RCB
Rządowe Centrum Bezpieczeństwa

CENTRUM OPERACYJNO-ANALITYCZNE

BIULETYN

KWARTALNY

NUMER 15 KWIECIEŃ – CZERWIEC 2016

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Martyna Olejnik

Anna Zasadzińska-Baraniewska

Recenzenci:

Grzegorz Świszcz – Zastępca Dyrektora RCB

Krzysztof Malesa – Zastępca Dyrektora RCB

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Ustawa o działaniach antyterrorystycznych w kontekście systemu zarządzania kryzysowego

Mariusz Cichomski, Ilona Idzikowska
Ministerstwo Spraw Wewnętrznych i Administracji

Terroryzm stanowi aktualnie jedno z największych wyzwań w kontekście zapewnienia bezpieczeństwa zarówno z perspektywy globalnej, jak i regionalnej czy krajowej, wykraczając poza ramy tradycyjnie rozumianych konfliktów i sytuacji kryzysowych. Wprawdzie Polska nie była dotychczas bezpośrednim celem ataku terrorystycznego, nie oznacza to jednak, że pozostaje zupełnie wolna od tego zagrożenia. Mając na uwadze wzrost poziomu zagrożenia terrorystycznego obserwowany w ostatnim okresie w szczególności w państwach Europy Zachodniej, jak również fakt, że terytorium RP uznawane jest w materiałach rozpowszechnianych przez organizacje terrorystyczne jako potencjalny cel ewentualnych zamachów, podjęto działania legislacyjne w celu poprawy możliwości rozpoznawania i oceniania potencjalnych zagrożeń oraz zapewnienia adekwatnych mechanizmów reagowania na zagrożenia terrorystyczne. Efekt tych działań stanowi obowiązująca od 1 lipca 2016 roku ustawa z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych.

Podstawowym celem opisywanej regulacji jest podniesienie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP, poprzez: wzmocnienie mechanizmów koordynacji działań, doprecyzowanie zadań i obszarów odpowiedzialności poszczególnych służb i organów oraz zasad współpracy między nimi, zapewnienie możliwości skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego, zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń oraz dostosowanie przepisów karnych do nowych typów działań o charakterze terrorystycznym.

Do czasu uchwalenia ustawy *o działaniach antyterrorystycznych* w polskim systemie prawnym nie istniał jeden akt, który kompleksowo regulowałby problematykę rozpoznawania, przeciwdziałania i zwalczania zagrożeń o charakterze terrorystycznym. Wprawdzie do ustawy tej nie zostały inkorporowane wszystkie, rozproszone dotychczas, przepisy odnoszące się do kwestii terroryzmu – zabieg ten w praktyce wydaje się niewykonalny choćby z perspektywy braku możliwości rozpatrywania terroryzmu w oderwaniu od innych przestępstw, czy innego rodzaju sytuacji kryzysowych – jednak ustawa ta wprowadziła szereg nowych instytucji prawnych dedykowanych bezpośrednio tej problematyce oraz ma charakter integrujący.

Dotychczas częściowe regulacje w tym zakresie pozostały m.in. w ustawie z dnia 6 czerwca 1997 r. – *Kodeks karny*, w której uwzględniono definicję przestępstwa o charakterze terrorystycznym (art. 115 § 20), a także dokonano penalizacji zakładania, kierowania oraz udziału w zorganizowanej grupie albo związku mającym na celu popełnienie przestępstwa o charakterze terrorystycznym (art. 258 § 2 i 4), finansowania przestępstwa o charakterze terrorystycznym (art. 165a) oraz rozpowszechniania lub publicznego prezentowania treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym (art. 255a). Ponadto, istotna w opisywanym kontekście pozostaje ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, która określa organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania w tej dziedzinie, a także – do czasu wejścia w życie ustawy *o działaniach antyterrorystycznych* – definiowała pojęcie zdarzenia o charakterze terrorystycznym czy stanowiła podstawę do wydania przepisów wykonawczych wprowadzających do polskiego systemu prawnego stopnie alarmowe. Z kolei kwestie związane z przeciwdziałaniem finansowania terroryzmu zostały określone w ustawie z dnia 16 listopada 2000 r. *o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*. Problematyka reagowania na zagrożenia o charakterze terrorystycznym ujęta jest również w regulacjach dotyczących stanów nadzwyczajnych, a kwestie związane z zadaniami służb i instytucji w odniesieniu do zagrożeń o charakterze terrorystycznym są zawarte

w ustawach kompetencyjnych regulujących ich działanie, a także innych aktach prawa obejmujących wybrane aspekty dotyczące określonego rodzaju zagrożeń. Z kolei szczegółowe procedury reagowania zostały ujęte zarówno w dokumentach o charakterze rządowym czy resortowym, jak i wewnętrznych procedurach poszczególnych służb i instytucji, w tym w planach zarządzania kryzysowego.

Mając na uwadze powyższe, ustawie *o działaniach antyterrorystycznych* nadano charakter integrujący działania podmiotów polskiego systemu antyterrorystycznego z jasnym wskazaniem odpowiedzialności w poszczególnych obszarach. Zastosowane w tej regulacji systemowe podejście do problematyki zagrożeń o charakterze terrorystycznym ma w założeniu umożliwić wykorzystanie potencjału wszystkich służb, organów i instytucji posiadających ustawowe kompetencje do realizowania działań antyterrorystycznych i pozytywnie wpłynąć na szybkość i prawidłowość procesu decyzyjnego na poziomie strategicznym.

Przechodząc do kwestii powiązania ustawy *o działaniach antyterrorystycznych* i ustawy *o zarządzaniu kryzysowym* w pierwszym rzędzie należy zaznaczyć konstrukcyjną analogię podstawowych dla obu regulacji pojęć tj. „działań antyterrorystycznych" i „zarządzania kryzysowego". Poprzez działania antyterrorystyczne należy rozumieć „działania organów administracji publicznej polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków, w tym odtwarzaniu zasobów przeznaczonych do reagowania na nie" (art. 2 pkt 1 ustawy o działaniach antyterrorystycznych), podczas gdy zarządzanie kryzysowe „to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej" (zgodnie z art. 2 ustawy *o zarządzaniu kryzysowym*). Definicje te łączy nie tylko tożsamość zakresu podmiotowego (organy administracji publicznej), lecz również analogia wynikających z nich faz działania, jak stosowane w dotychczas obowiązujących procedurach na podstawie art. 2 ustawy *o zarządzaniu kryzysowym* – fazy zapobiegania, przygotowania, reagowania i odtwarzania. Ustawa *o działaniach antyterrorystycznych* pozostaje zatem spójna z konstrukcją systemu zarządzania kryzysowego, a procedury wynikające z obydwu regulacji mają charakter wzajemnie się uzupełniający. Co więcej, działania antyterrorystyczne, można w tym kontekście odczytywać jako szczególną formę zarządzania kryzysowego, a określające je przepisy jako *lex specialis* względem ogólniejszych przedmiotowo zapisów ustawy *o zarządzaniu kryzysowym*.

Odnosząc się do kolejnych form powiązań pojęciowych i proceduralnych obu regulacji, warto zaznaczyć, że uwzględniając potrzebę uporządkowania aktualnie obowiązujących przepisów, do ustawy *o działaniach antyterrorystycznych* przeniesiono definicję *zdarzenia o charakterze terrorystycznym*, zawartą dotychczas w ustawie *o zarządzaniu kryzysowym* i dostosowano ją do charakteru bieżących zagrożeń.

W opisywanej regulacji jednoznacznie przypisano odpowiedzialność za zapobieganie zdarzeniom o charakterze terrorystycznym Szefowi Agencji Bezpieczeństwa Wewnętrznego. Z kolei w odniesieniu do przygotowania do przejmowania kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć, reagowania w przypadku wystąpienia takich zdarzeń oraz odtwarzania zasobów wykorzystywanych do reagowania na te zdarzenia, jako podmiot wiodący wskazany został minister właściwy do spraw wewnętrznych. Również ten podział pozostaje zgodny z siatką odpowiedzialności dotychczasowego *Krajowego Planu Zarządzania Kryzysowego* wynikającego z ustawy *o zarządzaniu kryzysowym*.

Mając na uwadze dążenie do kompleksowości *nowej* regulacji, w art. 4 zawarto, umieszczony dotychczas w podobnym brzmieniu w art. 12a ustawy *o zarządzaniu kryzysowym*, obowiązek współpracy organów administracji publicznej, właścicieli i posiadaczy obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego. Obowiązek ten obejmuje m.in. niezwłoczne przekazywanie Szefowi Agencji Bezpieczeństwa Wewnętrznego, będących w ich

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

posiadaniu, informacji dotyczących zagrożeń o charakterze terrorystycznym dla infrastruktury administracji publicznej lub infrastruktury krytycznej, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodnokanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa. Wskazano także, że Szef ABW, w przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze administracji publicznej lub infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, może wydawać polecenia organom i podmiotom zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację oraz przekazywać im informacje niezbędne do tego celu. Z kolei ww. organy i podmioty informują Szefa ABW o podjętych w tym zakresie działaniach. Szef ABW, z uwagi na potrzebę zapewnienia możliwości nadzoru i koordynacji, został również zobowiązany do niezwłocznego informowania o podjętych działaniach Ministra Koordynatora Służb Specjalnych.

Na grunt ustawy przeniesiono także dostosowany do wymogów NATO czterostopniowy system stopni alarmowych na wypadek zagrożeń terrorystycznych oraz stopni alarmowych w cyberprzestrzeni (stopni CRP). Dotychczasowy system ten funkcjonował na podstawie zarządzenia nr 18 Prezesa Rady Ministrów z dnia 2 marca 2016 r. *w sprawie wykazu przedsięwzięć i procedur systemu zarzadzania kryzysowego*[1]. Umieszczenie przepisów dotyczących wprowadzania stopni alarmowych w przepisach prawa powszechnie obowiązującego nadało mu walor informacyjny, poza organami, służbami i instytucjami, również dla innych jednostek organizacyjnych i społeczeństwa, a także umożliwiło jego powiązanie z procesem decyzyjnym i realizacją działań nie tylko w sferze administracji publicznej.

W oparciu o art. 16 ust. 1 ustawy, stopnie alarmowe będą mogły być wprowadzane, zmieniane i odwoływane w drodze zarządzenia, w zależności od rodzaju zagrożenia zdarzeniem terrorystycznym, przez Prezesa Rady Ministrów, po zasięgnięciu opinii ministra właściwego do spraw wewnętrznych i Szefa ABW, a w sytuacjach niecierpiących zwłoki – przez ministra właściwego do spraw wewnętrznych, który informował będzie o tym niezwłocznie Prezesa Rady Ministrów, po zasięgnięciu opinii Szefa ABW. Stopień alarmowy lub stopień alarmowy CRP będzie mógł zostać wprowadzony: na całym terytorium Rzeczypospolitej Polskiej, na obszarze jednej lub kilku jednostek podziału terytorialnego kraju, na obszarze określonym w sposób inny niż przez odniesienie do jednostek podziału terytorialnego kraju, dla określonych obiektów jednostek organizacyjnych administracji publicznej, prokuratury, sądów lub innych obiektów infrastruktury administracji publicznej lub infrastruktury krytycznej oraz w przypadku, gdy skutki zdarzenia o charakterze terrorystycznym mogą dotyczyć obywateli polskich przebywających za granicą Rzeczypospolitej Polskiej lub instytucji polskich albo polskiej infrastruktury mieszczących się poza granicami Rzeczypospolitej Polskiej, innych niż placówki zagraniczne Rzeczypospolitej Polskiej, w rozumieniu ustawy z dnia 27 lipca 2001 r. *o służbie zagranicznej*.

W efekcie, w porównaniu do dotychczas obowiązującego porządku prawnego, na gruncie krajowym nastąpiło ograniczenie podmiotowe w zakresie kompetencji wprowadzania stopni alarmowych i jego przeniesienie wyłącznie na poziom odpowiedzialności Prezesa Rady Ministrów, ministra właściwego do spraw wewnętrznych i Szefa ABW (dotychczas w ograniczonym podmiotowo i obszarowo zakresie kompetencja ta przysługiwała również wojewodom, ministrom i kierownikom urzędów centralnych).

Ponadto, na podstawie art. 16 ust. 2 ustawy *o działaniach antyterrorystycznych*, dla określonych placówek zagranicznych Rzeczypospolitej Polskiej, w rozumieniu ustawy *o służbie zagranicznej* lub w odniesieniu do systemów teleinformatycznych ministra właściwego do spraw zagranicznych, stopnie alarmowe wprowadza, zmienia i odwołuje, w drodze zarządzenia, w zależności od rodzaju zagrożenia zdarzeniem o charakterze terrorystycznym, Prezes Rady Ministrów, po zasięgnięciu opinii ministra właściwego do spraw zagranicznych i Szefa Agencji Wywiadu, a w przypadkach niecierpiących zwłoki – minister właściwy do spraw zagranicznych, po zasięgnięciu opinii Szefa Agencji Wywiadu, informując o tym niezwłocznie Prezesa Rady Ministrów. W tym miejscu należy zwrócić uwagę, że w oparciu o zapisy zarządzenia nr 18 Prezesa Rady Ministrów *w sprawie wykazu przedsięwzięć i procedur*

[1] Wcześniej Zarządzenia Nr 74 Prezesa Rady Ministrów z dnia 12 października 2011 r.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

systemu zarzadzania kryzysowego, uprawnienie to przysługiwało również ministrom, kierownikom urzędów centralnych oraz wojewodom – w zakresie ich właściwości.

O wprowadzeniu, zmianie lub odwołaniu stopnia alarmowego lub stopnia alarmowego CRP Prezes Rady Ministrów będzie niezwłocznie informował Prezydenta Rzeczypospolitej Polskiej oraz Marszałka Sejmu i Marszałka Senatu.

Poszczególnym stopniom alarmowym i stopniom alarmowym CRP odpowiada obowiązek realizacji przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego przedsięwzięć, w ramach ich kompetencji ustawowych. Rodzaje i szczegółowy zakres tych przedsięwzięć na terenie Rzeczypospolitej Polskiej określone zostaną w drodze rozporządzenia Prezes Rady Ministrów, przy uwzględnieniu konieczności zapewnienia sprawności przepływu informacji oraz minimalizacji skutków zdarzeń o charakterze terrorystycznym. Natomiast w odniesieniu do rodzajów i szczegółowego zakresu przedsięwzięć wykonywanych przez kierowników polskich placówek zagranicznych w poszczególnych stopniach alarmowych, zostaną one określone w rozporządzeniu ministra właściwego do spraw zagranicznych. Do czasu wejścia w życie ww. aktów wykonawczych pozostaje w mocy, w zakresie nieuregulowanym w ustawie *o działaniach antyterrorystycznych*, zarządzenie nr 18 Prezesa Rady Ministrów *w sprawie wykazu przedsięwzięć i procedur systemu zarzadzania kryzysowego*. W ustawie *o zarządzaniu kryzysowym* pozostał jednak przepis (art. 7 ust. 4) stanowiący delegację dla Prezesa Rady Ministrów do określenia w drodze zarządzenia wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchamianie.

Należy podkreślić, że system stopni alarmowych jest niezależny od możliwości wprowadzenia stanów nadzwyczajnych, przewidzianych w: ustawie z dnia 29 sierpnia 2002 r. *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*, ustawie z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej* i ustawie z dnia 21 czerwca 2002 r. *o stanie wyjątkowym.*

Z systemem stopni alarmowych powiązany został system udzielania w trybie pilnym niezbędnego wsparcia ze strony Sił Zbrojnych RP w przypadku, jeśli siły i środki Policji mogłyby okazać się niewystarczające do reagowania w sytuacji zamachu. Zgodnie z ustawą - przy wprowadzeniu trzeciego lub czwartego stopnia alarmowego, jeżeli użycie oddziałów i pododdziałów Policji okaże się niewystarczające lub może okazać się niewystarczające – decyzję o użyciu Sił Zbrojnych wydaje Minister Obrony Narodowej na wniosek ministra właściwego do spraw wewnętrznych, stosownie do przygotowania specjalistycznego żołnierzy Sił Zbrojnych RP, posiadanego sprzętu i uzbrojenia oraz zaistniałych potrzeb. Rozwiązanie to, w celu minimalizacji niezbędnego czasu reakcji, stanowi uproszczenie dotychczasowego trybu decyzyjnego w zakresie uzyskiwania przez Policję wsparcia Sił Zbrojnych RP, w związku z zagrożeniami o charakterze terrorystycznym. O wydanej decyzji Minister Obrony Narodowej niezwłocznie informuje Prezydenta RP i Prezesa Rady Ministrów, przy czym Prezydent RP będzie mógł wydać postanowienie o zmianie lub uchyleniu decyzji Ministra Obrony Narodowej. Jednak to dopiero uchylenie decyzji będzie przerywało tryb aktywizacji i udzielania wsparcia, a prowadzenie tych działań nie będzie wymagało dodatkowego potwierdzenia.

Powyższa procedura pozostaje niezależna względem możliwości uzyskania wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej na podstawie innych przepisów, w tym na podstawie art. 25 ustawy *o zarządzaniu kryzysowym*.

Na uwagę zasługuje również mechanizm wprowadzony w art. 17 ustawy dotyczący powoływania przez Szefa ABW sztabu koordynacyjnego, w przypadku wprowadzenia stopnia alarmowego odnoszącego się do terytorium RP lub stopnia alarmowego CRP. W skład sztabu wchodzą przedstawiciele służb specjalnych, Policji, Straży Granicznej, Biura Ochrony Rządu, Państwowej Straży Pożarnej, Służby Celnej, Generalnego Inspektora Informacji Finansowej, Generalnego Inspektora Kontroli Skarbowej, Żandarmerii Wojskowej i Rządowego Centrum Bezpieczeństwa. Ponadto Szef ABW może powołać w skład sztabu przedstawicieli innych organów administracji publicznej, w zależności od rodzaju zdarzenia o charakterze terrorystycznym, a także przedstawiciela Prokuratora Generalnego. Zadaniem tego gremium jest rekomendowanie zmiany

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

lub odwołania stopnia alarmowego oraz form i zakresu współdziałania służb i organów wchodzących w skład sztabu koordynacyjnego i biorących udział w jego pracach.

Istotne pozostaje również wskazanie w art. 21, że w przypadku trzeciego lub czwartego stopnia alarmowego, minister właściwy do spraw wewnętrznych, z inicjatywy własnej albo na wniosek Szefa ABW lub Komendanta Głównego Policji, może zarządzić zakaz odbywania zgromadzeń publicznych lub imprez masowych na obszarze lub w obiekcie objętym stopniem alarmowym, jeżeli jest to konieczne dla ochrony życia i zdrowia ludzi lub bezpieczeństwa publicznego.

Odnosząc się do kwestii bezpieczeństwa budynków i infrastruktury użyteczności publicznej, istotny pozostaje w szczególności wprowadzony w ustawie *o działaniach antyterrorystycznych* obowiązek zapewnienia ochrony przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne w odniesieniu do obiektów infrastruktury krytycznej, w tym obiektów budowlanych, urządzeń, instalacji, usług kluczowych dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Co więcej, zgodnie z zapisami ustawy, w przypadku wprowadzenia drugiego lub wyższego stopnia alarmowego dokonywane będą sprawdzenia zabezpieczeń obiektów na obszarze objętym stopniem alarmowym przez Policję – w obiektach infrastruktury krytycznej oraz przez Żandarmerię Wojskową – w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne. Szef ABW, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, będzie mógł również wydać Policji zalecenie szczególnego zabezpieczenia poszczególnych obiektów, uwzględniające rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym.

Natomiast w celu zapobiegania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych. Ocena ta, co do zasady, powinna być prowadzona zgodnie z rocznym planem przeprowadzania ocen bezpieczeństwa i polega na przeprowadzeniu testów bezpieczeństwa systemu teleinformatycznego w celu identyfikacji jego podatności, tj. słabości zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie, wpływające na integralność, poufność, rozliczalność i dostępność tego systemu. Ponadto w przypadku powzięcia informacji o wystąpieniu zdarzenia o charakterze terrorystycznym dotyczącego ww. systemów, Szef ABW może żądać przedstawienia informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji posiadanych systemów teleinformatycznych, w tym informacji obejmujących hasła komputerowe, kody dostępu i inne dane umożliwiające dostęp do systemów oraz ich używanie, w celu zapobiegania, reagowania na zdarzenia o charakterze terrorystycznym dotyczące tych systemów lub danych, a także zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców. Szef ABW będzie również prowadził rejestr zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych.

Niezależnie od opisanych powyżej zmian wprowadzonych ustawą *o działaniach antyterrorystycznych* pozostających w ścisłym związku z systemem zarządzania kryzysowego, wśród istotnych zmian należy wymienić umieszczone w ustawie z dnia 6 czerwca 1997 r. – *Kodeks karny* przepisów definiujących nowe typy przestępstw, stanowiących odpowiedź na działania tak zwanych *zagranicznych bojowników* związane z konfliktem w Syrii i Iraku oraz dostosowanie krajowych rozwiązań do podpisanego przez Polskę Protokołu dodatkowego do sporządzonej w dniu 16 maja 2005 r. w Warszawie *Konwencji Rady Europy o Zapobieganiu Terroryzmowi*. W ustawie *o działaniach antyterrorystycznych* zawarto także szczegółowe przepisy odnoszące się do prowadzenia postępowania

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

przygotowawczego w odniesieniu do przestępstw o charakterze terrorystycznym.

W ustawie zawarto także przepisy odnoszące się do działań realizowanych na miejscu zdarzenia o charakterze terrorystycznym, określając m.in. kto i w jakich przypadkach wyznacza kierującego działaniami antyterrorystycznymi podejmowanymi przez właściwe służby lub organy w ramach ich ustawowych zadań na miejscu zdarzenia o charakterze terrorystycznym. Wprowadzono także uprawnienie do tzw. *specjalnego użycia broni,* oznaczającego możliwość użycia broni palnej przeciwko osobie dokonującej zamachu albo biorącej lub przetrzymującej zakładnika, którego skutkiem może być śmierć lub bezpośrednie zagrożenie życia lub zdrowia tej osoby, co zgodnie z ustawą będzie dopuszczalne w ramach działań kontrterrorystycznych, jeżeli jest to niezbędne do przeciwdziałania bezpośredniemu, bezprawnemu, gwałtownemu zamachowi na życie lub zdrowie człowieka lub do uwolnienia zakładnika, a użycie broni palnej w inny sposób nie jest możliwe, z uwzględnieniem wszelkich okoliczności zdarzenia o charakterze terrorystycznym oraz możliwości działań kontrterrorystycznych.

Ponadto ustawa przewiduje m.in.: szereg uprawnień i mechanizmów koordynacyjnych mających usprawnić realizację działań w fazie zapobiegania zagrożeniom terrorystycznym wykonywanych przez poszczególne służby (w szczególności ABW), przyznanie ministrowi właściwemu do spraw wewnętrznych kompetencji do wydania decyzji o czasowym zawieszeniu lub ograniczeniu ruchu na określonych przejściach granicznych, deanonimizację osób korzystających z tzw. przedpłaconych kart telefonicznych poprzez zobowiązanie ich do podania swych danych operatorowi telekomunikacyjnemu, zaostrzenie przepisów w zakresie dokonywania wydalenia z terytorium RP osób nieposiadających polskiego obywatelstwa oraz regulację kwestii zniszczenia lub unieruchomienia bezzałogowych statków powietrznych (dronów) w przypadkach mogących stanowić zagrożenie.

Dezinformacja w związku ze Szczytem NATO w Warszawie

Paweł Majcher
Rządowe Centrum Bezpieczeństwa

Internet i media społecznościowe stają się coraz częściej skutecznym narzędziem do prowadzenia wojny hybrydowej. Raport opublikowany przez samym szczytem przez NATO Strategic Communications Centre of Excellence (StratCom) wskazuje dezinformację jako jedną z broni stosowanych podczas konfliktów, a uczestnicy Szczytu NATO w Warszawie przyznali, że cyberprzestrzeń jest współczesnym polem walki. Nie dziwi więc fakt, że w związku ze Szczytem NATO w Warszawie dezinformacja była szeroko wykorzystywana, a jej celem było przede wszystkim podważenie zaufania do Polski oraz narzucenie polskiej opinii publicznej antynatowskiej optyki promowanej od dłuższego czasu przez Rosję. Wykorzystywane zostały fałszywe wypowiedzi oraz działania hakerskie. Ślady były na tyle skutecznie zacierane, aby nie można było dotrzeć do autorów dezinformacji.

Dynamiczny rozwój internetu oraz mediów społecznościowych spowodował, że w ostatnich latach nastąpiła zdecydowana zmiana środowiska informacyjnego. Autorzy raportu StratComu uznali, że najważniejszymi czynnikami, które to spowodowały są: dostępność, szybkość, anonimowość, wymiana informacji oraz brak granic. Wszystko to powoduje, że dzięki zorganizowanej akcji można narzucić swoją narrację i zmienić faktyczny wydźwięk ważnych dla danego kraju wydarzeń.

FAŁSZYWKI W WALCE O OPINIE PUBLICZNĄ

Wpuszczanie do obiegu medialnego fałszywych informacji to najbardziej prymitywna metoda wywierania wpływu na opinię publiczną. Szybkie dementi osób zainteresowanych powoduje, że sensacyjnie brzmiące teksty szybko tracą na wartości. Warunkiem jest jednak szybka i zdecydowana reakcja. Wrzucanie fałszywek polega na stworzeniu tekstu, najczęściej podpartego fałszywymi wypowiedziami autorytetów ważnych dla opinii publicznej danego kraju, które podważają

prowadzoną politykę zagraniczną oraz promują narrację krajów zainteresowanych jej zmianą.

A: Aleksander Kwaśniewski

Kilka tygodni przed szczytem NATO w prorosyjskim serwisie internetowym „Sputnik" pojawiały się antyeuropejskie i prorosyjskie komentarze podpisane imieniem i nazwiskiem byłego prezydenta Aleksandra Kwaśniewskiego.

„Jak to dobrze , że jest ktoś taki jak Prezydent Putin. Jego istnienie wytłumaczy każdą naszą głupotę, każde nasz niepowodzenie, każdy nasz błąd. Możemy czuć się bez winy , ponieważ wszystko to co w życiu zepsuliśmy nie jest naszą, ale winą Putina….."

Sam zainteresowany protestował, ale bezskutecznie. Całą sprawę nazywa prowokacją. Nie można wycofać ani zabronić publikacji. A sam serwis jest zarejestrowany w rosyjskiej Federalnej Służbie Nadzoru w Sferze Łączności, Technologii Informatycznych i Masowego Przekazu.

B: Mirosław Różański

W dniu rozpoczęcia Szczytu NATO w internecie pojawiają się relacje z rzekomych wywiadów generała Marka Tomaszyckiego Dowódcy Operacyjnego Rodzajów Sił Zbrojnych oraz generała Mirosława Różańskiego Dowódcy Generalnego Rodzajów Sił Zbrojnych. Oba sfingowane wywiady krytykowały prezydenta Andrzeja Dudę za inicjowanie działań wojennych z Rosją. Pierwszy pojawił się „wywiad" z generałem Różańskim. Na narodowym i skrajnie prawicowym serwisie neon24.pl (d. nowyekran.pl) ukazała się rozmowa z Dowódcą Generalnym RSZ. Całość sprawia wrażenie wywiadu spisanego z rozmowy telewizyjnej. Poniżej artykułu podany jest nieczynny link do „Twojej Telewizji Religijnej".

„Dziś w naszym studio gościmy Mirosława Różańskiego, Dowódca Generalny RSZ. (…)

Czego możemy, jako Polacy, oczekiwać po tym szczycie?

Mirosław Różański: Będzie więcej hałasu niż konkretów. Niczego dobrego nikt nie oczekuje. Spodziewamy się bardzo głośnych i mocnych oświadczeń pod adresem Rosji. Głównym zadaniem szczytu jest osiągnięcie efektu wizerunkowego ……."

Bardzo szybko zareagował rzecznik prasowy MON Bartłomiej Misiewicz, który w serwisie twitter.com napisał, że artykuł na neon.pl jest prowokacją, a cytowane słowa nie były wypowiedziane. Dementi znalazło się również na stronie internetowej Dowództwa Generalnego Rodzajów Sił Zbrojnych. Mimo interwencji pseudo-wywiad nadal widnieje w serwisie.

C: Marek Tomaszycki

O wiele większy zasięg miała informacja relacjonująca wywiad z generałem Tomaszyckim. Na kilku portalach internetowych zamieściła je osoba podpisana jako Leszek Bobikowski. W tekście zatytułowanym **„Marek Tomaszycki: Andrzej Duda inicjuje działania wojenne"** można przeczytać między innymi:

Według generała Tomaszyckiego „daliśmy się wciągnąć w grę która prowadzi do katastrofy", bo jeszcze przed rozpoczęciem szczytu NATO Pan Prezydent Andrzej Duda nadał mu antyrosyjski ton i w taki sposób inicjuje działania wojenne. (…) Minister Obrony Narodowej Antoni Macierewicz gada, że szczyt NATO ustabilizuje sytuację na wschodzie i południu ale jest to oszustwo. NATO ma dzisiaj więcej problemów i wyzwań, niż powodów do radości i zadowolenia – dodał Tomaszycki.

Również w tym wypadku szybko zareagował rzecznik MON, który na twitter.com napisał:

Krążący artykuł po internecie, w którym gen. M. Tomaszycki miałby atakować prezydenta Andrzeja Dudę jest kolejną prowokacją.

Dementi opublikował również rzecznik prasowy DORSZ. Mimo to artykuł umieszczony był między innymi na stronie głównej opiniotwórczej platformy blogerskiej Salon24.pl oraz na stronie mpolska24.pl. Został zdjęty dopiero po kilku godzinach. Szefowa salon24.pl Bogna Janke napisała później, że tekst nie powinien być polecany na stronie głównej. Powodem błędu było niedoświadczenie dyżurującego administratora, brak czujności i natłok informacji tego dnia.

W efekcie w serwisach społecznościowych trwała już dyskusja na temat wypowiedzi polskiego generała.

W tym samym czasie na brukselskim portalu „B2" specjalizującym się w polityce obronnej pojawia się artykuł pod tym samym tytułem **„Duda inicjuje działania wojenne"**. Zdaniem dziennikarza prezydent Polski wszystko zepsuł jeszcze przed rozpoczęciem szczytu nadając mu antyrosyjski ton. Mimo, że nie ma tu sfingowanych wypowiedzi gen. Tomaszyckiego, to wydźwięk obu artykułów jest bardzo podobny.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

HAKERZY W SŁUŻBIE DEZINFORMACJI

Hakerzy uaktywniają się zawsze przed ważnymi dla danego kraju imprezami. Ich celem jest nie tylko sparaliżowanie lub zakłócenie wydarzenia międzynarodowego, ale również sprawienie wrażenia na całym świecie, że kraj nie jest wystarczająco chroniony i stanowi obiekt łatwego ataku. Tak było również przed, w trakcie i po Szczycie NATO. Hakerzy wykradali dane lub informowali, że wykradli ważne dla obronności dokumenty. Doszło również do włamania na strony internetowe.

A: ŚDM Lublin i Mesko

Przed rozpoczęciem Szczytu NATO doszło do włamania na strony lubelskich Światowych Dni Młodzieży. W komunikacie na stronie pojawiły się groźby, rzekomo pochodzące od islamskich terrorystów. Hakerzy umieścili czarną planszę z arabskimi napisami, mapą Europy i sylwetką człowieka z karabinem. Na dole widniał napis: „Pozdrawiamy naszych braci z okazji święta Id Al-Fitr! Allahu akbar! Przyszedł czas na zapłatę. Nasi wrogowie zebrali się w jednym miejscu. Szczyt NATO razem z Warszawą spłoną w świętym ogniu!". Dziennikarze RMF powołując się na informacje z policji twierdzą, że włamania dokonano z francuskiego serwera, który odwołuje się do rosyjskiego portalu zarejestrowanego w Stanach Zjednoczonych. Włamano się również na stronę internetową polskiej firmy zbrojeniowej Mesko, gdzie również zamieszczono podobną planszę.

Do tych zdarzeń doszło w dniu rozpoczęcia w Warszawie Szczytu NATO. Strony internetowe, na które się włamano nie były przypadkowe. Były to działania celowe, które miały wywołać poczucie strachu wśród gości odwiedzających Polskę podczas Szczytu NATO oraz Światowych Dni Młodzieży.

B: Netia

Dzień przed rozpoczęciem Szczytu NATO doszło do włamania na serwery operatora telekomunikacyjnego Netia. Informacje o tym rozpowszechniał profil na twitter.com „pravyy sector", co miało wskazywać ukraińskich nacjonalistów jako autorów ataku. Informacje były również rozsyłane do dziennikarzy i polskich mediów. Konta, z których były rozpowszechniane informacje, zostały założone tuż przed atakiem i zamknięte po włamaniu. Netia kilka godzin po ataku poinformowała, że hakerzy dostali się do bazy zawierającej dane osób zgłaszających chęć kontaktu poprzez formularz zamieszczony na stronie internetowej Netii. Dodatkowo uzyskali dostęp do danych z formularza umów zawieranych drogą elektroniczną. Włamywacze nie mieli żadnych żądań. O incydencie jako pierwsze informowały tymczasowe fałszywe konta na twitter.com. Podkreślano, że jest to atak ukraińskich nacjonalistów na telewizyjnego i internetowego operatora.

C: MON

Kilka dni po Szczycie NATO w internecie pojawiają się informacje, że doszło do włamania na strony Ministerstwa Obrony Narodowej. Hakerzy ponownie podszywający się pod ukraińskich nacjonalistów z Prawego Sektora opublikowali dane mające pochodzić z serwerów MON. Zagrozili, że upublicznią resztę wykradzionych danych, jeżeli nie dostaną 50 tysięcy dolarów. Ministerstwo nie potwierdzało, ale też nie dementowało włamania, dlatego informacja obiegła wszystkie media, które na głównych stronach w serwisach internetowych informowały o hakerskim ataku na MON. Resort zareagował dopiero na drugi dzień rano. W specjalnym oświadczeniu rzecznik napisał, że informacje o włamaniu były manipulacją mającą stworzyć wrażenie groźnego ataku. W ocenie analityków ze specjalistycznego portalu zaufanatrzeciastrona.pl najbardziej prawdopodobny scenariusz jest taki, że włamywaczom udało się na chwilę dostać do komputera w sieci MON. Hakerzy wykonali zrzuty ekranów, ukradli dane znajdujących się na nim jawnych dokumentów i prywatnych zdjęć, lecz szybko zostali wykryci przez służby MON i wyrzuceni z sieci.

Na razie nie zatrzymano sprawców, ale trudno oprzeć się wrażeniu, że do obu ataków nieprzypadkowo doszło akurat w okolicach Szczytu NATO. To na co

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

warto zwrócić uwagę, to fakt, że oba uderzenia były firmowane przez Prawy Sektor, ale z dwóch różnych profili, które miały jednak taką samą ikonę. Miało to świadczyć, że napastnik jest ten sam.

Konto informujące o ataku na MON

Konto informujące o ataku na Netię

W polskich mediach pojawiają się spekulacje, że skoro autorzy ataków nazywali siebie ukraińskimi nacjonalistami może to dowodzić, że hakerami kierowały osoby sprzyjające Rosji. Od czasów zajęcia Krymu, Rosja w wojnie informacyjnej wobec Polski wykorzystuje jako narzędzie problemy historyczne w relacjach polsko – ukraińskich, zwłaszcza rzezi wołyńskiej, której rocznica była obchodzona tuż po Szczycie NATO.

W tekście nie omówiono przypadku jednej z firm telekomunikacyjnych, która miała awarię w przeddzień rozpoczęcia się Szczytu NATO w Warszawie. Kłopoty klientów tej firmy nie były przez nikogo wykorzystywane w walce informacyjnej podczas spotkania przywódców państw Sojuszu Północnoatlantyckiego.

KOMENTARZ

Polska jest od kilku lat adresatem działań dezinformacyjnych. Podczas wojny we wschodniej Ukrainie wielokrotnie były wysuwane rosyjskie oskarżenia, że z naszego kraju są wysyłane oddziały najemników, którzy walczą po stronie Ukrainy. Każdy, nawet najmniejszy incydent, jest wykorzystywany do krytyki Polski za aktywną obecność w strukturach NATO. W lipcu przy okazji Szczytu NATO nastąpiła jednak kulminacja ataków. W ciągu kilku tygodni Polska stała się adresatem kilku akcji dezinformacyjnych.

Wszystkie przytoczone wyżej przykłady wykorzystywania fałszywych informacji mają jeden wspólny mianownik. Prezentują narrację od dawna promowaną przez Rosję: NATO nie gwarantuje Polsce bezpieczeństwa, a atakując naszego wschodniego sąsiada Polska ulega zachodnim mocarstwom prowokując agresję i angażując się w konflikt z Rosją. Polskie społeczeństwo jest odporne na tego typu propagandę, jednak w najbliższym czasie należy się spodziewać coraz większej liczby działań dezinformacyjnych, które mogą uzyskiwać podatny grunt w Polsce. Dlatego konieczne są szybkie i zdecydowane akcje informacyjne, które demaskują takie postępowania oraz uświadamiają, że część informacji pojawiających się w przestrzeni publicznej służy obcym Polsce interesom.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Procedura mostu powietrznego jako element zapewnienia bezpieczeństwa medycznego Światowych Dni Młodzieży 2016

mgr Marcin Podgórski, dr hab. n. o zdr. Robert Gałązkowski
SP ZOZ Lotnicze Pogotowie Ratunkowe

W dniach 26-31 lipca 2016 r. odbędą się 31. Światowe Dni Młodzieży. W uroczystościach na terenie województwa małopolskiego i śląskiego udział weźmie Papież Franciszek, młodzież z ponad 180 krajów świata, kardynałowie i biskupi z Polski i zagranicy, duchowieństwo, przedstawiciele najwyższych władz państwowych Rzeczpospolitej Polskiej na czele z Prezydentem RP i Premier polskiego rządu.

Organizacja i zabezpieczenie pod kątem medycznym wydarzenia jakim są Światowe Dni Młodzieży, podczas którego przewidywana liczba uczestników może znacznie przekroczyć milion, generuje między innymi konieczność przygotowania się na wypadek zdarzeń, w których liczba poszkodowanych w ciężkim stanie może znacznie przekraczać potencjał ochrony zdrowia funkcjonujący na terenie jednego województwa. Zatem organizacja zabezpieczenia medycznego musi uwzględniać wszelkie ryzyka i skutki mogące mieć wpływ na jakość udzielanej pomocy medycznej w stanach nagłego zagrożenia zdrowotnego.

W ramach organizacji zabezpieczenia medycznego Światowych Dni Młodzieży podjęto szereg działań mających na celu przygotowanie potencjału sił i środków, które umożliwią w krótkim czasie relokację poszkodowanych poza granice województwa, w którym doszło do zdarzenia. W tym celu nawiązano współpracę pomiędzy obszarem Państwowego Ratownictwa Medycznego a komponentem medycznym Sił Zbrojnych Rzeczpospolitej Polskiej, której efektem było opracowanie procedury pod roboczą nazwą „Most powietrzny".

Zgodnie z przyjętymi założeniami uruchomienie procedury następuje w sytuacji:

- wyczerpania się możliwości krakowskich i małopolskich szpitali pod kątem zabezpieczenia pacjentów w stanie ciężkim lub/i wymagających intensywnej terapii medycznej lub/i wymagających specjalistycznego leczenia w zakresie oparzeń, replantacji, hiperbarii, chirurgii, traumatologii, zatruć, neurochirurgii, neurologii;
- wyczerpania możliwości szpitali będących w zasięgu śmigłowców LPR;
- wyczerpania sił i środków Lotniczego Pogotowia Ratunkowego.

Dla zrealizowania działań zgodnie z procedurą określono niezbędny potencjał sił i środków:

- samolot CASA (2 szt.) – m. stacjonowania Kraków – Balice – gotowość całodobowa:
  - jeden z samolotów w konfiguracji umożliwiającej transport 2 pacjentów wymagających intensywnej terapii i 5 pacjentów leżących;
  - drugi samolot w konfiguracji umożliwiającej transport 24 pacjentów leżących;
- Medyczna Wojskowa Jednostka Etapowa (MWJE) zlokalizowana w wojskowej części Lotniska Kraków – Balice umożliwiająca hospitalizację 50 pacjentów, w tym 5 pacjentów intensywnej terapii oraz wykonywanie w ramach sali operacyjnej zabiegów operacyjnych i pełnej diagnostyki laboratoryjno-obrazowej – gotowość całodobowa;
- wojskowe zespoły wyjazdowe bez lekarza – 20 szt. ambulansów czteronoszowych – gotowość całodobowa;
- gotowość wytypowanych szpitali w 12 województwach posiadających lotniska kontrolowane;

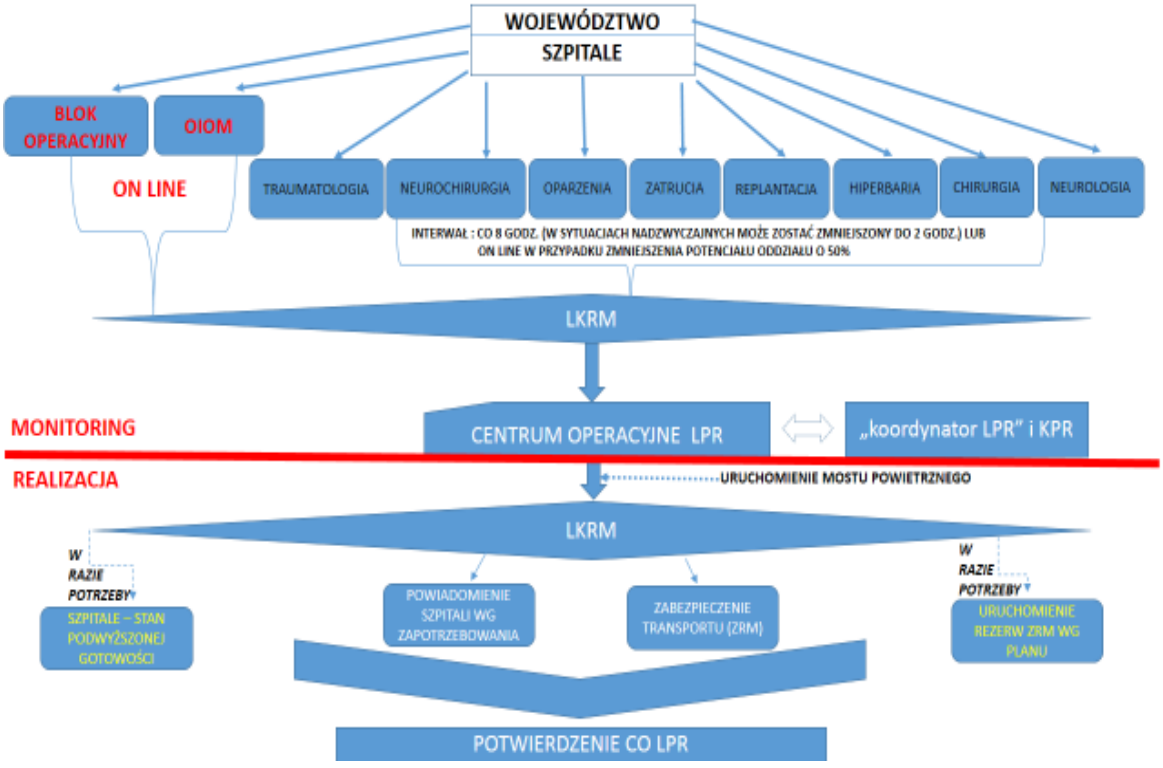
  zespoły Śmigłowcowej Służby Ratownictwa Medycznego (HEMS) – 11 zespołów:

LP.	BAZA	LICZBA ZESPOŁÓW HEMS/LZR	KRYPTONIM	GOTOWOŚĆ	ORIENTACYJNY CZAS DOLOTU W REJON KRAKOWA/BRZEGÓW
1.	Kraków Czyżyny	5	Ratownik 6, Ratownik 106, Ratownik 206, Ratownik 306, Ratownik 406,	24/24	6 min.
2.	Gliwice	1	Ratownik 4	7-20	33 min.
3.	Kielce	1	Ratownik 5	7-20	35 min.
4.	Sanok	1	Ratownik 10	7-20	50 min.
5.	Łódź	1	Ratownik 16	7-20	60 min.
6.	Lublin	1	Ratownik 7	7-20	70 min.
7.	Wrocław	1	Ratownik 13	24/24	70 min.

W celu maksymalnego skrócenia czasu podejmowania decyzji o uruchomieniu procedury „Most powietrzny", Ministerstwo Zdrowia zaleciło w wytypowanych szpitalach 12 województw system monitoringu potencjału łóżkowego na wybranych oddziałach. Każdy z powyższych szpitali co 8 godzin (z możliwością zwiększenia częstotliwości raportowania) przekazuje informacje o dostępności wolnych łóżek w poszczególnych oddziałach do właściwego lekarza koordynatora ratownictwa medycznego, a ten w oparciu o przygotowaną przez SP ZOZ Lotnicze Pogotowie Ratunkowe aplikację, przekazuje informację do Centrum Operacyjnego Lotniczego Pogotowia Ratunkowego (CO LPR).

CO LPR jest odpowiedzialne za koordynację transportu na każdym jego odcinku, współpracując ściśle z lekarzem lub lekarzami koordynatorami ratownictwa medycznego z województw, do których pacjenci mogą być potencjalnie transportowani.

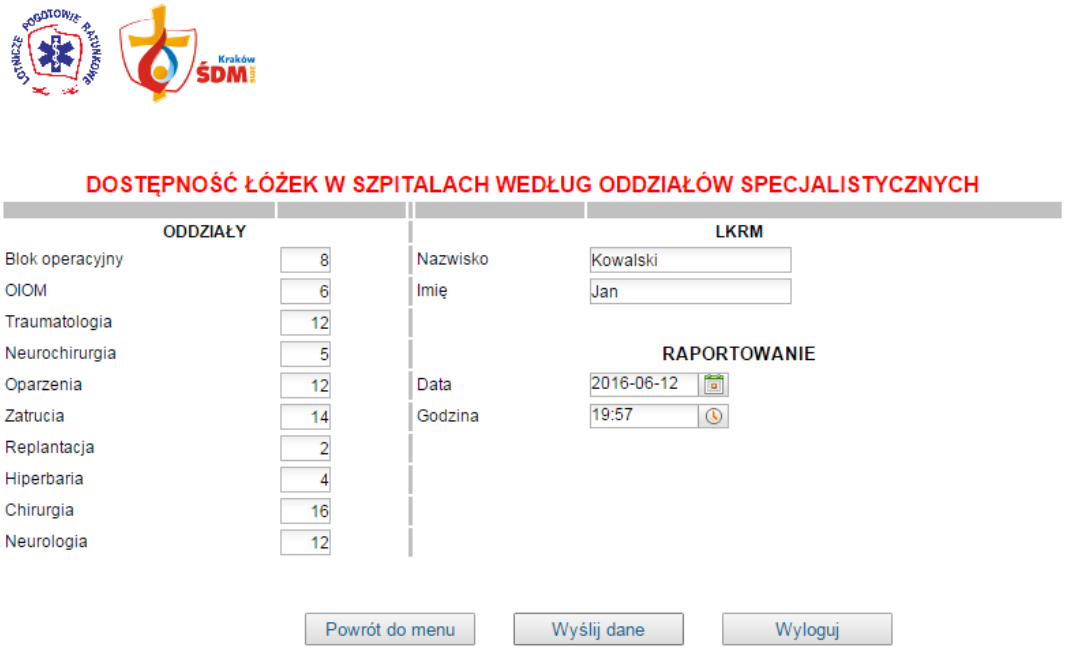
Proces realizacji działań w ramach opisywanej procedury obrazuje poniższy schemat.



Źródło: SP ZOZ Lotnicze Pogotowie Ratunkowe

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Wojewoda Małopolski podejmuje decyzję o uruchomieniu procedury „Most Powietrzny" w oparciu o szczegółową analizę przedstawioną przez Zespół Doradców Wojewody Małopolskiego ds. Światowych Dni Młodzieży, w skład którego wchodzą m.in. przedstawiciele Lotniczego Pogotowia Ratunkowego oraz Wojskowy Koordynator Medyczny. Zespół w oparciu o bieżącą analizę sytuacji posiadanego potencjału łóżkowego małopolskich i śląskich szpitali oraz analizę sytuacji w przypadku wystąpienia zdarzenia o charakterze nadzwyczajnym, wypracowuje optymalne działania zapewniające udzielanie pomocy medycznej w jak najkrótszym czasie, przede wszystkim poszkodowanym w stanie bezpośredniego zagrożenia zdrowotnego. Aby w sposób optymalny realizować procedurę „Most powietrzny" przygotowano specjalną aplikację, w oparciu o którą procedura ta będzie realizowana. Aplikacja umożliwia ciągły monitoring potencjału łóżkowego wielu szpitali w poszczególnych województw, podejmowanie natychmiastowych decyzji co do alokacji pacjentów do ośrodków posiadających gotowość, pełny monitoring czynności podejmowanych wobec pacjenta transportowanego do ośrodka docelowego wraz z czasami na poszczególnych etapach realizacji procedury, realizowanie zbiorczych raportów z poszczególnych transportów i czasookresów.



„Aplikacja do procedury Most Powietrzny"
Źródło: SP ZOZ Lotnicze Pogotowie Ratunkowe

KOMENTARZ

Procedura „Most powietrzny" jest unikalnym rozwiązaniem w zakresie planowania i organizacji, a przede wszystkim wykorzystania potencjału Sił Zbrojnych RP we współpracy z cywilnym systemem ratownictwa medycznego i ochrony zdrowia, w celu zapewnienia zabezpieczenia medycznego Światowych Dni Młodzieży na jak najwyższym poziomie. Przedstawiony moduł działania może stanowić punkt wyjścia dla wypracowania rozwiązań, które po dokonaniu niezbędnych modyfikacji uwzględniających konkretne warunki, będą mogły być wykorzystane w przyszłości.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Problematyka tworzenia miejsca przyjmowania rozbitków podczas katastrofy morskiej wymagającej masowej operacji ratowniczej

kpt. ż. w. Janusz Maziarz
Morska Służba Poszukiwania i Ratownictwa

Niniejsze opracowanie ma na celu wskazanie głównych problemów/wyzwań, jakie pojawią się przed reagującymi na lądzie w sytuacji kryzysowej będącej elementem masowej operacji ratowniczej na morzu zwanej dalej MRO (Mass Rescue Operation). Masowe Ratownicze Operacje (MRO) to operacje wymagające natychmiastowej asysty ratowniczej w stosunku do dużej liczby osób w sytuacji zagrożenia, w której normalnie dostępne siły i środki poszukiwawczo-ratownicze Służby SAR mogą być niewystarczające. MRO występują w małej częstotliwości w stosunku do typowych działań Służb SAR, ale w skali globalnej incydenty wymagające masowych operacji ratowniczych nie są rzadkością. Natura wielkich operacji ratowniczych może być słabo rozumiana w Polsce ze względu na ich rzadkość, a tym samym małe doświadczenie w ich prowadzeniu. Należy jednak zdawać sobie sprawę z faktu, że mogą one wystąpić wszędzie i w każdej chwili. Moralne i prawne obowiązki oraz społeczne i polityczne oczekiwania wymagają przygotowania się do prowadzenia MRO w sposób efektywny i bezpieczny. Kompleksowe plany prowadzenia natychmiastowych i szeroko zakrojonych działań ratowniczych są podstawą do zapobieżenia utraty życia na dużą skalę.

W przypadku MRO trudno jest opierać się na praktycznym doświadczeniu. Każda MRO będzie inna, ale jest kilka generalnych zasad wynikających z doświadczeń wyniesionych z historii. Efektywna operacja ratownicza w wypadku wielkiej katastrofy morskiej wymaga natychmiastowej, dobrze przygotowanej i dokładnie koordynowanej, akcji ratowniczej z użyciem wielu sił i środków różnych organizacji i instytucji. Wyznaczone miejsce/a lądowania – (LS – Landing Site) to bezpieczne, chronione i odpowiednio wyposażone lokalizacje, gdzie jednostki ratownicze i/lub ratunkowe, podczas masowej operacji ratowniczej na morzu, wyokrętują na ląd ewakuowanych/uratowanych pasażerów i członków załogi oraz dostarczają podjęte ciała. Na LS rozpoczyna się działalność lądowych służb ratowniczych, proces dochodzeniowy i dokumentacyjny. Każde LS powinno być odpowiednio przygotowane i zarządzane.

Wyznaczenie właściwego LS jest krytyczne podczas MRO. Lądowe siły i środki, zazwyczaj ograniczone, powinny być zgromadzone w jednym miejscu tak, aby sprostać przewidywanym wymaganiom danego incydentu. Jeżeli LS nie zostanie wyznaczone ewakuowani/uratowani mogą lądować w wielu nieprzygotowanych miejscach. Tak sytuacja może skomplikować lub uniemożliwić prawidłowe postępowanie, w tym przede wszystkim udzielenie natychmiastowej pomocy i opieki.

Miejsce lądowania musi zapewnić jednocześnie bezpieczeństwo prowadzonej operacji ratowniczej i ochronę rejonu jej prowadzenia. Musi zapewnić bezpieczne miejsca cumowania jednostek ratowniczych oraz bezpieczne zejście z ich pokładów na ląd. Musi zapewnić możliwość selekcji medycznej, udzielenia pierwszej pomocy medycznej, pomocy humanitarnej, liczenia i identyfikacji. Musi zapewnić ochronę rozbitków przed wpływem warunków atmosferycznych, swobodę wjazdu i wyjazdu pojazdów ratowniczych i transportowych. Od momentu postawienia stopy na lądzie, uratowani/ewakuowani powinni być pod opieką odpowiednich służb i instytucji lądowych, aż do czasu ich dotarcia do miejsc docelowych (przetransportowani do miejsc zamieszkania lub przekazani instytucjom lub organizacjom, które taki transport będą odpowiedzialne). Najlepszym rozwiązaniem byłoby wyznaczenie jednego LS, co umożliwi wszystkim stronom lądowego reagowania skonsolidowanie sił i środków w jednym miejscu, ułatwi zarządzanie i koordynację, a także zredukuje koszty operacji. Kilka LS to konieczność użycia większej ilości sił i środków, a szczególnie większej ilości kwalifikowanego personelu. W większości operacji może to być bardzo ograniczone lub, z braku wystarczających sił

i środków, wręcz niemożliwe. Wyznaczone LS powinno zapewniać: możliwość liczenia, identyfikacji, rejestracji uratowanych/ewakuowanych, sprawnego kierowania i kontroli tłumu, egzekwowania i przestrzegania prawa, ochronę przed osobami niepowołanymi, kontrolę i wsparcie mediów, kontrolę i ochronę ruchu pojazdów na LS i na drogach dojazdowych.

Rozważając lokalizację miejsca lądowania należy brać pod uwagę następujące elementy:

- bliska odległość do miejsca zdarzenia;
- wystarczająca ilość miejsca dla spodziewanej ilości uratowanych/ewakuowanych oraz koniecznych sił i środków ratowniczych do ich przyjęcia;
- dostęp od strony wody dla małych jednostek ratunkowych;
- możliwość bezpiecznego wyokrętowania uratowanych/ewakuowanych z jednostek ratowniczych i/lub ratunkowych;
- możliwość zapewnienia odpowiedniego miejsca dla działań różnych służb, w szczególności służb medycznych;
- łatwy dostęp dla lądowych środków transportu;
- urządzenia dla ludzi niesprawnych i wymagających specjalnej opieki;
- możliwość kontroli dostępu i ochrony miejsca lądowania;
- możliwość zapewnienia schronienia przed warunkami atmosferycznymi;
- możliwości sanitarne itp.

Podstawowy katalog problemów związanych z działaniami na lądzie składa się z następujących elementów:

- zapewnienie efektywnego dowodzenia, koordynacji i kontroli w przypadku współdziałania wielu instytucji, organizacji i służb zarówno krajowych jak i międzynarodowych;
- zapewnienie odpowiedniej, skutecznej łączności na wszystkich płaszczyznach;
- zapewnienie efektywnego przepływu, informacja do właściwych odbiorców;
- zapewnienie ochrony, bezpieczeństwa i przestrzegania prawa;
- problemy językowe i problemy związane ze wzajemnym zrozumieniem (obywatele różnych państw z jednej strony, a z drugiej strony specjalistyczny żargon używany przez różne służby i organizacje);
- współpraca służb, organizacji i instytucji, które nigdy wcześniej z sobą nie współdziałały;
- mobilizacja w krótkim czasie dużej ilości sił i środków przy jednoczesnym zachowaniu, w miarę możliwości, zdolności do „codziennych" działań;
- organizacja pomocy i opieki medycznej dla wielu poszkodowanych;
- organizacja pomocy psychologicznej i wsparcia dla poszkodowanych;
- mobilizacja dużej ilości środków transportowych;
- organizacja miejsc czasowego schronienia i pobytu;
- współpraca z mediami, rodzinami i bliskim;
- aspekty polityczne i międzynarodowe;
- reagowanie na zmęczenie i stres (możliwość rotacji lub wymiany reagującego personelu).

Przedstawiony powyżej katalog problemów nie jest i nigdy nie będzie zamknięty. Każda MRO jest inna i pojawiają się problemy do rozwiązania, których wcześniej, w fazie planowania, nie brano pod uwagę. Wcześniejsze przygotowania do prowadzenia natychmiastowej operacji ratowniczej na olbrzymią skalę są podstawą do zapobieżenia utraty życia setek czy tysięcy osób. Działania takie są szczególnie istotne w sytuacji, gdy występowanie wielkich katastrof morskich jest relatywnie rzadkie. Przygotowanie personelu do natychmiastowych działań w takich nadzwyczajnych sytuacjach jest krytycznym punktem i zwykle odnosi się do niezwykłego poziomu koordynacji i współdziałania. Olbrzymim problemem jest, często występujący, sprzeciw w ponoszeniu dużych kosztów w postaci czasu, wysiłku i funduszy, które pozwolą przygotować się do wielkich katastrof. Realizacja tego typu działań uzależniona jest od silnego i wizjonerskiego kierownictwa wielu resortów, a przede wszystkim osób odpowiedzialnych za szeroko pojęte bezpieczeństwo na morzu.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

KOMENTARZ

W powyższym opracowaniu zasygnalizowane zostały tylko generalne problemy i wyzwania jakie mogą lub pojawią się podczas reagowania lądowego w czasie MRO na morzu. Reagowanie kryzysowe podczas katastrofy morskiej wymagającej masowej operacji ratowniczej, gdzie w zagrożeniu będą setki czy tysiące osób, wymaga na lądzie współdziałania i współpracy setek czy tysięcy osób z różnych służb, organizacji i instytucji, które na co dzień z sobą nie współpracują, nie znają swoich zadań, możliwości, struktur dowodzenia, koordynacji, stosowanych systemów łączności itd. Większość problemów i wyzwań powinno być rozwiązanych na etapie przygotowywania planów reagowania kryzysowego w przypadku wystąpienia MRO na morzu. Przygotowanie takich planów wymaga, z jednej strony odpowiedniego podejścia osób na kierowniczych stanowiskach, a z drugiej strony współpracy wielu służb, instytucji i organizacji na wszystkich poziomach począwszy od szczebla lokalnego przez wojewódzki do szczebla krajowego – rządowego. Plany powinny być jasne i zrozumiałe dla wszystkich, którzy mogą być zaangażowani w reagowanie kryzysowe w wyniku MRO na morzu. Każdy powinien znać strukturę dowodzenia i koordynacji oraz swoją rolę i zadania. Plany powinny być „otwarte" i ciągle aktualizowane, nie mogą być „łapaczem kurzu" i muszą być sprawdzane podczas różnego typu ćwiczeń.

W morskich służbach ratowniczych nie zadajemy sobie pytania: „czy i gdzie katastrofa morska może się wydarzyć", lecz „kiedy?". Odpowiedź jest zawsze taka sama: „w każdej chwili i w każdym miejscu". Takie podejście wymaga ciągłych analiz, kontroli planów, ćwiczeń tak, aby być, tak jak to tylko jest możliwe, przygotowanym do reagowania w przypadku wystąpienia MRO.

Międzynarodowe ćwiczenie pk. ANAKONDA

Martyna Olejnik
Rządowe Centrum Bezpieczeństwa

Opracowanie przygotowane na podstawie materiałów przekazanych przez Dowództwo Operacyjne Rodzajów Sił Zbrojnych oraz Departament Strategii i Planowania Obronnego MON.

ANAKONDA-16, najważniejsze przedsięwzięcie szkoleniowe Sił Zbrojnych RP w 2016 r., było szóstą edycją tego ćwiczenia, natomiast po raz trzeci odbywało się w wymiarze międzynarodowym z udziałem przedstawicieli sił zbrojnych państw sojuszniczych i partnerskich.

Celem ćwiczenia, prowadzonego w dniach 7-17 czerwca br., było zgrywanie narodowych i koalicyjnych dowództw oraz pododdziałów w ramach połączonej operacji obronnej w warunkach zagrożeń hybrydowych. Dodatkowym aspektem podlegającym weryfikacji i sprawdzaniu było działanie systemu i procedury realizacji zadań w ramach funkcji państwa gospodarza. Zamierzonym efektem końcowym było potwierdzenie gotowości do dowodzenia w sposób kompleksowy połączoną operacją obronną, w warunkach zagrożeń hybrydowych, obejmującą układ pozamilitarny, we współdziałaniu z siłami sojuszniczymi.

W ćwiczeniu ANAKONDA-16 udział wzięli żołnierze z osiemnastu państw Sojuszu Północnoatlantyckiego i czterech państw Partnerstwa dla Pokoju oraz dwóch elementów sojuszniczych struktur dowodzenia. W czterech komponentach: lądowym, powietrznym, morskim i wojsk specjalnych, ćwiczyło ok. 31 000 żołnierzy, w tym ok. 12 000 polskich. Zaangażowane zasoby sprzętowe to ok. 3000 różnego rodzaju pojazdów, w tym czołgi Leopard, transportery opancerzone ROSOMAK, 105 statków powietrznych, łącznie z myśliwcami F-16 oraz 12 okrętów marynarki wojennej.

Autorzy zdjęć: st. chor. mar. Arkadiusz Dwulatek, st. chor. Waldemar Młynarczyk (Combat Camera DO RSZ)

31 maja br. zakończona została faza przygotowawcza ćwiczenia, w ramach której dokonano przemieszczenia wojsk w rejon ćwiczeń. W etapie pierwszym ćwiczenia siły polskie oraz jednostki wydzielone przez kraje sojusznicze dowodzone były przez stanowiska dowodzenia czterech komponentów sformowane przez Siły Zbrojne Rzeczypospolitej Polskiej. Ćwiczące dowództwa i wojska prowadziły demonstrację siły realizując proces zgrywania bojowego oraz wykonując zadania związane z przeciwdziałaniem zagrożeniom hybrydowym we współdziałaniu z układem pozamilitarnym we wszystkich środowiskach walki, w tym w cyberprzestrzeni.

W tym samym czasie mobilny element Dowództwa Komponentu Lądowego NATO, na stałe stacjonujący w Turcji, przemieścił się do Krakowa po czym, wraz ze Stanowiskiem Dowodzenia Wielonarodowego Korpusu Północ-Wschód rozwiniętym w Szczecinie, rozpoczął przygotowania do włączenia się w system dowodzenia operacją. Po zakończeniu pierwszego etapu nastąpiło skoordynowane przemieszczenie jednostek polskich, amerykańskich i brytyjskich pomiędzy poligonami z wykorzystaniem przepraw na Odrze i Wiśle. Dodatkowo manewr jednostek odbywał się w warunkach zakłócania funkcjonowania systemów teleinformatycznych, co pozwoliło na zademonstrowanie mobilności wojsk w warunkach oddziaływania elektronicznego przeciwnika.

Jednocześnie nastąpiła rekonfiguracja systemu dowodzenia zapewniająca przećwiczenie procedur przekazania zadań między wybranymi stanowiskami dowodzenia Sił Zbrojnych RP i elementami struktur dowodzenia NATO. Mobilny element dowodzenia Dowództwa Komponentu Lądowego NATO przejął zadania od Polskiego Dowództwa Komponentu Lądowego, a większość sił lądowych przejął w podporządkowanie Wielonarodowy Korpus Północ-Wschód.

W etapie drugim, w ramach ćwiczenia dowódczo-sztabowego wspomaganego komputerowo, ćwiczące dowództwa realizowały zadania związane z prowadzeniem operacji obronnej po wybuchu konfliktu. Z kolei wojska do szczebla brygady kontynuowały zgrywanie bojowe w zmienionej konfiguracji sił oraz realizowały zadania w ramach przeciwdziałania zagrożeniom hybrydowym.

Pododdziały realizowały szereg zadań obejmujących przede wszystkim: integrację taktyczną dowództw i wojsk w układzie międzynarodowym, kierowanie ogniem broni połączonych, ewakuację medyczną, likwidację skutków użycia broni masowego rażenia, realizację zadań państwa-gospodarza oraz przemieszczenie i ruch wojsk na dużą odległość.

W trakcie tegorocznego ćwiczenia po raz pierwszy wykorzystano sojusznicze tło operacyjno-taktyczne SKOLKAN. W regionie Morza Bałtyckiego głównymi aktorami były fikcyjne państwa Sojuszu Czerwonych oraz rzeczywiste kraje NATO, w tym Polska, Estonia, Łotwa, Litwa, Niemcy, Norwegia, tworzące Sojusz Niebieskich. Sojusz Czerwonych dążył do opanowania regionu Morza Bałtyckiego, w tym fizycznego zajęcia Estonii, Łotwy, Litwy i wybranych regionów Polski.

Kierowanie ćwiczeniem realizowane było ze stanowiska rozwiniętego w Akademii Obrony Narodowej w Warszawie i obejmowało koordynację działania praktycznego wojsk w siedmiu ośrodkach szkolenia wojsk lądowych oraz na akwenach morskich i w przestrzeni powietrznej. Realne działanie wojsk zostało zsynchronizowane z systemem symulacji działania wojsk Joint Theatre Level System (JTLS) oraz z systemem Joint Exercise Management Module

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

(JEMM), które zapewniały dopływ informacji do ćwiczących i pozwoliły na dokonanie oceny ich działania.

Ćwiczenie ANAKONDA-16 powiązane było z realizacją szeregu krajowych przedsięwzięć szkoleniowych, z których ważny element stanowiło **Regionalne Ćwiczenie Obronne**. Dowództwo Operacyjne Rodzajów Sił Zbrojnych przeprowadziło ćwiczenia taktyczno-specjalne z zakresu reagowania kryzysowego pk. **KAPER**, którego celem było sprawdzenie procedur współdziałania oraz przeciwdziałanie zagrożeniom terrorystycznym z powietrza i morza oraz pk. **RENEGADE/SAREX** z zakresu obrony powietrznej oraz poszukiwania i ratownictwa. Głównemu ćwiczeniu towarzyszyły przedsięwzięcia szkoleniowe Sojuszu odbywające się w tej części Europy. Najważniejsze to: ćwiczenie SWIFT RESPONSE dotyczące międzykontynentalnego przerzutu strategicznych sił USA do Polski oraz SABRE STRIKE obejmujące przemieszczenie sił USA do krajów bałtyckich i prowadzenie operacji na ich terytorium. Przed rozpoczęciem ćw. ANAKONDA-16 odbyło się również ćw. BRILLIANT JUMP, będące najistotniejszym w tym roku sprawdzianem Połączonych Sił Zadaniowych Bardzo Wysokiej Gotowości – VJTF (tak zwanej Szpicy NATO). Siły hiszpańskiego korpusu NATO, stanowiące trzon lądowego komponentu Szpicy NATO, zostały przemieszczone do Polski i wzięły udział w ANAKONDZIE jako siły międzynarodowe. Również w terminie ANAKONDY Flota Uderzeniowa NATO przeprowadziła odrębne ćwiczenie sił morskich BALTOPS na akwenie Morza Bałtyckiego.

REGIONALNE ĆWICZENIE OBRONNE 2016

Ćwiczenie zorganizowane w dniach 7-17 czerwca br. było jednym z ważniejszych zamierzeń szkoleniowych dedykowanych doskonaleniu funkcjonowania części pozamilitarnej systemu obronnego państwa. Przygotowuje administrację publiczną do działania podczas podwyższania gotowości obronnej i w czasie wojny. Wzięło w nim udział ponad 7000 osób z ponad 700 jednostek organizacyjnych wchodzących w skład administracji rządowej, samorządowej szczebla wojewódzkiego, powiatowego oraz gminnego, administracji zespolonej i niezespolonej oraz przedsiębiorców, operatorów infrastruktury krytycznej, organizacji paramilitarnych i stowarzyszeń z województw: lubuskiego, dolnośląskiego, śląskiego, opolskiego, małopolskiego i podkarpackiego oraz działów administracji rządowej: informatyzacja, łączność, administracja publiczna, sprawiedliwość, gospodarka, transport, zdrowie i sprawy wewnętrzne. Dodatkowo do udziału zaproszona została Kancelaria Prezesa Rady Ministrów oraz Agencja Bezpieczeństwa Wewnętrznego. Rządowe Centrum Bezpieczeństwa w przebiegu ćwiczenia odgrywało rolę elementu centralnego systemu wymiany informacji.

Przyjęta na potrzeby realizacji celów ćwiczenia hipotetyczna sytuacja zakładała działanie na terenie kraju grup dywersyjno-sabotażowych w kontekście zagrożeń hybrydowych działających na wielu polach funkcjonowania państwa (w tym w cyberprzestrzeni). Na to zostało nałożone przemieszczenie wydzielonych Sojuszniczych Sił Wzmocnienia (w sile korpusu) po drogach południowej Polski. Przebiegiem ćwiczenia kierowano poprzez szereg zaplanowanych aplikacyjnych wydarzeń, o których informacja była przesyłana ćwiczącym jednostkom w zależności od rozwoju sytuacji. Podjęte działania pozwoliły na sprawdzenie zdolności reagowania i współdziałania służb, inspekcji i straży, Sił Zbrojnych RP, organów administracji rządowej i samorządowej oraz organizacji proobronnych na wypadek wystąpienia zagrożenia bezpieczeństwa państwa. Ponadto zweryfikowano przyjęte rozwiązania i założenia dotyczące tworzenia jednostek obrony terytorialnej na terenie województw, a także przećwiczono niektóre procedury w ramach systemu wsparcia przez państwo gospodarza w stosunku do wojsk sojuszniczych.

Ponadto na terenie województwa podkarpackiego przeprowadzono epizod praktyczny związany z przeciwdziałaniem zagrożeniom hybrydowym. Scenariusz obejmował prowadzenie działań antyterrorystycznych w obiekcie opanowanym przez uzbrojoną niezidentyfikowaną grupę oraz ochronno-obronnych na obiekcie infrastruktury krytycznej z wykorzystaniem etatowych sił ochronnych obiektu wspieranych pozamilitarnymi strukturami obronnymi i jednostkami obrony cywilnej. Na potrzeby scenariusza wykorzystano Ośrodek Szkolenia Górskiego w Trzciańcu oraz zaporę wodną w Solinie. Do udziału zaproszono służby i straże województwa podkarpackiego, a także przedstawicieli Górskiego Ochotniczego Pogotowia Ratunkowego, Wodnego Ochotniczego Pogotowia Ratunkowego oraz Lotniczego Pogotowia Ratunkowego. Strona militarna podgrywana była przez żołnierzy z 21 Brygady Strzelców Podhalańskich. Obrona Terytorialna

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

reprezentowana była przez siły wydzielone z organizacji proobronnej „Strzelec". Głównym organizatorem przedsięwzięcia, przy współpracy z Departamentem Strategii i Planowania Obronnego MON, był Wojewoda Podkarpacki. Przebieg epizodu zademonstrował zdolności podsystemu niemilitarnego do reagowania na współczesne zagrożenia bezpieczeństwa narodowego oraz jednocześnie pozwolił pokazać zasadności utworzenia jednostek Obrony Terytorialnej.

KAPER 16

W ramach scenariusza ćwiczenia w dniach 8-9 czerwca br. przepływający morzem na wysokości Kołobrzegu prom pasażerski został uprowadzony przez terrorystów. Do akcji wkroczyły siły i środki Sił Zbrojnych RP oraz ogniwa pozamilitarne. Zapadła decyzja o skierowaniu w rejon akcji okrętu dyżurnego Marynarki Wojennej oraz żołnierzy JW. GROM. W pierwszym etapie operacji do akcji wkroczyli funkcjonariusze Straży Granicznej oraz policyjni negocjatorzy. Wojsko zdobyło w ten sposób czas, aby przygotować się do działania. Operację uwolnienia zakładników i odbicia promu przeprowadzili komandosi z Jednostki Wojskowej GROM przy wsparciu m.in. Marynarki Wojennej, Straży Granicznej, Sił Powietrznych i Policji. W Rządowym Centrum Bezpieczeństwa w związku z sytuacją aplikacyjnie odbyło się posiedzenie Rządowego Zespołu Zarządzania Kryzysowego, któremu przewodniczyła Prezes Rady Ministrów. W ramach ćwiczenia sprawdzono procedury związane z wymianą informacji pomiędzy dyżurnymi służbami operacyjnymi ćwiczących ogniw, a siłami wydzielonymi do rzeczywistego działania. Przećwiczono również elementy dotyczące realnego zwalczania zagrożeń terrorystycznych na morzu.

źródło www.anakonda.do.wp.mil.pl

źródło www.anakonda.do.wp.mil.pl

RENEGADE/SAREX 16

Celem ćwiczenia, które odbyło się 7-9 czerwca, było sprawdzenie gotowości elementów resortu obrony narodowej oraz podmiotów cywilnych do przeciwdziałania zagrożeniom terrorystycznym z powietrza oraz prowadzenia działań poszukiwawczo-ratowniczych na terytorium Rzeczypospolitej Polskiej. W tej edycji ćwiczenia rozgrywano po trzy epizody w obszarach zadaniowym SAREX i RENEGADE. Zdarzenia związane były m.in. z poszukiwaniem rozbitków po katastrofie samolotu pasażerskiego, współdziałaniem i reakcją na naruszenie przez cywilny śmigłowiec strefy ograniczonych lotów oraz ochroną przestrzeni powietrznej RP. W ramach elementu RENEGADE przeprowadzono również trening powszechnego ostrzegania i alarmowania ludności. Informacja o przewidywanym w trakcie ćwiczenia włączeniu syren została umieszczona również w Regionalnym Systemie Ostrzegania, na stronach internetowych urzędów wojewódzkich i powiatowych oraz w mediach. Oprócz strony wojskowej w ćwiczeniu uczestniczyli m.in.: Państwowa Straż Pożarna, Policja, Polska Agencja Żeglugi Powietrznej, Straż Graniczna, Lotnicze Pogotowie Ratunkowe, Żandarmeria Wojskowa, Agencji Bezpieczeństwa Wewnętrznego, Urząd Morski w Gdyni, GOPR i urzędy wojewódzkie.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl






Autorzy zdjęć: st. chor. mar. Arkadiusz Dwulatek, st. chor. Waldemar Młynarczyk (Combat Camera DO RSZ)

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l