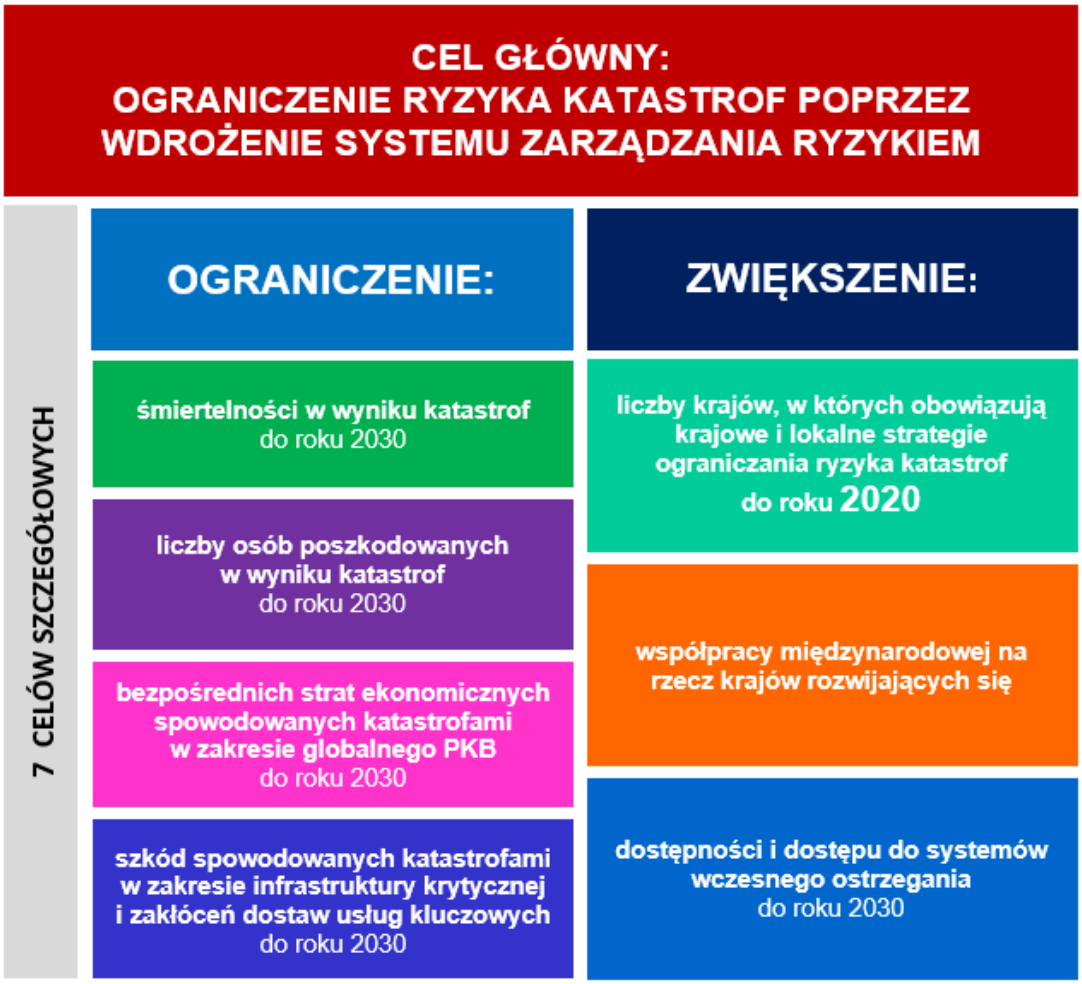
Według danych Organizacji Narodów Zjednoczonych, do katastrof powodujących w ostatnich latach największe straty należą: powodzie, susze, silne burze, huragany oraz wielkoobszarowe pożary lasów. Najdobitniej potwierdzają to dane ekonomiczne. W latach 1998-2017 kraje dotknięte klęskami odnotowały straty finansowe w wysokości 3 tys. miliardów dolarów, co stanowi 150 proc. więcej w porównaniu do poprzedniego 20-lecia. Jeśli chodzi o Unię Europejską, ze środków Funduszu Solidarności w latach 2009-2018 udzielono pomocy dla 24 państw o wartości 5,5 mld Euro.

Wskazane powyżej trendy doprowadziły do zmiany nie tylko w sposobie myślenia, ale również w podejściu do przeciwdziałania klęskom żywiołowym i katastrofom. Zrozumienie ryzyka związanego z katastrofami jest pierwszym priorytetem *Programu działań z Sendai*. Zaczynamy dążyć do tego, aby z jednej strony minimalizować prawdopodobieństwo zdarzeń, z drugiej zaś ograniczać ich skutki. Koncepcja ta, oparta na zarządzaniu ryzykiem wystąpienia katastrof, jest drugim priorytetem *Programu*. Wpisuje się także w politykę Unii Europejskiej i *Unijnego Mechanizmu Ochrony Ludności*[1], który nałożył na państwa członkowskie obowiązek osiągnięcia w 2020 r. pełnej zdolności zarządzania ryzykiem. Jest to proces rozpoczynający się od oceny ryzyka, poprzez planowanie zarządzania nim w celu zapobiegania wystąpieniu zagrożenia, a następnie skutecznego przygotowania się do reagowania w przypadku zaistnienia sytuacji kryzysowych. W tym celu konieczne jest opracowanie planów zarządzania ryzykiem, powiązanych ze strategiami adaptacji do zmian klimatu. Ocena ryzyka wystąpienia katastrof musi opierać się na scenariuszach zmian klimatu.

Warunkiem spełnienia tych wymagań będzie przesłanie do końca roku do Komisji Europejskiej *Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem*. Jest to także wymóg kolejnej perspektywy finansowej Unii Europejskiej na lata 2021-2027, a więc realizacja tego zadania będzie miała bezpośrednie przełożenie na pozyskiwanie środków finansowych w ramach polityki spójności.

Kolejnym wyzwaniem, które stoi przed Polską, jest zmiana w obszarze inwestowania w zarządzanie ryzykiem związane z katastrofami. Jednym z priorytetów *Programu działań z Sendai* jest właśnie wzmocnienie wysiłków na rzecz budowania odporności państwa poprzez inwestycje, także w obszarze sektora prywatnego, w szczególności infrastruktury krytycznej. Oczywiste jest, że bardziej opłaca się budować infrastrukturę odporną na katastrofy niż modernizować konstrukcje niespełniające warunków bezpieczeństwa.

[1] Decyzja Parlamentu Europejskiego i Rady (UE) 2019/420 z dnia 13 marca 2019 r. zmieniająca decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności.



Cele *Ramowego programu działań z Sendai na lata 2015-2030 w sprawie ograniczenia ryzyka katastrof*

Według Biura Narodów Zjednoczonych ds. Ograniczenia Ryzyka Katastrof, problemem w skali światowej jest to, że na usuwanie skutków katastrof wydajemy cztery razy więcej niż na zapobieganie. Ideą *Programu działań z Sendai* jest m.in. zestawienie strat spowodowanych katastrofami. Dzięki temu będziemy posiadać wiedzę, która pomoże nam podjąć decyzję, które obszary wymagają zwiększonych nakładów finansowych na ograniczenie ryzyka. Kolejnym celem *Programu działań z Sendai* jest znaczne zwiększenie dostępu do systemów wczesnego ostrzegania.

Rządowe Centrum Bezpieczeństwa pełni funkcję krajowego punktu kontaktowego dla Organizacji Narodów Zjednoczonych ds. wdrażania postanowień *Programu działań z Sendai*. Jednym z przedsięwzięć wpisanych w te działania jest stworzenie platformy wymiany informacji o krajowych i międzynarodowych inicjatywach podejmowanych na rzecz ograniczania ryzyka katastrof. W platformie uczestniczą nie tylko przedstawiciele administracji rządowej i samorządowej, ale także instytutów naukowo-badawczych, uczelni wyższych, organizacji pozarządowych oraz sektora prywatnego. W ramach platformy, Rządowe Centrum Bezpieczeństwa zorganizowało w dniach 25-26 listopada 2019 r. pierwsze *Krajowe forum ograniczenia ryzyka katastrof*. Konferencja umożliwiła spotkanie wielu środowisk zaangażowanych we wdrożenie *Programu działań z Sendai*. Była to okazja do zapoznania się z przykładami dobrych praktyk w tym zakresie, także pod kątem inicjatyw lokalnych dotyczących adaptacji do zmian klimatu. Jednym z wyzwań, które stoi przed platformą jest określenie zakresu danych o stratach, które będą przesyłane do Organizacji Narodów Zjednoczonych.

Najważniejsza jest jednak kwestia zmiany ustawy o zarządzaniu kryzysowym, która umożliwi wdrożenie w Polsce systemu zarządzania ryzykiem. 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

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

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. 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*.

Od wielu miesięcy Rządowe Centrum Bezpieczeństwa podejmuje działania, aby to osiągnąć. Dostosowania do procesu oceny ryzyka wymaga także *Raport o zagrożeniach bezpieczeństwa narodowego*. Według rozwiązań, zaproponowanych w projekcie zmiany ustawy o zarządzaniu kryzysowym, dokonanie korelacji między regulacjami krajowymi a unijnymi będzie odbywać się bez konieczności opracowywania od podstaw nowych dokumentów planistycznych, lecz z wykorzystaniem obowiązujących. *Raport* w dalszym ciągu dotyczyć będzie oceny ryzyka. Po jej przeprowadzeniu i wskazaniu najistotniejszych zagrożeń dla bezpieczeństwa narodowego, konieczne będzie 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.

Natomiast plany zarządzania kryzysowego podzielone zostaną na plany zarządzania ryzykiem oraz plany reagowania kryzysowego. Plany zarządzania ryzykiem odnosić się będą do działań uczestników zarządzania kryzysowego w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do przejmowania nad nią kontroli, a plany reagowania kryzysowego dotyczyć będą przedsięwzięć realizowanych w sytuacji kryzysowej, w tym związanych z usuwaniem jej skutków.

Podkreślenia wymaga fakt, że rozwiązania te zostały już zapoczątkowane w *Krajowym planie zarządzania kryzysowego* z 2018 r., który podzielono na cześć A, odnoszącą się do zarządzania ryzykiem, czyli de facto dwóch pierwszych faz zarządzania kryzysowego: zapobiegania i przygotowania oraz część B, dotyczącą reagowania i odbudowy. 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.

Termin wykonania wymaganych przez Komisję Europejską planów zarządzania ryzykiem upływa 8 sierpnia 2020 r. Realizacja tego zadania wiąże się z zaangażowaniem wszystkich szczebli administracji i jak najszybszego rozpoczęcia prac nad przygotowaniem dokumentów. Czas stanowi największe zagrożenie dla tego przedsięwzięcia, a jego realizacja wymaga nowelizacji ustawy o zarządzaniu kryzysowym. Mając na uwadze powiązanie tego zadania z wymogiem spełnienia warunkowości podstawowej w kolejnej perspektywie finansowej UE na lata 2021-2027, brak planów zarządzania ryzykiem uniemożliwi Polsce wykorzystanie środków z funduszy unijnych. Oznaczałoby to straty rzędu kilkunastu miliardów Euro.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

LIBERO 2019 – ćwiczenie sprawdzające procedury systemu zarządzania kryzysowego

Martyna Olejnik-Kołodziej
Rządowe Centrum Bezpieczeństwa

Zgodnie z ustawą 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2018 r. poz. 1401 z późn. zm.) do zadań Rządowego Centrum Bezpieczeństwa (RCB) należy planowanie cywilne, w tym opracowywanie i aktualizowanie Krajowego Planu Zarządzania Kryzysowego (KPZK). Jednym z etapów planowania jest testowanie opracowanego planu przede wszystkim poprzez ćwiczenia. W związku z powyższym, Rządowe Centrum Bezpieczeństwa wspólnie z Ministerstwem Gospodarki Morskiej i Żeglugi Śródlądowej (MGMiŻŚ) oraz Miejskim Przedsiębiorstwem Wodociągów i Kanalizacji w m.st. Warszawie S.A. (MPWiK) zaplanowało i przeprowadziło ćwiczenie sprawdzające działanie podmiotów w sytuacji wystąpienia zakłóceń w systemie zaopatrzenia w wodę i odprowadzania ścieków. Była to piąta edycja ćwiczenia LIBERO. Kolejne tego typu krajowe ćwiczenie odbędzie się w 2021 roku.

Ogólnopolskie, wieloszczeblowe ćwiczenie o charakterze sztabowym z epizodem praktycznym LIBERO 2019 odbyło się od 5 do 7 listopada 2019 r. Kierownikiem przedsięwzięcia był Grzegorz Świszcz – zastępca dyrektora RCB. Udział w nim wzięły ministerstwa, służby, województwa, gminy, powiaty i przedsiębiorstwa[1]. Uczestnicy ćwiczenia mogli również zaangażować służby i jednostki podległe lub nadzorowane. Przedsięwzięcie służyło sprawdzeniu rozwiązań organizacyjnych zawartych w planach zarządzania kryzysowego podmiotów ćwiczących oraz ich funkcjonalności w sytuacji zakłóceń w systemie zaopatrzenia w wodę i odprowadzania ścieków. Ponadto przetestowano procedury współpracy organów administracji publicznej, służb i instytucji w przypadku powyższych zakłóceń. Sprawdzony zostały obieg informacji, sposób prowadzenia polityki informacyjnej przez podmioty zaangażowane oraz koordynacja polityki informacyjnej przez instytucję wiodącą w sytuacji kryzysowej. W trakcie ćwiczenia uruchomiona była Ćwiczebna Internetowa Strona Komunikacji Medialnej (CISKOM), która stanowiła dla wszystkich uczestników dodatkową platformę informacyjną – z jednej strony symulującą aktywność mediów, z drugiej pokazującą aktywność i działania służb prasowych poszczególnych instytucji zaangażowanych w kryzys. Wszystkie podmioty ćwiczące zobowiązane były do bieżącego monitorowania tej strony.

Ćwiczenie prowadzone było na rzeczywistych stanowiskach pracy w siedzibach podmiotów ćwiczących z wykorzystaniem funkcjonujących kanałów łączności i środków przekazu. Wykreowana w scenariuszu sytuacja ćwiczenia dotyczyła całego kraju, ale jedynie trzy województwa podejmowały działania: mazowieckie, łódzkie i śląskie.

Pierwszy dzień ćwiczenia (5.11.2019) rozpoczął się o godz. 9:00 epizodem praktycznym na terenie obiektów należących do Miejskiego Przedsiębiorstwa Wodociągów i Kanalizacji w m.st. Warszawie S.A. Scenariusz zakładał, iż grupa terrorystów dokonała ataku na obiekty MPWiK i wzięła 50 zakładników (podoficerów SGSP będących na zaplanowanej wizycie), a także wtargnęła na teren dyspozytorni. Na miejsce zdarzenia przybyli funkcjonariusze Centralnego Pododdziału Kontrterrorystycznego Policji „BOA" i Agencji Bezpieczeństwa Wewnętrznego. Prowadzone były negocjacje. Ostatecznie przeprowadzono siłowe odbicie zakładników.

[1] Kancelaria Prezesa Rady Ministrów, Rządowe Centrum Bezpieczeństwa, Ministerstwa: Gospodarki Morskiej i Żeglugi Śródlądowej, Energii, Spraw Wewnętrznych i Administracji, Obrony Narodowej, Zdrowia, Cyfryzacji, Środowiska, Komendy Główne: Policji i Państwowej Straży Pożarnej, Agencja Bezpieczeństwa Wewnętrznego, Urzędy Wojewódzkie: Mazowiecki, Łódzki i Śląski, Urzędy Miasta: Stołecznego Warszawy, Grodziska Mazowieckiego, Rybnika, Wodzisławia Śląskiego, Brzeziny, Skierniewice, Wielunia, Łodzi, Starostwa Powiatów: Grodziskiego, Rybnickiego, Wodzisławskiego, Brzezińskiego, Skierniewickiego, Wieluńskiego, a także Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A., Zakład Wodociągów i Kanalizacji Sp. z o. o. w Grodzisku Mazowieckim, Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. w Rybniku, Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. w Wodzisławiu Śląskim, Zakład Usług Komunalnych Sp. z o.o. w Brzezinach, Zakład Wodociągów i Kanalizacji WOD-KAN Sp. z o.o. w Skierniewicach, Przedsiębiorstwo Komunalne Sp. z o.o. w Wieluniu oraz Zakład Wodociągów i Kanalizacji Sp. z o.o. w Łodzi.

Źródło: Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji w m.st. Warszawie S.A.

Równolegle rozpoczęła się część aplikacyjna ćwiczenia. Zespół Kierowania Ćwiczeniem przy wykorzystaniu środków łączności jawnej (e-mail, telefon) przekazywał wybranym ćwiczącym informację o aplikacyjnym wydarzeniu. Była to informacja ogólna, wymuszająca potrzebę zdobycia przez ćwiczących bardziej szczegółowych danych o zdarzeniu, np. poprzez kierowanie pytań do innych ćwiczących lub monitorowanie strony internetowej symulującej pracę mediów (CISKOM) oraz podjęcie właściwych działań. Zdarzenia rozgrywały się w ośmiu przedsiębiorstwach na terenie trzech województw. Każde zdarzenie dostosowane było do specyfiki miejscowości i lokalizacji przedsiębiorstwa. W ramach scenariusza wprowadzonych zostało 5 zdarzeń, o bardzo zbliżonej treści dla każdego przedsiębiorstwa.

Pierwszym zdarzeniem było porwanie ciężarówki przewożącej chlor, sforsowanie ogrodzenia i uderzenie w budynek na terenie przedsiębiorstwa. Siła uderzenia i prędkość pojazdu powoduje wywrócenie się na bok samochodu, a z naczepy spada 6 beczek płynnego chloru. Z jednej z nich obserwowany był wyciek.

Drugim, pożar wywołany prowadzonymi pracami remontowymi (pożarowo niebezpiecznymi) w jednym z obiektów przez pracowników firmy zewnętrznej. W tym miejscu czujki przeciwpożarowe zostały szczelnie zakryte. Jeden z pracowników zaprósza niedopałkiem papierosa pożar, który błyskawicznie się rozprzestrzenia na inne obiekty.

Trzecim, zniszczenie przewodu tłocznego, które spowodowało ogromny wyciek wody, w postaci gejzeru kilkumetrowej wysokości, i zalanie dróg. Okoliczni mieszkańcy licznie zgłaszali brak wody. Następnie w trakcie prac naprawczych pracownicy przedsiębiorstwa ujawnili pocisk pochodzący z czasów wojny.

Drugiego dnia na wewnętrznym parkingu przedsiębiorstwa doszło do eksplozji i pożaru wielu samochodów należących do pracowników przedsiębiorstwa. Następnie, w wyniku kolejnej eksplozji, doszło do całkowitego zniszczenia dwóch istotnych dla funkcjonowania przedsiębiorstwa obiektów. Zginęło pięciu pracowników przedsiębiorstwa.

Ostatnim zdarzeniem, z którym musieli zmierzyć się uczestnicy ćwiczenia był przeprowadzony w trzecim dniu atak hackerski, w wyniku którego doszło do przerwania komunikacji pomiędzy serwerami oraz stacjami operatorskimi SCADA.

Miesiąc po ćwiczeniu jego uczestnicy mieli możliwość podzielenia się wstępnymi wnioskami podczas konferencji podsumowującej przedsięwzięcie. Zwrócono uwagę, że dalszego doskonalenia wymaga

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

obieg informacji w sytuacji kryzysowej, procedura wprowadzania stopni alarmowych, podział zadań między CSIRT MON, CSIRT GOV i CSIRT NASK oraz współpraca rzeczników prasowych z komórkami merytorycznymi instytucji. Zdiagnozowano także potrzebę dokonania zmian w aktach prawnych.

W pierwszym kwartale 2020 r. zostanie sporządzony Raport Końcowy z ćwiczenia LIBERO 2019, który następnie zostanie przekazany do Kancelarii Prezesa Rady Ministrów i zaprezentowany na Międzyresortowym Zespole do spraw Zagrożeń Terrorystycznych.

Ćwiczenie wojsk USA w Polsce „DEFENDER 2020" – sprawdzian dla cywilnej gotowości do wsparcia operacji obronnej

Sławomir Łazarek
Rządowe Centrum Bezpieczeństwa

Planowane na wiosnę ćwiczenie „DEFENDER 2020" będzie trzecim największym ćwiczeniem wojskowym na kontynencie europejskim od czasu zimnej wojny. Nie będzie to ćwiczenie natowskie, lecz amerykańskie – szczebla dywizyjnego. Jego głównym celem będzie sprawdzenie zdolności armii amerykańskiej do przerzutu sił lądowych z baz w głębi USA do portów na wschodnim wybrzeżu, a następnie do portów morskich w Europie. Po rozładunku sprzętu wojskowego ze statków nastąpi jego dalsze przemieszczenie transportem lądowym do rejonów operacyjnego przeznaczenia poprzez terytorium Niemiec i Polski do państw bałtyckich. Główny ciężar zabezpieczenia transportowego spocznie na stronie cywilnej – administracji państwowej, zarządcach infrastruktury portowej, drogowej i kolejowej oraz na przewoźnikach komercyjnych. W połączonych manewrach weźmie udział łącznie 37 tys. żołnierzy ze Stanów Zjednoczonych, ale też państw sojuszniczych i partnerskich.

Polska i Stany Zjednoczone Ameryki kontynuują wzmacnianie swoich strategicznych relacji, które mają na celu poprawę naszego bezpieczeństwa, a także bezpieczeństwa całego NATO. Na podstawie „Wspólnej deklaracji o współpracy obronnej w zakresie obecności sił zbrojnych Stanów Zjednoczonych na terytorium Rzeczypospolitej Polskiej" z 12 czerwca 2019 r. kontynuowane są prace nad umacnianiem więzi wojskowych między Rzeczpospolitą a USA oraz zwiększaniem amerykańskich zdolności do odstraszania i obrony Polski. Zdolności te obecnie obejmują około 4500 personelu wojskowego, który stacjonuje u nas na zasadzie rotacyjnej[1]. Siły o takiej wielkości nie będą jednak wystarczające do odparcia ewentualnej zbrojnej napaści, ale w połączeniu z wojskami państwa czy też państw zagrożonych są poważnym elementem odstraszania oraz mogą „kupić czas" niezbędny dla rozwinięcia głównych sił obrony.

ROLA PAŃSTWA-GOSPODARZA

Dla powodzenia skutecznej obrony północno-wschodniej flanki NATO, w tym Polski i państw bałtyckich, kluczowym czynnikiem jest zabezpieczenie terminowego i sprawnego przemieszczenia sił sojuszniczych oraz ich logistycznego wsparcia podczas prowadzenia operacji[2]. Odnosi się to także do sytuacji, w której nie mamy do czynienia z działaniami pod egidą NATO, ale kiedy w operacji biorą udział wojska tylko jednego państwa sojuszniczego udzielającego wsparcia w ramach współpracy dwustronnej, np. polsko-amerykańskiej. Od sprawności w wypełnieniu tej roli w razie kryzysu i wojny zależy w dużej mierze bezpieczeństwo Polski, jak również państw bałtyckich, dla których zabezpieczenie dróg wejścia sojuszniczych sił wzmocnienia od strony Przesmyku Suwalskiego jest kwestą zasadniczą.

Tak duże planowane zaangażowanie sił zbrojnych USA na naszym obszarze, doprowadziło do podjęcia przez Waszyngton w 2018 roku decyzji o przeprowadzeniu serii ćwiczeń wojskowych pod kryptonimem „DEFENDER" nie tylko na półkuli południowej, jak to miało miejsce w poprzednich latach, ale również na terytorium Europy. Począwszy

[1] Źródło: https://www.gov.pl/web/obrona-narodowa/wielki-dzien-dla-polski-deklaracja-o-wspolpracy-obronnej-podpisana.

[2] Polska – jako członek NATO – zobligowana została do przestrzegania zobowiązań sojuszniczych. Jednym z nich jest udzielanie siłom sojuszniczym przybywającym do naszego kraju wsparcia jako państwo-gospodarz w ramach systemu Host Nation Support (HNS). Prawidłowe funkcjonowanie wsparcia przez Polskę ma kluczowe znaczenie dla obronności naszego kraju, a także jego wiarygodności jako partnera działań wojsk sojuszniczych związanych z obronną kolektywną.

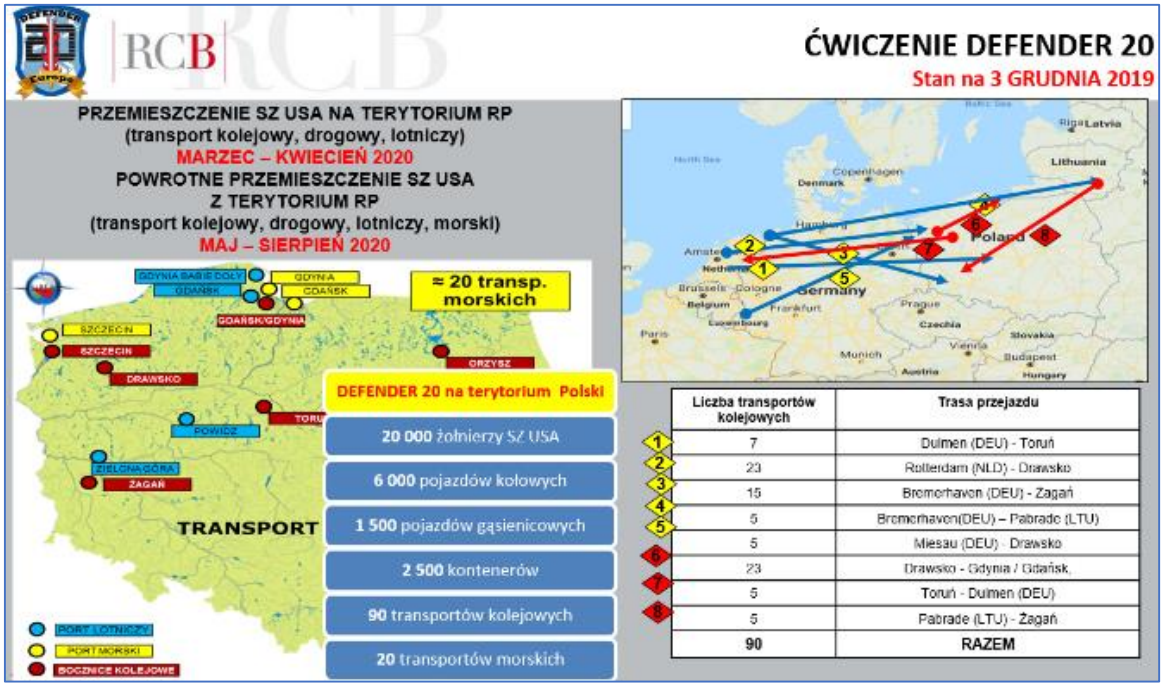
od 2020 roku „DEFENDER" stanie się ćwiczeniem cyklicznym prowadzonym na dwóch obszarach strategicznych: Pacyfiku oraz Europy[3]. Scenariusz manewrów obejmuje przerzut aż 25 tys. żołnierzy do Europy z baz położonych w USA.

W manewrach 2020 roku wezmą udział siły m.in. z wojsk lądowych: dowództwo dywizji, trzy brygady pancerne, brygada artylerii oraz jednostki wsparcia tych sił. Oprócz tego będą uczestniczyć także jednostki sił powietrznych i piechoty morskiej USA.

W czasie pierwszego z serii ćwiczenia „DEFENDER 2020", które w znacznej części realizowane będzie na terytorium Polski, wsparcie przez państwo-gospodarza odgrywać będzie kluczową rolę dla zabezpieczenia ćwiczenia.

Będzie to największe, jak dotychczas, ćwiczenie wojsk amerykańskich w Polsce. Głównym celem szkoleniowym nie jest jednak, jak to określił Szef Sztabu Generalnego WP, generał Rajmund Andrzejczak „*typowa wojskowa strzelanka*", tylko sprawdzenie możliwości przemieszczenia na dużą odległość znacznej ilości wojsk wraz ze sprzętem, i to tym najcięższym, a także sprawdzenie możliwości zabezpieczenia logistycznego ich na terenie Polski. **Skala ćwiczenia, tj. przegrupowanie do Polski około 20 tys. żołnierzy SZ USA, 6 000 pojazdów kołowych, 1 500 pojazdów gąsienicowych, 2 500 kontenerów wymagać będzie współpracy w zasadzie wszystkich komórek organizacyjnych resortu obrony narodowej oraz układu pozamilitarnego.** Do powyższych liczb należy doliczyć pojazdy kołowe oraz sprzęt gąsienicowy Wojska Polskiego, biorącego udział czy to w równoległych ćwiczeniach towarzyszących czy też w zabezpieczeniu logistycznym. Z większych zaangażowanych jednostek wojskowzch po polskiej stronie należy wymienić: 12 oraz 16 Dywizje Zmechanizowane, 6 Brygadę Powietrzno-Desantową oraz 1 Brygadę Logistyczną.

Ponadto, z polskiej perspektywy, ćwiczenie będzie doskonałą sposobnością do przetestowania wdrażanego właśnie nowego narodowego systemu wsparcia przez państwo-gospodarza[4], jak również procedur wynikających z aktów prawnych regulujących obecność wojsk obcych na terytorium Polski. Ramowy plan przemieszczeń przedstawia rysunek nr 1.



Rys. nr 1. Ramowy plan przemieszczeń.

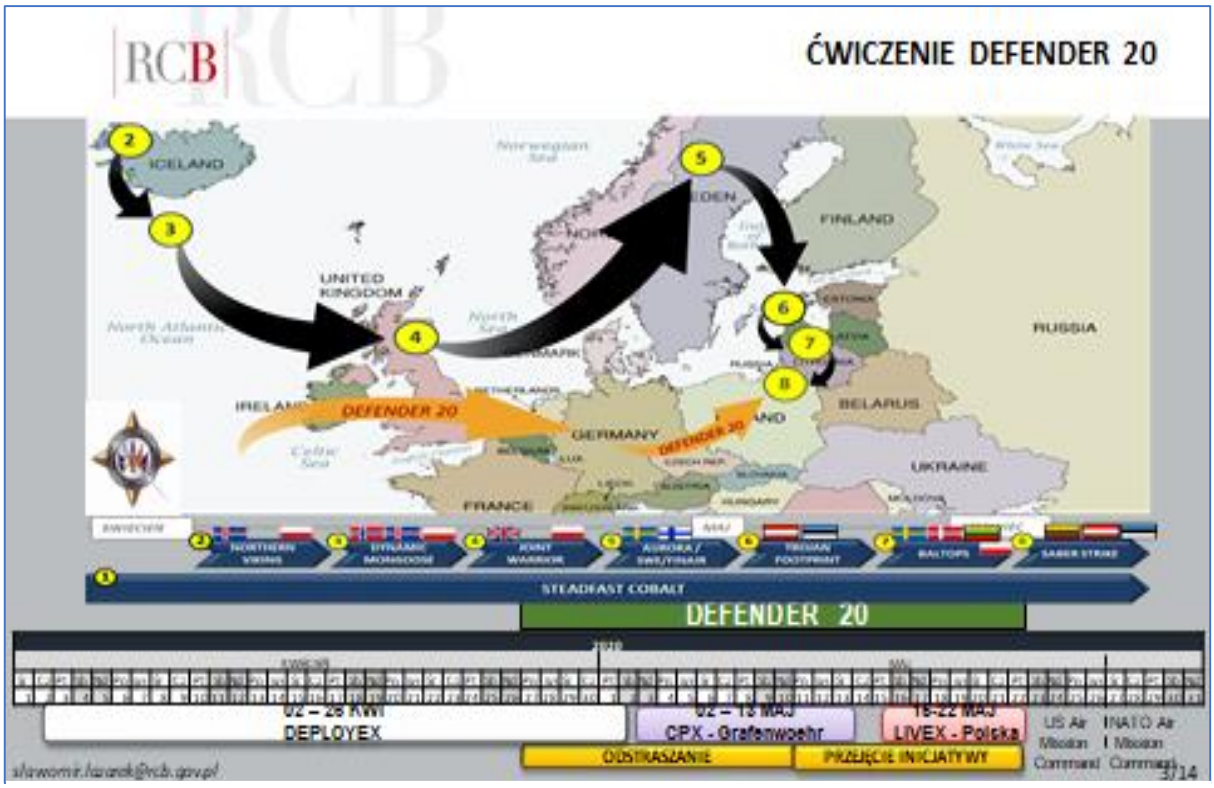
[3] Zgodnie z wypowiedzią Dowódcy Sił Lądowych USA na Pacyfik Generała Johna Johnsona „co drugi rok będzie „lekkim" w odniesieniu do zaangażowanych sił i środków dla danego regionu. W 2020 r. będzie „ciężki" na obszarze Europy, a „pacyficzna wersja" będzie mniejsza. W kolejnym 2021 r. będzie odwrotnie.

[4] Tak jak to wynika z „Koncepcji funkcjonowania narodowego systemu wsparcia przez państwo-gospodarza (HNS)" zatwierdzonej przez Ministra Obrony Narodowej 4 grudnia 2018 r.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Zgodnie ze schematem przedstawionym na rysunku nr 2 (poniżej), przemieszczenie sił USA na terytorium Polski rozpocznie się na początku marca, natomiast zakończy się pod koniec kwietnia 2020 r. Realizowane będzie przy wykorzystaniu transportu drogowego, kolejowego i lotniczego. Sprzęt kołowy przemieszczany będzie w konwojach po drogach publicznych, natomiast sprzęt gąsienicowy głównie transportem kolejowym, ale także częściowo również na kołowych zestawach niskopodwoziowych. Należy zaznaczyć, że część sprzętu zostanie przemieszczona z USA, a część jednostek wykorzysta wyposażenie składowane w Europie w ramach systemu *Army Prepositioned Stock* (APS)[5]. Aktualnie APS znajdują się głównie na zachodzie Europy i jest w nich składowany sprzęt dla jednej brygady pancernej, jednostek artylerii oraz wsparcia i dowodzenia. Trwają prace, aby niedługo taki APS dla kolejnej brygady pancernej powstał w Polsce (m.in. trwa rozbudowa bazy w Powidzu). „DEFENDER 2020" będzie między innymi testował ten nowy system baz „wysuniętego składowania sprzętu wojskowego" w Europie.

Bardzo istotną sprawą podczas ćwiczenia będzie zapewnienie swobody przemieszczania (*Freedom of Movement*) przez terytorium naszego państwa dla ćwiczących wojsk amerykańskich (przekraczanie granic na kolejowych i drogowych przejściach granicznych, korzystanie z naszych dróg i kolei, koordynacja transportów kołowych i kolejowych). Poza organizacją przerzutu, która jest bardzo ważna, sporym wyzwaniem będzie infrastruktura. Pomimo upływu wielu lat od rozwiązania Układu Warszawskiego państwa naszego regionu, w tym Polska, mają jeszcze sporo do zrobienia w dziedzinie modernizacji infrastruktury transportowej[6].



Rys. nr 2. Harmonogram ćwiczenia „DEFENDER 20".

[5] *Army Prepositioned Stock* (APS) – system baz „wysuniętego składowania sprzętu wojskowego".

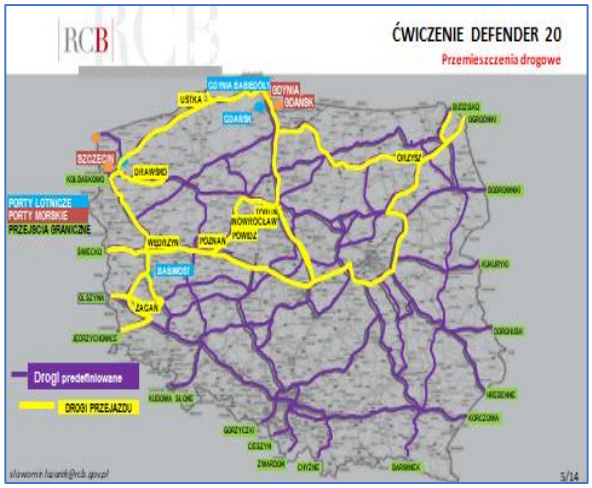
[6] Szczególnymi „wąskimi gardłami" na naszych drogach są obiekty inżynierskie (przede wszystkim mosty i wiadukty oraz tunele), których nośność czy wielkość nie pozwala na swobodny przejazd ciężkiego sprzętu wojskowego. Nierozwiązanym wyzwaniem jest brak kompatybilności połączenia kolejowego Polski z państwami bałtyckimi. W Polsce tory zbudowane są wg rozstawu normalnotorowego (1435 mm) a na Litwie szerokotorowego (1520 mm), z tego też powodu transporty kolejowe muszą być przeładowywane na inne wagony. A to zabiera wojskowym cenny czas niezwykle ważny szczególnie w pierwszej fazie operacji odstraszania czy już obrony.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

WYZWANIE DLA SFERY CYWILNEJ

Ogromną rolę w realizacji wsparcia przez państwo-gospodarza podczas tego wielkiego ćwiczenia odgrywać będzie strona cywilna wraz ze służbami podległymi MSWiA, a w tym w szczególności:

- **Generalna Dyrekcja Dróg Krajowych i Autostrad** (GDDKiA), która będzie koordynować i zabezpieczać transporty kołowe po drogach publicznych, czyniąc to we współpracy z Szefostwem Transportu i Ruchu Wojsk – Centrum Koordynacji Ruchu Wojsk (STRW-CKRW) oraz innymi zarządcami dróg publicznych. Przemieszczenia będą się odbywały na terenie całej Polski z wykorzystaniem wszystkich kategorii dróg (tj. krajowych, wojewódzkich, powiatowych i czasami gminnych). Okresowo będą występowały w związku z tym duże utrudnienia w ruchu dla pojazdów cywilnych na poszczególnych odcinkach dróg. Główne drogi planowanych przemieszczeń drogowych przedstawiono na rysunku nr 3.



Rys. nr 3. Główne trasy przemieszczeń drogowych.

- **Polskie Koleje Państwowe PKP Cargo S.A.**, które będą zabezpieczać transporty kolejowe (około 90 transportów) przy ścisłej współpracy i koordynacji z zarządcą narodowej infrastruktury kolejowej **PKP Polskie Linie Kolejowe S.A.** oraz koordynatorem po stronie wojskowej czyli z STiRW-CKRW. Przemieszczenia te będą również zabezpieczane po raz pierwszy z użyciem nowo zakupionych ciężkich platform kolejowych do przewozu techniki wojskowej o wadze do 90 ton. Dzięki temu zakupowi (sfinansowanemu przez MON z programu Pozamilitarnych Przygotowań Obronnych RP) Polska uzyskała możliwość transportu najcięższych czołgów naszych sojuszników (np. amerykańskich typu M1 Abrams czy brytyjskich typu Challenger) bez konieczności użyczania wagonów od kolei niemieckich, tak jak się to zdarzało dotychczas.
- **Zarządy Portów Morskich w Gdyni, Gdańsku i Szczecinie** – skąd realizowane będzie przemieszczenie powrotne sprzętu wojskowego do USA (około 20 transportów morskich). W tym miejscu warto wyjaśnić, że z uwagi na zamiar strony amerykańskiej, przećwiczenia i sprawdzenia różnych opcji przemieszczenia strategicznego, transporty morskie ze sprzętem znajdującym się w bazach na terenie Stanów Zjednoczonych będą realizowane do portów na Morzu Północnym (gównie do Niemiec oraz Holandii), a nie bezpośrednio do portów polskich. Następnie będą przeładowywane na transport kolejowy (przede wszystkim ciężki sprzęt gąsienicowy) oraz drogowy i kierowane szlakami lądowymi do Polski.
- **Porty lotnicze w Gdyni, Gdańsku, Zielonej Górze, Powidzu i Gdyni-Babie Doły** przez które zabezpieczane będą transporty wojsk amerykańskich, głównie żołnierzy bez sprzętu.
- **Straż Graniczna**, która będzie zabezpieczała przekraczanie granic. Okresowo na tzw. „zielonej granicy" będą widoczne wzmożone patrole SG, wspierane często przez żołnierzy z podsystemu transportu i ruchu wojsk (działających w ramach Grup Kontroli Ruchu (GKR) wydzielanych z Wojskowych Komend Transportu).
- **Krajowa Administracja Skarbowa** (oddziały celne), która będzie realizowała zadania związane z odprawami celnymi.
- **Policja**, która swoimi siłami będzie uczestniczyła w zabezpieczeniu przemieszczeń drogowych, głównie na terenie dużych aglomeracji miejskich oraz wspierała Żandarmerię Wojskową w zabezpieczeniu prewencyjnym wojsk biorących udział w ćwiczeniu.

Do zabezpieczenia ćwiczenia wykorzystywanych będzie większość baz szkoleniowych SZ RP zlokalizowanych na terytorium Polski. Głownie będą to:

- ośrodki szkolenia poligonowego w: Drawsku Pomorskim, Żaganiu, Wędrzynie, Toruniu, Ustce i Orzyszu;
- bazy Lotnicze w: Mirosławcu i Świdwinie;

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

- tereny jednostek wojskowych w: Poznaniu, Powidzu, Inowrocławiu.

Ponadto, po zakończeniu głównej części ćwiczenia, w celu czasowego przechowania sprzętu wojskowego i przygotowania go do transportu morskiego (m.in. mycie sprzętu przed załadunkiem) planuje się wykorzystać tereny jednostek wojskowych w miejscowościach: Szczecin, Stargard, Gdynia-Babie Doły, Pruszcz Gdański.

W ramach powrotu wojsk amerykańskich do macierzystych baz, które realizowane będzie od końca maja do sierpnia 2020 r.:

- sprzęt gąsienicowy będzie czyszczony na terenie poligonu drawskiego i przemieszczany transportem kolejowym lub drogowym na zestawach niskopodwoziowych z powrotem do magazynów APS w Niemczech i Holandii,
- sprzęt kołowy przemieszczany będzie po drogach do portu w Szczecinie, czyszczony i transportowany drogą morską do magazynów APS w Niemczech i Holandii,
- sprzęt kołowy, który był przerzucony na ćwiczenie z USA, przemieści się po drogach do portów w Gdańsku i Gdyni, gdzie będzie wyczyszczony, zabezpieczony i przetransportowany statkami do baz w USA.

W związku ze skalą ćwiczenia i koniecznością koordynacji zabezpieczenia wojsk ćwiczących w ramach wsparcia przez państwo-gospodarza, w Inspektoracie Wsparcia SZ rozwinięte zostaną z początkiem stycznia 2020 r. struktury Centrum Koordynacji HNS (Host Nation Support Coordination Centre, HNSCC).

W proces koordynacji wsparcia przez państwo-gospodarza włączona zostanie także sieć etatowych i nieetatowych punktów kontaktowych HNS w ogniwach militarnych i niemilitarnych. Aktualnie trwają prace planistyczne oraz uzgodnienia, które mają określić zakres oczekiwanego przez wojsko wsparcia ze strony cywilnej. Decydują się też sprawy związane zaangażowaniem osób z cywilnych instytucji i przedsiębiorstw w trakcie ćwiczenia (np. uruchomienie stałego dyżuru, powołanie grup operacyjnych w miejscu pracy czy czasowe delegowanie przedstawicieli do HNSCC).

„DEFENDER 2020" będzie, według słów Dowódcy Armii Amerykańskiej na Europę, generała Chrisa Cavoli „bardzo wielką sprawą," ponieważ pokaże, że Stany Zjednoczone oraz ich sojusznicy, w tym Polska, posiadają zdolności do odstraszania i powstrzymania konfliktu na kontynencie europejskim dzięki szybkiemu przerzutowi i zabezpieczeniu licznych sił w zagrożone rejony Sojuszu. Ćwiczenie zdolności poszczególnych państw do szybkiego przerzutu na ogromne odległości bardzo dużych i ciężkich jednostek wojskowych, która to zdolność jest postrzegana jako kluczowa dla powstrzymywania potencjalnej agresji, jest koniecznością i zarazem odpowiedzią na aktualne wyzwania i zagrożenia.

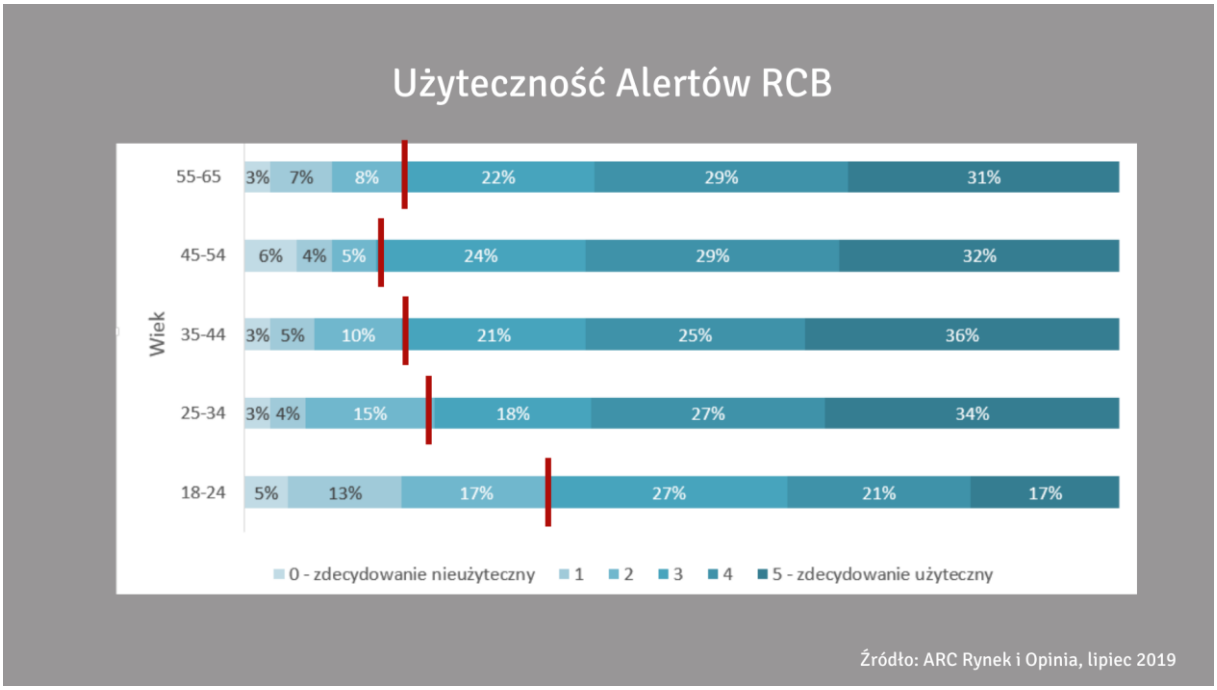
Alert RCB – dotychczasowe doświadczenia

Paweł Majcher
Rządowe Centrum Bezpieczeństwa

SMS-owy system powiadamiania o zagrożeniach – Alert RCB w pełnej funkcjonalności działa już ponad rok. 12 grudnia 2018 roku weszła w życie nowelizacja ustawy o zarządzaniu kryzysowym, która prawnie usankcjonowała system po 6 miesiącach pilotażu. W ciągu tego czasu, według badań opinii publicznej, Alert RCB – SMS-a z ostrzeżeniem otrzymało 81% Polaków. Dotychczasowe doświadczenia podsumowano na grudniowej konferencji zorganizowanej przez Rządowe Centrum Bezpieczeństwa.

Odbiór społeczny Alertu RCB wskazuje, że ostrzeżenia wysyłane SMS-ami wpisują się w oczekiwania Polaków, którzy chcą być powiadamiani właśnie przez telefon komórkowy o zdarzeniach, które mogą zagrozić ich życiu i zdrowiu. Badania opinii społecznej przeprowadzone przez „ARC Rynek i Opinia" to potwierdzają. Polacy twierdzą, że Alert RCB jest pomocny i potrzebny. 58% Polaków uważa, że Alerty RCB są bardzo użyteczne[1]. Tylko 10% jest odmiennego zdania.

[1] https://arc.com.pl/Mlodzi-rzadziej-przejmuja-sie-alertami-Rzadowego-Centrum-Bezpieczenstwa-blog-pol-1564647838.html.



Najwyższy odsetek osób, które twierdzą, że ostrzeżenia są bezużyteczne jest wśród osób młodych – 18%, dlatego Rządowe Centrum Bezpieczeństwa będzie prowadziło kolejne kampanie informacyjne skierowane głównie do młodzieży. Do tej pory RCB wspólnie z Ośrodkiem Rozwoju Edukacji przygotowało kurs e-learningowy dla nauczycieli, scenariusze lekcji, plakaty oraz animacje o SMS-owym systemie ostrzegania.

JAK POLACY REAGUJĄ PO OTRZYMANIU ALERTU RCB

Zdecydowana większość Polaków deklaruje stosowanie się do zaleceń zawartych w ostrzeżeniach otrzymanych SMS-em – tak wynika z badań. Robi to aż 72% respondentów. Częściej są to kobiety (80% kobiet, 64% mężczyzn), najrzadziej osoby najmłodsze, do 24 roku życia – tylko 57% z nich stosuje się do zaleceń.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Tylko 1% respondentów w ogóle nie czyta alertów, co oznacza, że krótka, skondensowana SMS-owa forma ostrzeżenia wydaje się być najskuteczniejsza.

ALERT RCB ZAPOBIEGA SKUTKOM ŻYWIOŁÓW

Obecny na konferencji podsumowującej funkcjonowanie Alertu RCB wiceminister spraw wewnętrznych i administracji Maciej Wąsik zaznaczył, że Alert RCB to niezwykle ważny instrument państwa w zapobieganiu skutkom żywiołów. Przypomniał, że system powstał w wyniku tragicznych wydarzeniach w Suszku, gdzie w 2017 roku, w wyniku bardzo gwałtownej burzy, zginęło 2 dzieci odpoczywających na obozie harcerskim. Teraz, gdy funkcjonuje już Alert RCB, informacja o zagrożeniu powinna dotrzeć do zainteresowanych osób przed zdarzeniem, co pozwoli uniknąć tragedii.

O zwiększaniu dostępności do systemów wczesnego ostrzegania przed zagrożeniami mówiła podczas swojej prezentacji doktor Dorota Rucińska z Wydziału Geografii i Studiów Regionalnych Uniwersytetu Warszawskiego. Zdaniem naukowców globalne ocieplanie się klimatu powoduje, że ekstremalne zdarzenia pogodowe będą zdarzały się coraz częściej, dlatego rolą państwa jest ograniczenie ich skutków. Rozwijanie Alertu RCB, szeroka edukacja o zagrożeniach i prawidłowych reakcjach społecznych jest w związku z tym bardzo ważna w najbliższych latach. Dr Michał Brzeziński z Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego podczas omawiania SMS-owych systemów ostrzegania w krajach Unii Europejskiej, zwrócił uwagę, że nowe przepisy wspólnoty nakładają na wszystkie kraje członkowskie obowiązek uruchomienia publicznych systemów ostrzegania na telefony komórkowe. Wicedyrektor Rządowego Centrum Bezpieczeństwa Grzegorz Świszcz zaznaczył, że Alert RCB, jako system SMS-owego ostrzegania ludności, wpisuje się w nowe, europejskie regulacje ujęte w Europejskim Kodeksie Łączności Elektronicznej.

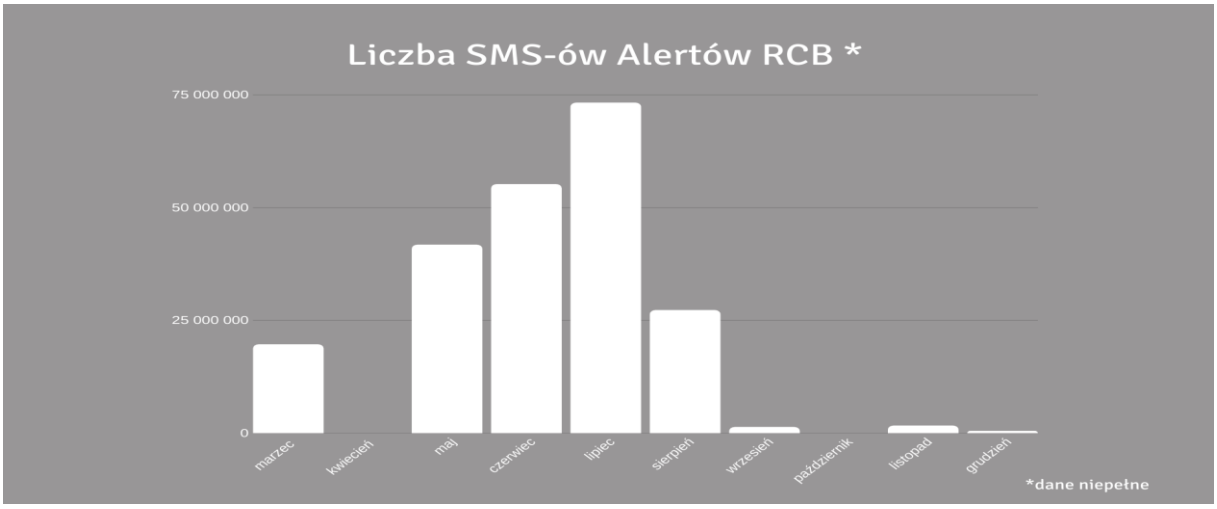
ALERT RCB NIE TYLKO PRZY ZDARZENIACH METEOROLOGICZNYCH

Alert RCB do tej pory był uruchamiany 39 razy, ostrzeżenia rozesłano w ponad 220 milionach SMS-ów. Najczęściej do mieszkańców południowo-wschodniej Polski. Dominowały zdarzenia meteorologiczne, takie jak burze i wichury.

Województwa, na terenie których uruchomiono Alert RCB

województwo	Alert RCB
1. podkarpackie	15
2. małopolskie	15
3. mazowieckie	14
4. świętokrzyskie	12
5. lubelskie	11
6. śląskie	10
7. zachodniopomorskie	10
8. wielkopolskie	7
9. pomorskie	6
10. dolnośląskie	5
11. łódzkie	5
12. lubuskie	5
13. warmińsko-mazurskie	4
14. kujawsko-pomorskie	4
15. podlaskie	4
16. opolskie	2

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l



Coraz częściej Alert RCB jest wykorzystywany również przy innych zdarzeniach. Osoby przebywające na terenie Świnoujścia były ostrzegane, na przykład, podczas neutralizacji niewybuchów z II wojny światowej. Podczas majowego zagrożenia powodziowego, SMS-y były rozsyłane w powiatach położonych wzdłuż Wisły, wraz z przemieszczającą się fala wezbraniową. Były to punktowe ostrzeżenia dla stosunkowo niewielkiej grupy osób bezpośrednio narażonych na zagrożenia.

TECHNOLOGICZNE PROBLEMY ALERTU RCB

Nie ma systemu ostrzegania o 100 procentowej skuteczności. Przede wszystkim, nie wszyscy są użytkownikami telefonów komórkowych. Istnieją jednak bariery technologiczne, które powodują, że Alert RCB nie trafi do każdej, potencjalnie zagrożonej osoby. Mówili o tym przedstawiciele operatorów komórkowych, którzy są odpowiedzialni za dystrybucje ostrzeżeń do użytkowników komórek: Wojciech Maciejczak z Orange oraz Piotr Skibiński z Polkomtela. W swych wystąpieniach zwracali uwagę na ograniczenia wynikające z przepustowości systemów SMS. Zbyt duża liczba abonentów, którzy powinni otrzymać ostrzeżenie powoduje, że nie można w jednym czasie przesłać komunikatu do wszystkich odbiorców. Przy bardzo dużym obszarze (w marcu 2019 roku Alert był uruchomiony na terenie całej południowej Polski) czas dostarczenia SMS-a może trwać nawet 3-4 godziny. Dlatego ważne jest, żeby w przyszłości Alert RCB uruchamiać na zdecydowanie mniejszych obszarach, gdzie prawdopodobieństwo wystąpienia zagrożenia jest najwyższe.

Drugą barierą jest tworzenie przez operatorów bazy numerów, na które są wysyłane ostrzeżenia. Telefony, które znajdą się w tym czasie poza zasięgiem danej sieci, mogą nie otrzymać Alertu RCB, mimo, że znajdują się na obszarze objętym zagrożeniem.

PRZYSZŁOŚĆ ALERTU RCB

Alert RCB, mimo, że jest uzupełnieniem dotychczasowych sposobów ostrzegania, jest najskuteczniejszy. Głównie przez SMS-owy przekaz, który jest najbardziej powszechną formą komunikacji, dostępną na wszystkich telefonach komórkowych. Komunikaty, dzięki temu, że powstają w jednym ośrodku decyzyjnym są ustandaryzowane i zawierają informacje nie tylko o rodzaju zagrożenia, lecz także rekomendacje podstawowych działań dla zagrożonych osób. Jest wykorzystywany tylko w nadzwyczajnych sytuacjach, które zagrażają życiu lub zdrowiu. Największym wyzwaniem, przed którymi stoi teraz Alert RCB, to sprawdzalność prognozowanych zdarzeń. Dyrektor Centrum Meteorologicznej Osłony Kraju IMGW-PIB Agnieszka Harasimowicz podczas relacjonowania dotychczasowych doświadczeń związanych z Alertem RCB zapowiedziała uruchomienie dodatkowych, automatycznych systemów monitoringu niebezpiecznych zjawisk, takich jak intensywne opady deszczu, grad, burze czy silny wiatr – nowcasting (prognoza ultrakrótkoterminowa), które w przyszłości mogą być wykorzystywane przy SMS-owym ostrzeganiu. Wówczas Alert RCB mógłby być wysyłany do osób przebywających w wybranych powiatach tuż przed zdarzeniem. Najważniejszą konkluzją konferencji było to, że powinniśmy dążyć do tego, aby SMS-owe ostrzeżenia były wysyłane jak najbardziej precyzyjnie, tylko do osób bezpośrednio zagrożonych. Jest to najważniejszym zadaniem zarówno instytucji, które dostarczają informacji o potencjalnych zagrożeniach, jak i Rządowego Centrum Bezpieczeństwa.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

VII Krajowe Forum Ochrony Infrastruktury Krytycznej

Witold Skomra
Rządowe Centrum Bezpieczeństwa

13 grudnia 2019 r. odbyło się kolejne, siódme już, Krajowe Forum Ochrony Infrastruktury Krytycznej. Forum jak zwykle zgromadziło operatorów IK, przedstawicieli ministrów nadzorujących poszczególne systemy IK, wojewodów i przedstawicieli nauki. Mimo, że było to kolejne spotkanie w tym gronie, miało ono inny charakter niż poprzednie z uwagi na dwie okoliczności. Po pierwsze po 2 latach przygotowań, RCB rozpoczęło proces zmiany podejścia do wyłaniania infrastruktury krytycznej. Z podejścia obiektowo-systemowego w najbliższych latach zostanie wdrożone podejście usługowo-systemowe. Jest to podejście analogiczne do tego, które już zostało zastosowane przy wdrażaniu ustawy o Krajowym Systemie Cyberbezpieczeństwa. Druga okoliczność, wskazująca na szczególny charakter Forum, to zbliżający się koniec funkcjonowania obowiązującej wersji Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) – rok 2020 powinien zaowocować nową wersją programu. Podjęcie prac uzależnione jest jednak od przebiegu prac legislacyjnych nad nowelizacją ustawy o zarządzaniu kryzysowym, która m.in. diametralnie zmieni krąg podmiotów zaangażowanych w ochronę IK poprzez ustanowienie kategorii infrastruktury lokalnej nadzorowanej przez poszczególnych wojewodów.

Kiedy w roku 2013 przyjmowano pierwszą wersję NPOIK zakładano, że zaplanowane cele zostaną osiągnięte w ciągu 6 lat licząc od 2014 roku. Zbliżamy się więc do wyznaczonego terminu. Zanim jednak nowy NPOIK zostanie opracowany, warto podsumować osiągnięcia i porażki dotychczasowej jego wersji w kilku danych liczbowych, zaprezentowanych podczas Forum. W czasie pierwszego Krajowego Forum Ochrony IK, które odbyło się 4 października 2013. na Stadionie Narodowym w Warszawie, w ramach infrastruktury krytycznej funkcjonowało 169 operatorów odpowiedzialnych za bezpieczeństwo 760 obiektów. Dzisiaj funkcjonuje 128 operatorów i 565 obiektów. Ten pozorny spadek liczby zarówno operatorów, jak i obiektów jest głównie skutkiem procesów konsolidacyjnych w sektorze telekomunikacji i w bankowości. Coraz częściej dostępem do transmisji danych zarządzają scentralizowane systemy teleinformatyczne, zaś klasyczna telefonia oparta o centrale wojewódzkie przestała istnieć. Podobny proces konsolidacji dotknął sektor bankowy, gdzie w miejsce samodzielnych oddziałów powstały ogólnokrajowe korporacje zarządzane w jednolity sposób z wykorzystaniem zintegrowanych narzędzi informatycznych. W efekcie mniejsza liczba operatorów i obiektów IK oznacza dużo poważniejsze skutki społeczne ewentualnej dysfunkcji usług świadczonych przez tych operatorów. Dlatego tak istotnym jest fakt, że ponad 80% obiektów IK posiada funkcjonujące plany ochrony spełniające wymagania opisane w NPOIK.

Kolejny ważny aspekt, omówiony w czasie ostatniego Forum IK, to zintegrowanie procesu wyłaniania operatorów usług kluczowych w rozumieniu ustawy o cyberbezpieczeństwie i w rozumieniu ustawy o zarządzaniu kryzysowym. Problem wynika z faktu, że w ramach Unii Europejskiej obowiązują dwie niespójne regulacje. Jedna dotycząca wyłaniania i ochrony Europejskiej Infrastruktury Krytycznej, a druga, tzw. dyrektywa NIS, dotycząca wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. W efekcie wyłoniono operatorów usług kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, operatorów IK w rozumieniu ustawy o zarządzaniu kryzysowym i takich, którzy podlegają obu tym regulacjom jednocześnie. Pamiętając, że ochrona cyber dotyczy wszystkich operatorów IK i wszystkich form ochrony obiektu IK, celem strategicznym powinno być takie dobranie kryteriów wyłaniania infrastruktury krytycznej, by operator usługi kluczowej wskazał jaką infrastrukturą krytyczną zarządza we własnej organizacji i ta infrastruktura powinna się znaleźć w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. W efekcie, jak podkreślono w czasie Forum, każdy operator usługi kluczowej powinien być operatorem infrastruktury krytycznej. Pozostaje natomiast do dyskusji, czy powinna to być infrastruktura uznawana za lokalną, czy krajową.

Omawiana szeroko w czasie Forum aktualizacja postanowień NPOIK nie wynika wyłącznie z terminów

zawartych w tym programie i konieczności uwzględnienia dyrektywy NIS. We wszystkich dokumentach planistycznych należy uwzględnić proces przekształceń własnościowych w organizacjach biznesowych, a także inne zmiany w otoczeniu prawnym, jak również zmiany w środowisku bezpieczeństwa. Odnosząc się do tego ostatniego zagadnienia, jak podkreślono w czasie Forum, warto zauważyć, że do niedawna ochrona IK była kojarzona wyłącznie z potrzebą utrzymania na akceptowalnym poziomie jakości usług świadczonych na rzecz obywatela. Dzisiaj, w dobie zagrożeń hybrydowych, ochrona IK staje się elementem przygotowań obronnych, zadaniem realizowanym w ramach zobowiązań sojuszniczych w ramach NATO i stanowi zasadniczy komponent budowania odporności państwa na ewentualne zakłócenie i utrzymania ciągłości świadczenia usług kluczowych na wypadek, gdyby to zakłócenie faktycznie wystąpiło. Innymi słowy, klasycznie rozumiane zarządzanie bezpieczeństwem jest zastępowane takimi pojęciami jak „continuity" czyli ciągłość oraz „resilience" czyli odporność. Te dwa ujęcia powinny znaleźć swoje miejsce w nowej wersji NPOIK obok znanego już nam wszystkim kompleksowego zarządzania bezpieczeństwem opartego o tzw. sześciopak czyli sześć form zapewnienia minimalnego poziomu bezpieczeństwa obiektu IK. Podsumowując tę część Forum stwierdzono, że przestajemy się koncentrować wyłącznie na utrzymaniu wysokiego poziomu ochrony (zakładamy, że to już potrafimy), lecz w sposób planowy powinniśmy zapobiegać przyszłym zdarzeniom.

Poza wskazaniem kierunków zmian w zakresie ochrony IK, spotkanie miało na celu omówienie szeregu problemów, jakie dotykają operatorów. Najważniejsze poruszone zagadnienia to ochrona cyber, możliwości wprowadzenia do porządku prawnego minimalnych standardów w zakresie bezpieczeństwa fizycznego, osobowego i teleinformatycznego oraz konieczność włączenia kultury bezpieczeństwa do podstawowych procesów biznesowych u operatorów IK. Odrębnym blokiem zagadnień omawianych w czasie Forum była możliwość zastosowania do ochrony obiektów IK systemów antydronowych. W czasie debaty z udziałem przedstawicieli Ministerstwa Infrastruktury, Polskiej Agencji Żeglugi Powietrznej, Urzędu Lotnictwa Cywilnego, Urzędu Komunikacji Elektronicznej oraz Zarządu Morskiego Portu Gdynia S.A. udało się jedynie wyspecyfikować listę problemów, jakie należy przezwyciężyć, aby zastosowanie ochrony antydronowej było możliwe. Stwierdzono ponadto, że aby prace nad tym zagadnieniem zakończyły się sukcesem, konieczne jest utworzenie zespołu lub grupy eksperckiej o charakterze ponadresortowym.

Zasadniczą konkluzją dyskusji podczas siódmego Krajowego Forum Ochrony IK jest postulat, aby poza możliwością przedstawienia kierunków zmian prawnych, spotkania tego typu stwarzały okazję do omówienia poszczególnych problemów, z jakimi spotykają się operatorzy, w formie zajęć warsztatowych. Sugestia ta zostanie uwzględniona przy organizacji kolejnego Forum na szczeblu ogólnokrajowym.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l