RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

CYBER.MIL.PL – TWORZYMY WOJSKA OBRONY CYBERPRZESTRZENI 3

OCHRONA INFRASTRUKTURY KRYTYCZNEJ W ŚWIETLE POLSKICH ZOBOWIĄZAŃ SOJUSZNICZYCH 5

POLSKA JAKO PAŃSTWO-GOSPODARZ W RAMACH SYSTEMU HNS 7

WYBORCZY TEST UKRAIŃSKIEGO SYSTEMU BEZPIECZEŃSTWA 11

GRYPA W SEZONIE EPIDEMICZNYM 2018/2019 W POLSCE I EUROPIE 15

PROCES MONITOROWANIA ZAGROŻEŃ REALIZOWANY W MINISTERSTWIE GOSPODARKI MORSKIEJ I ŻEGLUGI ŚRÓDLĄDOWEJ 18

NUMER 26 STYCZEŃ – MARZEC 2019

Zespół redakcyjny
Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:
Grzegorz Świszcz – Zastępca Dyrektora RCB
Martyna Olejnik
Anna Zasadzińska-Baraniewska

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

Cyber.mil.pl – tworzymy wojska obrony cyberprzestrzeni

gen. bryg. Karol Molenda
Pełnomocnik ministra obrony narodowej do spraw tworzenia wojsk obrony cyberprzestrzeni
Dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni

Obszar bezpieczeństwa narodowego ewoluował na przestrzeni ostatnich kilkudziesięciu lat w sposób bezprecedensowy. To, co jeszc ze wczoraj wydawało się daleką przyszłością, dziś stało się niezaprzeczalnym faktem. Podobnie jak kiedyś samoloty i czołgi, tak dziś komputery i dostęp do globalnej sieci zrewolucjonizowały sposób postrzegania rzeczywistości pola bitwy. Pola, które swoim ogromem wykracza dużo dalej niż jakiekolwiek mapy sztabowe. Cyberprzestrzeń staje się dziś miejscem prowadzenia operacji nie tylko o charakter ze stricte militarnym, ale również prowadzonych bezpośrednio pod tzw. progiem wojny.

Powszechna dostępność, olbrzymi potencjał oddziaływania, niskie koszty oraz szybka ewolucja technologiczna utrudniająca skuteczne przeciwdziałanie – to atuty przemawiające za coraz szerszym wykorzystaniem możliwości oferowanych przez cyberprzestrzeń. Potencjalnym zagrożeniem nie muszą być już tylko same państwa, ale również coraz liczniejs ze grono grup ponadnarodowych. Prędkość z jaką rozrasta się dostęp do sieci jest wprost proporcjonalna do ilości zagrożeń, jakie z niej płyną. Pierwszy miliard użytkowników korzystających z Internetu osiągnęliśmy w 2005 r., kolejny w 2010, trzeci w 2014, dziś ta liczba przekroczyła już znacznie 4 miliardy. Analogicznie, w samym tylko 2015 r. United States Government Accountability Office (GAO) zarejestrowało ponad 77 tysięcy incydentów stanowiących zagrożenie dla bezpieczeństwa sieci i systemów wspomagających rząd Stanów Zjednoczonych. W porównaniu z rokiem 2005 był to wzrost o przeszło 1300%. Polski Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL tylko w 2017 r. odnotował 28 tysięcy zgłoszeń, wskazujących na zagrożenie dla kluczowych zasobów informatycznych państwa. Te dane pokazują bardzo niepokojący trend, z którym mierzyć się muszą nie tylko państwa, ale również organizacje międzynarodowe, takie jak np. NATO.

Podczas szczytu w Walii w 2014 r. sojusznicy zgodnie potwierdzili, że zagrożenia i ataki płynące z cyberprzestrzeni będą się nasilały, jednocześnie skala oddziaływania tego typu incydentów będzie coraz szersza. Podkreślono wówczas, że obrona cybernetyczna należy do podstawowych zadań kolektywnej obrony NATO. Rozwinięciem tej myśli było uznanie podczas szczytu NATO w Warszawie w 2016 r. cyberprzestrzeni jako osobnej domeny działań zbrojnych, która obok lądu, powietrza, morza i kosmosu stanowi klucz do bezpieczeństwa państw zrzeszonych w Sojuszu. W efekcie, decyzje podjęte podczas szczytu NATO w Brukseli w 2018 r. doprowadziły do reformy w struktur ze dowodzenia NATO – powstało Centrum Operacji Cyberprzestrzeni. Centrum, obok powołanych Zespołów Przeciwdziałających Zagrożeniom Hybrydowym, stanowi główną oś, na której NATO opiera swoje zdolności do reagowania na zagrożenia płynące z cyberprzestrzeni.

Także Polska musi dbać o cyberbezpieczeństwo swoich obywateli nie tylko w układzie sojuszniczym, ale również narodowym. Efekty tych prac są widoczne już dziś. Ich podstawą są przyjęte w 2017 r. na poziomie Rady Ministrów „Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022" oraz ustawa o krajowym systemie bezpieczeństwa, która weszła w życie w 2018 r. To właśnie ona określa rolę i pozycjonuje Ministra Obrony Narodowej w krajowym systemie cyberbezpieczeństwa. Zadania dla wojska są jasne: rozwijanie już posiadanych zdolności w obszar ze cyberbezpieczeństwa, budowa nowych kompetencji i narzędzi oraz zapewnienie swobody i efektywności działania Sił Zbrojnych RP w cyberprzestrzeni.

Powyżs ze zadania realizowane są w ramach programu Cyber.mil.pl, zainaugurowanego w lutym tego roku. Projekt skupia się na konsolidacji już posiadanych zdolności oraz budowie nowych

i obejmuje tak szeroką tematykę jak edukacja, rozwój sektora badawczego, czy ścieżki zawodowe dla specjalistów.

Zadanie stworzenia Sił Obrony Cyberprzestrzeni, które po sformowaniu staną się rodzajem wojsk – Wojskami Obrony Cyberprzestrzeni, Minister Obrony Narodowej Mariusz Błaszczak powierzył pełnomocnikowi ds. tworzenia wojsk obrony cyberprzestrzeni. Wśród mechanizmów i narzędzi mających usprawnić ten proces jest m. in. trzykrotne zwiększenie etatów przewidzianych dla ekspertów zajmujących się obszarem cyberbezpieczeństwa. Do końca czerwca bieżącego roku pełnomocnik ma przedstawić koncepcję tworzenia wojsk, uwzględniającą ich charakter prawny, struktury i zasady działania, katalog wymaganych zdolności, zasady współdziałania z poszczególnymi rodzajami Sił Zbrojnych oraz harmonogram formowania i osiągania gotowości operacyjnej. Powstanie zunifikowana siła, zdolna do efektywnego działania w cyberprzestrzeni.

Wspomniana unifikacja jest tutaj kluczowa. Obecnie w resorcie obrony narodowej funkcjonuje wiele instytucji zajmujących się problematyką informatyczną. Dokonywana konsolidacja ma zapobiegać rozproszeniu kompetencji i zminimalizować ryzyko wydłużania procesów decyzyjnych. Wojsko jako instytucja hierarchiczna musi mieć jasno określony system dowodzenia i prowadzone obecnie działania właśnie do tego zmierzają. Łączenie instytucji wojskowych z tego obszaru ma doprowadzić do skupienia w jednym miejscu ekspertów odpowiedzialnych za zabezpieczenia teleinformatyczne i kryptologiczne oraz za zakup sprzętu i utrzymanie sieci oraz systemów. W efekcie z połączenia dwóch instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne – Narodowego Centrum Kryptologii i Inspektoratu Informatyki powstało Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni – będzie to swego rodzaju „hub" w obszar ze polskiej cyberobrony.

Obok rozwiązań strukturalnych priorytetem jest kształcenie przyszłych kadr. Już dziś zwiększone zostały limity przyjęć na tematyczne studia wojskowe. W latach 2015-2016 limit miejsc na kierunki związane z informatyką wynosił 156 osób, w roku akademickim 2019/2020 tych miejsc będzie już 469. W przyszłym roku akademickim studia na uczelniach wojskowych będzie mogło rozpocząć aż 1482 absolwentów szkół średnich, którzy myślą o służbie zawodowej. Ponadto, w oparciu o Wojskową Akademię Techniczną, realizowane będą podyplomowe studia typu MBA w zakresie cyberbezpieczeństwa, a już od 1 września 2019 roku, również przy WAT, powstanie informatyczne liceum ogólnokształcące. Równolegle położono nacisk na rozwój korpusu podoficerskiego.To dla niego przeznaczona będzie nowotworzona Szkoła Podoficerska Informatyki i Łączności w Zegrzu. Już teraz informatycy Sił Zbrojnych RP należą do jednych z najlepszych na świecie. Dlatego tak istotna jest konsolidacja tego potencjału i przygotowanie ścieżki umożliwiającej jego trwały rozwój.

Odrębnym tematem jest przyciągnięcie do służby i pracy w tym środowisku zewnętrznych specjalistów. Od dłuższego czasu Wojsko Polskie buduje swoją markę w obszar ze cyberbezpieczeństwa. Wojskowi są rozpoznawani i cenieni jako znakomici fachowcy, a wywodzące się z armii zespoły informatyczne święcą triumfy na międzynarodowych zawodach, np. w 2018 r. zespoły z WAT i Inspektoratu Informatyki zajęły w odpowiednich kategoriach 1. i 2. miejsce podczas TIDE Hackath on organizowanego przez Dowództwo ds. Transformacji NATO. Kolejną edycję TIDE Hackatonu Polska zorganizowała w tym roku już jako gospodarz – tak jak w 2018 r. także i tym razem zespoły reprezentujące Wojskową Akademię Techniczną i Inspektorat Informatyki MON zajęły czołowe miejsca w swoich kategoriach. Ten sukces jest tym cenniejszy, że po raz kolejny udało się zdystansować kraje, które aspirują do roli wiodących w obszar ze cyberbezpieczeństwa. Należy pamiętać również o tym, że wojsko przestaje być hermetyczne – w 2018 r., podczas warszawskiego „HackYeah" to właśnie armia przygotowywała zadania dla uczestników mierzących się w kategorii cyberbezpieczeństwa. Właśnie to otwarcie na zewnątrz jest jednym z podstawowych zadań stojących przed nowa formacją. Wychodząc mu naprzeciw Ministerstwo Obrony Narodowej przygotowało rozbudowę komponentu cyber w ramach Wojsk Obrony Terytorialnej. Rozwijane są również inwestycje w polskie narzędzia kryptologiczne i oprogramowanie. Do 2026

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

roku wydane zostanie na ten cel rekordowe 3 miliardy złotych. Program „Cyber.Mil" został uznany przez ministra obrony narodowej za jeden z priorytetów w najnowszym Planie Modernizacji Technicznej.

Polska traktuje obszar cyberbezpieczeństwa jako jeden z kluczowych dla bezpieczeństwa kraju. Środowisko cyberprzestrzeni jest zmienne, a zmiany zachodzą w nim dużo szybciej niż w innych obszarach – jest to ciągły wyścig zbrojeń, w którym bier ze udział bardzo wielu aktorów. W ramach projektu Cyber.mil.pl powstaje zaplec ze naukowe, szkoleniowe i technologiczne, tak aby potencjał polskich informatyków mógł zostać wykorzystany do budowy optymalnego systemu bezpieczeństwa cyberprzestrzeni.

Ochrona infrastruktury krytycznej w świetle polskich zobowiązań sojuszniczych

Krzysztof Malesa
Rządowe Centrum Bezpieczeństwa

Polski system ochrony infrastruktury krytycznej (IK) został formalnie uruchomiony 26 marca 2013 r., kiedy to Rada Ministrów przyjęła Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK). Od tego dnia zaczęły biec określone w NPOIK terminy, dotyczące m. in. obowiązków związanych z opracowaniem i wdrożeniem planów ochrony IK oraz ewaluacją i aktualizacją samego NPOIK, która odbywa się w cyklu dwuletnim.

Aktualizacje NPOIK odbyły się w latach (2015, 2018), w których dochodziło do dość dynamicznych zmian w środowisku bezpieczeństwa międzynarodowego. Nowa sytuacja geopolityczna, związana z rosnącym zagrożeniem ze strony Rosji, wywarła znaczący wpływ na prace Sojuszu Północnoatlantyckiego, w tym Komitetu Planowania Cywilnego NATO (NATO CEPC). Chociaż kwestie współpracy cywilno-wojskowej kilkanaście lat po zakończeniu zimnej wojny ulegały stopniowej marginalizacji, to jednak po ukraińskim Euromajdanie w NATO odżyła dyskusja na temat roli planowania cywilnego wobec potencjalnych operacji wojskowych. Na forum Sojuszu znów zaczęto podkreślać, że pierwszą i główną rolą planowania cywilnego jest wsparcie cywilne dla wojskowych działań Sojuszu wynikających z art. 5 Traktatu Waszyngtońskiego (obrona kolektywna).

Z polskiego punktu widzenia sprawa ta nabrała konkretnego wymiaru podczas szczytu NATO w Warszawie w dniach 8-9 lipca 2016 r., kiedy szefowie państw i rządów państw członkowskich przyjęli zobowiązanie do wzmacniania odporności (Resilience) oraz dalszego rozwijania indywidualnej i zbiorowej zdolności do odparcia ewentualnego ataku na Sojusz (zgodnie z art. 3 TW). W zobowiązaniu tym gotowość cywilna – mierzona głównie poziomem odporności – jest opisana jako „centralny filar odporności sojuszników oraz krytyczny czynnik, od którego zależy zdolność Sojuszu do obrony kolektywnej".

Wspomniane powyżej zobowiązanie odwołuje się również do wytycznych zatwierdzonych przez ministrów obrony narodowej państw członkowskich Sojuszu, definiujących siedem obszarów odporności:

1. ciągłość działania administracji i kluczowych procesów państwa,
2. zaopatrzenie w energię,
3. zdolność do reagowania na masowe niekontrolowane migracje,
4. zaopatrzenie w wodę i żywność,
5. zdolność do reagowania na zdarzenia z dużą liczbą ofiar,
6. zapewnienie łączności oraz
7. transport cywilny.

Jak na tle polityki całego NATO, a zwłaszcza owych wytycznych, przedstawia się kwestia odporności w Polsce? Wystarczy sięgnąć do ustawy z dnia 26 lipca 2007 r. o zarządzaniu kryzysowym, żeby zauważyć, iż wskazane powyżej obszary odporności w znacznej części (to znaczy: wszystkie z wyjątkiem pozycji 3 i 5[1]) figurują wśród jedenastu systemów wchodzących, wraz z obiektami, urządzeniami, instalacjami i usługami, w skład polskiej infrastruktury krytycznej. Oznacza to, że zarówno same usługi, jak i wspierająca je infrastruktura, są objęte specjalnym nadzorem mającym na celu zapewnienie ich ciągłości, rozumianej również jako odporność na wszelkie zakłócenia.

Taka sytuacja stanowi doskonały punkt wyjścia do harmonizacji rozproszonych dotychczas wysiłków, którym przyświeca przecież wspólny cel: utrzymanie ciągłości kluczowych usług świadczonych przez państwo, administrację i biznes prywatny. Skorzystać z tego mogą wszystkie zainteresowane strony i nie są to tylko puste słowa, lecz rzeczywiste działania. Polityka NATO – w połączeniu z dużą aktywnością RCB na tym polu – spowodowała wzrost liczby polskich ekspertów cywilnych akredytowanych przy NATO i biorących czynny udział w pracach czterech grup roboczych CEPC zajmujących się kwestiami odporności w różnych obszarach, w tym IK. Seminaria organizowane przez Centrum na temat współpracy cywilno-wojskowej przyciągają więcej chętnych, niż jesteśmy w stanie przyjąć, a ich poziom merytoryczny świadczy o rosnącym zrozumieniu wzajemnych potrzeb i zależności pomiędzy NATO-wskimi wojskami przebywającymi w naszym kraju a administracją centralną i lokalną jak też podmiotami prywatnymi, zwłaszcza tymi o znaczeniu gospodarczo-obronnym.

Miernikiem poziomu gotowości cywilnej Polski jako członka NATO jest od niedawna przegląd zdolności obronnych Sojuszu. (NATO Defence Planning Capability Survey; DCPS). W 2017 roku, po raz pierwszy od czasu zakończenia zimnej wojny, zdecydowano się na włączenie do tego istotnego przedsięwzięcia kwestii gotowości cywilnej i odporności. Rządowe Centrum Bezpieczeństwa w uzgodnieniu z Ministerstwem Obrony Narodowej wzięło na siebie rolę koordynatora rozdziału dotyczącego gotowości cywilnej i przeprowadziło zaangażowane resorty cywilne przez wszystkie etapy odbywającego się co dwa lata przeglądu – począwszy od kwestionariusza samooceny, poprzez audyt NATO aż po końcowe wielostronne konsultacje w Kwater ze Głównej NATO. W tym roku rozpoczynamy pracę nad kolejną edycją DCPS, na analogicznych zasadach i z nadzieją, że Polska – jako państwo członkowskie z pozytywną oceną z ostatniego przeglądu – wypadnie w tej edycji jeszc ze lepiej. Jeśli tak się stanie, będzie to w sporej części zasługą naszych kolegów zajmujących się współpracą cywilno-wojskową i ochroną infrastruktury krytycznej.

Odporność we wszystkich obszarach, a w szczególności infrastruktury krytycznej rozumianej nowocześnie (czyli nie tylko jako obiekty wymagających ochrony, lecz również usługi, których ciągłość należy zapewnić) determinuje w bardzo znacznym stopniu możliwość zapobieżenia zagrożeniom hybrydowym i podprogowym.

1. Zasady postępowania w przypadku masowego napływu cudzoziemców na terytorium RP oraz zdarzenia o charakter ze masowym lub z czynnikiem CBRN (medyczny most powietrzny) zostały włączone jako standardowe procedury operacyjne do najnowszej edycji Krajowego Planu Zarządzania Kryzysowego.

Ustawa o zarządzaniu kryzysowym, scalająca kilka obszarów – w tym planowanie cywilne, ochronę infrastruktury krytycznej oraz zadania administracji rządowej w Systemie Reagowania Kryzysowego NATO (NCRS) – jest rozwiązaniem, które kładzie nacisk na międzyresortową koordynację przedsięwzięć o kluczowym znaczeniu dla bezpieczeństwa Polski.

Zasady przedstawione w Narodowym Programie Ochrony Infrastruktury Krytycznej umożliwiają zaangażowanie sektora prywatnego w działania mające na celu zapewnienie ciągłości świadczenia kluczowych usług, które są niezbędne dla bezpieczeństwa obywateli, pozwalają na nieprzerwaną pracę administracji państwowej i umożliwiają prowadzenie działalności gospodarczej. Jednocześnie – co doskonale widać na agendzie Komitetu Planowania Cywilnego NATO – ciągłość świadczenia tych usług jest warunkiem skorzystania przez Polskę z ochrony przewidzianej Traktatem Waszyngtońskim, a w szczególności z kolektywnej obrony zgodnie z art. 5 Traktatu.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

Polska jako państwo-gospodarz w ramach systemu HNS

Sławomir Łazarek
Rządowe Centrum Bezpieczeństwa

Polska, jako członek Organizacji Traktatu Północnoatlantyckiego (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 Nati on Support (HNS). Prawidłowe realizowanie wsparcia przez Polskę ma kluczowe znaczenie dla obronności naszego kraju, a także jego wiarygodności jako partnera działań wojsk sojuszniczych. Od sprawności w wypełnieniu tej roli w razie kryzysu i wojny zależy w dużej mier ze bezpieczeństwo Polski, jak również pozycja i postrzeganie naszego kraju na arenie międzynarodowej.

Aktualna polityka NATO, związana ze zwiększeniem obecności wojskowej w rejonie flanki wschodniej, spowodowała duży wzrost przebywających na terytorium RP wojsk sojuszniczych. Stanowi to nowe wyzwanie dla naszego kraju jako państwa-gospodarza z uwagi na znaczne zwiększenie zakresu obowiązków wynikających z pełnienia tej roli. Realizacja zadań, wynikających z obowiązków państwa-gospodarza (ang. Host Nati on Support, HNS), wymaga przygotowania elementów państwa, w tym również jego infrastruktury, w taki sposób, by móc optymalnie wykorzystać istniejące narodowe zasoby obronne. Celem jest posiadanie sprawnego, krajowego systemu wsparcia sił Sojuszu, które będą realizować zadania na terytorium Rzeczypospolitej Polskiej lub przemieszczać się przez to terytorium. Jednym z filarów takiego systemu są przejrzyste i spójne procedury zapewniające właściwe planowanie, przygotowywanie, realizowanie, a także rozliczanie dostarczonego wsparcia.

W celu dokonania nowelizacji zasad funkcjonowania HNS w Polsce, w lutym 2018 roku powołany został – pod przewodnictwem Pełnomocnika Ministra Obrony Narodowej ds. HNS (Szef Zarządu Logistyki – P4 SG WP) – Międzyresortowy Zespół do opracowania „Koncepcji funkcjonowania narodowego systemu wsparcia przez państwo-gospodarza (HNS)". W jego skład weszli przedstawiciele jednostek i komórek organizacyjnych kompetentnych ministerstw i agend rządowych, w tym również Rządowego Centrum Bezpieczeństwa.

PODSTAWY FORMALNO-PRAWNE

Problematyka funkcjonowania systemu wsparcia przez państwo-gospodarza ujęta została w prawie międzynarodowym i krajowym. System ten ma swoje odzwierciedlenie w ratyfikowanych umowach międzynarodowych zawierających postanowienia dotyczące sił zbrojnych państw nimi objętych. Umowy te są punktem odniesienia dla dwu i wielostronnych porozumień zawieranych na potrzeby konkretnych operacji i ćwiczeń NATO.

Wśród najważniejszych międzynarodowych dokumentów należy wskazać:

1. Traktat Północnoatlantycki[1], sporządzony w Waszyngtonie 4 kwietnia 1949 r., w którym postanowiono w artykule 3, że dla skuteczniejszego osiągnięcia celów tego traktatu, strony – każda z osobna i wszystkie razem – będą zapewniały warunki do realizacji zadań wsparcia przez państwo-gospodarza, a także poprzez stałą i skuteczną samopomoc i pomoc wzajemną, będą utrzymywały i rozwijały indywidualną i zbiorową zdolność do odparcia zbrojnej napaści;
2. Umowa między Państwami-Stronami Traktatu Północnoatlantyckiego, dotycząca statusu ich sił zbrojnych, sporządzona w Londynie 19 czerwca 1951 roku[2] (znana również jako NATO SOFA[3]), która zawiera postanowienia dotyczące m.in. warunków i wymagań wobec sił zbrojnych państwa wysyłającego[4] lub znajdujących się na terytorium pań-

1. Dz. U. z 2000 r. nr 87 poz. 970, (art. 3).
2. Dz. U. z 2000 r. nr 21 poz. 257, z późn. zm.
3. Agreement between the Parties to the North Atlantic Treaty regarding the status of their forces.
4. Zgodnie z art. I ust. 1 lit. d NATO SOFA „Państwo wysyłające" oznacza Umawiającą się Stronę, do której należą siły zbrojne.

stwa przyjmującego[5] objętego obszarem Traktatu Północnoatlantyckiego, członków sił zbrojnych i personelu cywilnego oraz kompetencji i zasad postępowania organów wojskowych państwa wysyłającego oraz organów państwa przyjmującego.

Postanowienia wyżej wymienionych umów międzynarodowych stanowiły podstawę do zawarcia w 2005 roku Porozumienia Ogólnego (MOU) między Rządem Rzeczypospolitej Polskiej a Naczelnym Dowództwem Połączonych Sił Zbrojnych NATO w Europie oraz Kwaterą Naczelnego Sojuszniczego Dowódcy NATO do Spraw Transformacji, w sprawie zapewnienia wsparcia przez państwo-gospodarza dla operacji NATO prowadzonych na naszym terytorium. MOU ustala zasady postępowania i procedury zapewnienia przez Polskę wsparcia siłom zbrojnym znajdującym się na naszym terytorium lub wspieranych z terytorium Polski podczas operacji NATO. Porozumienie stanowi dokument ramowy i tworzy warunki niezbędne do szybkiego wejścia i rozwinięcia sił sojuszniczych na terytorium państwa-gospodarza. Polska zobowiązała się do udzielenia wsparcia sojuszniczym siłom zbrojnym w pełnym zakresie swoich możliwości, ale co należy podkreślić, tylko pod warunkiem jego dostępności i w ramach ograniczeń wynikających z zaistniałych okoliczności. Najczęściej takie wsparcie będzie obejmowało m.in.: wodę i żywność, paliwo, energię elektryczną, czy usługi bytowe. Z reguły nie dotyczy to takich spraw jak zaopatrzenie w amunicję czy części zapasowe do sprzętu wojskowego.

Dokumentem stosowanym przy realizacji i rozliczaniu HNS w ramach NATO jest porozumienie standaryzacyjne STANAG 2034 – Standard Procedures for Mutual Logistic Assistance (tzw. Standardowe procedury wzajemnego wsparcia logistycznego w NATO). Wprowadza on procedury udzielania oraz rozliczania wzajemnego wsparcia logistycznego w sytuacji, gdy siły zbrojne państwa NATO udzielają wsparcia logistycznego siłom zbrojnym innego państwa, dowództwom lub formacjom wielonarodowym w czasie pokoju, kryzysu i wojny.

Ponadto dokumentami mającymi zastosowanie w określaniu wytycznych dla wsparcia cywilnego dla sił zbrojnych, w tym HNS są m.in.:

- „Zobowiązanie do podnoszenia odporności" przyjęte przez szefów państw i rządów na Szczycie NATO w Warszawie w 2016 roku;
- „Wytyczne do podnoszenia odporności" zaakceptowane przez ministrów obrony NATO w czerwcu 2016 roku;
- Wspólny Komunikat do Parlamentu Europejskiego i Rady dotyczący Planu działania na rzecz mobilności wojskowej z 28 marca 2018 r. (Joint communicati on to the European Parliament and the Council on the Acti on Plan on Military Mobility).

Warto podkreślić, że współpraca pomiędzy NATO a Unią Europejską w tym zakresie jest rozwijana na podstawie Wspólnej Deklaracji Przewodniczącego Rady Europejskiej, Przewodniczącego Komisji Europejskiej oraz Sekretarza Generalnego z 8 lipca 2016 (NATO Joint declarati on by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization).

Krajowe przepisy prawne i regulacje związane ze wsparciem przez państwo-gospodarza ujęte są w szczególności w następujących aktach normatywnych:

1. Konstytucja Rzeczypospolitej Polskiej, zgodnie z którą zasady pobytu obcych wojsk na terytorium naszego państwa i zasady przemieszczania się ich przez to terytorium określają ratyfikowane umowy międzynarodowe lub ustawy;
2. Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej[6], w której ujęto zagadnienia wsparcia przez państwo-gospodarza;
3. Ustawa o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej oraz zasadach ich przemieszczania się przez to terytorium[7], która określa zasady pobytu i przemieszczania się wojsk obcych na terytorium Polski oraz zawiera unormowania dotyczące m.in. zgód wydawanych przez Radę Ministrów oraz Ministra Obrony Narodowej;
4. Ustawa o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i za-

5. Zgodnie z art. I ust. 1 lit. e NATO SOFA „Państwo przyjmujące" oznacza Umawiającą się Stronę, na której terytorium przebywają siły zbrojne lub ich personel cywilny, niezależnie od tego, czy tam stacjonują, czy też przejeżdżają przez nie tranzytem.

6. Dz. U. z 2017 r. poz. 1430 i 2217 oraz z 2018 r. poz. 138 i 398.

7. Dz. U. z 1999 r. nr 93, poz. 1063.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

sadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[8], która w czasie obowiązywania stanu wojennego nakłada na Ministra Obrony Narodowej obowiązek koordynowania realizacji zadań przez państwo-gospodarza wynikający z umów międzynarodowych (art. 12 pkt 7).

NOWA „KONCEPCJA"

Ze względu na wzrost obecności sił sojuszniczych na terytorium Polski, a co za tym idzie zwiększone potrzeby tych wojsk, zaistniała konieczność podjęcia działań, które spowodują znowelizowanie, a w niektórych aspektach unormowanie podstaw formalno-prawnych w zakresie wsparcia przez państwo-gospodarza.

Aktualnie, Minister Obrony Narodowej posiada nałożony ustawowo[9] obowiązek koordynowania realizacji zadań przez państwo-gospodarza wynikających z umów międzynarodowych, ale tylko w czasie stanu wojennego. Natomiast, co jest istotne w obecnej sytuacji geopolitycznej związanej m.in. z zagrożeniami hybrydowymi, w czasie pokoju i kryzysu, nie ma w państwie ustawowo określonego organu koordynującego realizację zadań HNS. Ponadto, Minister Obrony Narodowej, który ma przedstawiać Prezesowi Rady Ministrów informację o realizacji zadań HNS, nie posiada wystarczających uprawnień do koordynowania realizacji zadań państwa-gospodarza pozostających w gestii organów administracji publicznej, które są kluczowym elementem wykonawczym. Dlatego też, zgodnie z wolą MON, aby móc pełnić rolę ośrodka koordynującego również działania sfery cywilnej, minister powinien posiadać właściwe kompetencje ustawowe oddziaływania na koordynowane podmioty. Jednocześnie istnieje potrzeba zdefiniowania na nowo zadań realizowanych przez wszystkie organy administracji publicznej.

Nie został również szczegółowo określony zakres pomocy cywilnej i wojskowej, udzielanej przez państwo-gospodarza wojskom sojuszniczym w czasie pokoju, kryzysu i wojny. Tymczasem powinien on uwzględniać rzeczywiste możliwości państwa-gospodarza, które są pomniejszone o siły i środki zaangażowane w zapewnienie realizacji narodowych zadań obronnych. Szczególnie istotne jest, aby celem ułatwienia realizacji zadań HNS, w jednostkach wojskowych i podmiotach cywilnych zaplanować je w powiązaniu z wydatkami ujętymi w planach finansowych obu tych sfer. Wprowadzone regulacje powinny stanowić podstawę działań systemowych, porządkujących obszar narodowego wsparcia przez państwo-gospodarza, w tym koordynowanie i monitorowanie działań międzyresortowych podejmowanych w ramach HNS.

Doprecyzowania wymaga ponadto zakres udziału organów administracji publicznej w pracach na forum NATO i UE, dotyczących wymogów i zadań HNS. Za zasadne uchodzi nałożenie na cywilne organy administracji obowiązku regularnego i aktywnego uczestniczenia w pracach obu wspomnianych organizacji międzynarodowych. Umożliwić to powinno bardziej efektywne i zgodne z interesem bezpieczeństwa RP kształtowanie polityki i wymogów organizacji międzynarodowych w sprawach związanych z HNS.

WYZWANIA DLA SYSTEMU HNS

Międzyresortowy Zespół wskazał następujące ograniczenia w prawidłowej realizacji zadań wsparcia przez państwo-gospodarza:

1. Brak jednego źródłowego aktu prawnego (na poziomie ustawy) regulującego obszar realizacji zadań HNS. Obecnie problematyka ta jest rozproszona w różnych regulacjach prawnych;
2. Przepisy prawa powszechnie obowiązującego dotyczącego systemu HNS nie regulują w pełnym zakresie udzielanej pomocy cywilnej i wojskowej. Należałoby mieć na uwad ze rzeczywiste możliwości państwa-gospodarza, uwzględniając priorytety narodowe oraz czas (pokoju, kryzysu i wojny), w jakim pomoc jest udzielana. Jednocześnie, warto określić zakres udziału podmiotów cywilnych w pracach na forum NATO[10] i UE[11], dotyczących wymogów dla HNS (resorty reprezentujące podstawowe działy administracji rządowej takie jak: energia, gospodarka morska, gospodarka wodna, łączność, zdrowie, sprawy wewnętrzne, transport, finanse i inne);

8. Dz. U. z 2002 r. nr 156, poz. 1301, z późn. zm.

9. Ustawa z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (art. 12 pkt 7).

10. Koordynację współpracy z Civil Emergency Planning Committee (CEPC) i podporządkowanej temu komitetowi NATO grupy roboczej ochrony ludności (CIvil Protection Group, CPG) zapewnia RCB.

11. W odniesieniu do prac w UE nad Military Mobility w ramach PESCO.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

3. Przyznanie, tak jak zakłada „Koncepcja", Ministrowi ON w czasie pokoju i w czasie kryzysu kompetencji ustawowych do koordynowania zadań HNS powinno usprawnić zharmonizowanie realizowanych zadań przez wszystkie zaangażowane organy administracji publicznej. Umożliwić to powinno również kompleksowe uregulowanie funkcjonowania systemu HNS w czasie pokoju, kryzysu i wojny;
4. Konieczność ujednolicenia istniejącej Bazy Danych HNS, czyli podstawowego zbioru informacji na temat posiadanych narodowych możliwości wsparcia wojsk sojuszniczych;
5. Konieczność uregulowania zasad finansowania oraz rozliczania wpływów z tytułu udzielonego wsparcia. Ponadto określenie, jaki zakres HNS podlega refundacji przez państwo wysyłające wojska, a jakie wydatki ponosi państwo-gospodarz;
6. Brak jednolitego i klarownego systemu wymiany informacji, przekazującego do sfery cywilnej potrzeby sił zbrojnych w zakresie HNS, w szczególności w fazie planowania operacji. Istnieje potrzeba dookreślenia, jaki poziom dowodzenia sił zbrojnych może generować potrzeby oraz do kogo po stronie cywilnej te potrzeby powinny spływać.

PROCEDURY NA KAŻDY CZAS

Kluczowym dla wprowadzenia proponowanych zmian jest podtrzymanie stanowiska, że głównym zadaniem narodowego systemu HNS jest stworzenie warunków niezbędnych do przyjęcia sojuszniczych sił zbrojnych na terytorium Rzeczypospolitej Polskiej oraz ułatwienie tym siłom funkcjonowania w warunkach umożliwiających wykonanie przez nich zadań. Szczególnie ważne jest przyjęcie procedur, które będą wspierały te zadania w czasie pokoju, bez wprowadzonych stanów nadzwyczajnych.

Kierowanie i koordynowanie przedsięwzięć HNS odbywać się będzie zgodnie z „Koncepcją" w ramach systemu kierowania bezpieczeństwem narodowym. W czasie pokoju podsystem obronny oparty będzie na organach dowodzenia Sił Zbrojnych RP i organach decyzyjnych administracji publicznej państwa działających w ramach przypisanych im konstytucyjnych kompetencji. W sytuacji podwyższania gotowości obronnej państwa i w czasie wojny, podsystem obronny organizowany będzie w oparciu o rozwijany w Siłach Zbrojnych RP Wojenny System Dowodzenia oraz o stanowiska kierowania organów władzy i administracji publicznej. Organy administracji publicznej realizować będą przedsięwzięcia wynikające z obowiązków państwa-gospodarza w ramach bieżącej działalności oraz pozamilitarnych przygotowań obronnych państwa i ujmować je będą w stosownych regulaminach organizacyjnych, zakresach zadaniowych oraz dokumentach sporządzanych w ramach planowania obronnego.

Minister Obrony Narodowej, w zakresie powierzonym przez Prezesa Rady Ministrów, uprawniony zostanie do koordynowania – nie tylko w czasie wojny jak obecnie, ale również w czasie pokoju i kryzysu – całokształtu działań podejmowanych przez organy administracji publicznej, a także sprawować będzie ogólny nadzór nad realizacją zadań HNS w państwie. Za poszczególne działy administracji rządowej w ramach realizacji zadań HNS odpowiedzialni będą ministrowie kierujący tymi działami, a na szczeblu wojewódzkim – wojewodowie.

W celu podniesienia efektywności realizowanych zadań na rzecz wojsk sojuszniczych stacjonujących lub przemieszczających się przez terytorium Rzeczypospolitej Polskiej, a także poprawy dotychczasowego systemu wsparcia przez państwo-gospodarza, przewiduje się:

1. Nadanie Ministrowi Obrony Narodowej odpowiednich uprawnień do koordynacji realizacji zadań wynikających z roli państwa-gospodarza zarówno w zakresie odpowiedzialności resortu obrony narodowej jak i resortów cywilnych, reprezentujących podstawowe działy administracji rządowej takie jak: energia, gospodarka morska, gospodarka wodna, łączność, zdrowie, sprawy wewnętrzne, transport, finanse. Zostało to wstępnie uzgodnione w trakcie międzyresortowych konsultacji podczas opracowania „Koncepcji" przez MON;
2. Powołanie pełnomocników do spraw HNS w ministerstwach, urzędach wojewódzkich oraz innych instytucjach pełniących ważną rolę w systemie HNS;
3. Powołanie Narodowego Komitetu Koordy-

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

nacyjnego HNS pod przewodnictwem Pełnomocnika Ministra Obrony Narodowej do spraw HNS (Szef Zarządu Logistyki – P4 SG WP), w skład którego wchodzić będą pełnomocnicy ministrów, wojewodów oraz innych instytucji;

4. Uregulowanie zakresu udzielanej pomocy przez podmioty administracji cywilnej i wojskowej na rzecz wsparcia przez państwo-gospodarza oraz stałego udziału w pracach grup roboczych NATO i UE zajmujących się wymogami i zadaniami HNS;
5. Określenie zasad współpracy między ogniwami militarnymi i niemilitarnymi w zakresie działań podejmowanych na rzecz HNS.

Prace Międzyresortowego Zespołu nad opracowaniem „Koncepcji funkcjonowania narodowego systemu wsparcia przez państwo-gospodarza (HNS)" wykazały, że w celu pełnego włączenia ogniw pozamilitarnych w realizację zadań wynikających z obowiązków państwa-gospodarza konieczne są zmiany legislacyjne regulujące funkcjonowanie systemu HNS w Polsce.

Koncepcja została zatwierdzona przez Ministra Obrony Narodowej 4 grudnia 2018 r. Harmonogram prac zakłada, że przedstawienie systemowego rozstrzygnięcia na szczeblu Rady Ministrów nastąpi do końca 2019 roku po przygotowaniu i uzgodnieniu międzyresortowym projektu nowelizacji ustawy o powszechnym obowiązku obrony wraz z projektem rozporządzenia nadającego Ministrowi Obrony Narodowej oraz jego Pełnomocnikowi do spraw HNS kompetencje w zakresie koordynowania zadań HNS w państwie w czasie pokoju, kryzysu i wojny.

Wyborczy test ukraińskiego systemu bezpieczeństwa

Piotr Żochowski
Ośrodek Studiów Wschodnich

Rok 2019 upłynie na Ukrainie w atmosfer ze permanentnej kampanii wyborczej. Nowego prezydenta poznamy w ostatniej dekadzie kwietnia, a w październiku będziemy świadkami formowania się nowego układu partyjnego w Radzie Najwyższej. Zostanie utworzony również nowy rząd. Dynamiczne zmiany na scenie politycznej kraju są wyzwaniem, ale też i testem dla ukraińskiego systemu bezpieczeństwa kształtowanego od 2014 roku pod względem jego podatności na atmosferę walki politycznej i zachowania skuteczności wobec działań destabilizacyjnych prowadzonych przez rosyjskie służby specjalne.

PERCEPCJA ZAGROŻEŃ

Ukraina jest państwem podatnym na destrukcyjne działania Rosji w sfer ze politycznej, gospodarczej, informacyjnej i bezpieczeństwa. Moskwa nadal będzie podejmować niemilitarne działania destabilizacyjne, których długoterminowym celem jest zmuszenie ukraińskich elit do nawiązania dialogu z Rosją, uznanie jej interesów politycznych i gospodarczych, a w efekcie polityczne podporządkowanie kraju. W katalogu działań rosyjskich istotne miejsce zajmuje nadal ewentualne wznowienie operacji militarnej, poprzedzonej realizacją scenariusza prowokacji uzasadniającego użycie sił zbrojnych.

Rosyjskie działania mogą przybrać następujące formy:

- próby dyskredytacji w sfer ze informacyjnej obecnie rządzących prozachodnich polityków; gra na pogłębienie konfliktów wewnątrz klasy politycznej Ukrainy, w tym wewnątrz koalicji rządzącej; wsparcie finansowe, polityczne i informacyjne partii/środowisk/mediów opowiadających się za rosyjską interpretacją realizacji porozumień mińskich, a w szerszym aspekcie – za odbudową relacji z Rosją, ingerencja w przebieg wyborów prezydenckich i parlamentarnych obejmująca spektrum działań od cyberataków, po wpływanie na postawy wyborcze;
- próby wywołania konfliktów na tle narodowościowym/językowym, wspierania separatyzmów (Węgrów i Rusinów w obwodzie zakarpackim, kilku mniejszości narodowych w obwodzie odeskim, ludności rosyjskoję-

zycznej na terytorium całej Ukrainy), podsycanie konfliktu na tle konfesyjnym związanym z przejmowaniem obiektów sakralnych należących do Ukraińskiego Kościoła Prawosławnego, uznającego zwierzchność patriarchy Moskwy (UPC);

- próby pogłębienia kryzysu społeczno-gospodarczego. Choć wskutek polityki restrykcji gospodarczych, Rosja obecnie ma ograniczone instrumentarium działań, wojna w Donbasie spowodowała na Ukrainie deficyt węgla antracytowego, spalanego w połowie elektrowni cieplnych. Nie można wykluczyć więc okresowych, np. w sezonach grzewczych, działań blokujących dostawy tego surowca z okupowanej części Donbasu i z Rosji (najtańs ze źródła dostaw). Takie blokady mogą być efektywnym sposobem zakłócenia pracy systemu energetycznego Ukrainy, których skutkiem mogą być okresowe wyłączenia prądu i ogrzewania gospodarstwom domowych, co może prowadzić do niepokojów społecznych;
- próby realizacji punktowych akcji sabotażowych i dywersyjnych. Szczególnie narażone w tym kontekście są regiony przygraniczne oraz Krym, a także strategiczna infrastruktura transportowa (linie i dworce kolejowe) i energetyczna (rurociągi i elektrownie, w tym jądrowe). Możliwe są działania destrukcyjne w sfer ze bezpieczeństwa cybernetycznego – złamanie systemów informatycznych ukraińskich instytucji państwowych i finansowych, a także obiektów energetycznych.

ROK WYBORCZY A BEZPIECZEŃSTWO PAŃSTWA

Wład ze Ukrainy regularnie podkreślają zagrożenia związane z działaniami destabilizacyjnymi ze strony Rosji. 5 marca 2019 roku prezydent Petro Poroszenko zatwierdził nową Koncepcję walki z terroryzmem, która zastąpiła zdezaktualizowany dokument przyjęty jeszc ze w 2013 roku. Koncepcja wskazuje Rosję jako źródło większości zagrożeń terrorystycznych, do których zaliczono m.in. inspirowanie działań separatystycznych i wszechstronne wspieranie działalności terrorystycznej marionetkowych quasi państw powstałych na tymczasowo okupowanych terytoriach obwodu donieckiego i ługańskiego, wspieranie przez Rosję ruchów separatystycznych wśród mniejszości narodowych na Ukrainie, a także agresywne działania Rosji na morzach Azowskim i Czarnym. Dokument, który można uznać za uszczegółowienie wątków zawartych w przyjętej w marcu 2016 roku Koncepcji rozwoju sektora bezpieczeństwa i obrony Ukrainy, zawiera plan działań mających służyć poprawie bezpieczeństwa stanu państwa, m.in. zapowiada przeprowadzanie operacji specjalnych mających zmniejszyć skalę zagrożenia terroryzmem. W kontekście umieszczenia Rosji jako głównego zagrożenia terrorystycznego, należy to uznać za zapowiedź prowadzenia działań specjalnych na terytoriach okupowanych.

Od początku 2019 roku przedstawiciele służb specjalnych Ukrainy prowadzą szeroko zakrojoną kampanię informacyjną przestrzegającą przed możliwością rosyjskiej ingerencji w kampanię wyborczą i przebieg wyborów. Za najbardziej prawdopodobne scenarius ze destabilizacji sytuacji na Ukrainie szefowie SBU i wywiadu zagranicznego uznają podjęcie przez Rosję próby cyberataku na serwer Centralnej Komisji Wyborczej, wywołanie zamieszek na tle religijnym mających osłabić ukraińską autokefalię i kontynuowanie długofalowych działań na rzecz wprowadzenia do różnych ugrupowań politycznych prorosyjskich polityków. Według służb ukraińskich, na realizację tych zadań rosyjskie służby specjalne otrzymały dotację budżetową w wysokości 350 mln USD. Strona ukraińska nie wyklucza możliwości realizacji przez Rosję scenariusza militarnego w celu otwarcia połączenia lądowego między Rosją a Krymem. Choć scenariusz ten wydaje się mało prawdopodobny, to nie można wykluczyć możliwości sprowokowania ukraińskich sił zbrojnych do otwarcia ognia i uznania incydentu przez Rosję za akt agresji.

Służba Bezpieczeństwa Ukrainy we współdziałaniu z Państwową Służbą Łączności Specjalnej podjęła działania prewencyjne mające na celu obniżyć podatność elektronicznego systemu wyborczego na ataki cybernetyczne. Prowadzone są szeroko zakrojone działania kontrwywiadowcze i policyjne mające utrudnić rosyjskim służbom specjalnym przeprowadzanie aktów sabotażu. Szef SBU wymienił jako jeden z obszarów rosyj-

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

skiej aktywności destabilizacyjnej podejmowanie prób dewastowania bądź niszczenia cerkwi znajdujących się pod kontrolą Patriarchatu Moskiewskiego. Inną sfera aktywności SBU jest ograniczanie aktywności w przestrzeni informacyjnej (wykorzystujących m.in. komunikatory internetowe) rosyjskich agitatorów wzywających do bojkotu wyborów bądź wzywających do protestów podważających wiarygodność procesu wyborczego, w tym okupacji punktów wyborczych bądź obiektów administracji publicznej. Od końca lutego SBU informuje o blokowaniu zmasowanych ataków cybernetycznych na infrastrukturę cyfrową Centralnej Komisji Wyborczej. Specjaliści SBU stwierdzili, że atak typu „http Flood" (odmiana ataku typu DDoS) został przeprowadzony przy wykorzystaniu przejętych bez wiedzy właścicieli witryn stworzonych w oparciu o bezpłatne oprogramowanie „WordPress", co pozwoliło na generowanie masowej liczby zapytań skierowanych do serwera CKW. Departament Ochrony Kontrwywiadowczej SBU i podległe mu Centrum sytuacyjne ds. cyberbezpieczeństwa nie wyklucza, że ataki zostały przeprowadzone pr ze grupy hakerskie kontrolowane przez rosyjskie służby specjalne.

W ATMOSFERZE POLITYCZNEGO KONFLIKTU

Zagrożeniem dla wyborów prezydenckich na Ukrainie jest duże prawdopodobieństwo podważenia zasady bezstronności działania organów porządkowych i służb specjalnych odpowiedzialnych za ich spokojny przebieg. Niepokojącym zjawiskiem jest wykorzystywanie w manifestacjach o charakter ze wyborczym pozapaństwowych („prywatnych") formacji mających charakter bojówek. W sytuacji, kiedy zgodnie z rankingami wyborczymi Julii Tymoszenko i Petro Poroszenki o ich przejściu do II tury wyborów może zadecydować nieduża liczba głosów, każdy potencjalny incydent zakłócający proces wyborów może mieć istotne znaczenie dla ich dalszego przebiegu, a także posłużyć do podważenia cząstkowych wyników. Ryzyko takiego scenariusza jest tym bardziej prawdopodobne ze względu na niski poziom zaufania społeczeństwa wobec administracji państwowej. Według badań opublikowanych 21 marca przez Instytut Gallupa, wskaźnik zaufania społecznego do instytucji państwowych wyniósł jedynie 9 procent, przy czym 12 procent badanych uważa, że wybory będą uczciwe. Ukraińska Grupa Socjologiczna „Rejtynh" w wynikach badań opublikowanych 20 marca przedstawiła społeczną percepcję zagrożeń dla przebiegu wyborów. Respondenci za czynniki mogące przeszkodzić im w udziale w wyborach wymienili: informacje o masowym kupowaniu głosów (49 procent), duże kolejki w lokalach wyborczych (47 procent), prowokacje w pobliżu lokali wyborczych (43 procent).

Niepokojącą cechą aktualnej sytuacji na Ukrainie są przejawy niestabilności systemu bezpieczeństwa wewnętrznego państwa. Oficjalne komunikaty przedstawicieli władz mają charakter uspokajający. Służba Bezpieczeństwa Ukrainy i MSW zapewniają, że bezpieczeństwo wyborów będzie zagwarantowane, a państwo nie utraci monopolu na wykorzystanie siły. Wiarygodność tych oświadczeń osłabiają przykłady świadczące o zaangażowaniu w walkę wyborczą przedstawicieli instytucji odpowiedzialnych za bezpieczeństwo państwa. Aktywność ministra spraw wewnętrznych Arsena Awakowa otwarcie krytykującego prezydenta Poroszenkę ma wpływ na sposób działania organów policji i podległej MSW Gwardii Narodowej. W atmosfer ze narastającej walki politycznej zachowanie organów porządkowych ma wpływ na sposób i charakter przeprowadzania manifestacji przedwyborczych. Nie można wykluczyć, że będą one reagować stronniczo na przejawy zakłócenia porządku publicznego pozwalając na eskalację wystąpień wymierzonych przeciwko urzędującemu prezydentowi.

W atmosfer ze rywalizacji przedwyborczej kwestionowana jest apolityczność podległej prezydentowi Służby Bezpieczeństwa Ukrainy. Przeciwnicy Poroszenki zwracają uwagę, że SBU i Państwowa Służba Łączności Specjalnej odpowiedzialne za zapewnienie bezpieczeństwa wyborów w kontekście osłony kontrwywiadowczej i cybernetycznej, sprawują kontrolę nad wyborczym systemem elektronicznym. Pozwala to na formułowanie tezy wskazującej na możliwość dokonywania fałszerstw wyników wyborów podczas wprowadzania danych do systemu elektronicznego Centralnej Komisji Wyborczej. Ze swej strony kierownictwo SBU stale podkreśla o prowadzeniu przez Rosję działań mających na celu sparaliżowa-

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

nie systemu informatycznego CKW oraz ostrzega o możliwości zmasowanego ataku informatycznego w dniu wyborów. Proces liczenia głosów jest najbardziej wrażliwym i podatnym na zakłócenia obszarem, pozwalającym kwestionować wiarygodność wyborów.

Specyfiką ukraińskich wyborów jest również wykorzystywanie przez polityków pozapaństwowych formacji o charakter ze paramilitarnym. Organizowane przez nich akcje, przybierające często formułę manifestacji, podczas których dochodzi do użycia siły, mają istotny wpływ na kształtowanie sympatii wyborczych. Obserwowana aktywność Drużyn Narodowych skupiających byłych ochotników walczących na wschodzie Ukrainy i wspieranych nieformalnie przez szefa MSW jest wymierzona bezpośrednio w prezydenta Poroszenkę.

Innym przykładem ograniczającym monopol użycia siły przez instytucje państwowe jest funkcjonowanie formacji tzw. „straży municypalnych". Na Ukrainie istnieje około 200 tego rodzaju formacji podległych merom miast, których zadaniem jest zapewnienie bezpieczeństwa publicznego i wspomaganie działalności policji. W rzeczywistości są to formacje służące ochronie interesów politycznych i ekonomicznych danego mera miasta, a w sposób ich działania wpisane jest użycie siły fizycznej czy zastraszanie.

UKRAIŃSKIE WYZWANIA

- Wład ze w Kijowie są świadome, że działania Rosji mające na celu destabilizację Ukrainy nie ograniczają się do działań natury militarnej. Społeczeństwo ukraińskie stało się celem wielopłaszczyznowych rosyjskich działań aktywnych, w tym poprzez środki oddziaływania informacyjnego. Wykorzystując brak bariery językowej i dysponując kierowanym przez państwo zaawansowanym organizacyjnie i technicznie systemem prowadzenia „wojny informacyjnej" Kreml prowadzi nadal różnorodne działania na Ukrainie.
- Wład ze ukraińskie, uznając oficjalnie Rosję jako państwo-agresora dążącego do podważenia fundamentów bytu państwowego Ukrainy, w ciągu ostatnich lat sformułowały nową politykę bezpieczeństwa skupiającą się na działaniach służących odparciu rosyjskiej agresji. Jednym z najważniejszych elementów tej polityki było skierowanie większości sił i środków na działania o charakter ze kontrwywiadowczym, skoncentrowanie się na zadaniach związanych z rozpoznaniem, przejmowaniem i zwalczaniem rosyjskich aktywów operacyjnych oraz ukształtowanie systemu obrony informacyjnej państwa. Zostały do niego włączone instytucje państwowe i – równolegle – wspierane przez państwo inicjatywy przedstawicieli społeczeństwa obywatelskiego.
- Czynnikiem mającym kapitalne znaczenie dla skuteczności ukraińskiego systemu bezpieczeństwa jest współpraca z USA i państwami UE w reformowaniu służb specjalnych oraz otrzymywane wsparcie finansowe (od października 2019 roku USA rozpoczną przekazywanie kwoty ponad 200 mln USD przeznaczonej na pomoc wojskową). Pozytywny obraz ukraińskich dokonań w sfer ze budowania instytucji odpowiedzialnych za bezpieczeństwo państwa, czy dotychczasowe sukcesy w starciu z rosyjską machiną destabilizacyjną, mogą się jednak okazać nietrwałe. Zależy to przede wszystkim od postawy ukraińskich elit politycznych, które często nie wahają się angażować instytucje odpowiedzialne za bezpieczeństwo państwa dla realizacji doraźnych celów politycznych. Angażowanie służb specjalnych, policji czy pozapaństwowych formacji paramilitarnych do walki politycznej w znaczący sposób osłabia spójność ukraińskiego systemu bezpieczeństwa i zmniejsza jego odporność na destrukcyjne działania ze strony Rosji.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

Grypa w sezonie epidemicznym 2018/2019 w Polsce i Europie

Izabela Kucharska, Beata Michulec
Główny Inspektorat Sanitarny

W ramach monitoringu sytuacji epidemiologicznej grypy w sezonie grypowym 2018/2019, w okresie od 1 września 2018 r. do 15 marca 2019 r., zanotowano łącznie 3 337 044 zgłoszeń przypadków zachorowań lub podejrzeń zachorowań na grypę i zachorowania grypopodobne (na podstawie tygodniowych raportów NIZP-PZH obejmujących następujące tygodnie sprawozdawc ze 1-7, 8-15, 16-22 i 23 – do końca miesiąca).

Grypa to ostre wirusowe zakażenie górnych dróg oddechowych, wywoływane przez wirusy grypy. Do akażenia dochodzi drogą kropelkową, a także przez kontakt ze skażoną powierzchnią. Każdy człowiek może przenieść wirusa na skór ze rąk, czy ubraniu.

Okres wylęgania grypy wynosi od 1 do 4 dni (średnio 1-2 dni). Osoba chora zakaża w okresie przed wystąpieniem objawów, w okresie tzw. prodromalnym, zazwyczaj 1 dobę przed wystąpieniem pierwszych dolegliwości. Charakterystyczne dla grypy jest to, że choroba najczęściej pojawia się nagle, charakteryzuje się dużą zakaźnością i towarzyszą jej objawy ze strony układu oddechowego takie jak kaszel, ból gardła, katar oraz objawy ogólnoustrojowe: wysoka gorączka powyżej 38°C, dreszcze, ból/sztywność mięśni, ból głowy, ból w klatce piersiowej, złe samopoczucie, brak łaknienia, czasem także nudności, wymioty.

Choroba zwykle ustępuje samoistnie po 3-7 dniach od wystąpienia pierwszych objawów, ale kaszel, zmęczenie i uczucie rozbicia mogą się utrzymywać do ok. 2 tyg.

Najczęsts ze powikłania grypy to wtórne bakteryjne zapalenie płuc, zapalenie oskrzeli, zapalenia ucha środkowego. Grypa może prowadzić również do ciężkich powikłań takich jak zapalenie mięśnia sercowego, mózgu i op on mózgowych. Powikłania pogrypowe mogą wystąpić u każdego, niezależnie od wieku i stanu zdrowia. Ryzyko powikłań jest szczególnie wysokie u osób z chorobami przewlekłymi, osób po 60 roku życia kobiet w ciąży i dzieci.

Przyczyną corocznych, sezonowych wzrostów zachorowań ludzi na grypę w okresie jesienno-zimowym są wirusy grypy typu A i B. Zachorowania mogą przybierać postać sezonową, epidemiczną lub pandemiczną. Grypa powoduje zachorowania w każdej grupie wiekowej. Światowa Organizacja Zdrowia szacuje, że rocznie może ona dotknąć 5-10% dorosłych i 20-30% dzieci. Śmiertelność grypy sezonowej wynosi 0,1-0,5% (tzn. umiera 1 do 5 na 1000 osób, które zachorowały), przy czym 90% zgonów występuje u osób po 60 roku życia.

W Polsce nadzór epidemiologiczny nad grypą prowadzony jest w ciągu całego roku, ze szczególnym nasileniem nadzoru wirusologicznego w okresie zwiększonej liczby zachorowań, który trwa zwykle od września do kwietnia, przy czym szczyt zachorowań przypada zwykle między styczniem a marcem. Rejestruje się wtedy nawet do kilku milionów zachorowań na grypę i choroby grypopodobne.

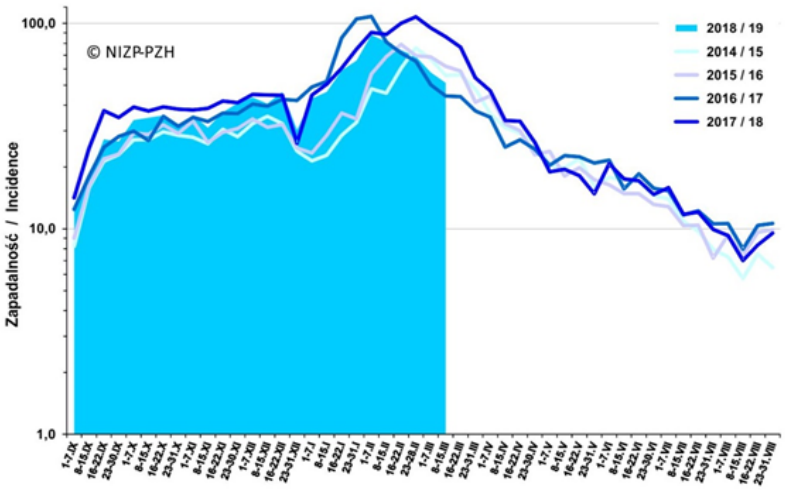
Zgodnie z informacją podaną w bieżącym meldunku epidemiologicznym „Zachorowania i podejrzenia zachorowań na grypę w Polsce" w ostatnim okresie sprawozdawczym tj. 08-15.03.2019 r. zarejestrowano w Polsce ogółem 157 867 zachorowań na grypę i zakażenia grypopodobne. Średnia dzienna zapadalność wynosiła 51,3 przypadków na 100 000 ludności, co stanowi 11,1% spadek w stosunku do poprzedzającego okresu sprawozdawczego (meldunek za okres 01-07 marca 2019 r.). W analogicznym okresie roku 2018 zarejestrowano w Polsce 264 781 zachorowań na grypę i zakażenia grypopodobne. W przypadkach zachorowań, które były diagnozowane laboratoryjnie od 03 września 2018 r. do 10 marca 2019 r., w 44,5% badanych próbek potwierdzono obec-

ność wirusa grypy. Próbki do badań laboratoryjnych w kierunku potwierdzenia zakażenia wirusami grypy pochodzą głównie od pacjentów, którzy są hospitalizowani z powodu ich stanu klinicznego lub współistniejącej choroby.

W sezonie epidemicznym grypy w Polsce od 1 września 2018 r. do 15 marca 2019 r. zmarło 108 osób, u których stwierdzono obecność wirusa grypy na podstawie badań wykonanych metodą RT-PCR. Obecnie sytuacja epidemiologiczna nie stwarza podstaw do prowadzenia zaostrzonego nadzoru epidemiologicznego grypy, ani do ogłoszenia specjalnego alertu przeciwepidemicznego.

miologicznego i wirusologicznego nad grypą (Sentinel), od pacjentów z objawami klinicznymi grypy pobrano 1 836 próbek do badania laboratoryjnego. Wirusa grypy potwierdzono w 786 próbkach (42,8%). Wirus grypy A wykryto w 774 próbkach, w tym A/H1N1/pdm2009 – 44,5%, A H3N2/ – 55,5%. Wirus typu B wykryto tylko w 12 próbkach (linia Yamagata).

Od początku trwania sezonu epidemicznego 2018/2019 zachorowania wywołane przez wirus grypy typu A stanowią 99,1%. Zarejestrowano łącznie 8 163 (56,9%) zachorowania wywołane przez wirus A/H1N1/pdm2009 oraz 6 195 (43,1%)



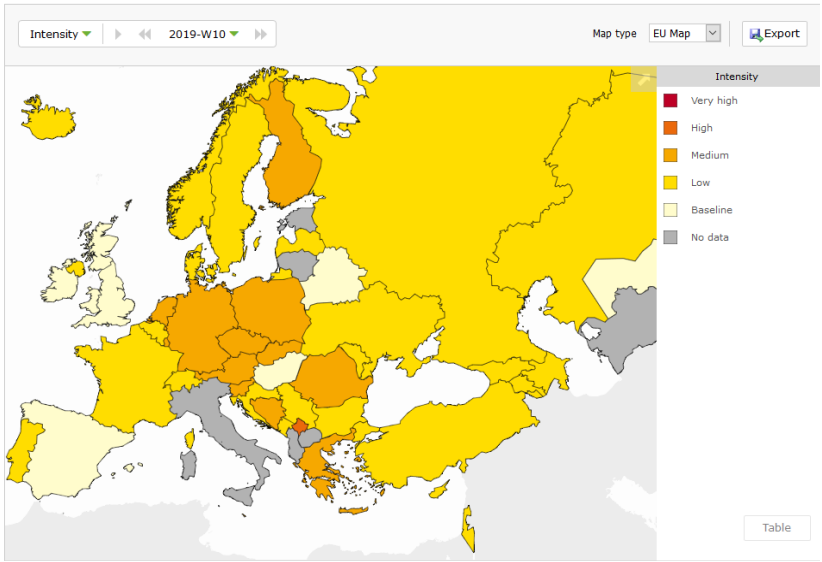
Wykres: Zachorowania i podejrzenia zachorowań na grypę.
Źródło: Meldunki Epidemiologiczne – Zachorowania i podejrzenia zachorowań na grypę w Polsce, 2019 nr 3B (10).

Zgodnie z informacją dostępną na stronie European Centre for Disease Preventi on and Control (ECDC), w większości krajów Unii Europejskiej/ Europejskiego Obszaru Gospodarczego obecnie aktywność wirusa grypy jest nadal rozległa. Od 4 do 10 marca 2019 r., w ramach nadzoru epide-

wywołanych przez wirus A/H3N2/.

Zachorowania wywołane przez wirus grypy typu B stanowią 0,9%.

Poniższa mapa przedstawia aktywność wirusa grypy w Europie w okresie od 4 do 10 marca 2019 r.



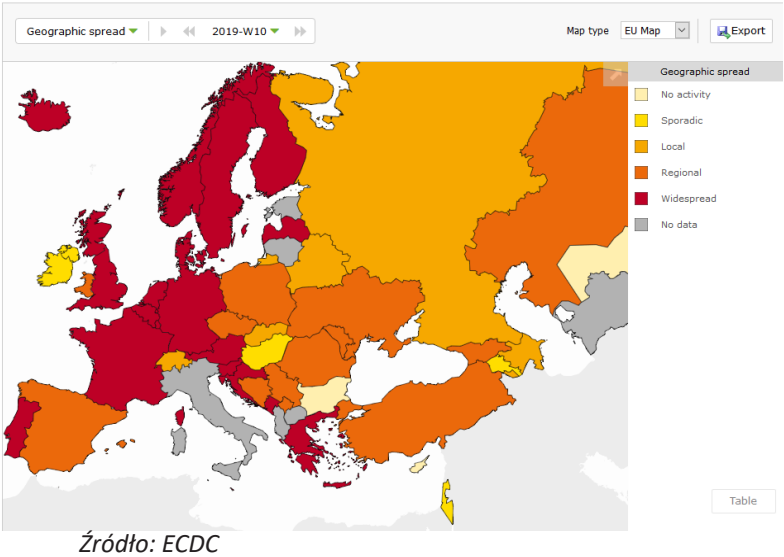
Źródło: ECDC

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

Z 46 krajów przekazujących dane epidemiologiczne do ECDC, w dziesiątym tygodniu 2019 roku (wg ECDC jest to 4-10 marca 2019 r.) w 8 krajach odnotowano podstawową aktywność wirusa grypy, w 24 krajach odnotowano niską aktywność wirusa grypy, w 13 odnotowano średnią aktywność wirusa grypy, zaś 1 kraj odnotował wysoką aktywność wirusa (Kosowo).

Ponadto, w 3 krajach nie odnotowano rozprzestrzeniania się wirusa grypy (Bułgaria, Cypr, Uzbekistan), w 5 krajach odnotowano sporadyczne rozprzestrzenianie się wirusa grypy (Armenia, Węgry, Irlandia, Izrael, Zjednoczone Królestwo (Północna Irlandia)), w 5 krajach odnotowano ogniska epidemiczne grypy o zasięgu lokalnym (Azerbejdżan, Białoruś, Federacja Rosyjska, Słowacja, Szwajcaria), w 13 krajach odnotowano ogniska epidemiczne grypy o zasięgu regionalnym, 20 krajów odnotowało ogniska epidemiczne na całym swoim obszarze (północne, południowe i zachodnie tereny).

Poniższa mapa, pobrana ze strony ECDC, przedstawia geograficzne rozprzestrzenienie wirusa grypy w Europie w okresie od 4 do10 marca 2019 r.



Źródło: ECDC

W sezonie 2018/2019, zgodnie z zaleceniami opracowanymi w Europejskiej Agencji Leków na podstawie obserwacji WHO, w skład szczepionek przeciw grypie dostępnych w Europie wchodzą:
trzy wirusy grypy:

- A/Michigan/45/2015 (H1N1)pdm09 – wirus podobny
- A/Singapore/INFIMH-16-0019/2016 (H3N2) – wirus podobny
- B/Colorado/06/2017 – wirus podobny (B/Victoria/2/87 lineage)1

lub cztery wirusy grypy:

- ww. i B/Phuket/3073/2013 – wirus podobny (B/Yamagata/16/88 lineage).

Szczepienia przeciw grypie są najskuteczniejszą i najtańszą strategią zapobiegania chorobie.

Zgodnie z rozporządzeniem Ministra Zdrowia z 16 września 2010 r. w sprawie wykazu zalecanych szczepień ochronnych oraz sposobu finansowania i dokumentowania zalecanych szczepień ochronnych wymaganych międzynarodowymi przepisami zdrowotnymi (Dz. U. Nr 180, poz. 1215) obecnie szczepienie przeciwko grypie należy w Polsce do szczepień zalecanych, tzn. niefinansowanych ze środków budżetu państwa pozostających w dyspozycji ministra właściwego do spraw zdrowia. Program Szczepień Ochronnych (PSO) na 2019 rok w części II uwzględnia szczepienie przeciwko grypie, jako szczególnie zalecane osobom ze wskazań klinicznych i indywidualnych (m. in. osobom po transplantacji narządów, przewlekle chorym dzieciom i dorosłym, osobom w stanach obniżonej odporności i chorym na nowotwory układu krwiotwórczego, dzieciom z wadami wrodzonymi serca zwłaszcza sinicznymi, z niewydolnością serca, z nadciśnieniem płucnym, kobietom w ciąży lub planującym ciążę) oraz epidemiologicznych (m.in. zdrowym dzieciom w wieku od ukończenia 6 miesiąca życia do ukończenia 18 roku życia, osobom w wieku powyżej 55 lat, osobom mającym bliski kontakt zawodowy lub rodzinny z dziećmi oraz z osobami w wieku podeszłym lub przewlekle chorymi, pracownikom ochrony zdrowia, szkół, handlu, transportu,

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl

funkcjonariuszom publicznym, pensjonariuszom domów spokojnej starości, domów pomocy społecznej oraz innych placówek zapewniających całodobową opiekę osobom niepełnosprawnym, przewlekle chorym lub osobom w podeszłym wieku), zgodnie z rekomendacjami Rady Sanitarno-Epidemiologicznej, będącej organem doradczym Głównego Inspektora Sanitarnego.

Według wytycznych Światowej Organizacji Zdrowia oraz obowiązującego Programu Szczepień Ochronnych w Polsce, szczepienie przeciwko grypie u osób z grup ryzyka jest zalecane do wykonania w każdym momencie sezonu epidemicznego. Szczepienia ochronne są najskuteczniejszą metodą zapobiegania zachorowaniom na choroby zakaźne, w tym m.in. grypie. Ponadto, zdaniem kardiologów, szczepienia przeciwko grypie zmniejszają ryzyko zawału serca, zgonu i hospitalizacji z powodów kardiologicznych, ponieważ chronią zarówno przed grypą, jak i przed uwolnieniem mediatorów zapalnych sprzyjających zawałom oraz nasilających niewydolność serca. Niekiedy odporność przeciwko jednemu rodzajowi wirusa (który może zostać podany w szczepionce) warunkuje częściową odporność na inny, podobny rodzaj (tzw. odporność krzyżowa). W takim przypadku zachorowanie na grypę wywołaną innym podtypem/wariantem wirusa, niż został podany w szczepionce, może mieć łagodniejszy przebieg.

Proces monitorowania zagrożeń realizowany w Ministerstwie Gospodarki Morskiej i Żeglugi Śródlądowej

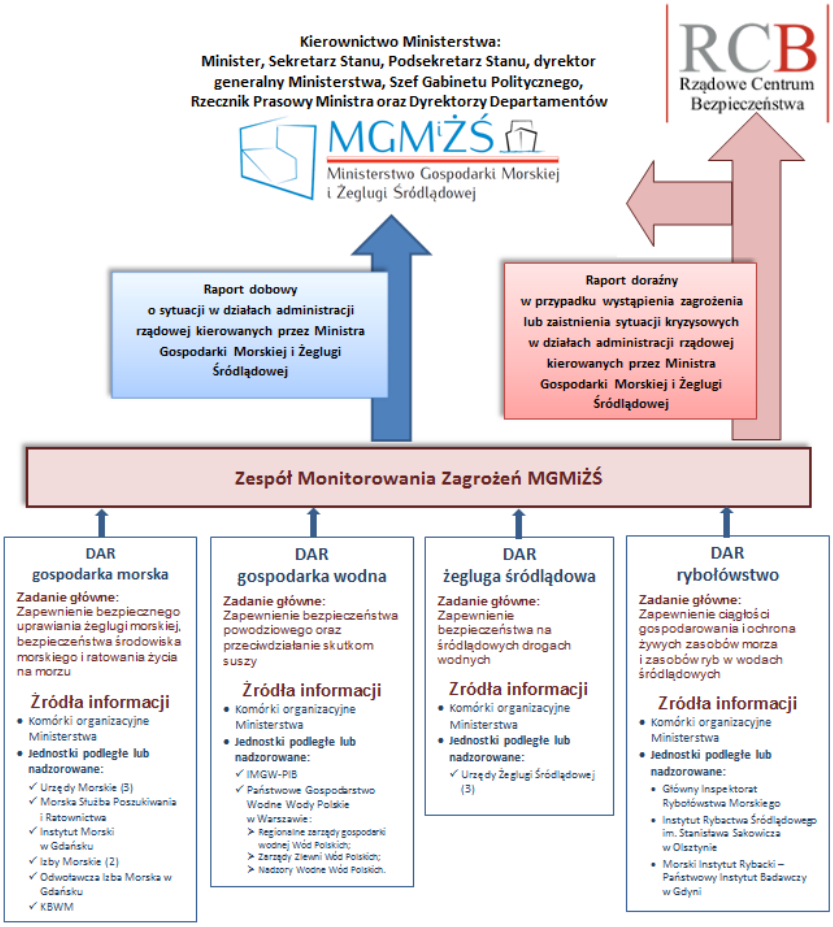
Katarzyna Śmiałek
Ministerstwo Gospodarki Morskiej i Żeglugi Śródlądowej

Ministerstwo Gospodarki Morskiej i Żeglugi Śródlądowej powstało 8 grudnia 2015 r. na mocy Rozporządzenia Rady Ministrów z 7 grudnia 2015 r. w sprawie utworzenia MGMiŻŚ (Dz. U. z 2015 r. poz. 2078). Zakres właściwości Ministra Gospodarki Morskiej i Żeglugi Śródlądowej obejmuje działy administracji rządowej: gospodarka morska (wcześniej Minister Infrastruktury i Rozwoju), rybołówstwo (wcześniej Minister Rolnictwa i Rozwoju Wsi), żegluga śródlądowa (wcześniej Minister Infrastruktury i Budownictwa), a także (od stycznia 2018 r.[1]) dział gospodarka wodna (wcześniej Minister Środowiska).

1. Rozporządzenie Rady Ministrów z dnia 11 stycznia 2018 r. zmieniające rozporządzenie w sprawie utworzenia Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej (Dz. U. 2018 poz. 105).

Wypełnianie zadań zarządzania kryzysowego przez ministra GMiŻŚ wynika z art. 12 ust. 1, art. 20a i art. 21 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401 i 1560) i wiąże się ściśle z realizacją zadań kompetencyjnych we wskazanych wyżej obszarach. W gospodarce morskiej dotyczy to m. in. takich dziedzin jak transport morski, porty i przystanie morskie czy ochrona środowiska morskiego. Sprawy z zakresu żeglugi śródlądowej to np. utrzymanie śródlądowych dróg wodnych o szczególnym znaczeniu transportowym, ruch wodny czy przewóz osób i rzeczy środkami żeglugi śródlądowej. Rybołówstwo obejmuje m. in. sprawy rybactwa śródlądowego i rybołówstwa morskiego, a także racjonalnego gospodarowania żywymi zasobami morza. Z kolei w obszar ze gospodarki wodnej leżą m. in. zadania z zakresu ochrony przeciwpowodziowej, w tym budowy, modernizacji oraz utrzymania urządzeń wodnych zabezpieczających przed powodzią oraz koordynacji przedsięwzięć służących osłonie i ochronie przeciwpowodziowej państwa.

W celu usprawnienia procesu monitorowania zagrożeń w obszar ze właściwości ministra GMiŻŚ opracowany został katalog przykładowych sytuacji kryzysowych w działach administracji rządowej gospodarka morska, gospodarka wodna, żegluga śródlądowa i rybołówstwo. Obejmuje on m. in. takie zdarzenia jak katastrofa morska wymagająca masowej operacji ratowniczej, katastrofalne zanieczyszczenie środowiska morskiego, zdarzenia podczas transportu materiałów niebezpiecznych, zablokowanie torów podejściowych



Schemat procesu monitorowania w działach administracji rządowej kierowanych przez Ministra Gospodarki Morskiej i Żeglugi Śródlądowej

do portów, zniszczenie lub uszkodzenie urządzeń i budowli hydrotechnicznych, zniszczenie lub uszkodzenie budowli piętrzącej wodę, zniszczenia infrastruktury wodnej w wyniku powodzi, zakłócenia w systemie zaopatrzenia w wodę, a także zagrożenia terrorystyczne.

Bardzo istotną rolę w realizacji zadań zarządzania kryzysowego odgrywa skuteczny i sprawny przepływ informacji między Ministrem Gospodarki Morskiej i Żeglugi Śródlądowej a jednostkami jemu podległymi lub przez niego nadzorowanymi. Wymiana informacji odbywa się poprzez Zespół Monitorowania Zagrożeń funkcjonujący w ramach Biura Obrony i Ochrony Informacji Niejawnych.

Zespół Monitorowania Zagrożeń funkcjonuje w sytuacjach zwyczajnych oraz w sytuacjach kryzysowych. Zespół Monitorowania Zagrożeń opracowuje dobowe raporty o sytuacji w działach administracji rządowej będących we właściwości Ministra Gospodarki Morskiej i Żeglugi Śródlądowej. W przypadku wystąpienia zagrożenia lub zaistnienia sytuacji kryzysowych lub mogących mieć wpływ na funkcjonowanie tych działów, sporządzane są raporty doraźne. Raporty są przekazywany kierownictwu ministerstwa: ministrowi, sekretarzom stanu, podsekretarzom stanu, dyrektorowi generalnemu ministerstwa, szefowi Gabinetu Politycznego, rzecznikowi prasowemu ministra oraz dyrektorom departamentów.

Raporty są sporządzane w godzinach pracy ministerstwa i przekazywane na adresy email członków kierownictwa.

W przypadku wystąpienia zagrożeń informacje są przekazywane poprzez:

- wiadomość sms wysyłaną na numery telefonów służbowych członków Kierownictwa;
- informację mailową przekazywaną na adresy poczty internetowej członków Kierownictwa;
- informację mailową przekazywaną na adres służby dyżurnej Rządowego Centrum Bezpieczeństwa.

Proces monitorowania sytuacji w działach administracji rządowej kierowanych przez Ministra Gospodarki Morskiej i Żeglugi Śródlądowej służy przeciwdziałaniu sytuacjom kryzysowym oraz skutecznemu usuwaniu ich skutków.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www.rcb.gov.pl