RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 31 PAŹDZIERNIK – GRUDZIEŃ 2020

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

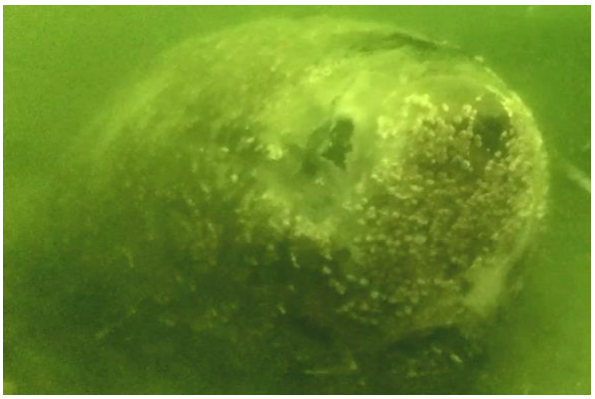
Neutralizacja bomby lotniczej TALLBOY – nowe technologie na rzecz poprawy bezpieczeństwa podczas oczyszczania terenu z niewybuchów

Piotr Nowak

Grupa Nurków Minerów, 12. dywizjon Trałowców Świnoujście

Oczyszczanie terenów z przedmiotów wybuchowych i niebezpiecznych (PWiN) to przedsięwzięcia realizowane przez wyznaczone, specjalistyczne poddziały Sił Zbrojnych RP, które polegają na rozpoznaniu, zabezpieczeniu, neutralizacji i usuwaniu, jak również ostatecznym niszczeniu znalezionych niewybuchów. Patrole saperskie współpracują z przedstawicielami administracji publicznej na podstawie ustawy o zarządzaniu kryzysowym[1]. Historia największej neutralizacji przedmiotu wybuchowego i niebezpiecznego w Polsce rozpoczęła się 16 kwietnia 1945 r., gdy 617. brytyjski Dywizjon RAF zrzucił na niemiecki ciężki krążownik „Lützow", w pobliżu Świnoujścia, trzynaści specjalnie zaprojektowanych bomb głęboko penetrujących. Twarda konstrukcja umożliwiała zagłębienie bomby głęboko pod powierzchnię gruntu, a detonacja 2400 kg materiału wybuchowego generowała falę sejsmiczną o niszczycielskim działaniu na infrastrukturę budowlaną, również podziemne bunkry i instalacje wojskowe.

Ukryty przez 75 lat na dnie Kanału Piastowskiego niewybuch bomby lotniczej o wadze 12 000 funtów został odnaleziony podczas modernizacji toru wodnego Szczecin-Świnoujście. 16 września 2019 r. zgłoszenie PWiN zostało przyjęte przez Grupę Nurków Minerów z 12. Dywizjonu Trałowców w Świnoujściu. Rekonesans przeprowadzony przez nurków potwierdził występowanie na głębokości 12 m unikatowego niewybuchu o nazwie Tallboy. Rozpoczął się długi proces planowania, mający na celu wybór najbezpieczniejszego sposobu neutralizacji.



Rys 1. Pierwszy rekonesans bomby Tallboy.
Źródło: Grupa Nurków Minerów 12.dTR.

Analiza źródeł historycznych, dokumentacji technicznej brytyjskiej bomby oraz ocena ryzyka związanego z poszczególnymi metodami neutralizacji doprowadziły do oczywistego wyboru techniki low-order, polegającej na wypaleniu (deflagracji) ładunku głównego. Decyzję o zastosowaniu modułowego systemu ładunku kumulacyjnego podjęto ze względu na potwierdzoną skuteczność techniki deflagracji w latach 2015-2020 oraz możliwość zdalnego inicjowania systemu, przy pełnej ewakuacji strefy zagrożenia.

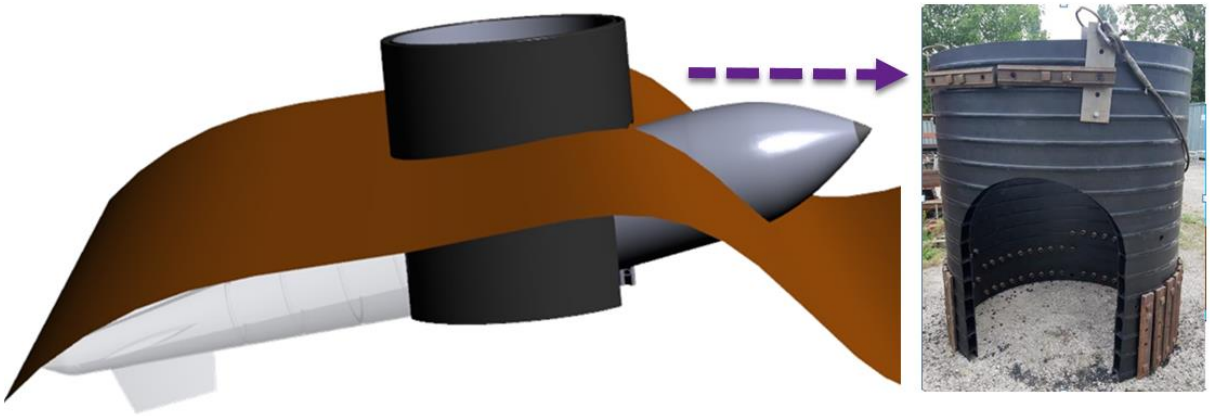
Podczas rocznych przygotowań, kluczowym elementem było usunięcie pozostałych niewybuchów z rejonu operacji oraz uzyskanie certyfikatu czystości – w promieniu 200 m od bomby Tallboy wydobyto ok. 400 sztuk PWiN o łącznej masie materiału wybuchowego wynoszącej 3 tony.

Ze względu na brak światowych doświadczeń w neutralizacji tak ogromnego niewybuchu, przy wyznaczeniu stref bezpieczeństwa korzystano zarówno ze standardowych obliczeń matematycznych dotyczących teorii wybuchu podwodnego, jak również ekspertyzy pracowników naukowych Instytutu Analizy Konstrukcji Politechniki Poznańskiej. Współpraca z naukowcami uczelni wyższych zwiększyła bezpieczeństwo wykonywania prac minerskich oraz pomogła zweryfikować zastosowane środki ostrożności.

Równolegle z opracowaniem technicznego planu neutralizacji PWiN nurkowie minerzy przeprowadzali testy optymalnej konfiguracji systemu low-order. Koncepcja neutralizacji zakładała użycie modułowego systemu ładunku kumulacyjnego w celu zmiany stanu bomby, poprzez usunięcie i likwidację zapalników z korpusu bomby lub/oraz znaczną redukcję ładunku głównego. Ostatecznym celem było usunięcie obiektu niebezpiecznego z rejonu przeprawy promowej Karsibór.

Wykonany, przy użyciu projektowania komputerowego, cyfrowy model niewybuchu na dnie, pozwolił na wykonanie pierścienia dystansowego, którego zadaniem było odkopanie płyty dennej i odsłonięcie zapalników.

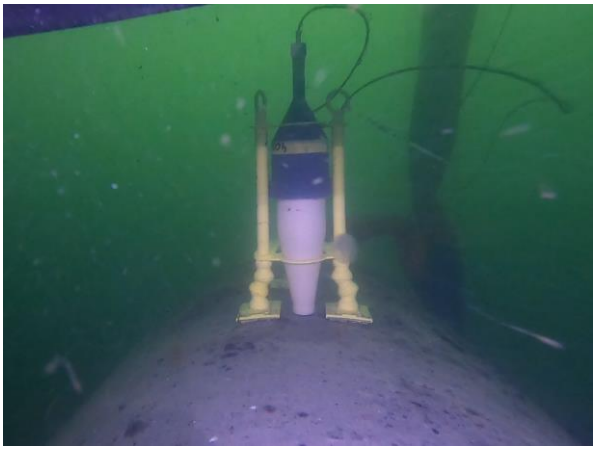
[1] Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.



Rys 2. Zastosowanie pierścienia dystansowego. Źródło: Grupa Nurków Minerów 12.dTR.

W realizacji tej nietypowej neutralizacji, podczas fizycznego przygotowania bomby do zastosowania systemu do deflagracji, konieczne było ścisłe współdziałanie specjalistów Marynarki Wojennej z firmą odpowiedzialną za oczyszczenie z niewybuchów toru Szczecin-Świnoujście.

W trakcie kluczowego etapu operacji, system do deflagracji został zdalnie zainicjowany. Wszystkie założone środki bezpieczeństwa uwzględniały możliwość przejścia procesu deflagracji w detonację, jako możliwy efekt przemiany termodynamicznej.



Rys 3. Zamocowanie ładunku kumulacyjnego na korpusie bomby. Źródło: Grupa Nurków Minerów 12.dTR.

Nowym elementem był również stworzony system monitoringu miejsca realizacji podwodnych prac minerskich składający się z:

- 12 czujników sejsmicznych rozmieszczonych w odległości 100 m – 7000 m;
- 4 czujników sejsmicznych na terminalu LNG;
- czujnika sejsmicznego na terenie budowy tunelu pod Świną;
- szybkiej kamery rejestrującej proces deflagracji;
- 2 kamer rejestrujących rejon operacji z podglądem na żywo;
- 2 dronów rejestrujących doraźnie przebieg operacji;
- bezzałogowego statku powietrznego monitorującego rejon w termowizji.

Neutralizacja bomby Tallboy stanowiła najlepiej opomiarowaną operację wojskową w historii oczyszczania terenów z PWiN. Analiza danych zebranych w trakcie detonacji pozwoliła pracownikom naukowym Politechniki Poznańskiej na wiarygodne oszacowanie wartości procesu deflagracji wynoszącego 37% masy początkowej materiału wybuchowego. Redukcja ładunku głównego przełożyła się bezpośrednio na brak odłamkowania fragmentów korpusu oraz brak zniszczeń infrastruktury promowej oraz nawigacyjnej po przejściu deflagracji w detonację. Powietrzna fala ciśnienia nie spowodowała uszkodzenia przeszklonych powierzchni wieży nawigacyjnej znajdującej się 100 m od punktu zalegania niebezpiecznego obiektu. Istotne jest również, że mniejsza energia detonacji nie doprowadziła do lokalnych wypłyceń na torze wodnym, a ruch statków handlowych o pełnym zanurzeniu przywrócono już po 6 godzinach.

Oczyszczenie Kanału Piastowskiego było możliwe dzięki rozwojowi technik i procedur niszczenia niewybuchów stosowanych przez Zespoły Rozminowania Marynarki Wojennej, współpracy nurków minerów z naukowcami uczelni wyższych oraz licznymi konsultacjami z producentem systemu. Nieodzownym elementem przy każdej realizacji zgłoszenia PWiN jest współpraca i wymiana informacji Sił Zbrojnych RP z przedstawicielami administracji publicznej oraz służbami odpowiedzialnymi za ochronę ludności. W ramach zabezpieczenia neutralizacji, z zagrożonego rejonu ewakuowano 751 mieszkańców. Niestety, mimo realnego zagrożenia życia i zdrowia, 40 osób odmówiło opuszczenia swoich nieruchomości i podpisało stosowne dokumenty. Możliwość odmowy ewakuacji z zagrożonego rejonu stanowi poważny problem dla służb i samorządów.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Likwidacja brytyjskiej bomby lotniczej nie miała jedynie aspektu lokalnego, ale była istotna z punktu widzenia interesu gospodarczego kraju, zapewniając terminową realizację inwestycji – pogłębienie toru wodnego do portu Szczecin. Na etapie planowania operacji, istotnym elementem były również rozpoczynające się prace związane z drążeniem tunelu pod Świną.

Rys 4. Przejście deflagracji w detonację. Źródło: Materiały 8.FOW.

Neutralizacja uzbrojenia z okresu działań wojennych w miejscu zalegania poprzez proces deflagracji, znacznie redukuje koszty przedsięwzięcia. Stosowana w Marynarce Wojennej procedura znacząco zmniejsza obszar oddziaływania niewybuchu na lokalną społeczność, jednocześnie minimalizując ryzyko dla żołnierzy realizujących prace minerskie przy zachowaniu najwyższych standardów ochrony środowiska. Krótsza realizacja zgłoszenia PWiN przekłada się bezpośrednio na aspekt ekonomiczny, związany ze skróconym czasem zamknięcia drogi wodnej.

Wysoki standard wszystkich wykonywanych prac umożliwił bezpieczne przeprowadzenie operacji, znacząco ograniczając ryzyko utraty zdrowia lub życia żołnierzy i służb realizujących zadanie. Bomba lotnicza D.P. 12000 lbs, największy niewybuch znaleziony w historii Polski, została zneutralizowana i nie będzie stanowiła zagrożenia na torze wodnym Szczecin-Świnoujście.

Działania realizowane przez WOT w celu zapewnienia wsparcia podmiotom układu pozamilitarnego w czasie trwania pandemii COVID-19

Ilona Wróbel, Sylwia Tratkiewicz
Dowództwo Wojsk Obrony Terytorialnej

Wojska Obrony Terytorialnej zostały utworzone 1 stycznia 2017 r. i są piątym, najmłodszym rodzajem Sił Zbrojnych RP. Misją formacji jest obrona i wspieranie lokalnych społeczności w czasie pokoju, poprzez przeciwdziałanie i zwalczanie skutków klęsk żywiołowych oraz prowadzenie działań ratowniczych w sytuacjach kryzysowych, w czasie wojny zaś przez wsparcie wojsk operacyjnych i wykonywanie zadań obronnych na terytorium kraju. W niniejszej analizie przedstawiono poziom oraz skalę zaangażowania WOT w działania przeciwepidemiczne, podejmowane przez państwo. Podczas całej operacji – „Odporna Wiosna" i „Trwała Odporność" – dotychczas zaangażowano łącznie 19 142[1] żołnierzy Wojsk Obrony Terytorialnej, w tym 15 267 żołnierzy OT oraz 3 875 żołnierzy zawodowych. Średnio, w ciągu każdego dnia, w działania zaangażowanych jest nawet 65 000 żołnierzy (z WOT i wojsk operacyjnych).

Pierwszy przypadek koronawirusa w Polsce został odnotowany 4 marca 2020 r. Mając na uwadze doświadczenia innych państw dotkniętych pandemią kilka tygodni wcześniej, Wojska Obrony Terytorialnej bardzo szybko przystąpiły do działań związanych z ograniczaniem transmisji wirusa.

Na mocy decyzji Ministra Obrony Narodowej o zaangażowaniu Wojska Polskiego w zwalczanie pandemii, uwzględniając wytyczne Ministra Zdrowia, 13 marca 2020 r. zmieniono model funkcjonowania WOT ze szkoleniowego na przeciwkryzysowy. Przygotowania do udzielenia wsparcia podmiotom cywilnym rozpoczęto od uruchomienia Zespołu Działań Przeciwkryzysowych (ZDP) w systemie 24/7, przeznaczonego do koordynowania i stawiania zadań podległym siłom na terenie całego państwa.

19 marca 2020 r. Wojska Obrony Terytorialnej rozpoczęły operację pk. „Odporna Wiosna", w ramach której z Dowództwa Generalnego Rodzajów Sił Zbrojnych, Żandarmerii Wojskowej, Inspektoratu Wsparcia Sił Zbrojnych oraz akademii wojskowych,

[1] Wartości liczbowe przytoczone w niniejszej analizie są zgodne ze stanem na 8 grudnia 2020 r.

na wniosek właściwego organu służb sanitarnych lub organu samorządu terytorialnego, udzielano wsparcia w zakresie zaopatrzenia w żywność, sprzęt medyczny i inne produkty dla potrzebujących, w tym dla osób objętych kwarantanną, w związku z podejrzeniem zarażenia wirusem SARS-CoV-2.

Kontynuacją wspomnianej wyżej operacji jest prowadzona od 22 czerwca 2020 operacja pk. „Trwała Odporność", w której główny wysiłek skoncentrowano na wsparciu służby zdrowia oraz podmiotów sanitarnych w realizacji zadań w ramach walki z pandemią COVID-19, utrzymywaniu sił w gotowości do wsparcia działań przeciwkryzysowych, wsparciu samorządów i NGO w zakresie dostarczania żywności i środków medycznych dla osób najbardziej potrzebujących, w tym seniorów. Ponadto, udzielane jest wsparcie Policji w zakresie kontroli procesu kwarantanny osób przebywających w długotrwałej izolacji, a także bezpośrednie wsparcie przedsiębiorstw najbardziej dotkniętych skutkami zarażeń. Obie operacje mają taki sam cel, zdefiniowany w pięciu słowach: Zapobiegaj, Identyfikuj, Izoluj, Wspieraj, Odtwarzaj, jednakże operację „Trwała Odporność" cechuje zwiększona intensywność oraz skupienie wysiłku na bezpośrednim wsparciu publicznej służby zdrowia.

Na skutek przywrócenia kontroli na granicach (od 15 marca do 3 maja 2020 r.), w pierwszej kolejności konieczne okazało się wsparcie Straży Granicznej. Na mocy postanowienia Prezydenta RP (art. 11b ustawy o Straży Granicznej) oraz stosownych dokumentów wykonawczych, Wojska Obrony Terytorialnej pomagały Straży Granicznej i Policji w organizacji przejść granicznych, zamykaniu dróg, pełniły służbę na punktach kontrolnych i odcinkach patrolowania, a także udzielały wsparcia logistycznego osobom przekraczającym granicę. Jednocześnie, siły Wojsk Obrony Terytorialnej zostały skierowane na teren 21 lotnisk oraz na morskie przejścia graniczne, gdzie żołnierze zbierali karty lokalizacyjne oraz dokonywali pomiarów temperatury podróżnych z 1 370 samolotów oraz 17 promów. Decyzją Ministra Obrony Narodowej, odpowiedzialność w zakresie wsparcia Straży Granicznej przekazana została wojskom operacyjnym, a Wojska Obrony Terytorialnej skupiły swój wysiłek na realizacji działań wewnątrz kraju.

W związku z dużą liczbą zachorowań i wzrostem liczby osób kierowanych do kwarantanny i izolacji, obszarem wymagającym wsparcia wojska okazały się działania Policji. Dzięki delegowaniu żołnierzy WOT możliwe było zwiększenie liczby patroli, a tym samym możliwości dotarcia do większej grupy osób w ramach monitoringu kwarantanny. W najtrudniejszym okresie, gdy trwał tzw. lockdown, Wojska Obrony Terytorialnej realizowały, wspólnie z funkcjonariuszami Policji, także patrole o charakterze prewencyjnym. Od czasu wydania, w marcu 2020 roku, postanowienia Prezydenta RP o użyciu SZ RP do wsparcia Policji, WOT uczestniczyły w 993 345 patrolach, z czego 967 159 były patrolami związanymi z monitoringiem kwarantanny, natomiast 26 186 to realizowane wspólnie z funkcjonariuszami Policji patrole o charakterze prewencyjnym. Monitoring kwarantanny prowadzony był również samodzielnie przez żołnierzy WOT. Ich działania miały trzy zasadnicze cele: określenia potrzeb wsparcia osób izolowanych, ogólną ocenę ich stanu zdrowia oraz potwierdzenie wykonywania obowiązku kwarantanny.

Kluczowe z punktu widzenia zwalczania pandemii są działania wspierające system ochrony zdrowia. Możliwość użycia wojska do zwalczania pandemii przewiduje ustawa *o przeciwdziałaniu i zwalczaniu chorób zakaźnych wśród ludzi*.[2] Na mocy powyższego dokumentu, Minister Obrony Narodowej wydał decyzje, na podstawie których Wojska Obrony Terytorialnej zostały zaangażowane w udzielanie wsparcia służbom medycznym i innym podmiotom zaangażowanym w walkę z COVID-19 na wielu płaszczyznach. W obliczu narastających potrzeb w zakresie wsparcia wojskowego, konieczne okazało się usprawnienie procesu komunikacji i wnioskowania o udzielenie wsparcia Sił Zbrojnych RP. Uruchomiona została dedykowana instytucjom zewnętrznym „Platforma wsparcia samorządów, organów sanitarnych i podmiotów leczniczych". Aplikacja internetowa, zaprojektowana przez podchorążych WAT, umożliwiła instytucjom cywilnym szybkie i sprawne wnioskowanie o wsparcie udzielane przez WOT. Do tej pory (tj. do 8 grudnia 2020 r.) do aplikacji zarejestrowało się 2 710 użytkowników, którzy łącznie skierowali 14 405 wniosków o wsparcie.

W początkowym etapie pandemii kluczowe okazały się dostawy i dystrybucja materiałów ochronnych, płynów do dezynfekcji, leków i innych środków medycznych. W związku z uruchomieniem rezerw strategicznych, żołnierze WOT zostali skierowani do realizacji zadań zarówno w składach Agencji Rezerw Materiałowych

[2] Art. 44a ustawy z 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (t.j. Dz. U. z 2020 r. poz. 1845 z późn. zm.).

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

(operatorzy wózków widłowych, ładowanie i rozładowywanie transportów, prace administracyjne), jak również dystrybucji materiałów do wskazanych miejsc.

Żołnierze WOT zostali także skierowani do wsparcia inspekcji sanitarnej, w ramach którego udzielono wparcia 194 stacjom sanitarno-epidemiologicznym na terenie kraju. Szczególnie istotne są działania zapewniające pomoc podmiotom leczniczym. W ramach tzw. „pierwszej linii" rządowej strategii walki z pandemią COVID-19, duży wysiłek organizacyjny został skierowany na sprawną organizację punktów wymazowych. Wojska Obrony Terytorialnej zorganizowały 12 punktów drive thru WOT, wydzielono samodzielne zespoły wymazowe dla osób niemobilnych, a także skierowano żołnierzy WOT do przyszpitalnych punktów pobrań. Efektem tych działań jest pobranie 600 000 wymazów. Duży wysiłek stanowi także transport materiału biologicznego do laboratoriów.

Wojska Obrony Terytorialnej zaangażowano w dekontaminację izb szpitalnych i karetek pogotowia, organizację polowych izb przyjęć i koordynowanie ich pracy, w tym triaż pacjentów oraz wsparcie administracyjne placówek. Żołnierze pomagają w szpitalach zakaźnych w opiece nad pacjentami leżącymi, wspierają w pracach administracyjnych (w tym w obsłudze baz danych ELC) i logistycznych (m.in. dostarczanie butli z tlenem). Reagując na bieżące zgłoszenia, siły WOT wspierają także inne placówki medyczne. Wojska Obrony Terytorialnej pracują przy budowie 13 szpitali tymczasowych, gdzie oprócz bezpośredniego wsparcia logistycznego, żołnierze WOT zapewniają i utrzymują zasilanie awaryjne z wykorzystaniem elektrowni polowych o dużej mocy.

Niezwykle istotnym obszarem związanym z walką z pandemią COVID-19 jest wsparcie i opieka nad osobami znajdującymi się w grupie największego ryzyka, tj. pensjonariuszami domów pomocy społecznej i innych placówek opiekuńczych na terenie kraju. Żołnierze Wojsk Obrony Terytorialnej, w ramach działań przeciwepidemicznych, wsparli dotychczas 743 ośrodki pomocy społecznej, zakłady opiekuńczo-lecznicze oraz inne instytucje pomocy społecznej w całej Polsce. Do 8 grudnia 2020 r. żołnierze uczestniczyli w 9 ewakuacjach pensjonariuszy oraz pobrali od nich 99 790 wymazów. W ramach pomocy dostarczano także żywność, środki ochrony indywidualnej, płyny odkażające, wykonywano dekontaminację pomieszczeń czy pomagano przy opiece nad pensjonariuszami.

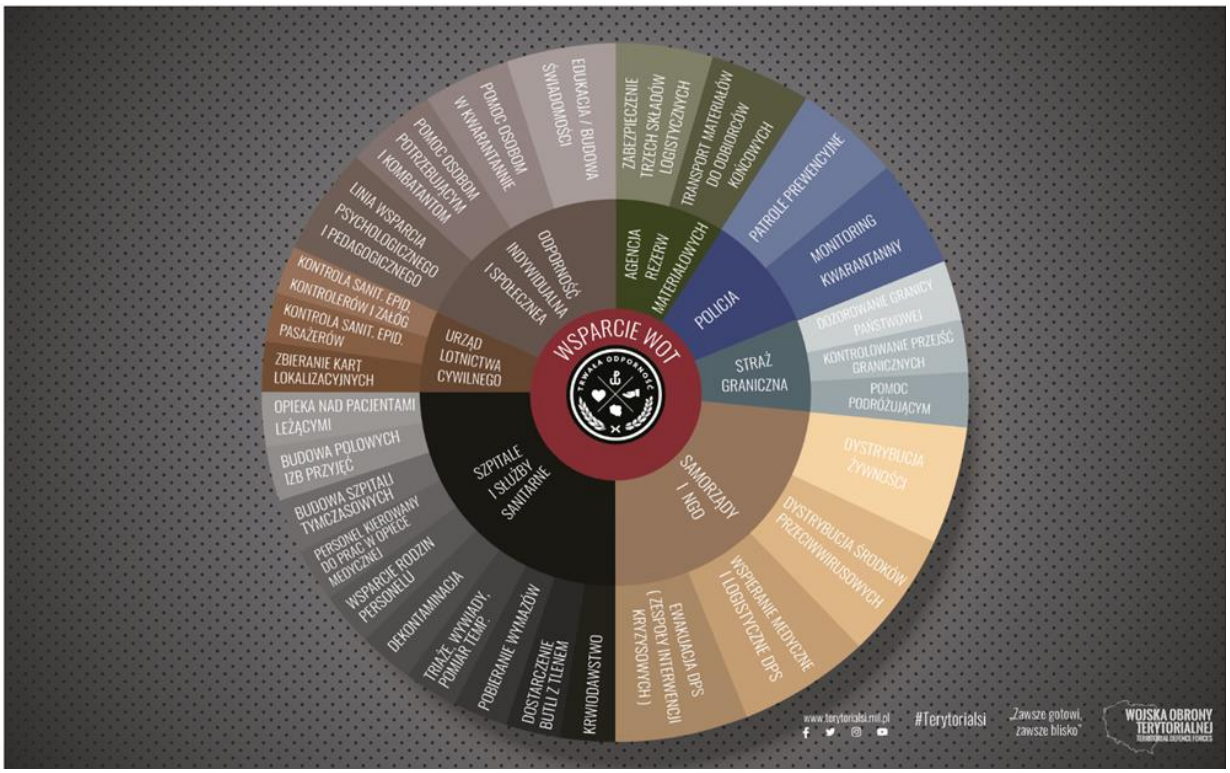
Wsparcie osób najstarszych stało się dla żołnierzy symbolicznym aktem obrony najsłabszych i najbardziej narażonych. Pośród nich są również weterani AK i powojennych organizacji niepodległościowych. W trakcie obu realizowanych operacji, pod opieką żołnierzy WOT znalazło się 9 185 kombatantów oraz 1 329 seniorów i innych osób na terenie całego kraju. Przełożyło się to na 15 364 działania faktycznego wsparcia, w tym 2 257 stanowiły zakupy żywności, leków, artykułów pierwszej potrzeby, natomiast 682 to pozostałe działania, jak np. zapewnienie transportu na wizyty lekarskie itp.

Ponadto, żołnierze WOT wspierają wszystkie z 21 Regionalnych Centrów Krwiodawstwa i Krwiolecznictwa w Polsce, ale też wiele powiatowych stacji krwiodawstwa, dokonując preselekcji dawców, transportując krew i jej składniki oraz wykonując triaże, pomiary temperatury, a także zajmując się wsparciem logistycznym. Od początku epidemii koronawirusa, WOT włącza się w akcje krwiodawstwa m.in. poprzez akcję „Krwioobieg Terytorialsa" (odnotowano imponującą liczbę oddanej krwi oraz jej składników, w ilości 5 351 litrów oraz 21,7 litrów osocza).

W ramach prowadzonych operacji, żołnierze Wojsk Obrony Terytorialnej wsparli dotychczas ok. 200 organizacji pozarządowych w zakresie transportu i logistyki, w tym transportu różnych środków pomocy z magazynów centralnych do lokalnych oraz ostatecznie do potrzebujących. Zrealizowano 585 transportów, co przełożyło się na ponad 3 510 ton przewiezionego asortymentu.

Zadania przedstawione powyżej nie wyczerpują całego spektrum zaangażowania WOT w przeciwdziałanie i zwalczanie pandemii COVID-19. Oprócz bezpośredniego wsparcia, Wojska Obrony Terytorialnej prowadziły działania informacyjno-edukacyjne oraz profilaktyczne organizując infolinie (wsparcie psychologiczne, wsparcie podmiotów organizujących wypoczynek dla dzieci i młodzieży, wsparcie ośrodków pomocy społecznej i organizacji pozarządowych, udzielających pomocy osobom starszym) czy szkolenia.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l



Zagrożenie pandemiczne pokazało, jak ważna jest współpraca Sił Zbrojnych z administracją państwową, organizacjami pozarządowymi oraz podmiotami środowiska cywilnego. W przypadku COVID-19, Siły Zbrojne RP pełniły rolę wspierającą, co niewątpliwie wpłynęło na skuteczność działania całego systemu w walce z zaistniałym kryzysem. Wojska Obrony Terytorialnej, poprzez udostępnienie potencjału osobowego oraz sprzętowego do wsparcia instytucji i służb cywilnych, istotnie przyczyniły się do zapobiegania i spowalniania transmisji wirusa SARS-CoV-2 oraz łagodzenia skutków pandemii.

SARS-CoV-2 – Sytuacja w Europie – przegląd restrykcji wprowadzonych w Republice Słowackiej, Republice Czeskiej oraz w Republice Federalnej Niemiec od września do grudnia 2020 r.

Paulina Nowicka
Główny Inspektorat Sanitarny

Pandemia COVID-19 trwa. Stopień, w jakim dotknęła różne kontynenty i państwa, różni się w zależności od wielu specyficznych dla danego państwa czynników – między innymi od tego, kiedy pojawił się na jego terenie pierwszy przypadek osoby zakażonej SARS-CoV-2, od systemu ochrony zdrowia i odpowiedzi rządu na sytuację zagrożenia. W celu spowolnienia rozprzestrzeniania się SARS-CoV-2 oraz ochrony życia i zdrowia ludzi na całym świecie, wprowadzono różnorodne ograniczenia.

W większości europejskich państw w lecie 2020 r. zaobserwowano spłaszczenie krzywej epidemii, jednak wskaźniki dotyczące zgłaszania nowych przypadków COVID-19 ponownie zaczęły wzrastać już od sierpnia 2020 r. Według oceny ryzyka Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) z 24 września 2020 roku, w niektórych krajach obserwowany wzrost korelował ze wzrostem liczby przeprowadzanych testów i intensywną transmisją wśród osób w wieku od 15 do 49 lat. W tych miejscach większość nowych przypadków dotyczyła osób, u których manifestacja objawów była łagodna lub byli oni bezobjawowi. Jednak w wielu innych krajach wzrost ten zbiegał się z wysoką lub rosnącą liczbą zakażeń SARS-CoV-2 u osób starszych, co wiązało się ze zwiększonym odsetkiem hospitalizowanych

i ciężkich przypadków COVID-19. Zaobserwowane podwyższone poziomy transmisji wskazują, że zastosowane niefarmaceutyczne interwencje nie przyniosły zamierzonego efektu, ponieważ przestrzeganie obostrzeń nie było wystarczające, aby zmniejszyć lub kontrolować narażenie na zakażenie SARS-CoV-2.[1]

REPUBLIKA SŁOWACKA

Po czterostopniowym okresie znoszenia obostrzeń, który zakończył się otwarciem instytucji kultury, restauracji, siłowni, galerii handlowych w Słowacji, od 1 października 2020 r. powrócił obowiązek noszenia masek również na zewnątrz, jeśli dystans od innej osoby wynosił mniej niż 2 metry. Imprezy masowe zostały ograniczone do 50 osób. Restauracje i bary zamykano przed godz. 22:00, a w centrach handlowych zaczęła obowiązywać zasada, iż na powierzchni 10 m^2 może znajdować się nie więcej niż 1 osoba. Uczelnie wyższe zostały zobligowane do prowadzenia nauki zdalnej. Od 15 października zakazano wszelkich imprez masowych i zgromadzeń, z wyłączeniem chrztów, pogrzebów i ślubów, podczas których należało stosować zasadę przebywania nie więcej niż 1 osoby na powierzchni 15 m^2. W październiku podjęto decyzję o próbie poddania testom w kierunku zakażenia SARS-CoV-2 wszystkich pełnoletnich osób w kraju. W dniach 31 października i 1 listopada badania zostały przeprowadzone w 5 000 punktów testowania. Poddanie się testom nie było obowiązkowe. Z 3 625 332 osób, które zgłosiły się do pobrania wymazu, u 38 359 potwierdzono zakażenie SARS-CoV-2 (1,06%). Najwięcej pozytywnych wyników w stosunku do osób przebadanych odnotowano w powiatach Czadca, Lubowla i Púchov.[2]

REPUBLIKA CZESKA

Obowiązek noszenia masek powrócił w Republice Czeskiej 1 września 2020 r. Należało stosować się do niego przemieszczając się transportem publicznym, przebywając wewnątrz budynków (takich jak galerie handlowe, biura, urzędy pocztowe). Nie obejmował osób przebywających w szkołach, które rozpoczęły funkcjonowanie w całym kraju. Każdy obywatel Republiki Czeskiej, który ukończył 60. rok życia, otrzymał za pośrednictwem poczty zestaw składający się z jednej maski FFP2 oraz pięciu masek twarzowych.[3]

25 września Ladislav Dušek, dyrektor Instytutu Informacji Medycznych i Statystyki[4] poinformował, że w ciągu dwóch pierwszych tygodni września prawie 400 nauczycieli zakaziło się SARS-CoV-2.[5] 5 października na terenie Czech wprowadzono stan wyjątkowy.[6] Zabroniono spotkań plenerowych, w których uczestniczyłoby powyżej 20 osób oraz spotkań w przestrzeniach zamkniętych, w których uczestniczyłoby powyżej 10 osób. Wydarzenia sportowe miały odbywać się bez udziału widzów, a wszelkie koncerty, przedstawienia teatralne, festiwale i próby zostały odwołane.

9 października zamknięto obiekty sportowe, włączając baseny i ośrodki spa, a także ogrody zoologiczne i kluby dziecięce. Wyłączono publiczne punkty WiFi. Trzy dni później wszystkie spotkania kulturalne, sportowe, socjalne czy religijne zostały odwołane, jeśli gromadziłyby łącznie powyżej 10 osób w przestrzeni zamkniętej lub powyżej 20 osób na zewnątrz. Udział w ślubach i pogrzebach oraz weselach i stypach został ograniczony do 30 osób. Fizyczna obecność studentów na terenie uczelni została zabroniona, z wyłączeniem zajęć praktycznych studentów kierunku lekarskiego, stomatologii, farmacji i innych kierunków medycznych. Od 14 października zabroniono zgromadzeń osób w liczbie przekraczającej 6. Restauracje rozpoczęły wydawanie posiłków wyłącznie na wynos, do godziny 20:00. Zakazano spożywania alkoholu w miejscach publicznych. Rząd zdecydował o przekazaniu 190 000 masek FFP2 oraz 1 mln masek twarzowych osobom niepełnosprawnym oraz zapewnił środki ochrony indywidualnej pracownikom placówek opiekuńczo-wychowawczych.

[1] Europejskie Centrum ds. Zapobiegania i Kontroli Chorób, Rapid Risk Assessment: Increased transmission of COVID-19 in the EU/EEA and the UK – twelfth update, 24.09.2020, https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-risk-assessment-increased-transmission-12th-update-september-2020.pdf [2.12.2020]

[2] More than 3.6 million people tested during the weekend, The Slovak Spectator, 2.11.2020, https://spectator.sme.sk/c/22525342/coronavirus-in-slovakia-nationwide-testing-final-results.html [5.12.2020]

[3] Measures adopted by the Czech Government against the coronavirus, Government of the Czech Republic, https://www.vlada.cz/en/media-centrum/aktualne/measures-adopted-by-the-czech-government-against-coronavirus-180545/#general [6.12.2020]

[4] Ústav zdravotnických informací a statistiky ČR, https://www.uzis.cz/ [5.12.2020]

[5] Almost 400 Czech teachers have caught COVID-19 since schools reopened, remix news, 25.09.2020, https://rmx.news/article/article/almost-400-czech-teachers-have-caught-covid-19-since-schools-reopened [5.12.2020]

[6] Important covid-19 measures for foreigners, Government of the Czech Republic, https://www.vlada.cz/en/media-centrum/aktualne/important-covid-19-measures-for-foreigners-183562/#State%20of%20emergency%2012%20December [6.12.2020]

21 października wprowadzono nakaz noszenia maski podczas podróży samochodem, jeśli osoby w nim przebywające nie mieszkają w jednym gospodarstwie domowym oraz na zewnątrz, w terenie zabudowanym, jeżeli niemożliwe jest utrzymanie 2-metrowego dystansu od innych osób. Kolejnego dnia zabroniono swobodnego przemieszczania się na terenie kraju z nielicznymi, określonymi wyjątkami oraz zamknięto sklepy, z wyłączeniem sklepów spożywczych, drogerii, stacji benzynowych, aptek, salonów z prasą, kwiaciarni. Całkowita nauka zdalna w szkołach zaczęła obowiązywać od 26 października. 28 października placówki lecznicze wstrzymały przyjęcia pacjentów na zabiegi planowe.

Od 4 listopada umożliwiono powrót do ćwiczeń i współzawodnictwa profesjonalnym sportowcom. Rozdysponowano 3 mln masek FFP2 dla rezydentów domów pomocy społecznej. Od 25 listopada umożliwiono powrót do nauki stacjonarnej uczniom ostatniej klasy gimnazjum, policealnych szkół zawodowych, a prowadzenia lekcji indywidualnych dozwolono w szkołach artystycznych i językowych. Ponadto, powróciły zajęcia praktyczne w uczelniach wyższych dla studentów ostatnich lat studiów. Od 30 listopada do szkół powrócili uczniowie klas 1-5 i 9, a pozostali zaczęli uczęszczać na zajęcia na zasadzie rotacji.

3 grudnia otwarto wszystkie sklepy i usługi, umożliwiono przeprowadzanie amatorskich zawodów sportowych bez udziału kibiców, zniesiono zakaz spożywania alkoholu w miejscach publicznych. W okresie 4-18 grudnia rozpoczęto przeprowadzanie testów antygenowych w kierunku COVID-19 wśród nauczycieli.[7]

REPUBLIKA FEDERALNA NIEMIEC

21 września minister zdrowia, Jens Spahn zapowiedział nową strategię testowania w kierunku SARS-CoV-2 i nowe zasady kwarantanny w okresie jesiennym i zimowym. Jej częścią miały stać się m.in. szybkie testy, ponieważ wzrosła ich jakość. 30 września, ze względu na utrzymującą się wysoką liczbę zakażeń SARS-CoV-2, rząd federalny i rządy krajów związkowych, bezpośrednio przed rozpoczęciem ferii jesiennych, ponownie zaostrzyły obostrzenia. Za podanie fałszywych danych osobowych w lokalach gastronomicznych wyznaczono grzywnę w wysokości co najmniej 50 euro. Wytyczne rządu dotyczące walki z rozprzestrzenianiem się SARS-CoV-2, zawarte w akronimie AHA, który oznaczał dystans, higienę i zakrywanie twarzy, zostały rozszerzone o „C" – aplikację ostrzegającą przed SARS-CoV-2 oraz „L" – wietrzenie pomieszczeń.[8]

Gwałtowny wzrost liczby nowych zakażeń SARS-CoV-2 doprowadził do wprowadzenia nowych obostrzeń 15 października. W miejscach dużych skupisk ludności, a także w przypadku przekroczenia liczby 35 nowych zakażeń na 100 000 mieszkańców w ciągu 7 dni, wprowadzono obowiązek noszenia masek ochronnych. W przypadku przekroczenia 50 nowych zakażeń na 100 000 mieszkańców w ciągu 7 dni wdrażano kolejne obostrzenia: udział w prywatnych uroczystościach ograniczony do maksymalnie 10 osób, będących członkami maksymalnie 2 gospodarstw domowych, wprowadzenie godziny policyjnej dla gastronomii (od godziny 23.00) oraz zamknięcie barów i klubów. 28 października rząd federalny i kraje związkowe uzgodniły nowe powszechne ograniczenia, m.in. zdecydowano o ponownym zamknięciu restauracji, obiektów rekreacyjnych, hoteli dla turystów oraz ograniczeniu kontaktów społecznych.[9] Zachęcano do pracy zdalnej i odwołania zbędnych podróży. Spotkania towarzyskie mogły gromadzić osoby z maksymalnie dwóch gospodarstw domowych w liczbie do 10 osób. Zamknięto kina, teatry, baseny, siłownie i sauny oraz zabroniono udziału publiczności w wydarzeniach sportowych.

18 listopada w Bundestagu przyjęto poprawki do ustawy o ochronie przed infekcjami. Wymieniono m.in. konkretne działania, które mogą zostać podjęte przez rządy krajów związkowych w celu zwalczania stanu zagrożenia zdrowia publicznego.[10] Od 1 grudnia ograniczono liczbę osób podczas spotkań towarzyskich do 5, nie licząc dzieci do 14 roku życia. Limit ten podniesiono do 10 osób w okresie od 21 grudnia 2020 r. do 1 stycznia 2021 r. Ferie dla dzieci w wieku szkolnym rozpoczęto 19 grudnia, aby

[7] Measures adopted by the Czech Government against the coronavirus, Government of the Czech Republic, https://www.vlada.cz/en/media-centrum/aktualne/measures-adopted-by-the-czech-government-against-coronavirus-180545/#general [6.12.2020]

[8] Connolly K., Germans embrace fresh air to ward off coronavirus, The Guardian, 30.09.2020, https://www.theguardian.com/world/2020/sep/30/germans-embrace-fresh-air-to-ward-off-coronavirus [6.12.2020]

[9] Coronavirus: Germany to impose one-month partial lockdown, Deutsche Welle, 28.10.2020, https://www.dw.com/en/coronavirus-germany-to-impose-one-month-partial-lockdown/a-55421241 [13.12.2020]

[10] Dlaczego regulacje covidowe potrzebują ustawy, Deutsche Welle, 19.12.2020, https://www.dw.com/pl/dlaczego-regulacje-covidowe-potrzebuj%C4%85-ustawy/a-55657444 [13.12.2020]

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

zmniejszyć ryzyko transmisji infekcji podczas spotkań bożonarodzeniowych.[11]

Rządy Niemiec, Czech i Słowacji nie były w swych działaniach odosobnione. Pod koniec października państwa Unii Europejskiej (UE), Europejskiego Obszaru Gospodarczego (EOG), a także Wielka Brytania (WB) zwiększyły skalę interwencji niefarmaceutycznych po ponownym pojawieniu się potwierdzonych przypadków COVID-19 i związanych z nimi hospitalizacji i zgonów.

Według oceny ryzyka ECDC z 4 grudnia 2020 r., po miesiącach ciągłego wzrostu najnowsze dane epidemiologiczne wskazały, że liczba nowych przypadków zaczęła spadać w państwach UE, EOG i WB. Jednak krajowe dane na temat zapadalności wykazują zmienne tendencje w poszczególnych państwach, a wskaźniki transmisji pozostają wysokie w większości państw Europy.

Wysokie poziomy transmisji stanowią zagrożenie dla wydolności systemów opieki zdrowotnej, ze względu na wzrost zapotrzebowania na opiekę zdrowotną oraz ryzyko choroby, izolacji lub kwarantanny u większej liczby pracowników ochrony zdrowia. W wielu krajach wskaźniki wykorzystania łóżek i oddziałów intensywnej opieki medycznej nadal rosną lub pozostają wysokie, a dalszy wzrost może stanowić wyzwanie systemów ochrony zdrowia.

Jednocześnie, państwa europejskie zgłaszają występowanie zjawiska zdefiniowanego przez WHO jako „pandemiczne zmęczenie", czyli pozbawienie motywacji do stosowania zalecanych środków ochronnych[12]. Zmęczenie pandemiczne niesie ze sobą ryzyko wystąpienia większej liczby nowych zakażeń, zwiększonych obciążeń dla systemów ochrony zdrowia, intensywniejszego wpływu na gospodarkę i społeczeństwo oraz prawdopodobieństwo, że w najbliższej przyszłości wystąpi konieczność wprowadzenia bardziej rygorystycznych środków kontroli dalszego rozprzestrzeniania się SARS-CoV-2.

Tabela 1. Dane dotyczące COVID-19 z państw UE/EOG i WB (COVID-19 situation update for the EU/EEA and the UK, as of 13 December 2020), 13.12.2020, https://www.ecdc.europa.eu/en/cases-2019-ncov-eueea [13.12.2020]

Państwa UE/EOG i Wielka Brytania	Liczba przypadków	Liczba zgonów	14-dniowa skumulowana zapadalność na 100 000 ludności
Francja	2 365 319	57 761	233.7
Wielka Brytania	1 830 956	64 026	338.8
Włochy	1 825 775	64 036	432.8
Hiszpania	1 730 575	47 624	218.1
Niemcy	1 320 716	21 787	334.9
Polska	1 126 700	22 676	403.2
Belgia	603 023	17 792	233.6
Holandia	602 878	10 005	521.8
Czechy	579 079	9 535	567.4
Rumunia	551 900	13 264	442.5
Portugalia	344 700	5 461	525.4
Szwecja	320 098	7 514	738.8
Austria	317 031	4 355	482.6
Węgry	280 400	6 965	704.7
Bułgaria	178 952	5 626	531.5
Chorwacja	172 523	2 562	1 197.9
Słowacja	127 087	1 122	412.0
Grecja	123 842	3 540	194.0
Dania	107 116	935	495.4
Słowenia	95 481	1 448	1 019.6
Litwa	93 101	815	1 177.7
Irlandia	75 756	2 123	77.8
Luksemburg	40 755	392	1 196.6
Norwegia	40 022	387	99.0
Finlandia	30 450	453	111.3
Łotwa	25 046	324	441.9
Estonia	17 713	148	454.0
Cypr	14 800	77	521.6
Malta	11 101	166	302.3
Islandia	5 552	28	50.7
Liechtenstein	1 502	18	596.7

[11] Deutschland verschärft Corona-Regeln, Detsche Welle, 25.11.2020, https://www.dw.com/de/deutschland-versch%C3%A4rft-corona-regeln/a-55724971 [13.12.2020]

[12] Światowa Organizacja Zdrowia, Regional Office for Europe, Pandemic fatigue – Reinvigorating the public to prevent COVID-19, 20 October 2020, https://www.who.int/news-room/feature-stories/detail/who-europe-discusses-how-to-deal-with-pandemic-fatigue [5.12.2020]

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Społeczeństwo odporne na zagrożenia

Robert Rey
Rządowe Centrum Bezpieczeństwa

Odporność, czyli utrzymanie i rozwijanie takich zdolności w sferze cywilnej i wojskowej, które znacząco utrudnią nieprzyjazne działania, uchodzi za jeden z podstawowych warunków bezpieczeństwa zarówno w wymiarze krajowym jak i unijnym oraz sojuszniczym. Budowa odporności stanowi odpowiedź na różnorodne zagrożenia regionalne, w tym o charakterze hybrydowym, a coraz częściej również globalne. Wzmacnianie odporności jest obowiązkiem i zadaniem każdego państwa, a także staje się kluczowym aspektem bezpieczeństwa UE i NATO. O ile jednak już od dłuższego czasu koncentrowano się na umacnianiu odporności w odniesieniu do potencjału państw i umiejętności zarządzania ich zasobami, o tyle od niedawna – częściowo pod wpływem pandemii – dostrzega się również potrzebę budowy odpornego społeczeństwa, obywateli odpornych na zagrożenia różnego typu. Jak zatem spowodować, by społeczeństwo, często nawet nieświadome zagrożeń, stało się na nie odporne?

W wymiarze krajowym odniesienia do odporności znalazły się już w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej zatwierdzonej 12 maja 2020 r.[1], co wskazuje, iż kwestia budowy odporności stała się bardzo ważna w kontekście utrwalania naszego bezpieczeństwa. Już we wstępie do SBN, w opisie środowiska bezpieczeństwa, znajdują się nawiązania do potrzeby zwiększania odporności państwa i społeczeństwa. Zostały one rozwinięte w rozdziale pt. Odporność państwa i obrona powszechna. Ponadto, pewne elementy związane z odpornością zawierają Krajowy Plan Zarządzania Kryzysowego[2] oraz Narodowy Program Ochrony Infrastruktury Krytycznej[3].

W ramach Unii Europejskiej toczą się prace zmierzające do skoordynowania działań państw członkowskich na rzecz odporności państw i społeczeństw wobec zagrożeń hybrydowych, cybernetycznych oraz mogących zakłócić infrastrukturę krytyczną. Trwa proces przyjmowania Konkluzji Rady Europejskiej w zakresie wzmacniania odporności i zwalczania zagrożeń hybrydowych w kontekście kryzysu związanego z COVID-19. Są w nich uwzględniane kwestie związane z „societal resilience". Unia dostrzega ponadto potrzebę budowania odporności poza granicami państw członkowskich – w myśl zasady, że im bardziej odporni sąsiedzi, tym bezpieczniejsza Unia. UE współpracuje także z NATO, co ma ogromne znaczenie dla podniesienia poziomu bezpieczeństwa na naszym kontynencie. Zostało to dodatkowo potwierdzone i wzmocnione w lipcu 2018 r. poprzez podpisanie nowej wspólnej deklaracji (*Joint Declaration on EU-NATO Cooperation*) o współpracy w przeciwdziałaniu zagrożeniom w zakresie bezpieczeństwa[4].

Podkreślić należy, że instytucją międzynarodową odgrywającą w budowie i wzmacnianiu odporności rolę pierwszorzędną jest Organizacja Traktatu Północnoatlantyckiego. Jedną z konkluzji szczytu NATO w Warszawie z 8-9 lipca 2016 r. było podjęcie przez szefów państw i rządów krajów członkowskich decyzji o przyjęciu wspólnego zobowiązania do wzmacniania odporności (*resilience*) oraz nieustannego rozwijania indywidualnej i zbiorowej zdolności do odparcia ewentualnego ataku na Sojusz (zgodnie z art. 3 Traktatu Waszyngtońskiego). W rozumieniu Sojuszu, odporność jest bardzo ważnym elementem polityki odstraszania, która ma zmusić ewentualnego przeciwnika do zaniechania ataku poprzez przekonanie go, że atak nie umożliwi mu osiągnięcia zamierzonych celów, bądź będzie dla niego zbyt kosztowny.

Wzmacnianie odporności winno się odbywać zgodnie z wytycznymi ujętymi w postaci siedmiu bazowych wymogów. Pomagają one państwom członkowskim NATO we wspólnym zrozumieniu założeń przyświecających wzmacnianiu odporności, a wśród nich efektywnego wsparcia dla sił zbrojnych na europejskim teatrze działań, przyczynieniu się do odstraszania, ale zarazem do sprawnego funkcjonowania państwa w kryzysie i ochronie ludności. Tak pojęta budowa odporności zakłada współdziałanie układu militarnego i pozamilitarnego

[1] https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf

[2] https://rcb.gov.pl/krajowy-plan-zarzadzania-kryzysowego/

[3] https://rcb.gov.pl/narodowy-program-ochrony-infrastruktury-krytycznej-2/

[4] https://www.nato.int/cps/en/natohq/official_texts_156626.htm

począwszy od fazy planowania.[5] Siedem wytycznych odnosi się do:

- ciągłości działania administracji publicznej i zapewnienia kluczowych procesów państwa,
- zaopatrzenia w energię,
- zdolności do reagowania na masowe niekontrolowane migracje,
- zaopatrzenia w wodę i żywność,
- zdolności do reagowania na zdarzenia z dużą liczbą ofiar,
- zapewnienia łączności,
- transportu cywilnego.

Wraz z rozwojem prac nad odpornością uświadamiano sobie coraz wyraźniej, że należy uwzględniać w nich trzy domeny, by uzyskać pełną synergię w działaniach.

Pierwszą jest sektor publiczny, w tym współdziałanie cywilno-wojskowe, co zaowocowało tzw. kompleksowym podejściem ze strony rządowej (cywilnym i wojskowym) (*whole of government approach*) do kwestii wzmacniania bezpieczeństwa. Współpraca i założenia te nie skończyły się jedynie na deklaracjach, ale znalazły swoje odbicie w realnych działaniach podczas tworzenia dokumentów, polityk, dokonywania wspólnych ocen czy przeprowadzania ćwiczeń tak wojskowych, jak i cywilnych na poziomie międzynarodowym i krajowym. Można pokusić się o ocenę, że współpraca cywilno-wojskowa, mimo że jest zadaniem ciągłym, wymagającym stałego monitorowania i udoskonalania, znacząco się poprawiła, a wytyczne dotyczące odporności pomagają w jej rozwoju i wspólnym rozumieniu potrzeb i wymagań każdej ze sfer.

Drugą domeną jest partnerstwo publiczno-prywatne (*public-private cooperation*). Sojusz w większości swoich działań i operacji uzależniony jest od zasobów cywilnych. Ocenia się, że nawet 90 procent zadań związanych z logistyką i zaopatrzeniem sił zbrojnych jest realizowanych przez sektor prywatny. Kompleksowe podejście umożliwia więc przyjęcie odpowiednich regulacji prawnych, w tym umów z podmiotami prywatnymi, pozwalających na utrzymanie zdolności cywilnych oraz zwiększenia możliwości wsparcia sił zbrojnych (krajowych oraz sojuszniczych)[6].

Trzecią domeną składającą się na skuteczną odporność jest społeczeństwo, a dokładniej jego świadomość potencjalnych zagrożeń, umiejętność adekwatnej reakcji, zaangażowana postawa w przeciwdziałaniu niebezpiecznym zjawiskom czy tendencjom. Budowa odporności w oparciu o wszystkie trzy domeny, czyli z udziałem sektora publicznego, prywatnego i społeczeństwa powoduje, że kraj wykazuje mniej słabości i podatności, które mogą być wykorzystane przez potencjalnego przeciwnika lub stać się celem jego ataku. NATO już pod koniec 2017 r. podjęło pierwsze prace nad możliwością włączenia społeczeństwa w budowę odporności, gdyż to właśnie ono jest często głównym celem ataków, w tym w szczególności hybrydowych. Z tego właśnie względu, strona polska, która nierzadko jest konfrontowana z zagrożeniami hybrydowymi, wystąpiła z inicjatywą intensyfikacji tych prac. Spotkało się to z poparciem większości Sojuszników. Trzeba przy tym zdawać sobie sprawę, iż kwestia uzyskania odporności społecznej nie jest prosta ze względu na różne tradycje, na zróżnicowane rozumienie problematyki w państwach członkowskich i wiele innych aspektów.

Należy sobie zadać przede wszystkim pytanie, na jakie kryzysy i na jakie zagrożenia/wrogie działania społeczeństwo powinno być odporne. Do głównych wyzwań trzeba zaliczyć nie tylko wrogie działania dezinformacyjne podmiotów państwowych i niepaństwowych, wymierzone w obce społeczeństwa, dla osiągnięcia własnych celów politycznych, gospodarczych czy kulturowych. Należy do nich włączyć ciągle ewoluujące zagrożenia hybrydowe, łącznie z działaniami poniżej progu wojny, które – groźne same w sobie – mogą skutkować np. brakiem dostępu do wody, żywności czy usług publicznych, a w następstwie np. paniką i nadwyrężeniem zaufania do władz.

Pandemia koronawirusa ukazała, jak bardzo nasze codzienne życie zależy też od globalnych zagrożeń, w tym np. poziomu świadczonych usług, kanałów zaopatrzenia czy finansów. Pewne zasoby, towary czy usługi, które wydają się dostępne stale i „od ręki" mogą stać się szybko towarem deficytowym. Wpływa to, nie

[5] https://www.nato.int/cps/en/natohq/topics_132722.htm

[6] Ponadto w NATO istnieje możliwość udziału ekspertów krajowych w pracach sojuszniczych w ramach poszczególnych grup planistycznych podległych Komitetowi Planowania Cywilnego NATO. Daje to możliwość, na poziomie cywilnym, zaangażowania w prace na rzecz odporności. Grupy te zajmują się kwestiami ochrony ludności, zdrowia, żywności, energii, komunikacji oraz transportu https://www.nato.int/cps/en/natohq/topics_50093.htm
Także RCB stara się przekazywać jak najwięcej informacji w tym temacie zarówno podmiotom publicznym jak i prywatnym, co ma swoje odbicie w organizowanych seminariach jak np: Gotowość cywilna a wsparcie operacji wojskowej — rola przedsiębiorstw w przygotowaniach obronnych https://rcb.gov.pl/gotowosc-cywilna-a-wsparcie-operacji-wojskowej-rola-przedsiebiorstw-w-przygotowaniach-obronnych .

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

tylko na potrzeby społeczeństwa, ale i na sprawne działanie gospodarki (kwestia dywersyfikacji dostaw dotyczy nie tylko gotowych produktów, lecz także materiałów i półproduktów do ich wytworzenia). Nie wolno przy tym zapomnieć o stale towarzyszących nam zagrożeniach: klęskach żywiołowych czy katastrofach. Wszystkie tego typu zdarzenia względnie zjawiska mogą mieć negatywny wpływ na dane społeczeństwo i państwo, w tym na ich zdolność do wsparcia narodowych i sojuszniczych sił zbrojnych.

Najważniejszym elementem, na który zwraca się uwagę podczas dyskusji w NATO, jest komunikacja ze społeczeństwem. Winna ona opierać się na zaufaniu pomiędzy władzą a obywatelem oraz zakładać jasne przedstawianie potencjalnej lub rzeczywistej sytuacji zagrożenia hybrydowego. W wypadku realnego zagrożenia, komunikacja ze społeczeństwem musi się opierać na prawdziwym, wiarygodnym, zrozumiałym przekazie. Niewłaściwa komunikacja czy niezrozumiała reakcja decydentów, może doprowadzić nawet do zaprzepaszczenia wspólnego wysiłku.

Drugim ważnym wyzwaniem jest edukacja, umożliwiająca nie tylko zrozumienie istoty niebezpiecznego zdarzenia/zjawiska i niejako oswajająca z nim, lecz dostarczająca wiedzy, jak zminimalizować ryzyko zagrożenia bądź jak sobie radzić w wypadku jego wystąpienia.

Kolejnym tematem prac sojuszniczych jest samoorganizacja obywateli. Zalety takiego działania najczęściej widać podczas przeciwdziałania skutkom gwałtownych zdarzeń naturalnych, wypadków czy katastrof. Co istotne, w dobie mediów społecznościowych mobilizacja społeczeństwa w tego typu sytuacjach może zostać zwiększona.

Wypracowanie koncepcji budowy odpornego społeczeństwa wydaje się szczególnie istotne wobec trudnych do przewidzenia i różnorodnych zagrożeń. Zadanie to zostało powierzone jednej z grup roboczych podporządkowanych Komitetowi Planowania Cywilnego NATO (CEPC), a mianowicie Grupie Ochrony Ludności (CPG). Jest szansa, aby „odporne społeczeństwo" stało się żywotnym elementem w polityce bezpieczeństwa europejskiego. Istotna rola może tu przypaść Polsce, państwu położonemu na wschodniej flance NATO. Budowanie odporności w każdym aspekcie to zadanie, które wymaga spójnych działań narodowych i międzynarodowych w wymienionych powyżej domenach, uwzględniając interakcje pomiędzy nimi, współzależności pomiędzy różnymi sektorami życia publicznego, w tym środowisk zajmujących się edukacją i szkolnictwem różnego szczebla, a także organizacji pozarządowych.

Wzmocnienie odporności infrastruktury krytycznej na zagrożenia o charakterze terrorystycznym

Aleksandra Gasztold
Uniwersytet Warszawski

Wyzwania dla bezpieczeństwa bez systemowego wysiłku ich racjonalizacji stają się zagrożeniami. Z perspektywy klasycznego ujmowania bezpieczeństwa, którego podmiotem i dysponentem jest państwo, minimalizacja negatywnego oddziaływania sytuacji niebezpiecznej na otoczenie winna być priorytetem architektury zarządzania w danym sektorze. Koniecznym wymogiem jest precyzyjne określenie elementów składowych systemu, instytucji zaangażowanych w ochronę i przeciwdziałanie zagrożeniom oraz ich kompetencji.

Fundamentem każdego systemu antyterrorystycznego, ochrony państwa, obiektu, osób, urządzeń jest pakiet prawny wraz z mechanizmami jego ciągłej ewaluacji i aktualizacji – tak, aby nadążał on za nieustanną ewolucją charakteru zagrożenia. Dlatego tak ważna jest penalizacja i kryminalizacja przestępstw składających się na poszczególne etapy aktywności terrorystycznej, a nie samo definiowanie tego pojęcia. Brak zgodności co do akceptowanej powszechnie definicji terroryzmu na arenie międzynarodowej i wielość prób wyjaśniania tego pojęcia przez środowisko naukowe nie są przeszkodą w zwalczaniu samego zjawiska.

Zwalczanie terroryzmu należy rozumieć jako zespół czynności oraz środków ochronnych i prewencyjnych, których zadaniem jest zmniejszenie wrażliwości i podatności danego podmiotu na ataki terrorystyczne. Zadania te realizowane są głównie poprzez środki bezpieczeństwa fizycznego (osobowe i techniczne), analizę informacji o zagrożeniu, prowadzenie działań

operacyjno-rozpoznawczych oraz podnoszenie świadomości społecznej w zakresie reagowania. Na użytek podmiotów zajmujących się przeciwdziałaniem, wystarczające są definicje administracyjne charakteryzujące dane zjawisko – w tym umyślność, zamiar bezpośredni o szczególnym zabarwieniu (*dolus directus coloratus*). W Polsce definicja taka została wprowadzona w 2004 r. w art. 115 § 20 Kodeksu karnego. Na dorobek prawa karnego w zakresie przeciwdziałania terroryzmowi niewątpliwie miały wpływ tzw. konwencje antyterrorystyczne Organizacji Narodów Zjednoczonych, konwencje Rady Europy oraz Decyzja Ramowa Rady Unii Europejskiej z 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (2002/475/WSiSW) oraz ją zmieniająca Decyzja Ramowa Rady z 28 listopada 2008 r. (2008/919/WSiSW). Również w ustawie z 10 czerwca 2016 r. o działaniach antyterrorystycznych (*Dz. .U. 2016 poz. 904*.) zareagowano na zmieniającą się naturę współczesnego terroryzmu (w szczególności na zjawisko zagranicznych bojowników – FF) poprzez wprowadzenie do kodeksu karnego artykułów 255a § 2 i 259a. Katalog czynów zabronionych, które mogą mieć znamiona przestępstwa umyślnego i kierunkowego o szczególnym zabarwieniu, mających charakter terrorystyczny, nie jest katalogiem zamkniętym i wymaga ciągłych aktualizacji prawno-karnych. Uwarunkowania prawne kształtują też mechanizmy współpracy międzynarodowej w zakresie przeciwdziałania terroryzmowi, na każdym etapie terrorystycznej aktywności, od radykalizacji, rekrutacji, propagowania, finasowania, szkolenia, wparcia logistycznego, po planowanie i przeprowadzenie finalnego ataku na wytypowany cel.

Infrastruktura Krytyczna (IK) obejmująca elementy takie jak obiekty fizyczne, systemy zaopatrzenia, sieci informatyczne i technologie informacyjne, znajduje się w polu zainteresowania współczesnych terrorystów. IK jest atrakcyjnym celem bezpośrednich ataków terrorystycznych ze względu na zakładany efekt psychologiczny, społeczny, ekonomiczny oraz polityczny – zakłócenie funkcjonowania, uszkodzenie lub zniszczenie obiektów lub systemów, kluczowych dla sprawnego działania całego państwa. Dlatego też, budowanie odporności i ochrona infrastruktury krytycznej (OIK) są dziś jednymi z największych wyzwań dla bezpieczeństwa państwa i jego obywateli[1].

Istotne jest wdrażanie nowych metod i środków mających na celu rozpoznanie potencjalnych zagrożeń, redukcja ich oddziaływania oraz rozpoznanie podatności na zagrożenia poszczególnych elementów systemu. Szczególne znaczenie ma w tym kontekście ocena ryzyka i standaryzacja analizy zagrożeń. Popularne metody stosowane do np. obiektów fizycznych to CARVER, CARVER+Shock, SVA, macierz zagrożeń[2]. Ważne dla zrozumienia jakiegokolwiek przedsięwzięcia terrorystycznego jest rozpoznanie możliwości działania terrorystów w konkretnej strukturze w danym obszarze geograficznym. Możliwości te sprowadzić można do czterech filarów[3]:

1) **cel bezpośredni ataku** – wybierany precyzyjnie przez zamachowca/zamachowców ze względu na wyróżniające cechy, np.: dostęp do obiektu, jego znaczenie dla określonej społeczności lub władzy (symbolika + rozpoznawalność = rozgłos), charakteru fizycznych zabezpieczeń, potencjalnej liczby ofiar przypadkowych itp.
2) **rodzaj broni** – wybór uwarunkowany jest: dostępem do określonej kategorii broni oraz umiejętnością jej użycia. Dodatkowo, jest podporządkowany celowi i zamierzonemu oddziaływaniu;
3) **narzędzia** – takie jak samochody, środki finansowe (przelewy pieniężne, karty kredytowe, gotówka), telefony komórkowe itp. Ułatwiają one przenikanie do struktur społecznych lub funkcjonowanie w nich oraz rozpoznanie miejsca i celu ataku; niewykluczona jest współpraca z otoczeniem zewnętrznym organizacji terrorystycznej (rosnący casus tzw. insiderów) czy środowiskiem przestępczym działającym w danym regionie (np. dostęp do fałszywych dokumentów, schronienie, planów ochrony celu);
4) **sprzyjające warunki** – m.in liberalne prawo dostępu do broni palnej w danym państwie, brak kontroli granicznych, nieszczelność systemu bankowego, wykorzystanie sytuacji kryzysowej (pandemia, katastrofy naturalne), konflikt w państwie granicznym, słabość organów ścigania, przewlekłość procedury karnej, postępująca polaryzacja społeczna itp.

[1] Zob. szerzej: Infrastruktura krytyczna – Rządowe Centrum Bezpieczeństwa (rcb.gov.pl) (14.12.2020 r.)

[2] Zob. szerzej M. Kupniewski, *Metody i kryteria oceny stopnia zagrożenia atakiem terrorystycznym*, „Przegląd Policyjny" 2018, nr 4 (132), s. 94-107.

[3] R.V.G. Clarke, G.R. Newman, *Outsmarting Terrorist*, Praeger Security International, Westport-London: 2006 s. 9.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Zamach terrorystyczny dokonywany jest tam, gdzie istnieją sprzyjające okoliczności. Związany jest z umiejętnością przenikania do środowiska społecznego i dotarcia do nowych technologii w celu przejęcia fizycznych systemów, zasobów i usług, które wspierają to społeczeństwo w codziennym funkcjonowaniu.

Ocena ryzyka zagrożenia o charakterze terrorystycznym dla obszarów, obiektów i urządzeń podlegających ochronie tworzona jest w oparciu o katalog incydentów zawarty w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 22 lipca 2016 r. (Dz. U. z 2016 r. poz. 1092). Szacowanie jednak poziomu zagrożenia terrorystycznego dla ochranianego obiektu, obszaru i urządzenia marginalizuje system zarządzania wiedzą w elementach infrastruktury krytycznej. **Odporność nie jest stałym elementem systemu. Umiejętność reagowania w czasie rzeczywistym na zmienną naturę zagrożeń zakłada elastyczne podejście do oceny ryzyka**. Ochrona IK w Polsce skupia się na krytycznych lukach (podatności), a nie na niezbędnych wymaganiach – czyli podstawowych warunkach wzmacniających odporność, środkach i zasobach (w tym zasobach ludzkich). Stałą bolączką systemową jest: odrzucanie mało prawdopodobnych scenariuszy, brak standaryzacji i certyfikacji szkoleń z zakresu bezpieczeństwa i ochrony oraz poszukiwanie oszczędności przez operatorów IK w sferze bezpieczeństwa fizycznego obiektów. Warto też zaznaczyć, że akty terroryzmu mogą być wykorzystane w strategii wojny hybrydowej. Pytaniem otwartym pozostaje, na ile polski system antyterrorystyczny może być wykorzystany w walce z zagrożeniami o naturze hybrydowej[4].

Nieoszacowaną rolę w wypracowywaniu standardów i dobrych praktyk w zakresie ochrony IK przed terroryzmem odgrywa debata w strukturach Unii Europejskiej. 9 grudnia 2020 r. Komisja Europejska zaprezentowała nową **Agendę Antyterrorystyczną**. Program walki z terroryzmem ma na celu wspieranie państw członkowskich w lepszym przewidywaniu, zapobieganiu, ochronie i reagowaniu na zagrożenie terrorystyczne. Wśród priorytetów wymieniono budowę odporności na ataki terrorystyczne infrastruktury krytycznej, m.in. węzłów transportowych, elektrowni i szpitali. Rozważane jest również wzmocnienie ochrony lotnictwa, w tym wprowadzenie europejskich ram prawnych do rozmieszczania funkcjonariuszy ochrony w czasie lotów, poprzez inicjatywę wprowadzoną w UE po zamachach z 11 września 2001 r., tzw. *sky marshals*.

W celu inwestowania w odporność IK Komisja Europejska, opierając się na doświadczeniu zespołu doradców UE ds. Bezpieczeństwa w zakresie ochrony (***EU Protective Security Advisors – PSE***), ustanowi misje eksperckie wspierające państwa członkowskie w przeprowadzaniu ocen ryzyka. Komisja zobowiązała się również do wzmocnienia odporności miast europejskich, jako głównych atraktorów (celów bezpośrednich) ataków terrorystycznych. Zostaną poszerzone sztandarowe cele projektu funkcjonującego w tym zakresie PACTESUR *(Protecting Allied Cities against TErrorism by Securing Urban aReas – Ochrona miast stowarzyszonych przed terroryzmem poprzez zapewnienie bezpieczeństwa obszarów miejskich)*[5].

Badania nad bezpieczeństwem prowadzone w poszczególnych krajach wesprą wczesne wykrywanie nowych zagrożeń, a inwestowanie w nowe technologie wzmocni konkurencyjność Europy w walce z terroryzmem. Inwestowanie w odporność to też walka z radykalizacją, co jest wyraźnie podkreślane w unijnej polityce antyterrorystycznej. Aby upowszechniać wiedzę i doświadczenie w zakresie zapobiegania radykalizacji postaw i zachowań, Komisja zaproponowała utworzenie centrum wiedzy UE (***EU Knowledge Hub***) skupiającego decydentów, praktyków i badaczy[6]. Ponadto, KE ma wypracować instrumenty wsparcia finansowego w ramach systemu grantowego z Funduszu Bezpieczeństwa Wewnętrznego.

Ochrona IK została umieszczona wśród najważniejszych zadań przewidzianych przez Komisję Europejską na najbliższe lata. **16 grudnia 2020 r. KE** zaproponowała dwie **dyrektywy promujące systemowe podejście do ochrony IK** i przeciwdziałania współczesnym zagrożeniom. Pierwsza **w sprawie zwiększenia odporności usług kluczowych** – tzw. dyrektywa CER rozszerzająca dyrektywę w sprawie europejskiej infrastruktury

[4] A. Gasztold & P. Gasztold, *The Polish Counterterrorism System and Hybrid Warfare Threats*, „Terrorism and Political Violence" 2020, online: The Polish Counterterrorism System and Hybrid Warfare Threats (tandfonline.com) (13.12.2020).

[5] Strona internetowa projektu: https://www.pactesur.eu/

[6] *Security Union: A Counter-Terrorism Agenda and stronger Europol to boost the EU's resilience Brussels*, 9 December 2020, online: A Counter-Terrorism Agenda (europa.eu) (13.12.2020).

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

krytycznej (ECI) z 2008 r.[7] Druga natomiast jest odpowiedzią na rosnące zagrożenia cybernetyczne i dotyczy środków **na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii tzw. dyrektywa NIS2.[8] Wszystkie krytyczne podmioty zidentyfikowane na mocy dyrektywy w sprawie odporności podmiotów krytycznych podlegałyby zobowiązaniom w zakresie cyberodporności w ramach NIS2.**

Te nowe impulsy określają wyraźnie kierunki ochrony infrastruktury krytycznej, również w Polsce. W latach 2021-2024 należy się spodziewać dynamicznego wzrostu ilości obiektów posiadających status IK oraz wzmożonego zapotrzebowania na budowanie ich odporności. Wieloaspektowa współpraca i realne zaangażowanie administracji publicznej, biznesu, środowiska akademickiego oraz edukacja antyterrorystyczna obywateli (tu duża odpowiedzialność Centrum Prewencji Terrorystycznej ABW) są kluczem do systemowej oraz efektywnej ochrony dóbr i usług, do których przywykliśmy.

Eksperckie Centrum Szkolenia Cyberbezpieczeństwa, jako odpowiedź MON na współczesne zagrożenia

Aleksandra Paulska
Eksperckie Centrum Szkolenia Cyberbezpieczeństwa

ARPANET, czyli pierwsza sieć rozległa i bezpośredni przodek współczesnego internetu został uruchomiony w 1968 r. w celu wymiany informacji między rządem, instytucjami badawczymi i naukowymi. Jego twórcy nie zakładali, że środowisko stworzone jako alternatywa dla tradycyjnej infrastruktury telekomunikacyjnej, która mogła zostać zniszczona przez potencjalnych agresorów, sama może stać się z czasem miejscem, które będzie tworzyć zagrożenie dla osób indywidualnych, firm i podmiotów państwowych, dając możliwość realizacji działań o charakterze chuligańskim, przestępczym, terrorystycznym, a nawet zostać wykorzystane jako istotny element współczesnych wojen hybrydowych.

Świadomość szans, ale także krytycznych zagrożeń związanych z istnieniem internetu, została podniesiona do rangi jednego z wiodących tematów na szczycie NATO w Warszawie w 2016 r., podczas którego cyberprzestrzeń została uznana za kolejną – po morzu, lądzie i powietrzu – domenę operacyjną[1] ze wszystkimi konsekwencjami płynącymi z tej decyzji oraz zobowiązaniami nałożonymi na państwa sojusznicze. Realizując te zobowiązania polskie Ministerstwo Obrony Narodowej podjęło szereg działań natury politycznej i legislacyjnej, wśród których jest wzmocnienie potencjału Sił Zbrojnych RP do działań w cyberprzestrzeni poprzez edukację w tym obszarze zarówno żołnierzy, jak i pracowników cywilnych resortu obrony narodowej. Zwieńczeniem tych wysiłków jest oficjalne otwarcie 18 listopada 2020 r. Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa (dalej: ECSC).

SKUTECZNOŚĆ W CYBERPRZESTRZENI – DZIAŁANIE METODĄ DUŻYCH KROKÓW

Obecnie w resorcie ON rozwijane są struktury odpowiedzialne za realizację zadań w obszarze cyberbezpieczeństwa. Rozbudowa dokonuje się poprzez formowanie nowych, dedykowanych jednostek organizacyjnych oraz rozwijanie i konsolidację struktur istniejących. Przekłada się to na tworzenie nowych stanowisk, a tym samym na zwiększone zapotrzebowanie na odpowiednio wykwalifikowanych specjalistów. Stały, systematyczny rozwój kadr, inwestowanie w podnoszenie kwalifikacji zarówno żołnierzy jak i pracowników cywilnych staje się w tej sytuacji koniecznością. Doskonalenie zawodowe umożliwia bowiem budowanie kompetencji personelu i pozwala przygotować osoby przeszkolone do podejmowania coraz bardziej wymagających działań, zaś – w dłuższej perspektywie czasowej – powinno zapewnić zwiększenie liczebności zasobu kadrowego resortu ON zdolnego do realizacji zadań w obszarze cyberbezpieczeństwa w pełnym spektrum.

[7] Wniosek dt. dyrektywy CER, online: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (16.12.2020).

[8] Wniosek dt. dyrektywy NIS 2, online https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union (16.12.2020).

[1] Od 2019 r. jest nią także przestrzeń kosmiczna.

Jednym ze sztandarowych rozwiązań jest zainaugurowany w lutym 2019 r. kompleksowy program CYBER.MIL.PL oparty na czterech filarach:

1. konsolidacja i budowa struktur cyberbezpieczeństwa obejmująca m.in. utworzenie Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC), powołanie Pełnomocnika Ministra Obrony Narodowej ds. Utworzenia Wojsk Obrony Cyberprzestrzeni itp.;
2. edukacja, szkolenia i treningi;
3. współpraca i budowanie silnej pozycji międzynarodowej;
4. podniesienie poziomu bezpieczeństwa resortowych i wojskowych systemów teleinformatycznych.

Z powyższych powodów, sformowanie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa wpisuje się w kluczowe potrzeby Sił Zbrojnych RP. Obszar planowanych kompetencji ECSC obejmuje zakres zadań, który do tej pory był nie był realizowany lub był realizowany w bardzo okrojonej formie. Dotychczas nie było w polskim resorcie obrony i Siłach Zbrojnych żadnej jednostki organizacyjnej zdolnej do koordynacji i konsolidacji aktualnych potrzeb w obszarze szkoleniowym z zakresu cyberbezpieczeństwa, choć ww. obszar zadaniowy niewątpliwie należy postrzegać jako newralgiczny. Resort Obrony Narodowej jest bowiem jednym z najistotniejszych ogniw tworzących krajowy system cyberbezpieczeństwa i z tego tytułu ma określone ustawowe zadania do realizacji, w tym także w zakresie doskonalenia własnych zasobów kadrowych.

Ponadto, kwestie przeciwdziałania cyberzagrożeniom stają się przedmiotem wielu programów, projektów badawczych, i z tego powodu, zarówno w ramach NATO jak i w całej Unii Europejskiej, podejmowane są próby ujednolicenia podejścia, terminologii, metod i strategii. W tym zakresie, chociażby ze względu na istniejące zobowiązania sojusznicze oraz współpracę międzynarodową, resort również musi dysponować jednostką zdolną do zapewnienia merytorycznej współpracy z partnerami zagranicznymi, w tym także na płaszczyźnie realizacji szkoleń, treningów, wspólnych ćwiczeń, a nawet wymiany doświadczeń. Nie bez znaczenia jest też fakt, iż w Siłach Zbrojnych dokonuje się obecnie szybki rozwój struktur odpowiedzialnych za aspekty cyberbezpieczeństwa. Wypracowywane są zadania, procedury i podział kompetencji. Rozwój ww. struktur nie będzie możliwy bez zapewnienia wymaganej liczby odpowiednio wyszkolonych i wykwalifikowanych kadr.

Z tego też powodu, sformowanie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa jako jednostki organizacyjnej, która może szkolić i przygotowywać przyszłe kadry, a także podnosić kwalifikacje aktualnych zasobów osobowych RON oraz SZ RP odpowiedzialnych za realizację działań w cyberprzestrzeni, jest dziś zadaniem priorytetowym z punktu widzenia interesów oraz aktualnych i prognozowanych potrzeb Resortu Obrony Narodowej oraz Sił Zbrojnych Rzeczpospolitej Polskiej i pozwala myśleć optymistycznie o bezpieczeństwie Polski w cyberprzestrzeni.

We współczesnym świecie cyberprzestrzeń jest jedną z najważniejszych dziedzin funkcjonowania państwa. Dotychczasowy podział na świat rzeczywisty i świat wirtualny staje się coraz bardziej umowny, zwłaszcza dziś, gdy ze względu na pandemię coraz więcej sfer naszego życia musiało praktycznie z dnia na dzień przenieść się do internetu – powiedział Mariusz Błaszczak podczas inauguracji ECSC, uzasadniając działania resortu dotyczące konieczności kształcenia kadr i powołania nowej jednostki.

ZADANIA CYBER EKSPERTÓW Z ECSC

Główne zadanie Centrum to kształtowania kierunków rozwoju systemu doskonalenia zawodowego w sferze cyberbezpieczeństwa, kryptologii oraz technologii informacyjnych.

Centrum Eksperckie podnosząc kwalifikacje żołnierzy i pracowników ma za zadanie rozwijać zdolności Sił Zbrojnych RP do prowadzenia działań w cyberprzestrzeni, a także pełnić rolę jednostki konsolidującej potencjał ekspercki oraz wspierającej Ministerstwo Obrony Narodowej w rozwijaniu współpracy krajowej i międzynarodowej.

Najważniejsze obszary zadaniowe ECSC:

- poszerzanie kompetencji SZ RP w zakresie działań w cyberprzestrzeni – kształcenie i szkolenie kadr,
- organizacja i prowadzenie ćwiczeń, treningów, gier wojennych z wykorzystaniem zintegrowanego środowiska szkoleniowego (wirtualny poligon tzw. Cyber Range),
- współpraca z podmiotami krajowymi i zagranicznymi,
- konsolidacja potencjału eksperckiego resortu obrony narodowej – kształtowanie priorytetowych

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

kierunków doskonalenia kadr w sferze cyberbezpieczeństwa, kryptologii oraz IT.

Centrum ma na celu także przygotowanie kadr pod budowane Wojska Obrony Cyberprzestrzeni, a także przygotowanie i utrzymanie środowiska dla potrzeb prowadzenia procesu certyfikacji personelu i jednostek w ramach tworzenia WOC.

Zadanie to ma być zrealizowane do 2022 r. w ścisłej współpracy między ECSC a Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC). Za utworzenie WOC odpowiada Dyrektor NCBC, gen. bryg. Karol Molenda będący również pełnomocnikiem MON ds. WOC.

Tak jak inne wojska, również cyberżołnierze muszą mieć swój poligon. ECSC będzie właśnie takim poligonem. To miejsce, w którym będą mogli kształcić się i trenować, dzięki czemu będą coraz skuteczniejsi – powiedział gen. bryg. Karol Molenda i zaznaczył, że ECSC będzie w pierwszej kolejności odpowiedzialne za szkolenie ekspertów z nadzorowanej przez niego instytucji, a w przyszłości także żołnierzy i pracowników WOC.

ECSC stanie się w ten sposób jednym z najważniejszych ogniw w systemie bezpieczeństwa państwa poprzez szkolenie najwyższej klasy ekspertów, pełniących zasadnicze role w strukturach odpowiedzialnych za obronę cyberprzestrzeni na wszystkich poziomach struktury polskiej armii.

PLANY ECSC

Harmonogram powstawania Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa podzielony został na 4 etapy.

Etap I – do końca października 2020 r.

Okres do końca października 2020 r. poświęcony był przygotowaniom związanym z formowaniem i otwarciem Centrum. Był to etap organizacyjny przeznaczony na opracowanie dokumentacji organizacyjno-etatowej i opracowanie Decyzji Ministra Obrony Narodowej i innych dokumentów resortowych w sprawie sformowania Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa (ECSC).

Etap II – od 1 listopada 2020 r.

Centrum Eksperckie powstało 1 listopada 2020 r. Obecnie posiada już zdolność do prowadzenia niektórych szkoleń, a pod koniec 2021 r. powinno osiągnąć gotowość do prowadzenia szkoleń specjalistycznych.

Etap ten obejmuje:

- zbudowanie zespołów eksperckich w ECSC,
- przygotowanie odpowiedniej infrastruktury do prowadzenia szkoleń na potrzeby NCBC, wojsk operacyjnych i WOT,
- rozpoczęcie działalności szkoleniowej w obszarach teleinformatyki i cyberbezpieczeństwa,
- rozpoczęcie konfiguracji środowiska szkoleniowego do prowadzenia ćwiczeń, treningów i gier wojennych.

Etap III – lata 2022-2023

Zakłada się, że na tym etapie Centrum osiągnie pełną zdolność do prowadzenia szkoleń specjalistycznych dla zainteresowanych podmiotów spoza resortu Obrony Narodowej, szczególnie tych funkcjonujących w ramach systemu bezpieczeństwa narodowego. W ramach tego etapu planuje się:

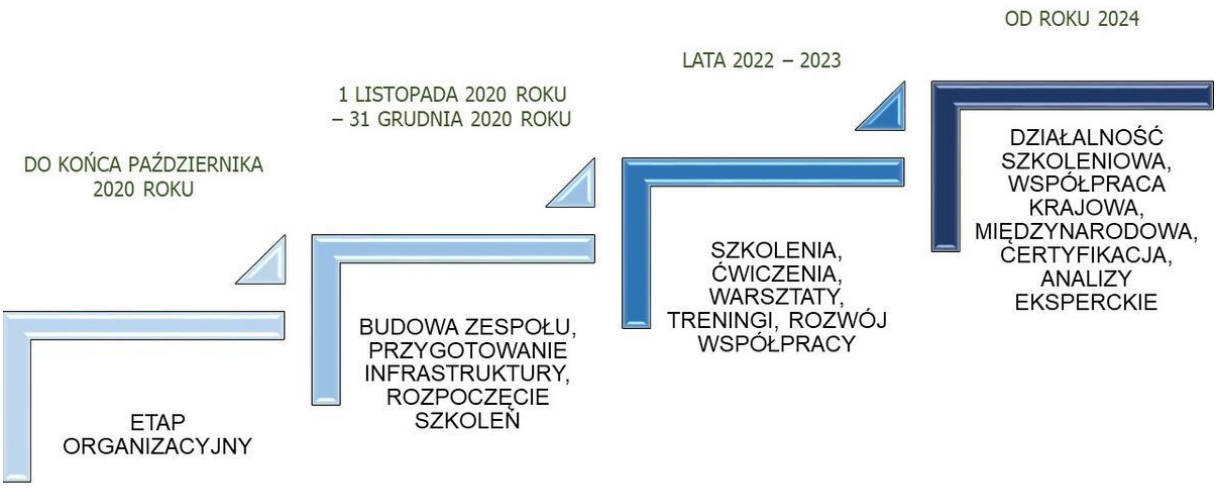
- realizację zadań w zakresie szkolenia personelu w obszarach teleinformatyki i cyberbezpieczeństwa na potrzeby wszystkich jednostek i komórek organizacyjnych resortu Obrony Narodowej,
- rozbudowę i włączenie w system kursów i szkoleń platformy e-learningowej,
- prowadzenie warsztatów, ćwiczeń, treningów i gier wojennych w obszarze cyberbezpieczeństwa,
- inicjowanie oraz rozwój współpracy i wymiany doświadczeń na szczeblu krajowym (np. uczelnie), a także międzynarodowym (NATO, UE).

Etap IV – od 2024 r.

W ramach tego etapu planuje się:

- dalszy rozwój współpracy krajowej i międzynarodowej, m.in. w zakresie kierunków badań naukowych i analiz eksperckich w obszarze szkolenia z zakresu cyberbezpieczeństwa,
- przygotowanie i utrzymywanie środowiska (zasobów) do prowadzania i wsparcia procesu certyfikacji Wojsk Obrony Cyberprzestrzeni,
- rozwój i umacnianie relacji międzynarodowych dotyczących aspektów cyberbezpieczeństwa poprzez organizację wspólnych warsztatów i konferencji,
- organizację i prowadzenie, we współpracy z NCBC i WOC, ćwiczeń i szkoleń narodowych i międzynarodowych w oparciu o infrastrukturę zintegrowanego środowiska szkoleniowego.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l



PODSUMOWANIE PIERWSZEGO ROKU DZIAŁANIA

Mimo, że ECSC funkcjonuje od listopada 2020 r., już może się poszczycić pierwszymi sukcesami: podpisanie porozumień dotyczących współpracy i szkoleń z Państwową Wyższą Szkołą Zawodową w Wałczu (gdzie jednostka ma oddział zamiejscowy), z Microsoft i CISCO. Dodatkowo, w 2020 r. Centrum uruchomiło 7 nowoczesnych sal szkoleniowych i – mimo niesprzyjających warunków z powodu pandemii – przeszkoliło blisko 200 osób: żołnierzy i pracowników cywilnych RON ze wszystkich rodzajów sił zbrojnych (Siły Powietrzne, Marynarka Wojenna, Wojska Lądowe) z m.in. technologii Palo Alto przygotowujące uczestników do planowania i wdrażania elementów bezpieczeństwa w systemach teleinformatycznych, z podstaw routingu i przełączania w sieciach komputerowych, Cyber Threat Intelligence (CTI) z wielopoziomowej analizy zagrożeń, zarówno technicznej, behawioralnej oraz kontekstowej (zawierająca także analizę typu INFOOPS).

Łącznie w 2021 r. ECSC planuje przeszkolić blisko 3 tys. żołnierzy i pracowników cywilnych do realizacji wymagających zadań w domenie operacyjnej cyberprzestrzeni, w której praca odbywa się w trybie 24/7/365.

Piśmiennictwo – materiały ze stron:
www.ecsc.wp.mil.pl

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l